DANIEL ALVES

Semigrupos de Weierstrass de dois lugares e códigos Hermitianos

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2019

DANIEL ALVES

Semigrupos de Weierstrass de dois lugares e códigos Hermitianos

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

Área de Concentração: Matemática.
Linha de Pesquisa: Teoria de códigos algébricos geométricos.

Orientador: Prof. Dr. Cicero F. Carvalho.

UBERLÂNDIA - MG
2019

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU, MG, Brasil.

A474s 2019

Alves, Daniel, 1995-
Semigrupos de Weierstrass de dois lugares e códigos Hermitianos [recurso eletrônico] / Daniel Alves. - 2019.

Orientador: Cicero Fernandes de Carvalho.
Dissertação (mestrado) - Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://dx.doi.org/10.14393/ufu.di.2019.318
Inclui bibliografia.
Inclui ilustrações.

1. Matemática. 2. Weierstrass, Pontos de. 3. Códigos de Goppa. I. Carvalho, Cicero Fernandes de, 1960- (Orient.) II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III. Título.

CDU: 51

Maria Salete de Freitas Pinheiro - CRB6/1262

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 152
Campus Santa Mônica, Uberlândia - MG, CEP 38400-902

ALUNO: Daniel Alves.

NÚMERO DE MATRÍCULA: 11712MAT001.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Teoria de códigos algébricos geométricos.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Semigrupos de Weierstrass de dois lugares e códigos Hermitianos.

ORIENTADOR(A): Prof. Dr. Cicero F. Carvalho.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 31 de Janeiro de 2019, às 10h00min, pela seguinte Banca Examinadora:

NOME	**ASSINATURA**
Prof. Dr. Cicero F. Carvalho UFU - Universidade Federal de Uberlândia	
Prof. Dr. Herivelto M. Borges Filho USP - Universidade de São Paulo	
Prof. Dr. Guilherme Chaud Tizziotti UFU - Universidade Federal de Uberlândia	

Uberlândia-MG, 31 de Janeiro de 2019.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

ALVES, D. *Semigrupos de Weierstrass de dois lugares e códigos Hermitianos.* 2019. 43 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho apresentamos resultados que melhoram a cota de Goppa para a distância mínima de códigos de Goppa de dois pontos sobre o corpo de funções Hermitiano, utilizando a distribuição de lacunas do semigrupo de Weierstrass de dois lugares associado. A partir destes resultados e sabendo a distância mínima exata para códigos de um ponto sobre o mesmo corpo de funções, determinamos os casos onde o código de dois pontos tem distância mínima maior ou igual à do código de um ponto de mesma dimensão.

Palavras-chave: Semigrupos de Weierstrass, Códigos Hermitianos, Códigos de Goppa.

ALVES, D. *Weierstrass semigroup of two places and Hermitian codes.* 2019. 43 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work we present results that improve the Goppa bound for the minimum distance of Goppa codes supported on two places and defined over the Hermitian function field, using the gap distribution of the associated Weierstrass semigroup. Also, from the knowledge of the minimum distance of Goppa codes defined over the same function field and supported on one place, we determine the cases where the two place code has minimum distance greater or equal the one place code of the same dimension.

Keywords: Weierstrass semigroup, Hermitian codes, Goppa codes.

Sumário

Introdução

Um código é um conjunto de símbolos que, associados a uma forma de interpretação, podem ser usados para transmitir informação. Durante uma transmissão, podem ocorrer erros, isto é, o símbolo recebido pode não ser o mesmo símbolo que foi enviado, e nesse caso a eficácia da comunicação está comprometida. Estamos interessados em códigos que permitem algum tipo de detecção e correção de erros. Para que seja possível detectar erros, é preciso que o conjunto dos símbolos interpretáveis (ou seja, o código) esteja mergulhado em um conjunto maior, de símbolos que podem ser recebidos. Assim, uma transmissão na qual o símbolo enviado (sempre interpretável) é substituído por um símbolo não interpretável pode ser acusada como um erro. Por outro lado, se o símbolo recebido ainda pertence ao código, o erro não poderá ser detectado. Dessa forma, procura-se métodos que permitam minimizar a probabilidade de ocorrência de um erro não detectável.

Uma estratégia para resolver este problema é definir uma métrica no conjunto dos símbolos que podem ser recebidos, de forma que símbolos mais próximos tenham maior probabilidade de serem confundidos entre si, isto é, de um deles ser enviado e o outro ser recebido. Nesse cenário, escolhemos os símbolos do código de forma que estejam bem distribuídos nesse universo, ou seja, de forma que a distância mínima entre símbolos do código seja a maior possível. Isso dificultaria a ocorrência de erros não detectáveis. A seguir, descrevemos um modelo para esta estratégia, que chamamos de código de bloco, munido da distância de Hamming.

Sejam $A \neq \emptyset$ um conjunto finito, o qual chamaremos de **alfabeto**, e seja $n \in \mathbb{N}$. Uma **palavra** sobre A de comprimento n é nada mais que um elemento de A^n. Um **código** (de bloco) sobre A de comprimento n é um subconjunto $\emptyset \neq C \subseteq A^n$. Dadas palavras $\mathbf{a}, \mathbf{b} \in A^n$, digamos $\mathbf{a} = (a_1, \ldots, a_n)$ e $\mathbf{b} = (b_1, \ldots, b_n)$, definimos a **distância de Hamming** entre $\mathbf{a}$ e $\mathbf{b}$ como sendo

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

Não é difícil provar que a distância de Hamming determina uma métrica em A^n. Para que esta métrica tenha a propriedade que destacamos no parágrafo anterior, é suficiente que:

1. Cada elemento de A tenha a mesma probabilidade de ser recebido errado.

2. A probabilidade de um elemento $a \in A$ ser enviado e outro elemento $b \in A \setminus \{a\}$ ser recebido seja independente de b.

Quando estas exigências são atendidas, dizemos que a transmissão está sendo realizada via um **canal simétrico**. Finalmente, escolhemos as palavras do código C de forma que a distância mínima $d(C) := \min\{d(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in C\}$ seja a maior possível. O problema principal da teoria de códigos [10] é o seguinte: dados $r, n, d \geq 1$, encontrar o número de elementos do maior código de comprimento n sobre um alfabeto de r elementos com distância mínima d.

Um caso particularmente interessante de códigos de bloco ocorre quando $A = \mathbb{F}_q$ é um corpo com q elementos e $C \subseteq \mathbb{F}_q^n$ é um $\mathbb{F}_q$-subespaço vetorial. Nesse caso, dizemos que C é um **código linear**. Definimos o **peso** da palavra $\mathbf{a} \in \mathbb{F}_q^n$ como sendo $\mathrm{wt}(\mathbf{a}) := d(\mathbf{a}, 0)$, e podemos caracterizar a distância mínima como $d(C) = \min\{\mathrm{wt}(\mathbf{a}) : \mathbf{a} \in C \setminus \{0\}\}$.

Em geral, não é fácil calcular a distância mínima de um código dado. Mesmo no caso de códigos lineares, utilizando a caracterização em termos do peso, o custo computacional pode ser muito alto. Assim, procura-se por métodos para construir códigos que tragam consigo alguma maneira de determinar (pelo menos uma cota inferior para) a distância mínima do código construído. Um exemplo são os chamados **códigos de avaliação**.

Seja $\mathscr{L}$ um $\mathbb{F}_q$-espaço vetorial cujos elementos são funções $V \to \mathbb{F}_q$, e sejam $P_1, \ldots, P_n \in V$, onde V é um conjunto arbitrário. A imagem da transformação linear

$$\begin{array}{rccc} \text{ev}: & \mathscr{L} & \to & \mathbb{F}_q^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array}.$$

é um código e, dependendo da estrutura de $\mathscr{L}$, pode-se deduzir a dimensão e a distância mínima, ou pelo menos cotas para tais parâmetros. Os códigos de Goppa são casos especiais de códigos de avaliação, onde $P_1, \ldots, P_n$ são pontos de uma curva algébrica V definida sobre $\overline{\mathbb{F}_q}$ e $\mathscr{L}$ é um certo tipo de $\mathbb{F}_q$-subespaço vetorial do corpo de funções racionais sobre V. A dimensão do código construído é determinada pela escolha de $\mathscr{L}$ e dos pontos $P_1, \ldots, P_n$, e usando o Teorema de Riemann-Roch encontramos uma cota inferior para a distância mínima que depende de $\mathscr{L}$ (Teorema 4.3). Uma segunda construção pode ser feita utilizando os chamados diferencial de Weil, para a qual também obtemos cotas para a dimensão e a distância mínima (Teorema 4.8). De acordo com a escolha da curva V e do subespaço $\mathscr{L}$, essas cotas podem ser melhoradas, e é nesse sentido que se apresentam os principais resultados discutidos neste trabalho.

Apesar de, classicamente, os códigos de Goppa serem descritos a partir da teoria de curvas algébricas, os aspectos geométricos da teoria não são necessários. Aqui, como em [12], a construção e os resultados sobre códigos de Goppa são baseados na teoria de corpos funções algébricas, e se mostra uma maneira logicamente mais rápida de introdução ao assunto, em comparação com a abordagem via curvas algébricas. Mesmo assim, a analogia entre curvas algébricas e corpos de funções se mostra bastante útil psicologicamente, unindo o intuitivo conceito de ponto de um ente geométrico à mais abstrata noção de lugar de um corpo de funções. Por esse motivo, dedicamos a primeira seção do Capítulo 1 à descrição dessa analogia. Nas duas seções seguintes desenvolvemos a teoria de corpos de funções, chegando ao Teorema de Riemann-Roch. No Capítulo 2, definimos semigrupos de Weierstrass de um e vários lugares, provamos as principais propriedades para semigrupos de Weierstrass de dois lugares e suas generalizações para m lugares e, no final, duas fórmulas envolvendo o número de lacunas para o caso de dois lugares. Algumas demonstrações (especialmente o Corolário 2.22) foram consideravelmente simplificadas em relação à fonte original. No capítulo 3, definimos o corpo de funções Hermitiano e descrevemos seus semigrupos de Weierstrass de um e dois lugares racionais. No Capítulo 4, descrevemos as duas construções dos códigos de Goppa, com as respectivas cotas mais gerais. O Capítulo 5 apresenta os resultados principais, reunindo o que foi visto nos capítulos anteriores para obter cotas cada vez melhores para a distância mínima de códigos de Goppa de dois pontos sobre o corpo de funções Hermitiano, apenas acrescentando hipóteses a respeito das lacunas do semigrupo de Weierstrass de dois lugares associado. Sabendo a distância mínima exata para códigos de um ponto, as novas cotas permitem comparar os códigos de dois pontos com códigos de um ponto de mesma dimensão.

Daniel Alves
Uberlândia-MG, 31 de Janeiro de 2019.

Capítulo 1

Corpos de Funções Algébricas

Apesar de terem surgido em associação com as curvas algébricas, os corpos de funções podem ser estudados de maneira independente. Esse é o ponto de vista adotado em [12], e é suficiente (além de ser um caminho mais rápido) para a maioria das aplicações em códigos corretores de erros. Mesmo assim, a literatura em códigos de Goppa ainda usa a linguagem da teoria de curvas algébricas. Além disso, a associação de lugares de um corpo de funções a pontos de uma curva algébrica é bastante útil do ponto de vista psicológico, e provê motivação para várias definições. Para mais detalhes sobre a relação entre curvas algébricas e corpos de funções, veja [4]. Neste capítulo, depois de uma breve discussão visando esclarecer essa relação, passamos à parte da teoria de corpos de funções necessária (e suficiente) para descrever a construção e obter as primeiras propriedades dos chamados códigos de Goppa.

1.1 Curvas Algébricas Projetivas

Nesta seção, K denota um corpo algebricamente fechado.

Considere em $K^{n+1} \setminus \{(0,\ldots,0)\}$ a relação de equivalência $\sim$ definida por: $(a_0,\ldots,a_n) \sim (b_0,\ldots,b_n)$ se, e somente se, existe $\lambda \in K \setminus \{0\}$ tal que $a_i = \lambda b_i$, $i = 0,\ldots,n$. O conjunto quociente $\mathbb{P}^n(K) := (K^{n+1} \setminus \{(0,\ldots,0)\})/\sim$ é chamado **espaço projetivo** de dimensão n sobre K. A classe do elemento $(a_0,\ldots,a_n) \in K^{n+1}$ será denotada por $(a_0 : \cdots : a_n)$, e pode ser identificada com a reta em K^{n+1} que passa por $(a_0,\ldots,a_n)$ e pela origem $(0,\ldots,0)$.

Observe que se $f \in K[X_0,\ldots,X_n]$ é um polinômio homogêneo (isto é, todos os monômios de f têm o mesmo grau), e $f(a_0,\ldots,a_n) = 0$, onde nem todos os a_i's são zero, então $f(b_0,\ldots,b_n) = 0$ sempre que $(b_0,\ldots,b_n) \sim (a_0,\ldots,a_n)$. Seja $I \subseteq K[X_0,\ldots,X_n]$ um ideal gerado por polinômios homogêneos (ou seja, um ideal homogêneo). O conjunto algébrico (projetivo) associado a I é (bem) definido como

$$\mathbf{V}(I) := \{(a_0 : \cdots : a_n) \in \mathbb{P}^n(K) : f(a_0,\ldots,a_n) = 0, \text{ para todo } f \in I\}.$$

Dizemos que $V \subseteq \mathbb{P}^n(K)$ é um conjunto algébrico se for o conjunto algébrico associado a algum ideal homogêneo. Um conjunto algébrico V pode estar associado a mais de um ideal, mas podemos destacar o que chamamos de ideal de V, definido por

$$\mathbf{I}(V) := \{f \in K[X_0,\ldots,X_n] : f(a_0,\ldots,a_n) = 0 \text{ para todo } (a_0 : \cdots : a_n) \in V\}.$$

Em geral, não podemos recuperar I a partir de $\mathbf{V}(I)$, mas vale o seguinte.

Teorema 1.1 (Nullstellensatz, [4], Corolário 4.1.4)**.** *Seja $I \subseteq K[X_0,\ldots,X_n]$ um ideal homogêneo. Então*

$$\boldsymbol{I}(\boldsymbol{V}(I)) = \{f \in K[X_0,\ldots,X_n] : f^m \in I \text{ para algum } m \geq 1\}.$$

Em particular, se I é um ideal primo, então $\boldsymbol{I}(\boldsymbol{V}(I)) = I$.

Seja $V \subseteq \mathbb{P}^n(K)$ um conjunto algébrico, e suponha que $\mathbf{I}(V)$ seja um ideal primo. Então o quociente $K[V] := K[X_0, \ldots, X_n]/\mathbf{I}(V)$ é um domínio. Denotamos por $K(V)$ o corpo de frações homogêneas de $K[V]$, isto é, o conjunto de frações onde numerador e denominador (não nulo) são elementos de $K[V]$ homogêneos de mesmo grau. Para $f \in K(V)$, e $P = (a_0 : \cdots : a_n) \in V$ a avaliação $f(P) \in K \cup \{\infty\}$ pode ser (bem) definida como segue. Se existem $f_1, f_2 \in K[X_0, \ldots, X_n]$ homogêneos de mesmo grau com $f_2(a_0, \ldots, a_n) \neq 0$, tais que $f = (f_1 + I)/(f_2 + I)$, defina $f(P) = f_1(a_0, \ldots, a_n)/f_2(a_0, \ldots, a_n)$; caso contrário, defina $f(P) = \infty$. Assim, os elementos de $K(V)$ podem ser vistos como funções $V \to K \cup \{\infty\} \cong \mathbb{P}^1(K)$, e por isso dizemos que $K(V)$ é o **corpo de funções racionais** do conjunto algébrico V. Dizemos que a função f tem zero ou polo em P se $f(P) = 0$ ou $f(P) = \infty$, respectivamente.

As **curvas algébricas** (irredutíveis) são caracterizadas da seguinte forma: uma curva algébrica (irredutível) V sobre K é um conjunto algébrico cujo ideal $\mathbf{I}(V)$ é primo, e cujo corpo de funções racionais $K(V)$ tem grau de transcendência um sobre K, isto é, existe $x \in K(V)$ tal que $K(V)$ é uma extensão algébrica de $K(x)$. Pode-se mostrar que, neste caso, $K(V)|K(x)$ é, na verdade, uma extensão finita (veja Definição 1.2).

Seja V uma curva algébrica e $P \in V$. Pode ser que existam funções $f \in K(V)$ tais que $f(P) = \infty$ e $(1/f)(P) = \infty$. O caso onde isto não ocorre caracteriza o que chamamos de ponto não singular. Em outras palavras, P é um ponto não singular se $(1/f)(P) \in K$ sempre que $f(P) = \infty$. Dizemos que a curva V é não singular se todo ponto de V é não singular. Observe que se $P \in V$ é um ponto não singular, então o conjunto $\mathcal{O}_P := \{f \in K(V) : f(P) \in K\}$ é um anel de valorização discreta (veja Definição 1.3). As funções racionais que se anulam em P são exatamente aquelas cujo inverso não está em $\mathcal{O}_P$, e formam um ideal maximal em $\mathcal{O}_P$. Por outro lado, se V é não singular, a cada anel de valorização discreta $\mathcal{O} \subseteq K(V)$ está associado um ponto $P \in V$, sendo este o zero comum das funções racionais no ideal maximal de $\mathcal{O}$ (veja Proposição 1.4). Pela Proposição 1.8, dentre as funções racionais que se anulam em P, existe uma função t que divide (em $\mathcal{O}_P$) todas as outras, e assim nos permite medir as ordens dos zeros e polos em P. Uma função $f \in K(V)$ tem um zero de ordem n em P se $f = t^n u$, onde $u \in K(V)$ não tem zero nem polo em P, e f tem um polo de ordem n em P se $f = t^{-n} u$, onde $u \in K(V)$ não tem zero nem polo em P.

Em algumas situações, é útil associar números inteiros a alguns pontos da curva, como por exemplo, os zeros e polos de uma função às respectivas ordens, ou os pontos de interseção da curva com outro conjunto algébrico às respectivas multiplicidades. Neste momento entra em cena o conceito de divisor, e a notação aditiva é sugerida pelas aplicações.

Uma das perguntas que podem ser feitas é a seguinte: dados pontos $P_1, \ldots, P_r$ em uma curva algébrica V, e inteiros $n_1, \ldots, n_r$, inicialmente positivos, quais são as funções que têm polo em P_i com ordem limitada por n_i, para $i = 1, \ldots, r$? Essa questão é generalizada para n_i's não nulos arbitrários, perguntando pelas funções que tem zero em P_i de ordem pelo menos $-n_i$, se $n_i < 0$. O Teorema de Riemann nos diz que existe um inteiro g (dependendo apenas da curva), denominado gênero da curva V, de forma que essas funções formam um K-espaço vertorial (um espaço de Riemann-Roch) de dimensão pelo menos $n_1 + \cdots + n_r + 1 - g$. O Teorema de Riemann-Roch substitui o "pelo menos"da frase anterior, determinando um termo de correção que também pode ser interpretado como a dimensão de um espaço de Riemann-Roch.

1.2 Lugares, Divisores e o Teorema de Riemann

Passamos a listar definições e resultados da teoria de corpos de funções algébricas, que é a base de tudo que será discutido neste trabalho. Todas as demonstrações omitidas podem ser encontradas em [12], Capítulo 1.

Definição 1.2. *Seja K um corpo. Dizemos que uma extensão $F \supseteq K$ é um* ***corpo de funções algébricas*** *sobre K (ou que $F|K$ é um corpo de funções) se existe $x \in F$ transcendente sobre K tal que $[F : K(x)] < \infty$.*

No restante deste capítulo, K denota um corpo arbitrário, e F é um corpo de funções algébricas sobre K.

Definição 1.3. *Seja $\mathcal{O} \subseteq F$ um subanel. Dizemos que $\mathcal{O}$ é um* ***anel de valorização*** *(discreta) de $F|K$ se*

1. *$K \subsetneq \mathcal{O} \subsetneq F$; e*
2. *para todo $z \in F$ temos $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.*

Proposição 1.4. *Seja $\mathcal{O}$ um anel de valorização de $F|K$. Então $\mathcal{O}$ possui um único ideal maximal P, que pode ser caracterizado da seguinte forma: para $0 \neq x \in F$, temos $x \in P$ se, e somente se, $x^{-1} \notin \mathcal{O}$.*

Demonstração. Seja $P := \{x \in \mathcal{O} \setminus \{0\} : x^{-1} \notin \mathcal{O}\} \cup \{0\}$. Temos $0 \in P$. Para $u \in \mathcal{O}$ e $x \in P$, $x \neq 0$, se $(ux)^{-1} = u^{-1}x^{-1} \in \mathcal{O}$, então $u(ux)^{-1} = x^{-1} \in \mathcal{O}$, contradição. Logo, $(ux)^{-1} \notin \mathcal{O}$, e $ux \in P$. Sejam $x, y \in P \setminus \{0\}$. Pela definição de anel de valorização podemos assumir, sem perda de generalidade, que $y/x \in \mathcal{O}$. Assim, temos $1+y/x \in \mathcal{O}$, e logo $x+y = x(1+y/x) \in P$. Isto prova que P é ideal de $\mathcal{O}$. Além disso, se $x \in \mathcal{O} \setminus P$, então $x^{-1} \in \mathcal{O}$, e logo $x\mathcal{O} = \mathcal{O}$, ou seja, qualquer ideal próprio de $\mathcal{O}$ deve estar contido em P. Portanto, P é o único ideal maximal de $\mathcal{O}$. □

Definição 1.5. *Um* ***lugar*** *do corpo de funções de $F|K$ é o ideal maximal de algum anel de valorização de $F|K$. Denotaremos o conjunto de lugares de $F|K$ por $\mathbb{P}_F$.*

Se $\mathcal{O}$ é um anel de valorização de $F|K$ e P é seu ideal maximal, então $\mathcal{O}$ é unicamente determinado por P. De fato, $\mathcal{O} = \{z \in F : z^{-1} \notin P\} \cup \{0\}$. Dado $P \in \mathbb{P}_F$, denotamos por $\mathcal{O}_P := \mathcal{O}$ o anel de valorização associado ao lugar P.

Proposição 1.6. *Se $P \in \mathbb{P}_F$ é um lugar, então P é um ideal principal em $\mathcal{O}_P$.*

Definição 1.7. *Um* ***parâmetro local*** *em $P \in \mathbb{P}_F$ é um elemento $t \in P$ com $P = t\mathcal{O}_P$, isto é, um gerador do ideal P em $\mathcal{O}_P$.*

Proposição 1.8. *Se t é um parâmetro local em $P \in \mathbb{P}_F$, então cada $z \in \mathbb{F}$, $z \neq 0$, tem uma única representação na forma $z = t^n u$, com $n \in \mathbb{Z}$ e $u \in \mathcal{O}_P^\times$, onde $\mathcal{O}_P^\times := \{u \in \mathcal{O}_P \setminus \{0\} : u^{-1} \in \mathcal{O}_P\}$.*

A um lugar P de $F|K$ associamos uma aplicação

$$v_P : F \to \mathbb{Z} \cup \{\infty\}$$

definida como segue. Escolha um parâmetro local $t \in P$. Então cada $z \in F$, $z \neq 0$, tem uma única representação $z = t^n u$, com $n \in \mathbb{Z}$ e $u \in \mathcal{O}_P^\times$. Defina $v_P(z) := n$ e $v_P(0) := \infty$. Nesse contexto, o símbolo ∞ representa um elemento que não está em $\mathbb{Z}$ tal que $\infty > m$ e $\infty + \infty = \infty + n = n + \infty = \infty$ para todos $m, n \in \mathbb{Z}$.

Vejamos que a aplicação v_P definida no parágrafo anterior não depende da escolha do parâmetro local $t \in P$. Seja $s \in P$ outro parâmetro local. Como $P = t\mathcal{O}_P = s\mathcal{O}_P$, temos $s = tw$, para algum $w \in \mathcal{O}^\times$. Dado $z \in F \setminus \{0\}$, existem únicos $n, m \in \mathbb{Z}$ e $u, v \in \mathcal{O}^\times$ tais que $z = t^n u = s^m v = (tw)^m v = t^m(w^m v)$, com $w^m v \in \mathcal{O}^\times$. Portanto, $n = m$.

Teorema 1.9. *Seja P um lugar de $F|K$. Então vale o seguinte:*

1. *Um elemento $t \in F$ é um parâmetro local para P se, e somente se, $v_P(t) = 1$.*

2. *$v_P(xy) = v_P(x) + v_P(y)$, para todos $x, y \in F$.*

3. $$\begin{aligned} \mathcal{O}_P &= \{z \in F : v_P(z) \geq 0\}, \\ \mathcal{O}_P^\times &= \{z \in F : v_P(z) = 0\}, \\ P &= \{z \in F : v_P(z) > 0\}. \end{aligned}$$

4. *$v_P(x+y) \geq \min\{v_P(x), v_P(y)\}$, para todos $x, y \in F$.*

5. *Se $x, y \in F$ são tais que $v_P(x) \neq v_P(y)$, então $v_P(x+y) = \min\{v_P(x), v_P(y)\}$.*

6. *Se $x \in F \setminus \{0\}$ é algébrico sobre K, então $v_P(x) = 0$.*

Demonstração. 1. Se $t \in P$ é um parâmetro local, como $t = t^1 \cdot 1$, temos $v_P(t) = 1$. Suponha que $v_P(t) = 1$ e seja $s \in P$ parâmetro local. Então $t = su$, com $u \in \mathcal{O}_P^\times$, e logo $t\mathcal{O}_P = su\mathcal{O}_P = s\mathcal{O}_P = P$, donde segue que t também é parâmetro local em P.

2. Se $xy = 0$, então a igualdade é trivial. Suponha $xy \neq 0$, e seja $t \in P$ parâmetro local. Então pela Proposição 1.8, $xy = (t^{v_P(x)}u)(t^{v_P(y)}v) = t^{v_P(x)+v_P(y)}uv$, com $u, v, uv \in \mathcal{O}_P^\times$, e portanto $v_P(xy) = v_P(x) + v_P(y)$.

3. Seja $z \in F$, $t \in P$ parâmetro local, e escreva $z = t^{v_P(z)}u$, com $u \in \mathcal{O}_P^\times$ (Proposição 1.8). Se $v_P(z) \geq 0$, então $z \in \mathcal{O}_P$. Por outro lado, se $z \in \mathcal{O}_P$, então $t^{v_P(z)} = zu^{-1} \in \mathcal{O}_P$. Se $v_P(z) < 0$, então $t^{-v_P(z)} \in P$, e logo $t^{v_P(z)} \notin \mathcal{O}_P$, o que é uma contradição. Logo, $v_P(z) \geq 0$. Portanto, $\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\}$. As outras igualdades são triviais.

4. Suponha, sem perda de generalidade, que $v_P(x) \leq v_P(y) < \infty$. Então $x + y = t^{v_P(x)}u + t^{v_P(y)}v = t^{v_P(x)}(u + t^{v_P(y)-v_P(x)}v)$, com $u + t^{v_P(y)-v_P(x)}v \in \mathcal{O}_P$, e logo, usando os itens (1), (2) e (3), temos $v_P(x+y) \geq v_P(x)$, como queríamos.

5. Sem perda de generalidade, podemos assumir $v_P(x) < v_P(y) < \infty$. Observando que $v_P(y) = v_P(-y)$, temos $v_P(x) = v_P(x+y-y) \geq \min\{v_P(x+y), v_P(y)\}$. Como $v_P(x) < v_P(y)$, temos $\min\{v_P(x+y), v_P(y)\} = v_P(x+y) \leq v_P(x)$. Mas $v_P(x+y) \geq v_P(x) = \min\{v_P(x), v_P(y)\}$. Portanto, $v_P(x+y) = v_P(x)$.

6. Afirmamos que se $v_P(x) > 0$ então $v_P(f(x)) \geq 0$ para todo $f(X) \in K[X]$. Para provar esta afirmação, procedemos por indução sobre o grau de $f(X)$. Se o grau de $f(X)$ é zero, a afirmação é trivial, já que $K \subseteq \mathcal{O}_P$. Suponha que o grau de $f(X)$ seja $d \geq 1$. Escreva $f(X) = f(0) + Xg(X)$. Como $\deg g(X) < d$, pela hipótese de indução temos $v_P(g(x)) \geq 0$, e logo $v_P(f(0) + xg(x)) \geq \min\{v_P(f(0)), v_P(x) + v_P(g(x))\} \geq 0$, como queríamos.

   Suponha que $a_r x^r + \cdots + a_1 x + a_0 = 0$, com $a_0, \ldots, a_r \in K$. Podemos supor $a_r \neq 0$ e $a_0 \neq 0$. Se $v_P(x) > 0$, então $v_P(a_r x^r + \cdots + a_1 x) = v_P(x) + v_P(a_r x^{r-1} + \cdots + a_1) > 0 = v_P(a_0)$, de acordo com a afirmação que acabamos de provar. Assim, $v_P(a_r x^r + \cdots + a_1 x + a_0) = v_P(a_0) = 0$, o que é uma contradição. Se $v_P(x) < 0$, então $v_P(x^{-1}) > 0$ e $a_r + \cdots + a_1(x^{-1})^{r-1} + a_0(x^{-1})^r = 0$, e o resultado segue de forma similar.

□

Seja P um lugar de $F|K$ e $\mathcal{O}_P$ o anel de valorização associado. Como P é um ideal maximal, o anel quociente $F_P := \mathcal{O}_P/P$ é um corpo. Para $x \in \mathcal{O}_P$, denotaremos por $x(P) \in F_P$ a classe de x módulo P, e para $x \notin \mathcal{O}_P$, definimos $x(P) := \infty$. Pelo Teorema 1.9 (4) e (5), temos $K \subseteq \mathcal{O}_P$ e $K \cap P = \{0\}$, logo a aplicação natural $\mathcal{O}_P \to \mathcal{O}_P/P = F_P$ induz um mergulho de K em F_P e, assim, podemos considerar $K \subseteq F_P$ via esse mergulho. Definimos o **grau** do lugar P como sendo $\deg P := [F_P : K]$. Dizemos que P é um **lugar racional** se $\deg P = 1$.

Proposição 1.10. *Seja P um lugar de $F|K$. Então* $\deg P < \infty$.

Seja P um lugar racional de $F|K$, isto é, $\deg P = 1$. Então temos $F_P = K$. Se K é algebricamente fechado, então todos os lugares são racionais e podemos ver um elemento $z \in F$ como uma função

$$\begin{array}{rcl} z : \mathbb{P}_F & \to & K \cup \{\infty\}, \\ P & \mapsto & z(P). \end{array}$$

Definição 1.11. *Seja $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um **zero** de z se $z(P) = 0$, e que P é um **polo** de z se $z(P) = \infty$.*

Observe que P é um zero de z se, e somente se, $v_P(z) > 0$; e P é um polo de z se, e somente se, $v_P(z) < 0$.

Proposição 1.12. *Seja $z \in F$ transcendente sobre K. Então z tem pelo menos um zero, e pelo menos um polo. Em particular, $\mathbb{P}_F \neq \emptyset$. Além disso, o número de zeros de z é finito, assim como o número de polos.*

A partir deste momento, vamos assumir que todo elemento de F algébrico sobre K já esteja em K.

Definição 1.13. *Um **divisor** de $F|K$ é uma soma formal*

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ com } n_P \in \mathbb{Z}, n_P = 0 \text{ para quase todo } P.$$

*O **suporte** de D é definido como*

$$\operatorname{Supp} D := \{P \in \mathbb{P}_F : n_P \neq 0\}.$$

Dois divisores $D = \sum n_P P$ e $D' = \sum n'_P P$ são somados coeficiente a coeficiente,

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P.$$

*O **divisor nulo** é definido por*

$$0 := \sum_{P \in \mathbb{P}_F} r_P P, \text{ com } r_P = 0 \text{ para todo } P.$$

Denotamos o conjunto dos divisores de $F|K$ por $\operatorname{Div}(F)$. *Com a soma definida acima,* $\operatorname{Div}(F)$ *é um grupo abeliano. Para $Q \in \mathbb{P}_F$ e $D = \sum n_P P$, definimos $v_Q(D) := n_Q$, e logo*

$$\operatorname{Supp} D = \{P \in \mathbb{P}_F : v_P(D) \neq 0\} \text{ e } D = \sum_{P \in \operatorname{Supp} D} v_P(D) \cdot P.$$

Podemos equipar o conjunto $\operatorname{Div}(F)$ *com uma ordem parcial definindo*

$$D_1 \leq D_2 : \iff v_P(D_1) \leq v_P(D_2) \text{ para todo } P \in \mathbb{P}_F.$$

*Dizemos que D é um **divisor efetivo** se $D \geq 0$. O **grau** de um divisor D é definido como*

$$\deg D := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \deg P,$$

e fornece um homomorfismo $\deg : \operatorname{Div}(F) \to \mathbb{Z}$.

Vimos que um elemento não nulo $x \in F$ tem um número finito de zeros e polos. Assim, faz sentido a seguinte definição.

Definição 1.14. *Seja $0 \neq x \in F$, e denote Z (resp. N) o conjunto de zeros (resp. polos) de x em $\mathbb{P}_F$. Definimos:*

$$\begin{aligned}(x)_0 &:= \sum_{P\in Z} v_P(x)P, \text{ o divisor de zeros de } x,\\ (x)_\infty &:= \sum_{P\in N} (-v_P(x))P, \text{ o divisor de polos de } x,\\ (x) &:= (x)_0 - (x)_\infty, \text{ o divisor principal de } x.\end{aligned}$$

É claro que $(x)_0 \geq 0$, $(x)_\infty \geq 0$ e

$$(x) = \sum_{P\in\mathbb{P}_F} v_P(x)P.$$

Definição 1.15. *Dizemos que dois divisores $D, D' \in \mathrm{Div}(F)$ são **equivalentes** (e denotamos $D \sim D'$) se $D = D' + (x)$ para algum $x \in F \setminus \{0\}$.*

A próxima definição tem um papel fundamental na teoria de corpos de funções algébricas.

Definição 1.16. *Seja $D \in \mathrm{Div}(F)$. O conjunto $\mathscr{L}(D) := \{x \in F : (x) + D \geq 0\} \cup \{0\}$ é um K-subespaço vetorial de F, denominado **espaço de Riemann-Roch** associado a D. Denotamos $\ell(D) := \dim_K \mathscr{L}(D)$.*

Seja $D = 0$ o divisor nulo. Se $x \in \mathscr{L}(D)$, então $(x) \geq 0$, isto é, x não tem polos. Pela Proposição 1.12, $x \in K$. Logo, temos $\mathscr{L}(0) = K$ e $\ell(0) = 1$.

Lema 1.17. *Se D e E são divisores tais que $D \leq E$, então $\mathscr{L}(D) \subseteq \mathscr{L}(E)$ e*

$$\dim_K \frac{\mathscr{L}(E)}{\mathscr{L}(D)} \leq \deg(E - D).$$

Em particular, para um divisor $D \geq 0$, temos $\dim_K \dfrac{\mathscr{L}(D)}{\mathscr{L}(0)} = \dim_K \dfrac{\mathscr{L}(D)}{K} \leq \deg D$, ou seja, $\ell(D) \leq \deg D + 1$.

Corolário 1.18. *Para cada divisor D, o K-espaço vetorial $\mathscr{L}(D)$ tem dimensão finita.*

Demonstração. Tomando um divisor E com $D \leq E$ e $0 \leq E$, temos $\ell(D) \leq \ell(E) \leq \deg E + 1$. □

Teorema 1.19. *Todos os divisores principais têm grau zero. Mais precisamente, dado $x \in F \setminus K$, temos $\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$, ou seja, o número de zeros de x é igual ao número de polos (ambos contados com os respectivos graus).*

Corolário 1.20. *Se D é um divisor com $\deg D < 0$, então $\ell(D) = 0$.*

Demonstração. Suponha que existe $x \in \mathscr{L}(D) \setminus \{0\}$, isto é, $E := (x) + D \geq 0$. Então $\deg D = \deg E \geq 0$. □

Corolário 1.21. *Um divisor D é principal se, e somente se, $\deg D = 0$ e $\ell(D) > 0$.*

Demonstração. Se $D = (x)$ é principal, então $\deg D = 0$ (Teorema 1.19) e $0 = (x^{-1}) + (x) \geq 0$, ou seja, $x^{-1} \in \mathscr{L}(D)$. Suponha que $\deg D = 0$ e $\ell(D) > 0$. Então existe $x \in \mathscr{L}(D) \setminus \{0\}$, isto é, $E := (x) + D \geq 0$ e $\deg E = 0$. O fato de $\deg E$ ser a soma nula de inteiros não negativos, implica que cada um desses inteiros deve ser zero, ou seja, $E = 0$, e ogo $D = (x^{-1})$. □

Teorema 1.22 (Teorema de Riemann)**.** *Existe um inteiro g tal que, para cada divisor $D \in \mathrm{Div}(F)$ vale*

$$\ell(D) \geq \deg D + 1 - g.$$

Pelo Teorema de Riemann, o conjunto $\{\deg D - \ell(D) + 1 : D \in \mathrm{Div}(F)\} \subseteq \mathbb{Z}$ é limitado, e portanto possui um máximo.

Definição 1.23. *Definimos o **gênero** do corpo de funções $F|K$ como sendo*

$$\max\{\deg D - \ell(D) + 1 : D \in \mathrm{Div}(F)\}.$$

1.3 O Teorema de Riemann-Roch

O termo de correção na desigualdade do Teorema de Riemann $i(D) := \ell(D) - \deg D - 1 + g$ é denominado **índice de especialidade** do divisor D. O Teorema de Riemann-Roch interpreta $i(D)$ como $\ell(W - D)$ para um divisor W adequado. No que segue, introduzimos as principais ferramentas para demonstrá-lo. Mais uma vez, todas as demonstrações omitidas podem ser encontradas em [12], Capítulo 1.

Seja D um divisor de $F|K$. Para construir o espaço $\mathscr{L}(D)$, procuramos os elementos $x \in F$ tais que $v_P(x) + v_P(D) \geq 0$ para cada P. A seguir, faremos uma espécie de generalização dessa construção: para cada lugar P, escolhemos uma função α_P tal que $v_P(\alpha_P) + v_P(D) \geq 0$. Observe que, pela definição de divisor, temos $v_P(D) = 0$ para quase todo P, e logo $v_P(\alpha_P) \geq 0$ para quase todo P. Isso motiva a seguinte definição.

Definição 1.24. *Um **adele** de $F|K$ é uma aplicação*

$$\alpha : \begin{cases} \mathbb{P}_F & \to & F, \\ P & \mapsto & \alpha_P, \end{cases}$$

*tal que $\alpha_P \in \mathcal{O}_P$ para quase todo $P \in \mathbb{P}_F$. Usamos a notação $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ ou, por simplicidade, $\alpha = (\alpha_P)$, e dizemos que α_P é a **componente** do adele α em P. Denotamos ainda*

$$\mathcal{A}_F := \{\alpha : \alpha \text{ é um adele de } F|K\}.$$

Dados $\alpha, \beta \in \mathcal{A}_F$ e $\lambda \in K$, definimos $\alpha + \beta : \mathbb{P}_F \to F$ por

$$(\alpha + \beta)_P := \alpha_P + \beta_P,$$

e

$$(\lambda\alpha)_P := \lambda\alpha_P.$$

*Note que $\alpha + \beta$ e $\lambda\alpha$ são elementos de $\mathcal{A}_F$, pois $v_P(\alpha_P + \beta_P) \geq \min\{v_P(\alpha_P), v_P(\beta_P)\} \geq 0$ e $v_P(\lambda\alpha_P) = v_P(\alpha_P) \geq 0$ para quase todo $P \in \mathbb{P}_F$. Dessa forma, $\mathcal{A}_F$ se torna um K-espaço vetorial. O **adele principal** de um elemento $x \in F$ é o adele cujas componentes são todas iguais a x. Assim, podemos ver F como K-subespaço de $\mathcal{A}_F$, identificando cada elemento de F a seu adele principal em $\mathcal{A}_F$. Para $\alpha \in \mathcal{A}_F$ e $P \in \mathbb{P}_F$, denotamos $v_P(\alpha) := v_P(\alpha_P)$.*

Para $D \in \mathrm{Div}(F)$, definimos

$$\mathcal{A}_F(D) := \{\alpha \in \mathcal{A}_F : v_P(\alpha) + v_P(D) \geq 0 \text{ para todo } P \in \mathbb{P}_F\}.$$

Observe que $\mathcal{A}_F(D)$ é um K-subespaço vetorial de $\mathcal{A}_F$. Além disso, por meio do mergulho $\theta : F \hookrightarrow \mathcal{A}_F$ descrito no parágrafo anterior, podemos identificar $\mathscr{L}(D)$ com $\mathcal{A}_F(D) \cap \theta(F)$.

Temos um resultado análogo ao Lema 1.17 para os espaços $\mathcal{A}_F(D)$.

Lema 1.25. *Se D e E são divisores tais que $D \leq E$, então $\mathcal{A}_F(D) \subseteq \mathcal{A}_F(E)$ e*

$$\dim_K \frac{\mathcal{A}_F(E)}{\mathcal{A}_F(D)} = \deg(E - D).$$

Além disso, para os divisores D que satisfazem a igualdade no Teorema de Riemann, o espaço $\mathcal{A}_F(D)$ é bastante grande.

Lema 1.26. *Se D é um divisor de $F|K$ com $\ell(D) = \deg D + 1 - g$, então $\mathcal{A}_F = \mathcal{A}_F(D) + F$.*

O resultado a seguir oferece uma interpretação do índice de especialidade de um divisor em termos das dimensões de espaços de adeles.

Teorema 1.27. *Para cada divisor D, o índice de especialidade é dado por*

$$i(D) = \dim_K \frac{\mathcal{A}_F}{\mathcal{A}_F(D) + F}.$$

Para uma segunda interpretação do índice de especialidade, que culminará no Teorema de Riemann-Roch, introduzimos o conceito de diferencial de Weil.

Definição 1.28. *Um **diferencial de Weil** de $F|K$ é uma aplicação K-linear $\omega : \mathcal{A}_F \to K$ que se anula em $\mathcal{A}_F(D) + F$ para algum $D \in \mathrm{Div}(F)$. Denotamos*

$$\Omega_F := \{\omega : \omega \text{ é um diferencial de Weil de } F|K\}.$$

Para $D \in \mathrm{Div}(F)$, definimos

$$\Omega_F(D) := \{\omega \in \Omega_F : \omega \text{ se anula sobre } \mathcal{A}_F(D) + F\}.$$

Podemos ver Ω_F como K-espaço vetorial. De fato, se ω_1 se anula sobre $\mathcal{A}_F(D_1) + F$ e ω_2 se anula sobre $\mathcal{A}_F(D_2) + F$, então $\omega_1 + \omega_2$ se anula sobre $\mathcal{A}_F(D_3) + F$ para qualquer divisor D_3 com $D_3 \leq D_1$ e $D_3 \leq D_2$, e $a\omega_1$ se anula sobre $\mathcal{A}_F(D_1) + F$ para todo $a \in K$. Observe que $\Omega_F(D)$ é um subespaço de Ω_F.

Lema 1.29. *Para $D \in \mathrm{Div}(F)$ temos $\dim \Omega_F(D) = i(D)$.*

Demonstração. O espaço $\Omega_F(D)$ é isomorfo ao espaço de funcionais lineares em $\mathcal{A}_F/(\mathcal{A}_F(D) + F)$. Como $\mathcal{A}_F/(\mathcal{A}_F(D) + F)$ tem dimensão finita $i(D)$ (Teorema 1.27), o resultado segue. □

Podemos ainda dar um estrutura de F-espaço vetorial a Ω_F. Para $x \in F$ e $\omega \in \Omega_F$ definimos $x\omega : \mathcal{A}_F \to K$ por

$$(x\omega)(\alpha) := \omega(x\alpha).$$

É fácil ver que $x\omega$ é um diferencial de Weil. De fato, se ω se anula sobre $\mathcal{A}_F(D) + F$ então $x\omega$ se anula sobre $\mathcal{A}_F(D + (x)) + F$.

Proposição 1.30. *Ω_F é um F-espaço vetorial de dimensão um.*

Gostaríamos de associar um divisor a um diferencial de Weil $\omega \neq 0$.

Lema 1.31. *Seja $0 \neq \omega \in \Omega_F$. Defina*

$$M(\omega) := \{D \in \mathrm{Div}(F) : \omega \text{ se anula em } \mathcal{A}_F(D) + F\}.$$

Então $M(\omega)$ tem um único máximo com respeito à relação $\leq$, isto é, existe um único $W \in M(\omega)$ tal que $D \leq M$ para todo $D \in M(\omega)$. A este divisor damos o nome de divisor do diferencial de Weil ω, e denotamos $(\omega) := W$.

Definição 1.32. *1. Para $0 \neq \omega \in \Omega_F$ e $P \in \mathbb{P}_F$ definimos $v_P(\omega) := v_P((\omega))$.*

*2. Dizemos que um lugar $P \in \mathbb{P}_F$ é um **zero** (resp. **polo**) de ω se $v_P(\omega) > 0$ (resp. $v_P(\omega) < 0$).*

*3. Dizemos que W é um divisor **canônico** se $W = (\omega)$ para algum $\omega \in \Omega_F \setminus \{0\}$.*

Segue imediatamente das definições que $\Omega_F(D) = \{\omega \in \Omega_F : (\omega) \geq D\} \cup \{0\}$.

Proposição 1.33. *1. Para $0 \neq x \in F$ e $0 \neq \omega \in \Omega_F$ temos $(x\omega) = (x) + (\omega)$.*

2. Quaisquer dois divisores canônicos são equivalentes.

Demonstração. Se ω se anula em $\mathcal{A}_F(D) + F$ então $x\omega$ se anula em $\mathcal{A}_F(D + (x)) + F$. Como ω se anula em $\mathcal{A}_F((\omega)) + F$, temos

$$(\omega) + (x) \leq (x\omega).$$

Da mesma forma, $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$. Combinando estas desigualdades, ficamos com

$$(\omega) + (x) \leq (x\omega) \leq -(x^{-1}) + (\omega) = (\omega) + (x).$$

Isto prova o item (1). Para o item (2), observe que, pela Proposição 1.30, dados quaisquer dois diferenciais de Weil ω_1 e ω_2 não nulos, existe $x \in F \setminus \{0\}$ tal que $\omega_2 = x\omega_1$. Pelo item (1), temos $(\omega_2) = (x) + (\omega_1)$. □

Teorema 1.34. *Seja $W = (\omega)$ um divisor canônico de $F|K$. Para cada $D \in \mathrm{Div}(F)$, a aplicação*

$$\mu : \begin{cases} \mathscr{L}(W - D) & \to & \Omega_F(D), \\ x & \mapsto & x\omega \end{cases}$$

está bem definida e é um isomorfismo de K-espaços vetoriais. Em particular, $i(D) = \ell(W - D)$.

Demonstração. Para $x \in \mathscr{L}(W - D)$, temos

$$(x\omega) = (x) + (\omega) \geq -(W - D) + W = D,$$

e logo $x\omega \in \Omega_F(D)$. Assim, μ leva $\mathscr{L}(W - D)$ em $\Omega_F(D)$. É fácil ver que μ é linear e injetora. Para mostrar que μ é sobrejetora, tome $\omega_1 \in \Omega_F(D)$. Pela Proposição 1.30, podemos escrever $\omega_1 = x\omega$ para algum $x \in F$. Como

$$(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geq D,$$

ficamos com $(x) \geq -(W - D)$, donde $x \in \mathscr{L}(W - D)$ e $\omega_1 = \mu(x)$. Provamos, assim, que $\ell(W - D) = \dim_K \Omega_F(D)$. Como $i(D) = \dim_K \Omega_F(D)$ pela Proposição 1.27, segue que $i(D) = \ell(W - D)$. □

Teorema 1.35 (Riemann-Roch)**.** *Para cada divisor $D \in \mathrm{Div}(F)$,*

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

Demonstração. Segue diretamente do Teorema 1.34 e da definição de $i(D)$. □

Corolário 1.36. *1. Para todo divisor canônico W temos $\deg W = 2g - 2$ e $\ell(W) = g$.*

2. Um divisor D é canônico se, e somente se, $\deg D = 2g - 2$ e $\ell(D) \geq g$.

3. Se D é um divisor com $\deg D > 2g - 2$, então $\ell(D) = \deg G + 1 - g$.

Demonstração. 1. Basta tomar, no Teorema de Riemann-Roch, $D = W$ e $D = 0$, respectivamente.

2. Suponha que $\deg D = 2g - 2$ e $\ell(D) \geq g$. Seja W um divisor canônico. Então

$$g \leq \ell(D) = \deg D + 1 - g + \ell(W - D) = g - 1 + \ell(W - D),$$

e logo $\ell(W - D) \geq 1$. Como $\deg(W - D) = 0$, segue pelo Corolário 1.21 que $W - D = (x)$ é principal. Assim, se $W = (\omega)$ temos que $D = \left(\frac{1}{x}\omega\right)$ é canônico.

3. Veja que pelo item (1), se W é um divisor canônico arbitrário, então $\deg(W - D) < 0$. Logo $\ell(W - D) = 0$, e o resultado segue do Teorema de Riemann-Roch.

□

O item (2) do Corolário 1.36 poderia ter sido enunciado considerando a igualdade $\ell(D) = g$ ao invés de $\ell(D) \geq g$. Entretanto, a afirmação $\ell(D) \geq g$ é mais fraca do que $\ell(D) = g$, de forma que para concluir que o divisor D é canônico, por exemplo, basta mostrar que existem g elementos linearmente independentes em $\mathscr{L}(D)$ (além de verificar que $\deg D = 2g - 2$). O seguinte resultado complementa a cota inferior dada para $\ell(D)$ no Teorema de Riemann.

Teorema 1.37 (Teorema de Clifford)**.** *Para todo divisor D com $0 \leq \deg D \leq 2g - 2$, tem-se*

$$\ell(D) \leq 1 + \frac{1}{2}\deg D.$$

Capítulo 2

Semigrupos de Weierstrass

Seja $F|K$ um corpo de funções algébricas. Dado $P \in \mathbb{P}_F$, consideremos o conjunto

$$H(P) := \{\alpha \in \mathbb{N}_0 : \text{ existe } x \in F \text{ com } (x)_\infty = \alpha P\}.$$

Proposição 2.1. *Para $\alpha \in N_0$, temos $\alpha \in H(P)$ se, e somente se, $\ell(\alpha P) > \ell((\alpha-1)P)$.*

Demonstração. Um elemento $x \in F$ é tal que $(x)_\infty = \alpha P$ se, e somente se, $v_P(x) = -\alpha$ e $v_Q(x) \geq 0$ para $Q \in \mathbb{P}_F \setminus \{P\}$, isto é, $x \in \mathscr{L}(\alpha P) \setminus \mathscr{L}((\alpha-1)P)$. □

Definição 2.2. *Um **semigrupo numérico** é um subconjunto $H \subseteq \mathbb{N}_0$ tal que:*

1. $0 \in H$.
2. *Se $\alpha_1, \alpha_2 \in H$, então $\alpha_1 + \alpha_2 \in H$.*
3. $\mathbb{N}_0 \setminus H$ *é finito.*

Observe que $0 \in H(P)$, já que $(1)_\infty = 0P$. Além disso, dados $\alpha_1, \alpha_2 \in H(P)$, digamos $(x_1)_\infty = \alpha_1 P$ e $(x_2)_\infty = \alpha_2 P$, então $(x_1 x_2)_\infty = (\alpha_1 + \alpha_2)P$, isto é, $\alpha_1 + \alpha_2 \in H(P)$. Assim, para concluir que $H(P)$ é um semigrupo numérico, precisamos mostrar que tem complemento finito em $\mathbb{N}_0$. Isso é garantido pelo seguinte.

Teorema 2.3 (Teorema das Lacunas de Weierstrass)**.** *Suponha que $F|K$ tenha gênero $g > 0$ e P é um lugar de grau um. Então existem exatamente g lacunas $i_1, \ldots, i_g$ em P. Temos*

$$i_1 = 1 \text{ e } i_g \leq 2g - 1.$$

Demonstração. Primeiro provemos cada lacuna em P é menor ou igual a $2g-1$. Suponha que $\alpha \geq 2g$. Pelo Corolário 1.36, item (3), $\ell(\alpha P) = \alpha + 1 - g$ e $\ell((\alpha-1)P) = (\alpha-1) + 1 - g$. Da Proposição 2.1, segue que $\alpha \in H(P)$.

Veja que $\alpha \in \mathbb{N}_0$ é uma lacuna em P se, e somente se, $\ell(\alpha P) = \ell((\alpha-1)P)$. Considere a sequência de K-espaços vetoriais

$$K = \mathscr{L}(0) \subseteq \mathscr{L}(P) \subseteq \mathscr{L}(2P) \subseteq \cdots \subseteq \mathscr{L}((2g-1)P),$$

onde $\dim \mathscr{L}(0) = 1$ e $\dim \mathscr{L}((2g-1)P) = g$. Pelo Lema 1.17, temos $\dim \mathscr{L}(\alpha P) - \dim \mathscr{L}((\alpha-1)P) \leq 1$ para todo $\alpha \in \mathbb{N}_0$. Logo existem exatamente $g-1$ números $1 \leq \alpha \leq 2g-1$ tais que $\mathscr{L}((\alpha-1)P) \subsetneq \mathscr{L}(\alpha P)$. Os g números restantes são as lacunas em P.

Resta mostrar que 1 é uma lacuna. Suponha $1 \in H(P)$. Como $H(P)$ é um semigrupo, devemos ter $H(P) = \mathbb{N}_0$, e não existem lacunas. Mas isso contradiz a hipótese $g > 0$. □

O conjunto $H(P)$ é denominado **semigrupo de Weierstrass** associado a P. Se $\alpha \in J(P) := \mathbb{N}_0 \setminus H(P)$, dizemos que α é uma lacuna em P.

De forma semelhante, definimos o semigrupo de Weierstrass associado a um m-upla de lugares $P_1 \ldots, P_m \in \mathbb{P}_F$ como sendo

$$H(P_1, \ldots, P_m) := \{(\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m : \text{ existe } x \in F \text{ com } (x)_\infty = \alpha_1 P_1 + \cdots + \alpha_m P_m\},$$

e dizemos que $(\alpha_1, \ldots, \alpha_m)$ é uma lacuna em $(P_1, \ldots, P_m)$ se $(\alpha_1, \ldots, \alpha_m) \in J(P_1, \ldots, P_m) := \mathbb{N}_0^m \setminus H(P_1, \ldots, P_m)$. Analogamente ao caso de um lugar, podemos mostrar que $H(P_1, \ldots, P_m)$ possui o elemento $(0, \ldots, 0)$ e é fechado em relação à soma. O Corolário 2.16 garante que, pelo menos no caso onde $\#K \geq m$, o complemento de $H(P_1, \ldots, P_m)$ em $\mathbb{N}_0^m$ é finito. A noção de semigrupo de Weierstrass de vários lugares foi introduzida em [1]. A seguir, listamos algumas propriedades no caso $m = 2$ que aparecem em [7], e suas generalizações para m arbitrário, feitas em [2].

Sejam $F|K$ um corpo de funções algébricas de gênero $g > 1$, e $P_1, P_2 \in \mathbb{P}_F$ lugares de grau um distintos.

Lema 2.4. *Se $(\alpha_1, \alpha_2), (\alpha_1', \alpha_2') \in H(P_1, P_2)$ com $\alpha_1 \geq \alpha_1'$ e $\alpha_2 \leq \alpha_2'$, então $(\alpha_1, \alpha_2') \in H(P_1, P_2)$.*

Demonstração. Se $\alpha_1 = \alpha_1'$ ou $\alpha_2 = \alpha_2'$, não há nada a provar. Suponha $\alpha_1 > \alpha_1'$ e $\alpha_2 < \alpha_2'$. Sejam $f_1, f_2 \in F$ tais que

$$(f_1)_\infty = \alpha_1 P_1 + \alpha_2 P_2 \text{ e } (f_2)_\infty = \alpha_1' P_1 + \alpha_2' P_2.$$

Tome $f = f_1 + f_2$. Temos $v_{P_1}(f) = -\alpha_1$ e $v_{P_2}(f) = -\alpha_2'$. Além disso, se P é um polo de f, então $0 > v_P(f) \geq \min\{v_P(f_1), v_P(f_2)\}$, e logo $P = P_1$ ou $P = P_2$. Portanto, $(f)_\infty = \alpha_1 P_1 + \alpha_2' P_2$ e $(\alpha_1, \alpha_2') \in H(P_1, P_2)$. □

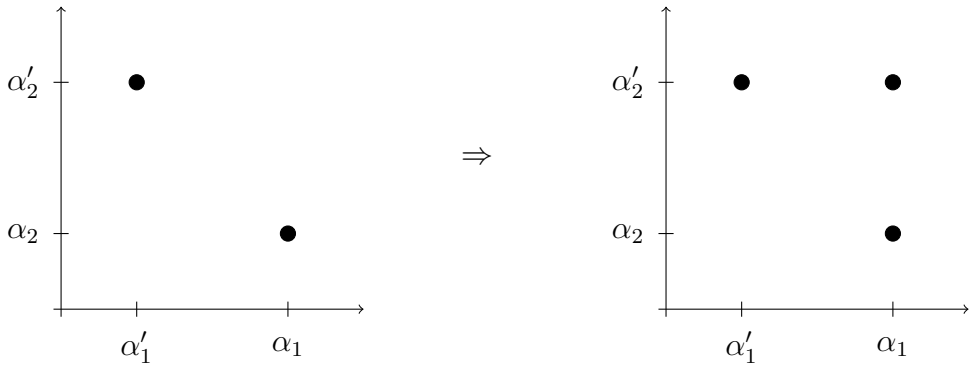

Figura 2.1: Interpretação gráfica do Lema 2.4.

Na Figura 2.1, os pontos marcados com ● pertencem a $H(P_1, P_2)$.

Lema 2.5. *Seja $\alpha_1 \geq 1$. Então $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2) + 1$ se, e somente se, existe α, $0 \leq \alpha \leq \alpha_2$, tal que $(\alpha_1, \alpha) \in H(P_1, P_2)$.*

Demonstração. Temos $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2) + 1$ se, e somente se, existe $f \in \mathscr{L}(\alpha_1 P_1 + \alpha_2 P_2) \setminus \mathscr{L}((\alpha_1 - 1)P_1 + \alpha_2 P_2)$, ou seja, $(f)_\infty = \alpha_1 P_1 + \alpha P_2$, com $0 \leq \alpha \leq \alpha_2$. □

Lema 2.6. *Para $(\alpha_1, \alpha_2) \in \mathbb{N}^2$, são equivalentes:*

1. $(\alpha_1, \alpha_2) \in H(P_1, P_2)$;

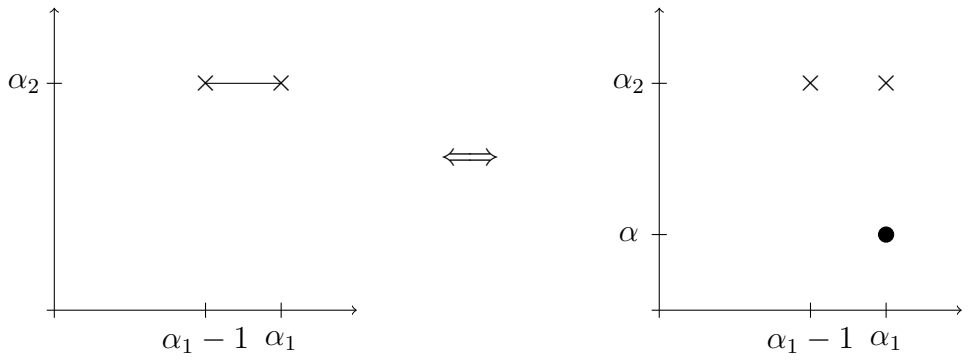

Figura 2.2: Interpretação gráfica do Lema 2.5. O segmento no gráfico do lado esquerdo ligando os pontos marcados com $\times$ indica que estes pontos representam divisores com dimensões diferentes.

2. $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2) + 1 = \ell(\alpha_1 P_1 + (\alpha_2 - 1)P_2) + 1$.

Demonstração. A implicação (1) $\Rightarrow$ (2) segue diretamente do Lema 2.5. Suponha (2). Pelo Lema 2.5, existem α_1', α_2' tais que $0 \leq \alpha_1' \leq \alpha_1$, $0 \leq \alpha_2' \leq \alpha_2$ tais que $(\alpha_1', \alpha_2), (\alpha_1, \alpha_2') \in H(P_1, P_2)$. Pelo Lema 2.4, temos $(\alpha_1, \alpha_2) \in H(P_1, P_2)$. □

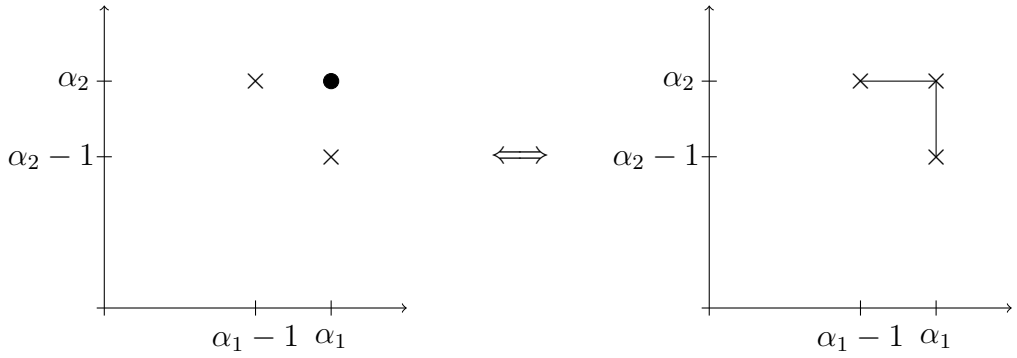

Figura 2.3: Interpretação gráfica do Lema 2.6.

Na Figura 2.3, um segmento ligando dois pontos indica que estes pontos representam divisores com dimensões diferentes, e o ponto marcado com $\bullet$ pertence a $H(P_1, P_2)$.

Corolário 2.7. *Se* $\alpha_1, \alpha_2 \in \mathbb{N}_0$ *e* $\alpha_1 + \alpha_2 \geq 2g$*, então* $(\alpha_1, \alpha_2) \in H(P_1, P_2)$.

Demonstração. Se $\alpha_1 = 0$ ou $\alpha_2 = 0$, o resultado segue do Teorema 2.3. Suponha $\alpha_1 \geq 1$ e $\alpha_2 \geq 1$. Tome $D := \alpha_1 P_1 + \alpha_2 P_2$. Por hipótese, $\deg D = \alpha_1 + \alpha_2 \geq 2g$. Pelo item (3) do Corolário 1.36, $\ell(D) = \alpha_1 + \alpha_2 + 1 - g$, $\ell(D - P_1) = \alpha_1 - 1 + \alpha_2 + 1 - g = \ell(D) - 1$ e $\ell(D - P_2) = \alpha_1 + \alpha_2 - 1 + 1 - g = \ell(D) - 1$. Pelo Lema 2.6, devemos ter $(\alpha_1, \alpha_2) \in H(P_1, P_2)$. □

Definição 2.8. *Para* $\alpha \in \mathbb{N}_0$*, definimos* $\beta_\alpha = \min\{\beta : (\alpha, \beta) \in H(P_1, P_2)\}$*. Observe que* $\alpha \in J(P_1)$ *se, e somente se,* $\beta_\alpha \geq 1$.

Corolário 2.9. *Sejam* $\alpha_1, \alpha_2 \in \mathbb{N}_0$*,* $\alpha_1 \geq 1$*. Então* $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2)$ *se, e somente se,* $\alpha_2 < \beta_{\alpha_1}$.

Demonstração. Segue diretamente do Lema 2.5. □

Lema 2.10. *Para uma lacuna* α_1 *em* P_1*, tem-se* $\alpha_1 = \min\{\alpha : (\alpha, \beta_{\alpha_1}) \in H(P_1, P_2)\}$*. Além disso,* $\{\beta_{\alpha_1} : \alpha_1 \in J(P_1)\} = J(P_2)$.

Demonstração. Temos $\alpha_1 \geq 1$ e $\beta_{\alpha_1} \geq 1$. Defina $D := \alpha_1 P_1 + \beta_{\alpha_1} P_2$. Pelo Lema 2.6, temos $\ell(D - P_1) = \ell(D - P_2) = \ell(D) - 1$. Pelo Corolário 2.9, $\ell(D - P_2 - P_1) = \ell(D - P_2) = \ell(D) - 1$. Suponha que exista $\alpha_1' < \alpha_1$ tal que $(\alpha_1', \beta_{\alpha_1}) \in H(P_1, P_2)$. Então, pelo Lema 2.5, $\ell(D - P_1 - P_2) = \ell(D - P_1) - 1 = \ell(D) - 2$, o que é uma contradição.

Agora, observe que $\beta_{\alpha_1} \in J(P_2)$ (já que $(0, \beta_{\alpha_1}) \notin H(P_1, P_2)$), e se $\alpha_2 \neq \alpha_1$ então $\beta_{\alpha_2} \neq \beta_{\alpha_1}$. Assim, $\{\beta_{\alpha_1} : \alpha_1 \in J(P_1)\}$ está contido em $J(P_2)$, e sua cardinalidade é g, portanto deve ser igual a $J(P_2)$. □

Observação 2.11. *Como consequência do Lema 2.10 e do Teorema 2.3, segue que a aplicação $J(P_1) \to J(P_2)$ dada por $\alpha \mapsto \beta_\alpha$ é bijetora. (A aplicação é sobrejetora e $\#J(P_1) = \#J(P_2)$.)*

Para generalizar estes resultados para semigrupos de Weierstrass de m lugares, fixemos a seguinte notação. Sejam $P_1, \ldots, P_m$ lugares racionais distintos de $F|K$. Denotaremos $H := H(P_1, \ldots, P_m)$ e $J := \mathbb{N}_0^m \setminus H$. Para $\mathbf{n} := (n_1, \ldots, n_m) \in \mathbb{Z}^m$, denotaremos $\mathscr{L}(\mathbf{n}) := \mathscr{L}(n_1 P_1 + \cdots + n_m P_m)$ e $\ell(\mathbf{n}) := \ell(\mathscr{L}(\mathbf{n}))$. Para $i \in \{1, \ldots, m\}$, definimos

$$\nabla_i(\mathbf{n}) := \{(p_1, \ldots, p_m) \in H : p_i = n_i \text{ e } p_j \leq n_j, \forall j \neq i\}.$$

Definimos ainda $\mathbf{n}^{(i)} := \mathbf{n} - n_i \mathbf{e}_i$, onde $\mathbf{e}_i$ denota o elemento de $\mathbb{N}_0^m$ com 1 na i-ésima coordenada e 0 nas outras.

No que segue, assumimos $\#K \geq m$. Os resultados acima podem ser generalizados, respectivamente, da seguinte forma.

Lema 2.12. *Para $(n_1, \ldots, n_m), (p_1, \ldots, p_m) \in H$, seja $q_i := \max\{n_i, p_i\}$ para $i = 1, \ldots, m$. Então $(q_1, \ldots, q_m) \in H$.*

Demonstração. Sejam $f, g \in F$ tais que $(f)_\infty = \sum_{i=1}^m n_i P_i$ e $(g)_\infty = \sum_{i=1}^m p_i P_i$. Para $i = 1, \ldots, m$, escolha um uniformizante local $t_i \in P_i$, e defina $a_i := \left(t_i^{-n_i} f\right)(P_i)$ e $b_i := \left(t_i^{-p_i} g\right)(P_i)$. Observe que $a_i, b_i \in K \setminus \{0\}$. Sejam $\alpha, \beta \in K$ e $h := \alpha f + \beta g$. Se $P \in \mathbb{P}_F \setminus \{P_1, \ldots, P_m\}$, então $v_P(h) \geq \min\{v_P(f), v_P(g)\} \geq 0$. Se $n_i \neq p_i$ então, $v_{P_i}(h) = \min\{v_{P_i}(f), v_{P_i}(g)\} = -q_i$. Se $n_i = p_i$, então $\left(t_i^{-n_i} h\right)(P_i) = \alpha a_i + \beta b_i$, e logo $v_{P_i}(h) = -q_i$ desde que $\alpha a_i + \beta b_i \neq 0$. Assim, se escolhemos (α, β) no conjunto

$$K^2 \setminus \bigcup_{i : n_i = p_i} \{(\alpha, \beta) \in K^2 : \alpha a_i + \beta b_i = 0\},$$

isto é, no complementar em K^2 de uma união de no máximo m subespaços de dimensão 1, teremos $(h)_\infty = \sum_{i=1}^m q_i P_i$. Mas essa escolha é possível, já que $\#K \geq m$. □

Lema 2.13. *Sejam $\boldsymbol{n} \in \mathbb{N}_0^m$ e $i \in \{1, \ldots, m\}$. Então $\ell(\boldsymbol{n}) = \ell(\boldsymbol{n} - \boldsymbol{e}_i) + 1$ se, e somente se, $\nabla_i(\boldsymbol{n}) \neq \emptyset$.*

Demonstração. Observe que $f \in \mathscr{L}(\mathbf{n}) \setminus \mathscr{L}(\mathbf{n} - \mathbf{e}_i)$ se, e somente se, $(f)_\infty = \sum_{j=1}^m p_j P_j$, com $p_i = n_i$ e $p_j \leq n_j$ para $j \neq i$. Portanto, o resultado segue. □

Lema 2.14. *Dado $\boldsymbol{n} \in \mathbb{N}^m$, temos $\boldsymbol{n} \in H$ se, e somente se, $\ell(\boldsymbol{n}) = \ell(\boldsymbol{n} - \boldsymbol{e}_i) + 1$ para todo $i = 1, \ldots, m$.*

Demonstração. Se $\mathbf{n} \in H$, então $\nabla_i(\mathbf{n}) \neq \emptyset$ para todo $i = 1, \ldots, m$. Pelo Lema 2.12, $\ell(\mathbf{n}) = \ell(\mathbf{n} - \mathbf{e}_i) + 1$ para todo $i = 1, \ldots, m$.

Para a implicação inversa, tome $f_i \in \mathscr{L}(\mathbf{n}) \setminus \mathscr{L}(\mathbf{n} - \mathbf{e}_i)$, isto é, $v_{P_i}(f_i) = -n_i$ e $v_{P_j}(f_i) \geq -n_j$ para $j \neq i$, onde $i, j \in \{1, \ldots, m\}$. Queremos mostrar que existe uma m-upla $(\alpha_1, \ldots, \alpha_m) \in K^m$ tal que o divisor de polos de $h := \sum_{i=1}^m \alpha_i f_i$ é precisamente $\sum_{i=1}^m n_i P_i$. Para cada $i = 1, \ldots, m$, escolha um uniformizante local t_i em P_i, e seja $a_{i,j} := \left(t_j^{n_j} f_i\right)(P_j)$. Então teremos $v_{P_j}(h) = -n_j$ desde que $\left(t_j^{n_j} h\right)(P_j) = \sum_{i=1}^m \alpha_i a_{i,j} \neq 0$. Assim, só precisamos escolher $(\alpha_1, \ldots, \alpha_n)$ no complemento em K^n da união de m subespaços de dimensão $m - 1$. Mas essa escolha é possível, já que $\#K \geq m$. □

Observação 2.15. *Demonstração alternativa do Lema 2.14. Suponha que* $\ell(\boldsymbol{n}) = \ell(\boldsymbol{n}-\boldsymbol{e}_i)+1$ *para cada* $i = 1, \ldots, m$. *Pelo Lema 2.12, podemos tomar* $\boldsymbol{p}_i = (p_{i,1}, \ldots, p_{i,m}) \in \nabla_i(\boldsymbol{n})$, *isto é,* $\boldsymbol{p}_i \in H$, $p_{i,i} = n_i$ *e* $p_{i,j} \leq n_j$ *para* $i \neq j$. *Para cada* $j = 1, \ldots, m$, *temos* $n_j = \max\{p_{i,j} : i \in \{1, \ldots, m\}\}$. *Pelo Lema 2.12 e um argumento de indução em* i, *concluímos que* $\boldsymbol{n} \in H$.

Corolário 2.16. *Se* $\boldsymbol{n} \in \mathbb{N}_0^m$ *e* $\sum_{i=1}^m n_i \geq 2g$, *então* $\boldsymbol{n} \in H$.

Demonstração. Procedemos por indução sobre m. O caso $m = 2$ é o Corolário 2.7. Seja $m > 2$, e suponha que o resultado é válido sempre que o número de lugares é menor que m. Assim, se algum n_i é nulo, estamos na hipótese de indução. Suponha então que $n_i \geq 1$ para todo $i = 1, \ldots, m$. Pelo item (3) do Corolário 1.36, temos $\ell(\mathbf{n}) = \sum_{i=1}^m n_i + 1 - g = \ell(\mathbf{n} - \mathbf{e}_i) + 1$ para cada $i = 1, \ldots, m$. Pelo Lema 2.14, temos $\mathbf{n} \in H$. □

Corolário 2.17. *Seja* $\boldsymbol{n} \in \mathbb{N}_0^m$. *São equivalentes:*

1. $\boldsymbol{n} \in J$;
2. *Existe* $i \in \{1, \ldots, m\}$ *tal que* $\ell(\boldsymbol{n}) = \ell(\boldsymbol{n} - \boldsymbol{e}_i)$;
3. *Existe* $i \in \{1, \ldots, m\}$ *tal que* $\nabla_i(\boldsymbol{n}) = \emptyset$.

Demonstração. Segue diretamente dos Lemas 2.13 e 2.14. □

Podemos equipar $\mathbb{N}_0^m$ com uma ordem parcial $\preceq$ como segue: $(n_1, \ldots, n_m) \preceq (p_1, \ldots, p_m)$ se $n_i \leq p_i$ para todo $i = 1, \ldots, m$.

A generalização do Lema 2.10 pode ser pensada da seguinte forma.

Lema 2.18. *Suponha que* n *seja uma lacuna em* P_i *e seja* $\boldsymbol{n}$ *um elemento minimal em* $\{\boldsymbol{p} \in H : p_i = n\}$ *com respeito a* $\preceq$. *Então* $\boldsymbol{n}^{(i)} \in J$ *e* $n = \min\{p \in \mathbb{N} : \boldsymbol{n}^{(i)} + p\boldsymbol{e}_i \in H\}$.

Demonstração. Suponha que $\mathbf{n}^{(i)} + q\mathbf{e}_i \in H$ para algum q com $0 \leq q < n$. Tome $f, g \in F$ com $(f)_\infty = \sum_{j=1}^m n_j P_j$ e $(g)_\infty = \sum_{\substack{j=1,\ldots,m \\ j\neq i}} n_j P_j + qP_i$. Para cada $j \in \{1, \ldots, m\}$, escolha um uniformizante local t_j em P_j, e defina $a := (t_i^n f)(P_i)$ e $b := (t_i^q g)(P_i)$. Tomando $h = bf - ag$, temos $(t_i^n h)(P_i) = b\,(t_i^n f)(P_i) - a\,(t_i^n g)(P_i) = ba \neq 0$, e logo $v_{P_i}(h) = -n$. Para $j \neq i$, temos $\left(t_j^{n_j} h\right)(P_j) = 0$, ou seja, e $v_{P_j}(h) > -n_j$. Assim $(h)_\infty = \sum_{j=1}^m p_j P_j$, com $p_i = n$ e $p_j < n_j$ para $j \neq i$, o que contradiz a minimalidade de $\mathbf{n}$. □

Por outro lado, se $\mathbf{n} \in \mathbb{N}_0^m$ é tal que $\mathbf{n}^{(i)} \in J$ para algum $i \in \{1, \ldots, m\}$, tomando $n := \min\{p \in \mathbb{N} : \mathbf{n}^{(i)} + p\mathbf{e}_i \in H\}$, pode-se concluir que n é uma lacuna em P_i. Nesse caso, nem sempre é verdade que $\mathbf{n}^{(i)} + n\mathbf{e}_i$ é minimal em $\{\mathbf{p} \in H : p_i = n\}$. Mas vale o seguinte.

Lema 2.19. *Sejam* $\boldsymbol{n} \in \mathbb{N}_0^m$ *e* $i \in \{1, \ldots, m\}$, *e suponha que* $\boldsymbol{n}^{(i)} \in J$. *Tome* $n := \min\{p \in \mathbb{N} : \boldsymbol{n}^{(i)} + p\boldsymbol{e}_i \in H\}$. *Se* $\boldsymbol{p} \in \mathbb{N}_0^m$ *é tal que* $p_i = n$, *e* $p_j < n_j$ *ou* $p_j = n_j = 0$ *para* $j \neq i$, *então* $\boldsymbol{p} \in J$. *Em particular,* n *é uma lacuna em* P_i.

Demonstração. Suponha que exista $\mathbf{p} \in H$ com $p_i = n$ e $p_j = n_j = 0$ ou $p_j < n_j$ para $j \neq i$. Tome $f, g \in F$ com $(f)_\infty = \sum_{\substack{j=1,\ldots,m \\ j\neq i}} n_j P_j + nP_i$ e $(g)_\infty = \sum_{j=1}^m p_i P_i$. Seja $t_j \in P_j$ uniformizante local para cada $j \in \{1, \ldots, m\}$. Tomando $a := (t_i^n f)(P_i)$ e $b := (t_i^n g)(P_i)$ e $h := bf - ag$, temos $(t_i^n h)(P_i) = 0$ e $(t_j^{n_j} h)(P_j) = b(t_j^{n_j} f)(P_j) + a(t_j^{n_j} g)(P_j) = b(t_j^{n_j} f)(P_j) \neq 0$. Assim, $v_{P_i}(h) > -n$ e $v_{P_j}(h) = -n_j$ para $j \neq i$, ou seja, $(h)_\infty = \sum_{j=1}^m q_j P_j$, com $q_i < n$ e $q_j = n_j$ para $j \neq i$, contradizendo a minimalidade de n. □

Observação 2.20. *Em [2], os autores descrevem um contra-exemplo para o Lema 2.14 quando se tira a hipótese* $\#K \geq m$.

Voltando ao caso $m = 2$, estamos interessados no número de lacunas que pode ter um semigrupo de Weierstrass. Para um lugar, o Teorema das Lacunas de Weierstrass nos diz que este número é g. Para obter uma fórmula para o caso de dois lugares, antes façamos uma descrição conveniente do conjunto de lacunas.

Teorema 2.21. *Temos*

$$J(P_1, P_2) = \{(\alpha, \beta) \in \mathbb{N}_0^2 : \alpha \in J(P_1), 0 \leq \beta < \beta_\alpha\} \cup \{(\alpha, \beta_{\alpha'}) : \alpha' \in J(P_1), 0 \leq \alpha < \alpha'\}.$$

Demonstração. Denotemos $J_1 := \{(\alpha, \beta) \in \mathbb{N}_0^2 : \alpha \in J(P_1), 0 \leq \beta < \beta_\alpha\}$ e $J_2 := \{(\alpha, \beta_{\alpha'}) : \alpha' \in J(P_1), 0 \leq \alpha < \alpha'\}$. Pela Definição 2.8, $J_1 \subseteq J(P_1, P_2)$, e pelo Lema 2.10, $J_2 \subseteq J(P_1, P_2)$.

Seja $(\alpha_1, \alpha_2) \in J(P_1, P_2)$. Se $\alpha_1 = 0$, então $\alpha_2 \in J(P_2)$, e pelo Lema 2.10 temos $\alpha_2 = \beta_{\alpha'}$ para algum $\alpha' \in J(P_1)$, e logo $(\alpha_1, \alpha_2) \in J_2$. Se $\alpha_2 = 0$, então $\alpha_1 \in J(P_1)$, e logo $(\alpha_1, \alpha_2) \in J_1$. Suponha agora $\alpha_1 \geq 1$ e $\alpha_2 \geq 1$. Pelo Lema 2.6, temos $\ell(\alpha_1 P_2 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2)$ ou $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell(\alpha_1 P_1 + (\alpha_2 - 1)P_2)$. No primeiro caso, o Lema 2.5 nos diz que $(\alpha_1, \alpha) \in J(P_1, P_2)$ para todo $0 \leq \alpha \leq \alpha_2$. Assim, $\alpha_1 \in J(P_1)$ e $\alpha_2 < \beta_{\alpha_1}$, donde segue que $(\alpha_1, \alpha_2) \in J_1$. No segundo caso, uma versão simétrica do Lema 2.5 nos dá $(\alpha_1, \alpha_2) \in J_2$. Portanto, $J(P_1, P_2) \subseteq J_1 \cup J_2$. □

Corolário 2.22. *O número de lacunas em* (P_1, P_2) *é*

$$\#J(P_1, P_2) = \sum_{\alpha_1 \in J(P_1)} \alpha_1 + \sum_{\alpha_2 \in J(P_2)} \alpha_2 - r(P_1, P_2),$$

onde $r(P_1, P_2) = \#\{(\alpha_1, \alpha_1') \in J(P_1)^2 : \alpha_1 < \alpha_1' \text{ e } \beta_{\alpha_1} > \beta_{\alpha_1'}\}$.

Demonstração. Sejam J_1 e J_2 como na demonstração do Teorema 2.21. Então

$$\#J(P_1, P_2) = \#J_1 + \#J_2 - \#(J_1 \cap J_2).$$

É fácil ver que

$$\#J_1 = \sum_{\alpha \in J(P_1)} \beta_\alpha = \sum_{\alpha \in J(P_2)} \alpha \text{ e } \#J_2 = \sum_{\alpha' \in J(P_1)} \alpha'.$$

Temos

$$J_1 \cap J_2 = \{(\alpha, \beta_{\alpha'}) \in \mathbb{N}_0^2 : \alpha, \alpha' \in J(P_1), 0 \leq \beta_{\alpha'} < \beta_\alpha \text{ e } 0 \leq \alpha < \alpha'\},$$

e logo $\#(J_1 \cap J_2) = \#\{(\alpha_1, \alpha_1') \in J(P_1)^2 : \alpha_1 < \alpha_1' \text{ e } \beta_{\alpha_1} > \beta_{\alpha_1'}\}$. □

Temos ainda uma elegante fórmula envolvendo dimensões de espaços de Riemann-Roch.

Proposição 2.23. *O número de lacunas em* (P_1, P_2) *é:*

$$\#J(P_1, P_2) = \sum_{\alpha=1}^{2g-1} \ell(\alpha P_1 + \beta_\alpha P_2) - 1.$$

Demonstração. Observe que se $\alpha \in H(P_1)$ então $\beta_\alpha = 0$. Sejam $\alpha \in J(P_1)$ e $\beta \geq 1$. Então $\ell(\alpha P_1 + \beta P_2) = \ell(\alpha P_1 + (\beta - 1)P_2)$ se, e somente se, $\beta = \beta_{\alpha'}$ para algum $\alpha' > \alpha$ (Corolário 2.9). Assim,

$$\begin{aligned} \ell(\alpha P_1 + \beta_\alpha P_2) &= \ell(\alpha P_1) + \sum_{\beta=1}^{\beta_\alpha} (\ell(\alpha P_1 + \beta P_2) - \ell(\alpha P_1 + (\beta - 1)P_2)) \\ &= \ell(\alpha P_1) + \beta_\alpha - \#\{\alpha' \in J(P_1) : \alpha' > \alpha \text{ e } \beta_{\alpha'} < \beta_\alpha\}. \end{aligned}$$

E logo, temos

$$\begin{aligned}\sum_{\alpha=1}^{2g-1}\ell(\alpha P_1+\beta_\alpha P_2) &= \sum_{\alpha=1}^{2g-1}\ell(\alpha P_1)+\sum_{\alpha\in J(P_1)}(\beta_\alpha-\#\{\alpha'\in J(P_1):\alpha'>\alpha \text{ e } \beta_{\alpha'}<\beta_\alpha\})\\ &= \sum_{\alpha\in J(P_1)}\ell(\alpha P_1)+\sum_{\substack{\alpha\in H(P_1)\\ 1\leq\alpha\leq 2g-1}}\ell(\alpha P_1)+\sum_{\beta\in J(P_2)}\beta-r(P_1,P_2).\end{aligned}$$

Agora, temos

$$\alpha\in H(P_1)\iff \ell(\alpha P_1)=\ell((\alpha-1)P_1)+1$$

e

$$\alpha\in J(P_1)\iff i(\alpha P_1)=i((\alpha-1)P_1)-1.$$

Daí

$$\sum_{\substack{\alpha\in H(P_1)\\ 1\leq\alpha\leq 2g-1}}\ell(\alpha P_1)=2+3+\cdots+g=\frac{(g+2)(g-1)}{2},$$

e

$$\begin{aligned}\sum_{\alpha\in J(P_1)}\ell(\alpha P_1) &= \sum_{\alpha\in J(P_1)}(\alpha+1-g+i(\alpha P_1))\\ &= \sum_{\alpha\in J(P_1)}\alpha+g(1-g)+(g-1)+\cdots+2+1\\ &= \sum_{\alpha\in J(P_1)}\alpha-\frac{g(g-1)}{2}.\end{aligned}$$

Portanto,

$$\begin{aligned}\sum_{\alpha=1}^{2g-1}\ell(\alpha P_1+\beta_\alpha P_2) &= \sum_{\alpha\in J(P_1)}\alpha-\frac{g(g-1)}{2}+\frac{(g+2)(g-1)}{2}+\sum_{\beta\in J(P_2)}\beta-r(P_1,P_2)\\ &= \#J(P_1,P_2)+1\end{aligned}$$

□

Capítulo 3

O Corpo de Funções Hermitiano

No Capítulo 4 falaremos de códigos, mais especificamente de códigos construídos a partir de corpos de funções. Observando as cotas para distância mínima apresentadas nos Teoremas 4.3 e 4.8, ($n - \deg G$ e $\deg G - 2g + 2$, respectivamente), percebemos que pode-se obter códigos com distância mínima maior em ambas as construções desde que o divisor G possa ser escolhido de grau bem menor que n e bem maior que $2g-2$, ou seja, desde que o número de lugares racionais seja grande em relação ao gênero. Isso serve de motivação para encontrar e estudar corpos de funções com o número máximo de lugares racionais para um dado gênero, os chamados **corpos de funções maximais**. Um exemplo é o corpo de funções Hermitiano ([12], Exemplo 6.3.6).

Definição 3.1. *Seja $q = p^s \in \mathbb{N}$ para algum primo p e algum $s > 0$. O **corpo de funções Hermitiano** sobre $\mathbb{F}_{q^2}$ é definido como sendo $\mathcal{H} = \mathbb{F}_{q^2}(x, y)$, onde $y^q + y = x^{q+1}$.*

No seguinte enunciado, colecionamos alguns resultados a respeito de $\mathcal{H}$, cujas demonstrações podem ser encontradas em [12] (Lema 6.4.4).

Teorema 3.2. *O corpo de funções Hermitiano $\mathbb{F}_{q^2}(x, y)|\mathbb{F}_{q^2}$, com $y^q + y = x^{q+1}$, tem gênero $g = q(q-1)/2$, e possui $q^3 + 1$ lugares de grau um sobre $\mathbb{F}_{q^2}$, que são*

- *o único polo comum P_∞ de x e y; e*
- *para cada $a \in \mathbb{F}_{q^2}$ existem q elementos $b \in \mathbb{F}_{q^2}$ tais que $b^q + b = a^{q+1}$, e para cada um desses pares $(a, b) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$, existe um único lugar P_{ab} de grau um tal que $x(P_{ab}) = a$ e $y(P_{ab}) = b$.*

Além disso, os divisores de polos de x e y são $(x)_\infty = qP_\infty$ e $(y)_\infty = (q+1)P_\infty$.

Observe que, pelo Teorema 3.2, existem q elementos $b \in \mathbb{F}_{q^2}$ tais que $b^q + b = 0$, e os q lugares associados P_{0b} são zeros de x. Como $\deg(x) = 0$, estes são todos os zeros de x:

$$(x) = \sum_{b^q+b=0} P_{0b} - qP_\infty.$$

Além disso, se um lugar é zero de y, então também será zero de x, e logo deve ser P_{00}. Daí:

$$(y) = (q+1)(P_{00} - P_\infty).$$

Queremos determinar o semigrupo de Weierstrass $H(P)$ para cada lugar P de grau um do corpo de funções Hermitiano.

Primeiro considere $P = P_\infty$. Pelo Teorema 3.2, temos $q, q+1 \in H(P)$, e logo, $iq + j(q+1) \in H(P)$ para i, j inteiros não negativos. Defina $H_0 := \{iq + j(q+1) : i, j \in \mathbb{N}_0\}$.

Lema 3.3. *Dado $n > 0$, existem únicos inteiros t e k, com $0 \leq k < q$ tais que $n = tq + k$. Então $n \in H_0$ se, e somente se, $t \geq k$.*

Demonstração. Suponha que $n \in H_0$. Então existem $i, j \in \mathbb{N}_0$ tais que $n = tq + k = iq + j(q + 1) = (i + j)q + j$. Seja j' o maior inteiro tal que $j'q \leq j$. Então $n = (i + j + j')q + j - j'q$, com $0 \leq j - j'q < q$, e logo, $k = j - j'q$ e $t = i + j + j' \geq j \geq k$. Por outro lado, se $t \geq k$, então $n = tq + k = (t - k + k)q + k = (t - k)q + k(q + 1) \in H_0$. □

Lema 3.4. *Seja P um lugar de $\mathcal{H}$ de grau um. Se $H_0 \subseteq H(P)$, então $H(P) = H_0$.*

Demonstração. Pelo Lema 3.3, dado $n > 0$ temos $n \in \mathbb{N}_0 \setminus H_0$ se, e somente se, $n = tq + k$ com $0 \leq t < k \leq q - 1$. Logo, o número de elementos de $\mathbb{N}_0 \setminus H_0$ é

$$\sum_{k=1}^{q-1} k = \frac{q(q-1)}{2}.$$

Mas pelo Teorema 3.2, esse número é o gênero do corpo de funções, e pelo Teorema 2.3, é igual a $\#J(P) = \#(\mathbb{N}_0 \setminus H(P))$. Assim, $\mathbb{N}_0 \setminus H(P) \subseteq \mathbb{N}_0 \setminus H_0$ e são conjuntos finitos de mesma cardinalidade. Portanto, $\mathbb{N}_0 \setminus H(P) = \mathbb{N}_0 \setminus H_0$, ou seja, $H(P) = H_0$. □

Como $H_0 \subseteq H(P_\infty)$, pelo Lema 3.4, temos $H(P_\infty) = H_0$. Tome $\tilde{x} = x/y$ e $\tilde{y} = 1/y$. Temos

$$\begin{aligned}(\tilde{x}) = (x) - (y) &= \sum_{\substack{b^q + b = 0 \\ b \neq 0}} P_{0b} + P_{00} - qP_\infty - (q+1)P_{00} + (q+1)P_\infty \\ &= \sum_{\substack{b^q + b = 0 \\ b \neq 0}} P_{0b} + P_\infty - qP_{00},\end{aligned}$$

e

$$(\tilde{y}) = -(y) = (q+1)(P_\infty - P_{00}).$$

Assim, $q, q+1 \in H(P_{00})$, e logo também temos $H(P_{00}) = H_0$.

Sejam agora $a, b \in \mathbb{F}_{q^2}$ tais que $b^q + b = a^{q+1}$. Considere $\tilde{x} = x - a$. Se um lugar P é um polo de $x - a$, então $0 > v_P(x - a) \geq \min\{v_P(x), 0\}$, e logo P é um polo de x, ou seja, $P = P_\infty$. Além disso, $v_{P_\infty}(x - a) = v_{P_\infty}(x) = -q$. Agora, pelo Teorema 3.2, $x - a$ tem q zeros da forma $P_{a\beta}$, onde $\beta \in \mathbb{F}_{q^2}$ é tal que $\beta^q + \beta = a^{q+1}$. Portanto,

$$(\tilde{x}) = \sum_{\beta^q + \beta = a^{q+1}} P_{a\beta} - qP_\infty.$$

Tome $\tilde{y} = y - a^q x + b^q$. Se P é um polo de $\tilde{y}$, então $0 > v_P(\tilde{y}) \geq \min\{v_P(y), v_P(x), 0\}$, e logo $v_P(x) < 0$ ou $v_P(y) < 0$, e novamente devemos ter $P = P_\infty$. Mais ainda, $v_{P_\infty}(\tilde{y}) = v_{P_\infty}(y) = -(q+1)$. Agora observe que

$$\begin{aligned}\tilde{y}^q + \tilde{y} &= (y - a^q x + b^q)^q + y - a^q x + b^q \\ &= y^q - a^{q^2} x^q + b^{q^2} + y - a^q x + b^q \\ &= y^q + y - a x^q - a^q x + b + b^q \\ &= x^{q+1} - a x^q - a^q x + a^{q+1}.\end{aligned}$$

Por outro lado,

$$\begin{aligned}\tilde{x}^{q+1} &= (x - a)^{q+1} \\ &= (x - a)^q (x - a) \\ &= (x^q - a^q)(x - a) \\ &= x^{q+1} - a x^q - a^q x + a^{q+1}.\end{aligned}$$

Assim, temos $\tilde{y}^q + \tilde{y} = \tilde{x}^{q+1}$, ou ainda, $\tilde{y} = \tilde{x}^{q+1} - \tilde{y}^q$. Se P é um zero de $\tilde{y}$, então também é um zero de $\tilde{x}$. Temos $v_P(\tilde{x}^{q+1}) = (q+1)v_P(\tilde{x}) = q+1$ (observe que todos os zeros de $\tilde{x}$ têm ordem 1) e $v_P(\tilde{y}^q) = qv_P(\tilde{y}) \neq q+1$. Se $v_P(\tilde{y}^q) < q+1$, então $v_P(\tilde{y}) = \min\{v_P(\tilde{x}^{q+1}), v_P(\tilde{y}^q)\} = v_P(\tilde{y}^q)$, donde $v_P(\tilde{y}) = 0$, o que é uma contradição. Logo, $v_P(\tilde{y}^q) > q+1$, e $v_P(\tilde{y}) = q+1$, mostrando ainda que P é o único zero de $\tilde{y}$. Veja que $\tilde{y}(P_{ab}) = y(P_{ab}) - a^q x(P_{ab}) + b^q = b - a^q a + b^q = 0$, donde segue que $P = P_{ab}$. Portanto,

$$(\tilde{y}) = (q+1)(P_{ab} - P_\infty).$$

Temos:

$$\begin{aligned}\left(\frac{\tilde{x}}{\tilde{y}}\right) &= (\tilde{x}) - (\tilde{y}) \\ &= \sum_{\substack{\beta^q+\beta=a^q \\ \beta\neq b}} P_{a\beta} + P_{ab} - qP_\infty - (q+1)P_{ab} + (q+1)P_\infty \\ &= \sum_{\substack{\beta^q+\beta=a^q \\ \beta\neq b}} P_{a\beta} + P_\infty - qP_{ab},\end{aligned}$$

e

$$\left(\frac{1}{\tilde{y}}\right) = (q+1)(P_\infty - P_{ab}).$$

Desse modo, concluímos que $q, q+1 \in H(P_{ab})$, e novamente $H(P_{ab}) = H_0$. Resumindo:

Teorema 3.5. *Seja P um lugar de $\mathcal{H}$ de grau um. Então $H(P) = \{iq + j(q+1) : i, j \in \mathbb{N}_0\}$, e $J(P) = \{tq + k : t, k \in \mathbb{N}_0, 0 \leq t < k \leq q-1\}$.*

Uma forma útil de dispor as lacunas em um lugar P de grau um é a seguinte:

$$\begin{array}{ccccccc} 1 & 2 & 3 & \cdots & q-2 & q-1 \\ & q+2 & q+3 & \cdots & q+(q-2) & q+(q-1) \\ & & 2q+3 & \cdots & 2q+(q-2) & 2q+(q-1) \\ & & & \ddots & \vdots & \vdots \\ & & & & (q-3)q+(q-2) & (q-3)q+(q-1) \\ & & & & & (q-2)q+(q-1) \end{array} \tag{3.1}$$

Lema 3.6. *Sejam $J_0 \subseteq \mathbb{N}_0$, $n_0 = \min J_0$ e $\sigma_1, \sigma_2 : J_0 \to J_0$ bijeções. Suponha que $\sigma_1(n) \geq \sigma_2(n)$ para todo $n \in J_0$, e que $\sigma_1(n_0) = \sigma_2(n_0)$. Então $\sigma_1 = \sigma_2$.*

Demonstração. Segue facilmente por indução. □

A seguir determinamos o conjunto de lacunas para um par qualquer de lugares de grau um distintos no corpo de funções Hermitiano.

Teorema 3.7 ([8], Teorema 3.4)**.** *Sejam P_1 e P_2 dois lugares de grau um distintos do corpo de funções Hermitiano $\mathcal{H}$. Então*

$$\beta_{tq+k} = (q-1-k)q + q - 1 - t \tag{3.2}$$

para $0 \leq t < k \leq q-1$.

Demonstração. Primeiro, observe que se os β_i's respeitam a regra dada em (3.2) em $H(P_1, P_2)$, então a mesma regra vale para $H(P_2, P_1)$; isso segue do Lema 2.10, e do fato de que a aplicação $\alpha \mapsto \beta_\alpha$ definida por (3.2) é a própria inversa. Suponha inicialmente $P_1 = P_{ab}$, onde $a, b \in \mathbb{F}_{q^2}$ são tais que $b^q + b = a^{q+1}$, e $P_2 = P_\infty$. Procuramos por $f \in \mathcal{H}$ tal que $(f)_\infty = (tq + k)P_1 + ((q - 1 - k)q + q - 1 - t)P_2$. Vimos que

$$(x - a) = \sum_{\beta^q + \beta = a^{q+1}} P_{a\beta} - qP_\infty \text{ e } (y - a^q x + b^q) = (q + 1)(P_{ab} - P_\infty).$$

Assim, obtemos o seguinte divisor:

$$\begin{aligned}\left(\frac{(x-a)^{q+1-k+t}}{(y-a^q x+b^q)^{t+1}}\right) &= (q+1-k+t)\left(\sum_{\beta^q+\beta=a^{q+1}} P_{a\beta} - qP_\infty\right) \\ &\quad -(t+1)(q+1)(P_{ab}-P_\infty) \\ &= (q+1-k+t)\sum_{\substack{\beta^q+\beta=a \\ \beta\neq b}} P_{a\beta} - (tq+k)P_{ab} \\ &\quad -((q-1-k)q+q-1-t)P_\infty.\end{aligned}$$

Isso mostra que

$$\beta_{tq+k} \leq (q - 1 - k)q + q - 1 - t. \tag{3.3}$$

Daí, temos $\beta_{(q-2)(q+1)+1} \leq 1$, e logo $\beta_{(q-2)(q+1)+1} = 1$. As aplicações $\alpha \mapsto \beta_\alpha$ e $tq + k \mapsto (q-1-k)q+q-1-t$ são bijeções $J(P_1) \to J(P_1)$, e suas inversas coincidem em $1 = \min J(P_1)$. A equação (3.3) coloca essas bijeções sob as hipóteses do Lema 3.6 e, portanto, o resultado segue no caso de um dos lugares ser P_∞.

Para terminar a demonstração, precisamos mostrar que o resultado vale também quando nenhum dos lugares é P_∞. Para isto, vamos utilizar o conceito de automorfismo de corpos de funções. Um **automorfismo** ϕ de $F|K$ nada mais é que um automorfismo de F que fixa K, isto é, $\phi(a) = a$, para todo $a \in K$.

Observe que se $\mathcal{O}$ é um anel de valorização de $F|K$, então $\phi(\mathcal{O})$ tambem é. De fato, é claro que $\phi(\mathcal{O})$ é um anel, com $K \subsetneq \phi(\mathcal{O}) \subsetneq F$; além disso, para $f \in F$, se $f \notin \phi(\mathcal{O})$, então $\phi^{-1}(f) \notin \mathcal{O}$, e logo $(\phi^{-1}(f))^{-1} \in \mathcal{O}$, ou seja, $\phi((\phi^{-1}(f))^{-1}) = \phi(\phi^{-1}(f^{-1})) = f^{-1} \in \phi(\mathcal{O})$. A restrição $\phi_\mathcal{O} : \mathcal{O} \to \phi(\mathcal{O})$ é um isomorfismo, e logo, se P é o lugar de $F|K$ associado a $\mathcal{O}$, então o lugar associado a $\phi(\mathcal{O})$ é $\phi(P)$. Além disso, para $P \in \mathbb{P}_F$, temos que $Q := \phi^{-1}(P)$ é um lugar com $\phi(Q) = P$. Assim, ϕ induz uma bijeção $\mathbb{P}_F \to \mathbb{P}_F$, dada por $P \mapsto \phi(P)$, ou ainda, um automorfismo do grupo $\mathrm{Div}(F)$.

É interessante observar o efeito desse automorfismo sobre os divisores associados a funções (ver Definição 1.14). Dado $P \in \mathbb{P}_F$, se $t \in P$ é um uniformizante local, então $\phi(t)$ é uniformizante local em $\phi(P)$. Se $f \in F$ se escreve como $f = ut^n$, com $n \in \mathbb{Z}$ e $u \in \mathcal{O}_P$ um elemento invertível, então $\phi(f) = \phi(u)\phi(t)^n$, onde $\phi(u)$ é um elemento invertível de $\phi(\mathcal{O})$. Consequentemente, se $(f)_0 = \sum_{i=1}^m n_i P_i$, então $(\phi(f))_0 = \sum_{i=1}^m n_i \phi(P_i)$, analogamente para o divisor de polos e o divisor principal de f.

Considere o automorfismo ϕ_1 de $\mathcal{H}|\mathbb{F}_{q^2}$ induzido por $\phi_1(x) := x/y$ e $\phi_1(y) := 1/y$. Na discussão que leva ao Teorema 3.5, determinamos os divisores principais de $\phi_1(x)$ e $\phi_1(y)$. Por eles percebemos que $\phi_1(P_{00}) = P_\infty$ e $\phi_1(P_\infty) = P_{00}$, isto é, ϕ_1 leva P_{00} em P_∞ e vice-versa. Sejam $a, b \in \mathbb{F}_{q^2}$ com $b^q + b = a^{q+1}$, e seja ϕ_2 o automorfismo induzido por $\phi_2(x) = x - a$ e $\phi_2(y) = y - a^q x + b^q$. Como antes, podemos concluir que $\phi_2(P_\infty) = P_\infty$, e $\phi_2(P_{00}) = P_{ab}$, ou seja, ϕ_2 fixa P_∞ e leva P_{00} em P_{ab}. Se ϕ_3 é um automorfismo que fixa P_∞ e leva P_{00} em P_{cd}, então $\phi_3 \circ \phi_2^{-1}$ fixa P_∞ e leva P_{ab} em P_{cd}. Observe que $\phi_1 \circ \phi_2^{-1}$ leva P_{ab} em P_∞.

Agora suponha $P_1 = P_{ab}$ e $P_2 = P_{cd}$ com $(a, b) \neq (c, d)$. Então existe um automorfismo que fixa P_{ab} e leva P_{cd} em P_∞ (a saber, a composição $\phi_4 \circ \phi_5$, onde ϕ_5 é um automorfismo que leva P_{cd} em P_∞ e ϕ_4 é um automorfismo que leva $\phi_4(P_{ab})$ em P_{ab} e fixa P_∞). Assim, os β_α's para o par (P_{ab}, P_{cd}) são os mesmos para o par (P_{ab}, P_∞), que já calculamos. □

Saber β_α para cada lacuna α em P_1 nos permite calcular $\#J(P_1, P_2)$ para quaisquer dois lugares racionais distintos P_1 e P_2 do corpo de funções Hermitiano.

Teorema 3.8 ([8], Teorema 3.6)**.** *Para quaisquer dois lugares distintos P_1 e P_2 de grau um do corpo de funções Hermitiano $\mathcal{H}$,*

$$\#J(P_1, P_2) = \frac{q}{12}(3q^3 - 4q^2 + 3q - 2).$$

Demonstração. Usaremos o Corolário 2.22. A soma de todas as lacunas em P_1 (equivalentemente, a soma de todas as lacunas em P_2) é

$$\begin{aligned}\sum_{\alpha_1 \in J(P_1)} \alpha_1 &= \sum_{k=1}^{q-1}\sum_{t=0}^{k-1} tq + k \\ &= \sum_{k=1}^{q-1} \frac{qk(k-1)}{2} + k^2 \\ &= \frac{q(q+1)(q-1)^2}{6}\end{aligned}$$

Agora calculamos $r(P_1, P_2)$. Fixe $(t, k) \in \mathbb{N}_0$ com $0 \leq t < k \leq q-1$. Procuramos pelo número de pares $(t', k') \in N_0$ com $0 \leq t' < k' \leq q-1$ satisfazendo:

$$tq + k < t'q + k' \tag{3.4}$$

e

$$(q - 1 - k')q + q - 1 - t' < (q - 1 - k)q + q - 1 - t. \tag{3.5}$$

Mas (3.4) e (3.5) são equivalentes, respectivamente, a

$$t < t', \text{ ou } t = t' \text{ e } k < k' \tag{3.6}$$

e

$$k < k', \text{ ou } k = k' \text{ e } t < t'. \tag{3.7}$$

De (3.6) e (3.7) temos

$$t \leq t', k \leq k', (t, k) \neq (t', k'). \tag{3.8}$$

Mas é fácil ver que as três condições em (3.8) implicam (3.6) e (3.7). Assim, para cada par (t, k), contamos

$$\begin{aligned}\#\{(t', k') : k \leq k' \leq q-1, t \leq t' \leq k'-1\} - 1 &= \left(\sum_{k'=k}^{q-1} k' - t\right) - 1 \\ &= \frac{(q-1+k)(q-k)}{2} - (q-k)t - 1.\end{aligned}$$

Assim, temos

$$\begin{aligned}r(P_1, P_2) &= \sum_{k=1}^{q-1}\sum_{t=0}^{k-1} \frac{(q-1+k)(q-k)}{2} - (q-k)t - 1 \\ &= \sum_{k=1}^{q-1} \frac{kq^2 - k^2q - 2k}{2} \\ &= \frac{q^4 - 7q^2 + 6q}{12}.\end{aligned}$$

Portanto,

$$\begin{aligned} \#J(P_1,P_2) &= \sum_{\alpha_1\in J(P_1)} \alpha_1 + \sum_{\alpha_2\in J(P_2)} \alpha_2 - r(P_1,P_2) \\ &= \frac{q(q+1)(q-1)^2}{3} - \frac{q^4-7q^2+6q}{12} \\ &= \frac{q}{12}(3q^3-4q^2+3q-2). \end{aligned}$$

Os cálculos foram feitos com o auxílio das ferramentas *Series Calculator* e *Simplify Expression*, disponíveis em [9]. □

Exemplo 3.9. *Considere* $\mathcal{H} = \mathbb{F}_{64}(x,y)|\mathbb{F}_{64}$, *com* $y^8+y=x^9$. *Seja* $P_1 = P_{00}$ *e* $P_2 = P_\infty$. *Usamos o Teorema 3.7 para determinar* β_α *para todas as lacunas* α *em* P_1 *e escrevemos* (α,β_α), *seguindo a disposição em (3.1):*

$$\begin{array}{ccccccc} (1,55) & (2,47) & (3,39) & (4,31) & (5,23) & (6,15) & (7,7) \\ & (10,46) & (11,38) & (12,30) & (13,22) & (14,14) & (15,6) \\ & & (19,37) & (20,29) & (21,21) & (22,13) & (23,5) \\ & & & (28,28) & (29,20) & (30,12) & (31,4) \\ & & & & (37,19) & (38,11) & (39,3) \\ & & & & & (46,10) & (47,2) \\ & & & & & & (55,1) \end{array} \tag{3.9}$$

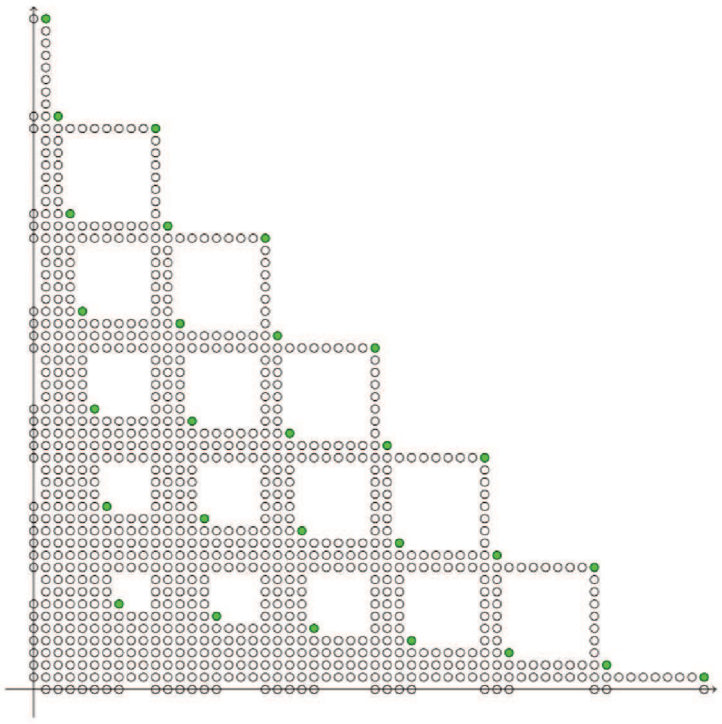

Figura 3.1: $J(P_1,P_2)$ no Exemplo 3.9

A Figura 3.9 mostra $J(P_1,P_2)$. *Os pontos em verde* ● *são os pares* $(\alpha,\beta_\alpha) \in H(P_1,P_2)$ *para* $\alpha \in J(P_1)$.

Capítulo 4

Códigos de Goppa

Sejam $n \geq 1$ e $A \neq \emptyset$ um conjunto finito, o qual chamaremos de alfabeto. Uma palavra de comprimento n é um elemento do produto cartesiano A^n. Um código de comprimento n sobre A é um subconjunto qualquer $\emptyset \neq C \subseteq A^n$.

Dadas palavras $a, b \in A^n$, definimos a distância (de Hamming) entre a e b, denotada por $d(a, b)$, da seguinte forma: se $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n)$, então

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

É fácil mostrar que $d : A^n \times A^n \to \mathbb{R}$ é uma métrica, isto é, para todos $a, b, c \in A^n$, tem-se:

- $d(a, b) \geq 0$;
- $d(a, b) = 0$ se, e somente se, $a = b$;
- $d(a, b) = d(b, a)$;
- $d(a, c) \leq d(a, b) + d(b, c)$.

A distância mínima de um código $C \subseteq A^n$ é definida por

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

Se A é um corpo finito e $C \subseteq A^n$ é um A-subespaço vetorial, dizemos que C é um código linear. Se $k = \dim_A C$ e $d = d(C)$, dizemos que C é um $[n, k, d]$-código.

Se A é um corpo, definimos o peso da palavra $a \in A^n$ como sendo $\mathrm{wt}(a) = d(a, 0)$. Assim, temos $d(a, b) = \mathrm{wt}(a - b)$ para todos $a, b \in A^n$. Se $C \subseteq A^n$ é um código, temos a seguinte caracterização para a distância mínima: $d(C) = \min\{\mathrm{wt}(a) : a \in C \setminus \{0\}\}$.

Seja $C \subseteq \mathbb{F}_q^n$ um código, onde $\mathbb{F}_q$ é um corpo com q elementos. Para $a, b \in \mathbb{F}_q^n$, digamos $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n)$, defina $a \cdot b := \sum_{i=1}^n a_i b_i$. O código **dual** de C é definido como $C^\perp := \{c' \in \mathbb{F}_q^n : c' \cdot c = 0 \text{ para todo } c \in C\}$.

Suponha que num certo canal a informação é transmitida em forma de palavras de comprimento n sobre um alfabeto A. O conjunto das palavras que possuem algum significado é um código $C \subseteq A^n$. Diremos que ocorreu um **erro** se uma das letras da palavra enviada foi substituída por outra letra de A, formando a palavra recebida. Se a é a palavra enviada e a' é a palavra recebida, o número de erros cometidos é $d(a, a')$. Se a' ainda é uma palava do código, este erro não poderá ser detectado. Observe que se a distância mínima de C for d, serão necessários d erros para que a palavra recebida esteja no código, e uma transmissão com $d - 1$ erros certamente será acusada. Além disso, se $d(a, a') \leq \lfloor (d-1)/2 \rfloor$, a será a palavra do código mais próxima de a' e, portanto, a com maior probabilidade de ser a palavra original. Nesse caso, o erro poderá ser corrigido. A grosso modo, quanto maior a distância mínima, mais erros podem ser detectados e corrigidos. No caso de códigos lineares, o seguinte resultado impõe algumas restrições.

Proposição 4.1 (Cota de Singleton)**.** *Seja C um $[n,k,d]$-código. Então $k+d \leq n+1$.*

Demonstração. Seja $E \subseteq \mathbb{F}_q^n$ o subespaço vetorial definido por

$$E := \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n : a_i = 0 \text{ para todo } i \geq d\}.$$

Todo $a \in E$ tem peso menor ou igual a $d-1$, e logo $E \cap C = \{0\}$. Como $\dim E = d-1$, temos

$$\begin{aligned} k + (d-1) &= \dim C + \dim E \\ &= \dim(C+E) + \dim C \cap E = \dim(C+E) \leq n. \end{aligned}$$

□

Os $[n,k,d]$-códigos para os quais vale $k+d = n+1$ são chamamos de **códigos MDS** (Maximum Distance Separable). Em geral, não é simples calcular a distância mínima de um código dado. Assim, procuramos métodos para construir códigos que permitam determinar a distância mínima, ou pelo menos fornecer uma cota inferior. O método que descrevemos neste trabalho foi proposto por V. D. Goppa em 1983([5]), e faz uso de ferramentas da teoria de corpos de funções algébricas.

Seja F um corpo de funções algébricas sobre $\mathbb{F}_q$ de gênero g, onde $\mathbb{F}_q$ é um corpo com q elementos. Sejam $P_1, \ldots, P_n \in \mathbb{P}_F$ lugares distintos de grau 1, e defina $D := P_1 + \cdots + P_n$. Seja G um divisor de $F|\mathbb{F}_q$ tal que $\operatorname{Supp} G \cap \operatorname{Supp} D = \emptyset$. Essa condição garante que, para $i \in \{1, \ldots, n\}$, tenhamos $v_{P_i}(x) \geq 0$ sempre que $x \in \mathscr{L}(G)$, e logo $x(P_i) \in F_{P_i} \cong \mathbb{F}_q$. Assim, faz sentido a seguinte definição.

Definição 4.2. *O **código de Goppa** $C_{\mathscr{L}}(D,G)$ associado aos divisores D e G é definido como*

$$C_{\mathscr{L}}(D,G) := \{(x(P_1), \ldots, x(P_n)) : x \in \mathscr{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Teorema 4.3. *$C_{\mathscr{L}}(D,G)$ é um $[n,k,d]$-código, com*

$$n = \deg D,\ k = \ell(G) - \ell(G-D) \text{ e } d \geq n - \deg G.$$

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

Demonstração. Considere a aplicação linear $\phi : \mathscr{L}(G) \to \mathbb{F}_q^n$ dada por

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

Então, por definição, temos $\operatorname{im}\phi = C_{\mathscr{L}}(D,G)$ e ainda

$$\ker\phi = \{x \in \mathscr{L}(G) : v_{P_i}(x) > 0 \text{ para } i = 1, \ldots, n\} = \mathscr{L}(G-D).$$

Assim, temos $k = \dim C_{\mathscr{L}}(D,G) = \dim \mathscr{L}(G) - \dim \mathscr{L}(G-D) = \ell(G) - \ell(G-D)$. Se $\deg G < n$, então $\ell(G-D) = 0$, e logo $k = \ell(G) \geq \deg G + 1 - g$ (Teorema de Riemann). Se $2g-2 < \deg G < n$, pelo Corolário 1.36 (3) temos $k = \deg G + 1 - g$.

A afirmação a respeito da distância mínima d só faz sentido se $C_{\mathscr{L}}(D,G) \neq \{0\}$. Seja $x \in \mathscr{L}(G)$ tal que $\operatorname{wt}(\phi(x)) = d$. Então exatamente $n-d$ lugares $P_{i_1}, \ldots, P_{i_{n-d}}$ são zeros de x, e logo, $0 \neq x \in \mathscr{L}(G - (P_{i_1} + \cdots + P_{i_{n-d}}))$. Pelo Corolário 1.20, temos $0 \leq \deg(G - (P_{i_1} + \cdots + P_{i_{n-d}})) = \deg G - n + d$, ou seja, $d \geq n - \deg G$. □

Observe que se $\deg G < \deg D$, então $C_{\mathscr{L}}(D,G)$ é um $[n,k,d]$-código com $n+1-g \leq k+d \leq n+1$, onde a segunda desigualdade é a cota de Singleton. Assim, se $g = 0$ então $C_{\mathscr{L}}(D,G)$ é um código MDS.

Um outro código pode ser associado aos divisores G e D, usando componentes locais de diferenciais de Weil.

Definição 4.4. *Seja $P \in \mathbb{P}_F$.*

1. *Para $x \in F$ denotamos por $\iota_P(x) \in \mathcal{A}_F$ o adele tal que $\iota_P(x)(P) = x$ e $\iota_P(x)(Q) = 0$ para $Q \in \mathbb{P}_F \setminus \{P\}$.*

2. *Para um diferencial de Weil $\omega \in \Omega_F$ a **componente local** de ω em P é a aplicação $\mathbb{F}_q$-linear $\omega_P : F \to \mathbb{F}_q$, definida por*

$$\omega_P(x) := \omega(\iota_P(x)).$$

Proposição 4.5 ([12], Proposição 1.7.3)**.** *Seja $\omega \neq 0$ um diferencial de Weil de $F|K$ e $P \in \mathbb{P}_F$. Então*

$$v_P(\omega) = \max\{r \in \mathbb{Z} : \omega_P(x) = 0 \text{ para todo } x \in F \text{ com } v_P(x) \geq -r\}.$$

Em particular, ω_P não é identicamente nulo.

Lema 4.6. *Seja P um lugar de grau um e seja ω um diferencial de Weil com $v_P(\omega) \geq -1$. Então*

$$\omega_P(1) = 0 \iff v_P(\omega) \geq 0.$$

Demonstração. Pela Proposição 4.5, para $r \in \mathbb{Z}$ temos

$$v_P(\omega) \geq r \iff \omega_P(x) = 0 \text{ para todo } x \in F \text{ com } v_P(x) \geq -r. \tag{4.1}$$

Se $v_P(\omega) \geq 0$, então por (4.1), temos $\omega_P(1) = 0$, já que $v_P(1) = 0$. Suponha agora que $\omega_P(1) = 0$. Seja $x \in F$ com $v_P(x) \geq 0$. Como $\deg P = 1$, podemos escrever $x = a + y$, com $a \in \mathbb{F}_q$ e $v_P(y) \geq 1$. Como $v_P(\omega) \geq -1$ e $v_P(y) \geq 1$, por (4.1) temos $\omega_P(y) = 0$, e logo $\omega_P(x) = \omega_P(a) + \omega_P(y) = a \cdot \omega_P(1) = 0$. □

Definição 4.7. *O **código de Goppa** $C_\Omega(D, G)$ associado aos divisores D e G é definido como*

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

Teorema 4.8. *Se $C_\Omega(D, G) \neq \{0\}$, então $C_\Omega(D, G)$ é um $[n, k, d]$-código, com*

$$n = \deg D,\ k = i(G - D) - i(G) \text{ e } d \geq \deg G - (2g - 2),$$

desde que $\deg G - (2g-2) \leq \deg D$. Se $\deg G > 2g-2$, então $k = i(G-D) \geq n+g-1-\deg G$. Se $2g - 2 < \deg G < n$, então $k = n + g - 1 - \deg G$.

Demonstração. Considere a aplicação linear $\psi : \Omega_F(G - D) \to \mathbb{F}_q^n$ definida por

$$\psi(\omega) := (\omega_{P_1}(1), \ldots, \omega_{P_n}(1)).$$

Então temos $\operatorname{im}\psi = C_\Omega(D, G)$ e pelo Lema 4.6,

$$\begin{aligned} \ker\psi &= \{\omega \in \Omega_F(G - D) : \omega_{P_i}(1) = 0, \text{ para } i = 1, \ldots n\} \\ &= \{\omega \in \Omega_F(G - D) : v_{P_i}(\omega) \geq 0, \text{ para } i = 1, \ldots, n\} \\ &= \Omega_F(G). \end{aligned}$$

Portanto, a dimensão de $C_\Omega(D, G)$ é $k = i(G - D) - i(G)$. Se $\deg G > 2g - 2$, pelo Corolário 1.36 (3) temos $i(G) = 0$, e logo $k = i(G-D) = \ell(G-D)+g-1+n-\deg G \geq n+g-1-\deg G$. Se $2g - 2 < \deg G < n$, então $\ell(G - D) = 0$ e $k = n + g - 1 - \deg G$.

Seja $\omega \in \Omega_F(G-D)$ com $\mathrm{wt}(\psi(\omega)) = m > 0$. Então $\omega_{P_i} = 0$ para certos índices $i = i_1, \ldots, i_{n-m}$, e pelo Lema 4.6, temos

$$\omega \in \Omega_F(G - (D - \sum_{j=1}^{n-m} P_{i_j})).$$

Pelo Corolário 1.36 (3), temos

$$2g - 2 \geq \deg G - (n - (n-m)) = \deg G - m.$$

Portanto, a distância mínima d de $C_\Omega(D,G)$ satisfaz a desigualdade $d \geq \deg G - (2g-2)$. □

Os códigos $C_{\mathscr{L}}(D,G)$ e $C_\Omega(D,G)$ estão intimamente relacionados.

Teorema 4.9 ([12], Teorema 2.2.8)**.** *Os códigos $C_{\mathscr{L}}(D,G)$ e $C_\Omega(D,G)$ são duais um do outro, isto é,*

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

Se $G = mP$ para algum lugar racional P, $m \in \mathbb{N}$, e D é a soma de todos os outros lugares racionais de $F|\mathbb{F}_q$, dizemos que $C_{\mathscr{L}}(D,G)$ e $C_\Omega(D,G)$ são **códigos de um ponto**. Se $G = \alpha_1 P_1 + \alpha_2 P_2$ para lugares racionais P_1 e P_2 distintos, $\alpha_1, \alpha_2 \in \mathbb{N}$, e D é a soma de todos os outros lugares racionais de $F|\mathbb{F}_q$, dizemos que $C_{\mathscr{L}}(D,G)$ e $C_\Omega(D,G)$ são **códigos de dois pontos**.

Capítulo 5

Resultados para códigos sobre o corpo de funções Hermitiano

Seguindo [8], podemos usar informação a respeito do semigrupo de Weierstrass de um par de lugares para construir códigos com uma cota para a distância mínima melhor do que a dada pelo Teorema 4.8. O primeiro resultado diz respeito a códigos sobre corpos de funções arbitrários.

Teorema 5.1. *Seja $F|\mathbb{F}_q$ um corpo de funções de gênero $g > 1$, e sejam P_1 e P_2 lugares racionais distintos. Assuma que $(\alpha_1, \alpha_2) \in J(P_1, P_2)$ com $\alpha_1 \geq 0$ e $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2)$. Suponha que $(\gamma_1, \gamma_2 - \delta - 1) \in J(P_1, P_2)$ para todo δ, $0 \leq \delta \leq \min\{\gamma_2 - 1, 2g - 1 - (\alpha_1 + \alpha_2)\}$. Tome $G = (\alpha_1 + \gamma_1 - 1)P_1 + (\alpha_2 + \gamma_2 - 1)P_2$, e seja $D = Q_1 + \cdots + Q_n$, onde os Q_i's são lugares racionais distintos, cada um dos quais não pertence ao suporte de G. Se a dimensão de $C_\Omega(D, G)$ é positiva, a distância mínima desse código é pelo menos* $\deg G - 2g + 3$.

Demonstração. De acordo com o Teorema 4.8, só precisamos mostrar que não existe uma palavra do código de peso $d := \deg G - (2g - 2)$. Se tal palavra existe, então pelo Lema 4.6, existe um diferencial $\omega \in \Omega_F(G - D)$ com exatamente d polos, digamos $Q_1, \ldots, Q_d$. Temos $(\omega) \geq G - (Q_1 + \cdots + Q_d)$. Assim, $2g - 2 = \deg(\omega) \geq \deg G - d = 2g - 2$, e logo

$$(\omega) = G - (Q_1 + \cdots + Q_d).$$

Pelo Teorema de Riemann-Roch, para um divisor canônico arbitrário W, temos

$$\ell(\alpha_1 P_1 + \alpha_2 P_2) = \deg(\alpha_1 P_1 + \alpha_2 P_2) + 1 - g + \ell(W - (\alpha_1 P_1 + \alpha_2 P_2))$$

e

$$\ell((\alpha_1 - 1)P_1 + \alpha_2 P_2) = \deg((\alpha_1 - 1)P_1 + \alpha_2 P_2) + 1 - g + \ell(W - ((\alpha_1 - 1)P_1 + \alpha_2 P_2)).$$

Como $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2)$, vale

$$\ell(W - ((\alpha_1 - 1)P_1 + \alpha_2 P_2)) = \ell(W - (\alpha_1 P_2 + \alpha_2 P_2)) + 1,$$

ou seja, existe $h \in \mathscr{L}(W - ((\alpha_1 - 1)P_1 + \alpha_2 P_2)) \setminus \mathscr{L}(W - (\alpha_1 P_1 + \alpha_2 P_2))$. Temos $v_{P_1}(h) = \alpha_1 - 1 - v_{P_1}(W)$, e logo $(h) = (\alpha_1 - 1)P_1 + \alpha_2 P_2 - W + E$, onde $E \geq 0$ é um divisor de grau $2g - 1 - (\alpha_1 + \alpha_2)$ cujo suporte não contém P_1. Escreva $E = E' + tP_2$, onde E' é um divisor efetivo cujo suporte não contém P_2 (ou seja, $0 \leq t \leq \deg E = 2g - 1 - (\alpha_1 + \alpha_2)$). Então podemos escrever

$$(h) = (\alpha_1 - 1)P_1 + (\alpha_2 + t)P_2 - W + E'.$$

Agora,

$$G - (Q_1 + \cdots + Q_d) = (\omega) \sim W \sim (\alpha_1 - 1)P_1 + (\alpha_2 + t)P_2 + E'.$$

Segue que existe $f \in F$ com divisor

$$\begin{aligned}(f) &= (\alpha_1 - 1)P_1 + (\alpha_2 + t)P_2 + E' - G + (Q_1 + \cdots + Q_d) \\ &= -\gamma_1 P_1 - (\gamma_2 - t - 1)P_2 + (Q_1 + \cdots + Q_d) + E'\end{aligned}$$

Se $t \leq \gamma_2 - 1$, então f tem divisor de polos $(f)_\infty = \gamma_1 P_1 + (\gamma_2 - t - 1)P_2$, contradizendo a hipótese de que $(\gamma_1, \gamma_2 - t - 1) \in J(P_1, P_2)$. Caso contrário, temos $\gamma_2 - 1 < t \leq 2g - 1 - (\alpha_1 + \alpha_2)$ e, por hipótese, $(\gamma_1, 0) \in J(P_1, P_2)$. Mas f tem divisor de polos $(f)_\infty = \gamma_1 P_1$, o que é uma contradição. □

Observação 5.2. *Trocando P_1 por P_2 e vice-versa no enunciado e na demonstração do Teorema 5.1, obtemos uma versão simétrica do resultado que contempla divisores G ignorados pela versão original. No caso onde $H(P_1, P_2) = H(P_2, P_1)$, como é o caso do corpo de funções Hermitiano, isso significa que se o divisor $G = n_1 P_1 + n_2 P_2$ satisfaz as hipóteses do Teorema 5.1, então a melhoria da cota para a distância mínima também vale se utilizamos o divisor $n_2 P_1 + n_1 P_2$ no lugar de G.*

Exemplo 5.3. *Seja $\mathcal{H}|\mathbb{F}_{16}$ corpo de funções com $\mathcal{H} = \mathbb{F}_{16}(x, y)$, $y^4 + y = x^5$. Tome $P_1 = P_{00}$ e $P_2 = P_\infty$ (notações como no Teorema 3.2). $\mathcal{H}|\mathbb{F}_{16}$ tem gênero $g = 4(4-1)/2 = 6$. A Figura 5.3 mostra $J(P_1, P_2)$. O segmento de reta na Figura 5.3 é dado $x + y = 12$.*

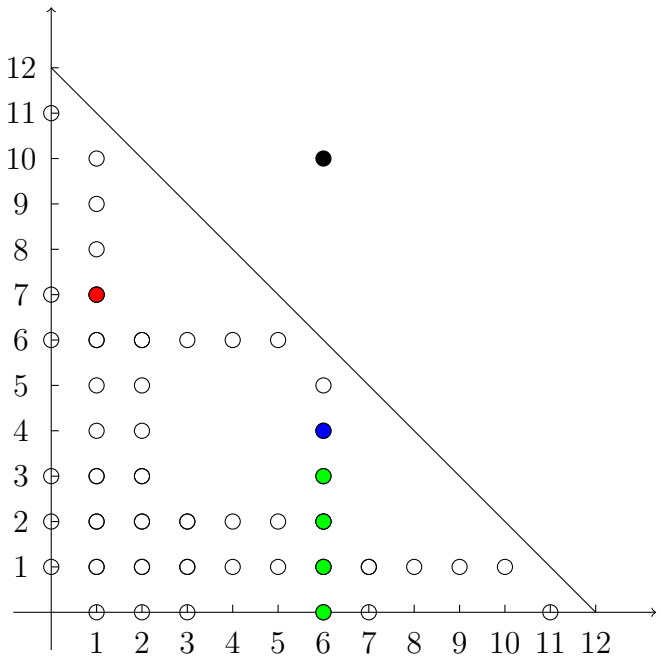

Figura 5.1: Escolha de (α_1, α_2) e (γ_1, γ_2) no exemplo 5.3

Seja $(\alpha_1, \alpha_2) = (1, 7)$ (em vermelho ●), $(\gamma_1, \gamma_2) = (6, 4)$ (em azul ●), e $G = (\alpha_1 + g_1 - 1)P_1 + (\alpha_2 + \gamma_2 - 1)P_1 = 6P_1 + 10P_2$ (em preto ●). Note que $7 < 11 = \beta_1$, e logo, pelo Corolário 2.9, $\ell(P_1 + 7P_2) = \ell(7P_2)$. Temos $2g - 1 - (\alpha_1 + \alpha_2) = 3$ e $(6, 3), (6, 2), (6, 1) \in J(P_1, P_2)$ (em verde ●). Assim, as hipóteses do Teorema 5.1 estão satisfeitas, e o código de dois pontos $C_\Omega(D, G)$ tem distância mínima pelo menos $\deg G - 2g + 3 = 7$. Temos $\deg D = 4^3 - 1 = 63$, e logo $2g - 2 < \deg G < \deg D$, e pelo Teorema 4.8, $C_\Omega(D, G)$ tem dimensão $k = n + g - 1 - \deg G = 63 + 6 - 1 - 16 = 52$. Portanto, $C_\Omega(D, G)$ é um $[63, 52, \geq 7]$-código.

Porque muito se sabe a respeito de corpos de funções Hermitianos, impor restrições ao conjunto de lacunas em um par de lugares permite obter códigos com cotas para a distância mínima ainda melhores que a do Teorema 5.1. Antes, façamos uma comparação dos parâmetros

dos códigos de dois pontos fornecidos pelo Teorema 5.1 com os de códigos de um ponto no corpo de funções Hermitiano. Para isso, precisamos de alguns resultados sobre códigos de um ponto. Com a notação do Teorema 3.2, defina

$$D' := \sum_{\substack{\alpha,\beta\in\mathbb{F}_{q^2} \\ \beta^q+\beta=\alpha^{q+1}}} P_{\alpha\beta}.$$

Observe que se $m > q^3 + q^2 - q - 2 = \deg D' + (2g-2)$, então

$$\begin{aligned} \dim C_{\mathscr{L}}(D', mP_\infty) &= \ell(mP_\infty) - \ell(mP_\infty - D') \\ &= m + 1 - g - (m - q^3 + 1 - g) = q^3, \end{aligned}$$

e logo $C_{\mathscr{L}}(D', mP_\infty) = \mathbb{F}_{q^2}^{q^3}$.

Proposição 5.4 ([12], Proposição 8.3.2)**.** *Para $0 \le m' \le q^3 + q^2 - q - 2$ temos*

$$C_\Omega(D', m'P_\infty) = C_{\mathscr{L}}(D', (q^3 + q^2 - q - 2 - m')P_\infty).$$

Proposição 5.5. *1. Se $0 \le m < q^2 - q$, então $\dim C_{\mathscr{L}}(D', mP_\infty) = \ell(mP_\infty) = \#\{t \in H(P_\infty) : t \le m\} \le g$.*

2. Se $q^2 - q - 2 < m < q^3$, então $\dim C_{\mathscr{L}}(D', mP_\infty) = m + 1 - g$.

3. Se $q^3 \le m \le q^3 + q^2 - q - 2$, defina $m' = q^3 + q^2 - q - 2 - m$. Então $\dim C_{\mathscr{L}}(D', mP_\infty) = \dim C_\Omega(D', m'P_\infty) = q^3 - \dim C_{\mathscr{L}}(D', m'P_\infty) = q^3 - \#\{t \in H(P_\infty) : t \le m'\} \ge q^3 - g$.

Demonstração. Segue diretamente do Teorema 4.3 e da Proposição 5.4. □

O seguinte resultado, devido a H. Stichtenoth([11]), K. Yang e P. V. Kumar([13]), fornece a dimensão e a distância mínima exata para códigos de um ponto do tipo $C_{\mathscr{L}}(D', mP_\infty)$ para qualquer valor de m.

Teorema 5.6. *Sejam $C := C_{\mathscr{L}}(D', mP_\infty)$, $n := \deg D' = q^3$ e $d' := d(C)$.*

1. Suponha que $0 \le m < q^2 - q = 2g$. Seja $\tilde{m} = \max\{t \in H(P_\infty) : t \le m\}$. Então $d' = n - \tilde{m}$.

2. Se $q^2 - q \le m < q^3 - q^2$, então $d' = n - m$.

3. Suponha $q^3 - q^2 \le m < q^3$ e $m = q^3 - q^2 + aq + b$ com $0 \le a, b \le q - 1$. Se $a < b$, então $d' = n - m$; se $a \ge b$, então $d' = n - m + b = q^2 - aq$.

4. Suponha que $q^3 \le m \le q^3 + q^2 - q - 2$. Seja $m_\perp = q^3 + q^2 - q - 2 - m$ e $\tilde{m}_\perp = \max\{t \in H(P_\infty) : t \le m_\perp\}$. Escreva $\tilde{m}_\perp = aq + b$ com $0 \le b \le a < q - 1$. Se $b = a$, então $d' = a + 2$; se $b < a$, então $d' = a + 1$.

5. Se $m > q^3 + q^2 - q - 2$, então $d' = 1$.

Utilizando estes valores, podemos ver quando o Teorema 5.1 pode ser usado para comparar os parâmetros de códigos de dois pontos aos de códigos de um ponto. Observamos que um código é mais eficiente à medida que a dimensão e a distância mínima são maiores *em relação ao comprimento*. Assim, para um $[n, k, d]$-código, é natural considerar os parâmetros relativos k/n, denominado **taxa de informação**, e d/n, denominado **taxa de correção de erros**. Quanto maiores essas taxas, mais eficiente será o código ([6]).

Seja $C_\Omega(D,G)$ um código de dois pontos satisfazendo as hipóteses do Teorema 5.1, isto é, $G = (\alpha_1+\gamma_2-1)P_1 + (\alpha_2+\gamma_2-1)P_2$, onde P_1 e P_2 são dois lugares de grau um distintos de $\mathcal{H}$, D é a soma de todos os outros lugares de grau um de $\mathcal{H}$, $(\alpha_1,\alpha_2) \in J(P_1,P_2)$ é tal que $\alpha_1 \geq 1$ e $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1-1)P_1 + \alpha_2 P_2)$, $(\gamma_1,\gamma_2-t-1) \in J(P_1,P_2)$ para $0 \leq t \leq \min\{\gamma_2-1, 2g-1-(\alpha_1+\alpha_2)\}$, e $k := \dim_{\mathbb{F}_{q^2}} C_\Omega(D,G) > 0$. Seja d a distância mínima de $C_\Omega(D,G)$. Pelo Teorema 5.1, $d \geq \deg G - 2g + 3$.

Se d' é a distância mínima do código de um ponto $C_\Omega(D', m'P_\infty)$ de dimensão k, então este código tem taxa de informação k/q^3, que já é menor que a taxa de informação $k/(q^3-1)$ do código $C_\Omega(D,G)$. Se $d \geq d'$, então também a taxa de correção de erros do código $C_\Omega(D,G)$ é maior que a do código $C_\Omega(D', m'P_\infty)$, e nesse caso, o código de dois pontos é mais eficiente. Vejamos sob que condições temos $d \geq d'$.

Se $\deg G \leq 2g-2$, o Teorema 5.1 não melhora a cota óbvia $d \geq 1$. Consideremos o caso $\deg G > 2g-2$. Como $(\alpha_1,\alpha_2), (\gamma_1,\gamma_2-1) \in J(P_1,P_2)$, devemos ter $\alpha_1+\alpha_2 \leq 2g-1$ e $\gamma_1+\gamma_2-1 \leq 2g-1$, e $\deg G = \alpha_1+\alpha_2+\gamma_1+\gamma_2-2 \leq 4g-3 = 2q^2-2q-3$. Como estamos assumindo $g>1$, temos $q>2$, e $2q^2 < q^3$, $2q+3>1$, e logo $\deg G < q^3-1 = \deg D$. Pelo Teorema 4.8, nessas condições a dimensão de $C_\Omega(D,G)$ é dada por

$$k = \deg D - 1 + g - \deg G = q^3 + g - 2 - \deg G.$$

Como $2g-1 \leq \deg G \leq 4g-3$, temos

$$q^3 - 3g + 1 \leq k \leq q^3 - g - 1. \tag{5.1}$$

Procuramos pelo código de um ponto $C_\Omega(D', m'P_\infty)$ cuja dimensão é k. Pela Proposição 5.4, temos $C_\Omega(D', m'P_\infty) = C_{\mathscr{L}}(D', mP_\infty)$ para $m = q^3+q^2-q-2-m'$. Pela Proposição 5.5, tendo em vista (5.1), devemos ter $q^2-q \leq m < q^3$, e logo $k = m+1-g$, e mais uma vez por (5.1),

$$q^3 - q^2 + q \leq m \leq q^3 - 2.$$

Estamos no item (3) do Teorema 5.6. Escreva $m = q^3 - q^2 + aq + b$ com $1 \leq a \leq q-1$ e $0 \leq b \leq q-1$. (Note que não podemos ter $a = b = q-1$.) Temos

$$k = m - g + 1 = q^3 - q^2 + aq + b - g + 1$$

e

$$\deg G = q^3 + g - 2 - k = 2g + q^2 - aq - b - 3.$$

A cota dada pelo Teorema 5.1 é $d \geq \deg G - 2g + 3 = q^2 - aq - b$. Temos dois casos para a distância mínima d' de $C_{\mathscr{L}}(D', mP_\infty)$:

- Se $a < b$, então $d' = q^3 - m = q^2 - aq - b$. Portanto, neste caso o Teorema 5.1 garante que o código de dois pontos $C_\Omega(D,G)$ possui distância mínima maior ou igual à do código de um ponto $C_\Omega(D', m')$ com a mesma dimensão.

- Se $b \leq a$, então $d' = q^2 - aq$. Nesse caso, os códigos do Teorema 5.1 são melhores que os códigos de um ponto com a mesma dimensão desde que $b = 0$.

Em resumo:

Proposição 5.7. *Considere um código de dois pontos $C_\Omega(D,G)$ satisfazendo as hipóteses do Teorema 5.1. Se $\deg G = 2g + q^2 - aq - b - 3$, $1 \leq a < b \leq q-1$, ou $\deg G = 2g + q^2 - aq - 3$, $1 \leq a \leq q-1$, então $C_\Omega(D,G)$ tem comprimento menor e distância mínima maior ou igual à do código de um ponto $C_\Omega(D', m'P_\infty)$ com a mesma dimensão.*

O seguinte resultado é um complemento à Proposição 5.7.

Proposição 5.8. *Dado $r = 2g+q^2-aq-b-3$ com $1 \leq a < b \leq q-1$, ou $r = 2g+q^2-aq-3$ com $1 \leq a \leq q-1$,existe um código de dois pontos $C_\Omega(D,G)$ no corpo de funções Hermitiano satisfazendo as hipóteses do Teorema 5.1 tal que o grau do divisor G é r.*

Demonstração. Seja $r = 2g + q^2 - aq - b - 3$ com $1 \leq a < b \leq q-1$, ou $r = 2g - q^2 - aq - 3$ com $1 \leq a \leq q-1$. Tome $(\alpha_1, \alpha_2) = (1, 2g-2)$ e $(\gamma_1, \gamma_2) = (1, q^2 - aq - b - 1)$. Pelo Teorema 3.7, temos $\beta_1 = q^2 - q - 1 = 2g - 1$. Logo, $(\alpha_1, \alpha_2) \in J(P_1, P_2)$, e pelo Lema 2.5, $\ell(P_1 + (2g-2)P_2) = \ell((2g-2)P_2)$. Temos $2g - 1 - (\alpha_1 + \alpha_2) = 0$, e $(\gamma_1, \gamma_2 - 1) \in J(P_1, P_2)$. Assim, $\deg G = \alpha_1 + \gamma_1 - 1 + \alpha_2 + \gamma_2 - 1 = r$. □

Exemplo 5.9. *Considere o código construído no Exemplo 5.3. Observe que* $\deg G = 16 = 2 \cdot 6 + 16 - 2 \cdot 4 - 1 - 3$*, donde os parâmetros a e b da discussão anterior à Proposição 5.7 são $a = 2$ e $b = 1$. Como $a \geq b$, e $b \neq 0$, o Teorema 5.1 não permite comparar este código ao código de um ponto de mesma dimensão.*

Exemplo 5.10. *Seja $\mathcal{H}|\mathbb{F}_{25}$ corpo de funções com $\mathcal{H} = \mathbb{F}_{25}(x,y)$ com $y^5 + y = x^6$. O gênero de $\mathcal{H}|\mathbb{F}_{25}$ é $g = 10$. A figura 5.10 mostra os possíveis valores para os coeficientes do divisor G satisfazendo as hipóteses do Teorema 5.1 ou as condições simétricas.*

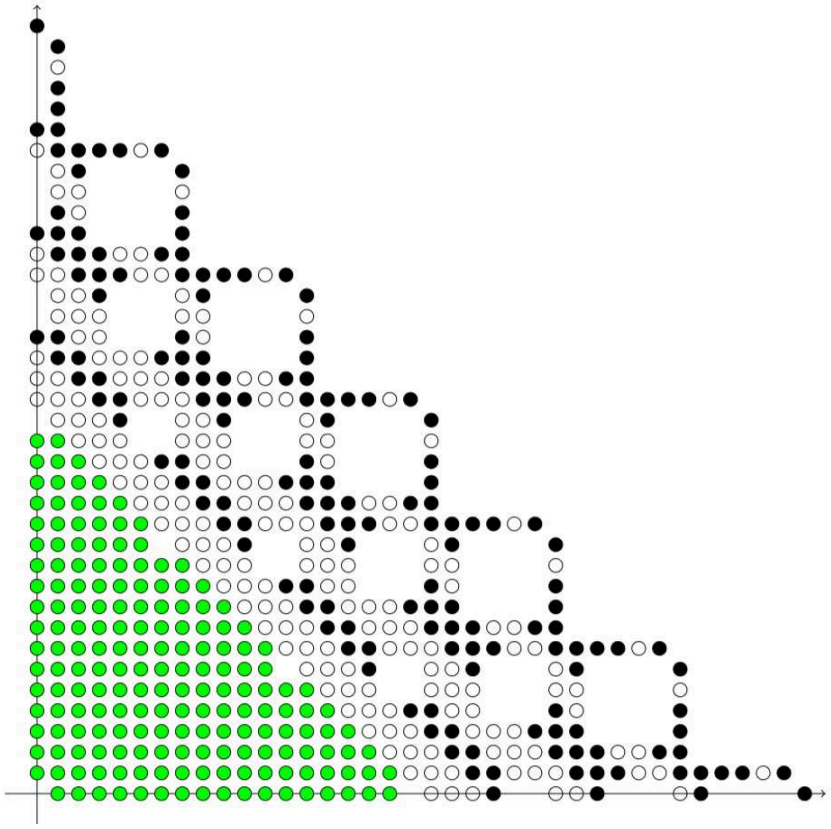

Figura 5.2: Possíveis coeficientes do divisor G no Teorema 5.1 para $q = 5$

Explicando as cores na figura 5.10: em verde ●, os divisores G com $\deg G \leq 2g - 2 = 18$*; em preto ●, os divisores G para os quais o Teorema 5.1 permite concluir que o código de dois pontos $C_\Omega(D,G)$ tem distância mínima maior ou igual à do código de um ponto de mesma dimensão; para os demais divisores (em branco ○), o Teorema 5.1 não permite uma conclusão desse tipo.*

Podemos seguir impondo restrições ao conjunto de lacunas $J(P_1, P_2)$ para produzir códigos com um cota inferior para a distância mínima melhor que a dada no Teorema 5.1.

Lema 5.11. *Se P_1 e P_2 são dois lugares racionais de $\mathcal{H}$ distintos, então existe $f' \in \mathcal{H}$ com $(f') = (q+1)(P_1 - P_2)$.*

Demonstração. Se $P_1 = P_{ab}$ e $P_2 = P_\infty$, vimos que $(y - a^q x + b^q) = (q+1)(P_{ab} - P_\infty)$. Se $P_1 = P_{ab}$ e $P_2 = P_{cd}$ temos $\left(\dfrac{y - a^q x + b^q}{y - c^q x + d^q}\right) = (q+1)(P_{ab} - P_{cd})$. Além disso, se $f' \in \mathcal{H}$ é tal que $(f') = (q+1)(P_2 - P_1)$, então $(1/f') = (q+1)(P_1 - P_2)$. □

Teorema 5.12. *Considere $C_\Omega(D, G)$ com $G = (\alpha_1+\gamma_1-1)P_1+(\alpha_2+\gamma_2-1)P_2$ e $D = Q_1+\cdots+Q_n$, onde $P_1, P_2, Q_1, \ldots, Q_n$ são lugares racionais distintos. Suponha que $(\alpha_1, \alpha_2) \in J(P_1, P_2)$, $\alpha_1 \geq 1$, e $\ell(\alpha_1 P_1+\alpha_2 P_2) = \ell((\alpha_1-1)P_1+\alpha_2 P_2)$. Suponha ainda que $(\gamma_1, \gamma_2-\delta-1), (\gamma_1+1, \gamma_2-\delta-1), (\gamma_1+q+1, \gamma_2-\delta-1), (\gamma_1, \gamma_2) \in J(P_1, P_2)$ para todo δ, $0 \leq \delta \leq \min\{\gamma_2-1, 2g-1-(\alpha_1+\alpha_2)\}$. Se a dimensão desse código é positiva, então a distância mínima é pelo menos* $\deg G - 2g + 4$.

Demonstração. Pelo Teorema 5.1, a distância mínima de $C_\Omega(D, G)$ é pelo menos $\deg G - 2g + 3$. Ponha $d =: \deg G - 2g + 3$. Se existe uma palavra do código de peso d, então existe um diferencial $\omega \in \Omega(G - D)$ com exatamente d polos simples $Q_1, \ldots, Q_d$. Temos $(\omega) \geq G - (Q_1 + \cdots + Q_d)$. Como $\deg(\omega) = 2g - 2 = \deg G - d + 1$,

$$(\omega) = G - (Q_1 + \cdots + Q_d) + A,$$

onde A é um lugar racional, $A \neq Q_i$, $1 \leq i \leq d$. Como na demonstração do Teorema 5.1, usando a hipótese $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2)$ e o Teorema de Riemann-Roch, existe $h \in \mathcal{H}$ cujo divisor pode ser escrito como

$$(h) = (\alpha_1 - 1)P_1 + (\alpha_2 + t)P_2 - W + E,$$

onde $0 \leq t \leq 2g - 1 - (\alpha_1 + \alpha_2)$, E é um divisor efetivo cujo suporte não contém P_1 ou P_2, e W é um divisor canônico arbitrário. Então

$$G - (Q_1 + \cdots + Q_d) + A = (\omega) \sim W \sim (\alpha_1 - 1)P_1 + (\alpha_2 + t)P_2 + E$$

implica que existe $f \in \mathcal{H}$ com divisor

$$(f) = -\gamma_1 P_1 - (\gamma_2 - t - 1)P_2 - A + (Q_1 + \cdots + Q_d) + E.$$

Primeiro, suponha que $t \leq \gamma_2 - 1$. Se A está no suporte de E, então $(f)_\infty = \gamma_1 P_1 + (\gamma_2 - t - 1)P_2$, contradizendo a hipótese $(\gamma_1, \gamma_2 - t - 1) \in J(P_1, P_2)$. Separamos os casos:

- Se $A = P_1$ então $(f)_\infty = (\gamma_1+1)P_1 + (\gamma_2 - t - 1)P_2$, contradizendo a hipótese $(\gamma_1 + 1, \gamma_2 - t - 1) \in J(P_1, P_2)$.
- Se $A = P_2$ então $(f)_\infty = \gamma_1 P_1 + (\gamma_2 - t)P_2$. Se $t = 0$, contradição com a hipótese $(\gamma_1, \gamma_2) \in J(P_1, P_2)$; se $t > 0$, tomando $\delta = t - 1$ temos $(\gamma_1, \gamma_2 - \delta - 1) \in J(P_1, P_2)$: contradição.
- Suponha $A \notin \{P_1, P_2, Q_1, ..., Q_d\} \cup \operatorname{Supp} E$. Seja $f' \in \mathcal{H}$ tal que $(f') = (q+1)(A - P_1)$ (Lema 5.11). Então $(ff')_\infty = (\gamma_1 + q + 1)P_1 + (\gamma_2 - t - 1)P_2$, contradizendo a hipótese $(\gamma_1 + q + 1, \gamma_2 - t - 1) \in J(P_1, P_2)$.

Agora suponha $\gamma_2 - 1 < t \leq 2g - 1 - (\alpha_1 + \alpha_2)$. Se A está no suporte de E ou $A = P_2$, então $(f)_\infty = \gamma_1 P_1$. Se $A = P_1$, então $(f)_\infty = (\gamma_1 + 1)P_1$. Cada um dos casos é uma contradição já que γ_1 e $\gamma_1 + 1$ são lacunas em P_1. Logo, $A \notin \{P_1, P_2, Q_1, ..., Q_d\} \cup \operatorname{Supp} E$. Então $(ff')_\infty = (\gamma_1 + q + 1)P_1$, contradizendo a hipótese de que $\gamma_1 + q + 1$ é uma lacuna em P_1. □

Exemplo 5.13. *Seja $\mathcal{H}|\mathbb{F}_{16}$, P_1 e P_2 como no Exemplo 5.3. Tome $(\alpha_1, \alpha_2) = (6, 3)$, $(\gamma_1, \gamma_2) = (1, 6)$, e $G = (\alpha_1 + g_1 - 1)P_1 + (\alpha_2 + \gamma_2 - 1)P_1 = 6P_1 + 8P_2$. Note que $3 < 6 = \beta_6$, e logo, pelo Corolário 2.9, $\ell(6P_1 + 8P_2) = \ell(5P_1 + 8P_2)$. Temos $2g - 1 - (\alpha_1 + \alpha_2) = 2$ e $(1, 5), (1, 4), (1, 3), (2, 5)(2, 4), (2, 3), (6, 5), (6, 4), (6, 3), (1, 6) \in J(P_1, P_2)$ (ver Figura 5.13). Assim, as hipóteses do Teorema 5.12 estão satisfeitas, e o código de dois pontos $C_\Omega(D, G)$ tem distância mínima pelo menos $\deg G - 2g + 4 = 6$. Temos $\deg D = 4^3 - 1 = 63$, e logo $2g - 2 < \deg G < \deg D$, e pelo Teorema 4.8, $C_\Omega(D, G)$ tem dimensão $k = n + g - 1 - \deg G = 63 + 6 - 1 - 14 = 54$. Portanto, $C_\Omega(D, G)$ é um $[63, 54, \geq 6]$-código.*

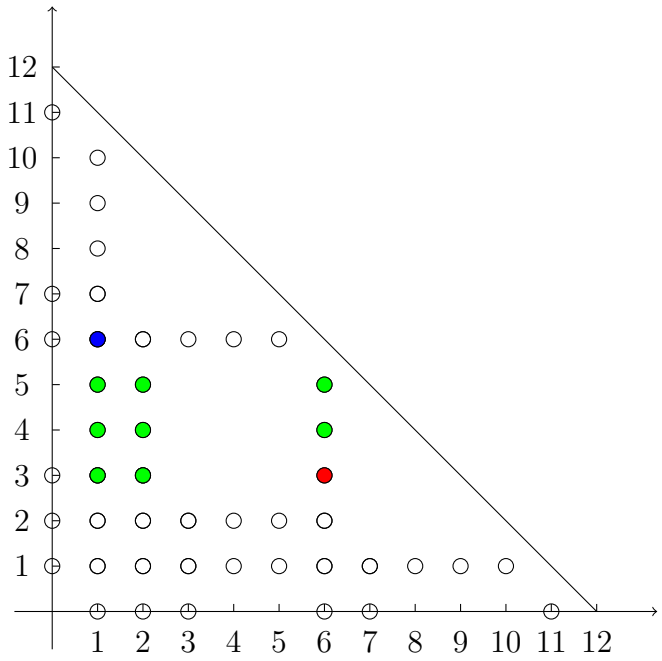

Figura 5.3: Escolha de (α_1, α_2) e (γ_1, γ_2) no Exemplo 5.13.

Podemos repetir a análise feita para o Teorema 5.1, agora para um código de dois pontos $C_\Omega(D, G)$ sob as hipóteses do Teorema 5.12. Dessa vez consideramos $\deg G > 2g - 3$. (O caso $\deg G \leq 2g - 3$ não oferece melhoria à cota $d \geq 1$.) Como $(\alpha_1, \alpha_2), (\gamma_1, \gamma_2 - 1), (\gamma_1 + 1, \gamma_2 - 1), (\gamma_1 + q + 1, \gamma_2 - 1), (\gamma_1, \gamma_2) \in J(P_1, P_2)$, devemos ter

$$\max\{\gamma_1 + \gamma_2 - 1, \gamma_1 + \gamma_2, \gamma_1 + \gamma_2 + q\} = \gamma_1 + \gamma_2 + q \leq 2g - 1,$$

e logo $\deg G = \alpha_1 + \alpha_2 + \gamma_1 + \gamma_2 - 2 \leq 4g - 4 - q$, isto é,

$$q^2 - q - 2 \leq \deg G \leq 2q^2 - 3q - 4. \tag{5.2}$$

Como antes, procuramos pelo código de um ponto $C_{\mathscr{L}}(D', mP_\infty)$ de dimensão k e distância mínima d'. Primeiro suponha $\deg G = 2g - 2 = q^2 - q - 2$. A cota dada pelo Teorema 5.12 é $d \geq 2$. Pelo Teorema 4.8, temos

$$\begin{aligned} k &= i(G - D) - i(G) \\ &= \ell(G - D) - \deg G + \deg D + g - 1 - (\ell(G) - \deg G + g - 1) \\ &= \deg D - \ell(G). \end{aligned}$$

Se G é canônico, então $\ell(G) = g$ e $k = q^3 - g - 1$. Separamos os casos:

- Se $0 \leq m < q^2 - q$, então $\dim C_{\mathscr{L}}(D', mP_\infty) \leq g < q^3 - g - 1$.

- Se $q^2-q \leq m < q^3$, então $\dim C_{\mathscr{L}}(D', mP_\infty) = m-g+1 = q^3-g-1$ implica $m = q^3-2 = q^3-q^2+(q-1)q+q-2$. Pelo Teorema 5.6, temos $d' = q^3-(q^3-2)+q-2 = q > 2$.

- Se $m \geq q^3$, então $\dim C_{\mathscr{L}}(D', mP_\infty) \geq q^3-g > q^3-g-1$.

Se G não é canônico, pelo item (2) do Corolário 1.36, temos $\ell(G) < g$, e pelo Teorema de Riemann, $\ell(G) \leq \deg G + 1 - g = g-1$. Logo, $\ell(G) = g-1$ e $k = q^3-g$.

- Se $0 \leq m < q^2-q$, então $\dim C_{\mathscr{L}}(D', mP_\infty) \leq g < q^3-g$.

- Se $q^2-q \leq m < q^3$, então $\dim C_{\mathscr{L}}(D', mP_\infty) = m-g+1 = q^3-g$ implica $m = q^3-1 = q^3-q^2+(q-1)q+q-1$. Pelo Teorema 5.6, temos $d' = q^3-(q^3-1)+q-1 = q > 2$.

- Se $q^3 \leq m \leq q^3+q^2-q-2$, definindo $\tilde{m}_\perp$ como no item (4) do Teorema 5.6, temos $k = q^3-g$ desde que $\tilde{m}_\perp = (q-2)q+(q-2) = q^2-q-2$. Nesse caso temos $d' = q > 2$.

Portanto, se $\deg G = 2g-2$ o Teorema 5.12 não produz códigos de dois pontos com distância mínima maior ou igual à dos códigos de um ponto com mesma dimensão.

Suponha agora $2g-1 \leq \deg G \leq 4g-4-q$. Do Teorema 4.8, $k = q^3+g-2-\deg G$, e logo

$$q^3-3g+q+2 \leq k \leq q^3-g-1.$$

Se $0 \leq m < q^2-q$ então $\dim C_{\mathscr{L}}(D', mP_\infty) \leq g < q^3-3g+2+q$. Se $m \geq q^3$, então $\dim C_{\mathscr{L}}(D', mP_\infty) \geq q^3-g > q^3-g-1$. Se $q^2-q \leq m < q^3$, então $\dim C_{\mathscr{L}}(D', mP_\infty) = m-g+1$, o que nos dá

$$q^3-q^2+2q+1 \leq m \leq q^3-2.$$

Assim, quando escrevemos $m = q^3-q^2+aq+b$, devemos ter $2 \leq a \leq q-1$ e $0 \leq b \leq q-1$, excluindo os casos $(a,b) = (2,0)$ e $a = b = q-1$. Pelo Teorema 5.12, $d \geq q^2-aq-b+1$.

- Se $a < b$, temos $d' = q^2-aq-b$, e o código de dois pontos $C_\Omega(D,G)$ tem distância mínima maior e comprimento menor que o código de um ponto com a mesma dimensão.

- Se $b \leq a$ então $d' = q^2-aq$. Temos $d \geq d'$ desde que $b = 0, 1$.

Proposição 5.14. *Considere um código de dois pontos $C_\Omega(D,G)$ satisfazendo as hipóteses do Teorema 5.12. Se $\deg G = 2g+q^2-aq-b-3$ com $2 \leq a < b \leq q-1$, ou $2 \leq a \leq q-1$ e $b = 0, 1$, então $C_\Omega(D,G)$ tem comprimento menor e distância mínima maior ou igual à do código de um ponto com a mesma dimensão. Além disso, dado qualquer número da forma $r = 2q+q^2-aq-b-3$, com $2 \leq a < b \leq q-1$, ou $2 \leq a \leq q-1$, $b = 0, 1$ e $(a,b) \neq (2,0)$, existe um código de dois pontos $C_\Omega(D,G)$ satisfazendo as hipóteses do Teorema 5.12 tal que o grau do divisor G é r.*

Demonstração. Seja $r = 2g+q^2-aq-b-3$, com $2 \leq a < b \leq q-1$, ou $2 \leq a \leq q-1$, $b = 0, 1$ e $(a,b) \neq (2,0)$. Tome $(\alpha_1, \alpha_2) = (1, 2g-2)$ e $(\gamma_1, \gamma_2) = (1, q^2-aq-b-1)$. Temos $\beta_1 = q^2-q-1 = 2g-1$, $\beta_2 = q^2-2q-1$, $\beta_{q+2} = q^2-2q-2$. Logo, $(\gamma_1, \gamma_2), (\alpha_1, \alpha_2) \in J(P_1, P_2)$ e pelo Lema 2.5, $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1-1)P_1 + \alpha_2 P_2)$. Ainda, $2g-1-(\alpha_1+\alpha_2) = 0$, e $(\gamma_1, \gamma_2-1), (\gamma_1+1, \gamma_2-1), (\gamma_1+q+1, \gamma_2-1) \in J(P_1, P_2)$. É claro que $\deg G = \alpha_1+\gamma_1-1+\alpha_2+\gamma_2-1 = r$. □

Exemplo 5.15. *Considere o código construído no Exemplo 5.13. Temos* $\deg G = 14 = 2 \cdot 6 + 16 - 2 \cdot 4 - 3 - 3$, *donde segue que $a = 2$ e $b = 3$. Como $a < b$, esse código de dois pontos é mais eficiente que o código de um ponto de dimensão* 54, *que tem distância mínima* 5.

Exemplo 5.16. *Seja $\mathcal{H}$ como no Exemplo 5.10. A figura 5.16 mostra os possíveis valores para os coeficientes do divisor G satisfazendo as hipóteses do Teorema 5.12 ou as condições simétricas. Explicando as cores na figura 5.16: em verde ●, os divisores G com $\deg G \leq 2g-3 = 17$; em preto ●, os divisores G para os quais o Teorema 5.12 permite concluir que o código de dois pontos $C_\Omega(D,G)$ tem distância mínima maior ou igual à do código de um ponto de mesma dimensão; para os demais divisores (em branco ○), o Teorema 5.12 não permite uma conclusão desse tipo.*

Figura 5.4: Possíveis coeficientes do divisor G no Teorema 5.12 para $q = 5$

Usando o fato de que não existem lugares de grau dois no corpo de funções Hermitiano [3] e adicionando restrições no conjunto de lacunas $J(P_1, P_2)$ podemos melhorar mais uma vez a cota inferior para a distância mínima do código de dois pontos correspondente.

Teorema 5.17. *Considere $C_\Omega(D,G)$ com $G = (\alpha_1+\gamma_1-1)P_1 + (\alpha_2+\gamma_2-1)P_2$ e $D = Q_1+\cdots+Q_n$, em $P_1, P_2, Q_1, \ldots, Q_n$ são lugares racionais distintos. Suponha que $(\alpha_1,\alpha_2) \in J(P_1,P_2)$, $\alpha_1 \geq 1$, e $\ell(\alpha_1P_1+\alpha_2P_2) = \ell((\alpha_1-1)P_1+\alpha_2P_2)$. Suponha ainda que $(\gamma_1,\gamma_2-t-1), (\gamma_1,\gamma_2), (\gamma_1,\gamma_2+1), (\gamma_1+1,\gamma_2-t-1), (\gamma_1+1,\gamma_2), (\gamma_1+2,\gamma_2-t-1), (\gamma_1+q+1,\gamma_2-t-1), (\gamma_1+q+1,\gamma_2), (\gamma_1+q+2,\gamma_2-t-1), (\gamma_1+2q+2,\gamma_2-t-1) \in J(P_1,P_2)$ para todo t, $0 \leq t \leq \min\{\gamma_2-1, 2g-1-(\alpha_1+\alpha_2)\}$. Se a dimensão de $C_\Omega(D,G)$ é positiva, então a distância mínima é pelo menos $\deg G - 2g + 5$.*

Demonstração. Pelo Teorema 5.12, a distância mínima de $C_\Omega(D,G)$ é $\deg G - 2g + 4$. Seja $d = \deg G - 2g + 4$. Se existe uma palavra do código de peso d, então existe um diferencial $\omega \in \Omega(G-D)$ com divisor $(\omega) = G - (Q_1+\cdots+Q_d) + A$ onde A é um divisor efetivo de grau dois cujo suporte não contém Q_i para $1 \leq i \leq d$. Note que não exitem lugares de grau dois no corpo de funções Hermitiano. Assim, $A = 2P_1, 2P_2, P_1+P_2, P_1+Q, P_2+Q, 2Q, P+Q$, onde P e Q são lugares distintos com $P, Q \notin \{P_1, P_2, Q_1, \ldots, Q_d\}$. Como antes, temos

$$0 \sim -\gamma_1 P_1 - (\gamma_2 - t - 1)P_2 - A + (Q_1+\cdots+Q_d) + E,$$

onde E é um divisor efetivo cujo suporte não contém P_1 ou P_2 e $0 \leq t \leq 2g-1-(\alpha_1+\alpha_2)$. Usando as hipóteses sobre o conjunto de lacunas do par, cada uma das possibilidades para A podem ser descartadas. Portanto, a distância mínima é pelo menos $\deg G - 2g + 5$. □

Exemplo 5.18. *Seja $\mathcal{H}|\mathbb{F}_{16}$, P_1 e P_2 como no Exemplo 5.3. Tome $(\alpha_1, \alpha_2) = (6, 5)$, $(\gamma_1, \gamma_2) = (0, 2)$, e $G = (\alpha_1 + g_1 - 1)P_1 + (\alpha_2 + \gamma_2 - 1)P_1 = 5P_1 + 6P_2$. Note que $5 < 6 = \beta_6$, e logo, pelo Corolário 2.9, $\ell(6P_1 + 5P_2) = \ell(5P_1 + 5P_2)$. Temos $2g - 1 - (\alpha_1 + \alpha_2) = 0$ e $(0,1), (0,2), (0,3), (1,1), (1,2), (2,1), (5,1), (5,2), (6,1), (10,1) \in J(P_1, P_2)$ (veja Figura 5.18). Assim, as hipóteses do Teorema 5.17 estão satisfeitas, e o código de dois pontos $C_\Omega(D, G)$ tem distância mínima pelo menos $\deg G - 2g + 5 = 4$ e dimensão $k = n + g - 1 - \deg G = 63 + 6 - 1 - 11 = 57$. Portanto, $C_\Omega(D, G)$ é um $[63, 57, \geq 4]$-código.*

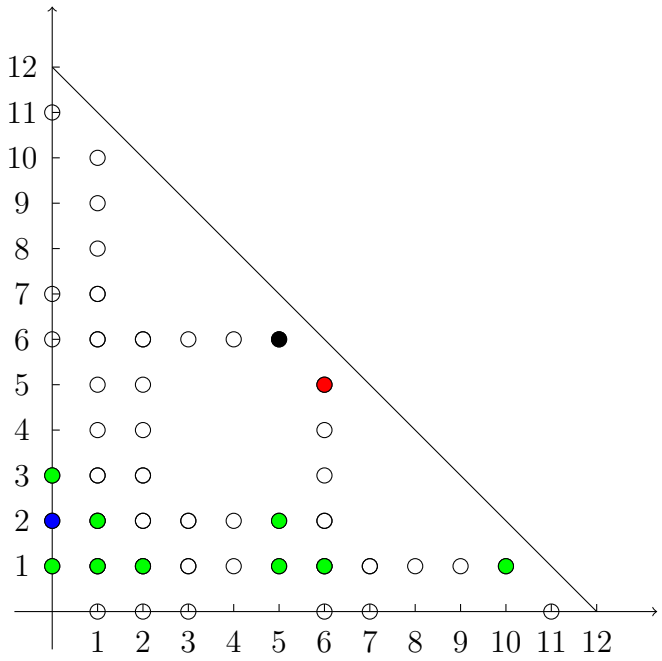

Figura 5.5: Escolha de (α_1, α_2) (em vermelho) e de (γ_1, γ_2) (em azul) no Exemplo 5.18

Vejamos quando os códigos de dois pontos $C_\Omega(D, G)$ sob as hipóteses do Teorema 5.17 têm melhores parâmetros que os códigos de um ponto com mesma dimensão. Consideramos apenas o caso $\deg G - 2g + 5 > 1$, isto é, $\deg G \geq 2g - 3$. Como $(\gamma_1 + 2q + 2, \gamma_2 - 1) \in J(P_1, P_2)$, devemos ter $\gamma_1 + 2q + 2 + \gamma_2 - 1 \leq 2g - 1$, isto é, $\gamma_1 + \gamma_2 - 1 \leq 2g - 2q - 3$. Assim, $\alpha_1 + \alpha_2 - 1 + \gamma_1 + \gamma_2 - 1 \leq 2g - 2 + 2g - 2q - 3 = 4g - 2q - 5$. Logo, $2g - 3 \leq \deg G \leq 4g - 2q - 5$, ou ainda, $q^2 - q - 3 \leq \deg G \leq 2q^2 - 4q - 5$. Note que devemos ter $2g - 3 \leq 4g - 2q - 5$, isto é, $2g - 2q - 2 \geq 0$, e logo $q \geq 4$.

Seja $C_\Omega(D', m'P_\infty) = C_{\mathscr{L}}(D', mP_\infty)$ o código de um ponto com distância mínima d' e dimensão $k = \dim C_\Omega(D, G)$. Suponha inicialmente $\deg G = 2g - 3$. Nesse caso o Teorema 5.17 nos diz que $C_\Omega(D, G)$ tem distância mínima $d \geq 2$. Pelos Teoremas 1.22 e 1.37, temos $g - 2 \leq \ell(G) \leq g - 1$. Se $\ell(G) = g - 2$, então $k = \deg D - \ell(G) = q^3 - g + 1$. Se $0 \leq m < q^3$, então $\dim C_{\mathscr{L}}(D', mP_\infty) < q^3 - g + 1$. Suponha que $q^3 \leq m \leq q^3 + q^2 - q - 2$. Se $\dim C_{\mathscr{L}}(D', mP_\infty) = q^3 - g + 1$, então $\#\{t \in H(P_\infty) : t \leq m'\} = g - 1$, e logo $m' = 2g - 2$ ou $m' = 2g - 1$. Em ambos os casos, $\max\{t \in H(P_\infty) : t \leq m'\} = 2g - 2 = q^2 - q - 2 = (q - 2)q + q - 2$, e $d' = q > 2$. Se $\ell(G) = g - 1$, então $k = q^3 - g$, e já vimos que os códigos de um ponto de dimensão $q^3 - g$ têm distância mínima $q > 2$.

Suponha agora $\deg G = 2g - 2$. A cota dada no Teorema é $d \geq 3$. Se $\ell(G) = g$, temos $k = q^3 - g - 1$. Se $\ell(G) = g - 1$, então $k = q^3 - g$. Já vimos que os códigos de um ponto de dimensão $q^3 - g - 1$ e $q^3 - g$ têm distância mínima $d' = q \geq 4$. Portanto, se $\deg G = 2g - 3$ ou $\deg G = 2g - 2$, o Teorema 5.17 não apresenta melhoria em relação aos códigos de um ponto com mesma dimensão.

Finalmente, suponha $2g-1 \leq \deg G \leq 4g-2q-5$. Então

$$q^3 - 3g + 2q + 3 \leq k \leq q^3 - g - 1.$$

Se $0 \leq m < q^2 - q$, então $\dim C_{\mathscr{L}}(D', mP_\infty) \leq g < q^3 - 3g + 2q + 3$. Se $m \geq q^3$, então $\dim C_{\mathscr{L}}(D', mP_\infty) \geq q^3 - q > q^3 - g - 1$. Para $q^2 - q \leq m < q^3$, temos $\dim C_{\mathscr{L}}(D', mP_\infty) = m - g + 1$, e logo

$$q^3 - q^2 + 3q + 2 \leq m \leq q^3 - 2.$$

Assim, $m = q^3 - q^2 + aq + b$ com $3 \leq a \leq q-1$ e $0 \leq b \leq q-1$, mas $(a,b) \notin \{(3,0),(3,1),(q-1,q-1)\}$. Pelo Teorema 5.17, $C_\Omega(D,G)$ tem distância mínima $d \geq q^2 - aq - b + 2$.

- Se $a < b$, então $d' = q^2 - aq - b$ e $d > d'$.
- Se $b \leq a$, então $d \geq d'$ desde que $b = 0, 1, 2$.

Proposição 5.19. *Considere um código de dois pontos $C_\Omega(D,G)$ satisfazendo as hipóteses do Teorema 5.17. Se $\deg G = 2g + q^2 - aq - b - 3$ com $3 \leq a < b \leq q-1$, ou $3 \leq a \leq q-1$ e $b = 0, 1, 2$, então $C_\Omega(D,G)$ tem comprimento menor e distância mínima maior ou igual à do código de um ponto com a mesma dimensão. Além disso, dado $r = 2g + q^2 - aq - b - 3$ com $3 \leq a < b \leq q-1$, ou $3 \leq a \leq q-1$, $b = 0, 1, 2$ e $(a,b) \neq (3,0),(3,1)$, existe um código de dois pontos $C_\Omega(D,G)$ satisfazendo as hipóteses do Teorema 5.17 tal que o grau do divisor G é r.*

Exemplo 5.20. *Considere o código construído no Exemplo 5.18. Temos $\deg G = 11 = 2 \cdot 6 + 16 - 3 \cdot 4 - 2 - 3$, donde $a = 3$ e $b = 2$. Pelo que vimos acima, esse código de dois pontos é mais eficiente que o código de um ponto de dimensão 57, que tem distância mínima 2.*

Exemplo 5.21. *Seja $\mathcal{H}$ como no Exemplo 5.10. A figura 5.21 mostra os possíveis valores para os coeficientes do divisor G satisfazendo as hipóteses do Teorema 5.17 ou as condições simétricas. Explicando as cores na figura 5.21: em verde ●, os divisores G com $\deg G \leq 2g-4 = 16$; em preto ●, os divisores G para os quais o Teorema 5.17 permite concluir que o código de dois pontos $C_\Omega(D,G)$ tem distância mínima maior ou igual à do código de um ponto de mesma dimensão; para os demais divisores (em branco ○), o Teorema 5.17 não permite uma conclusão desse tipo.*

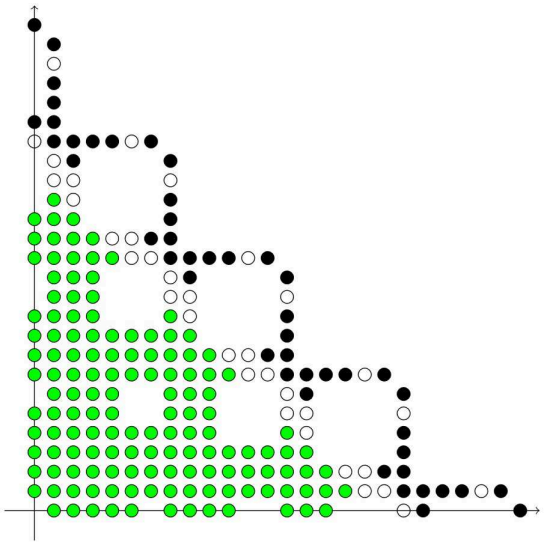

Figura 5.6: Possíveis coeficientes do divisor G no Teorema 5.17 para $q = 5$

Exemplo 5.22. *Seja $\mathcal{H}$ como no Exemplo 5.10. Na figura 5.22 vemos, em vermelho ●, os divisores G que satisfazem as hipóteses do Teorema 5.1 mas não do Teorema 5.12. Veja que para estes divisores, o código $C_\Omega(D, G)$ é candidato a ter distância mínima exatamente* $\deg G - 2g + 3$. *Em azul ●, os divisores G que satisfazem as hipóteses do Teorema 5.12 mas não do Teorema 5.17, para os quais o código $C_\Omega(D, G)$ é candidato a ter distância mínima exatamente* $\deg G - 2g + 4$.

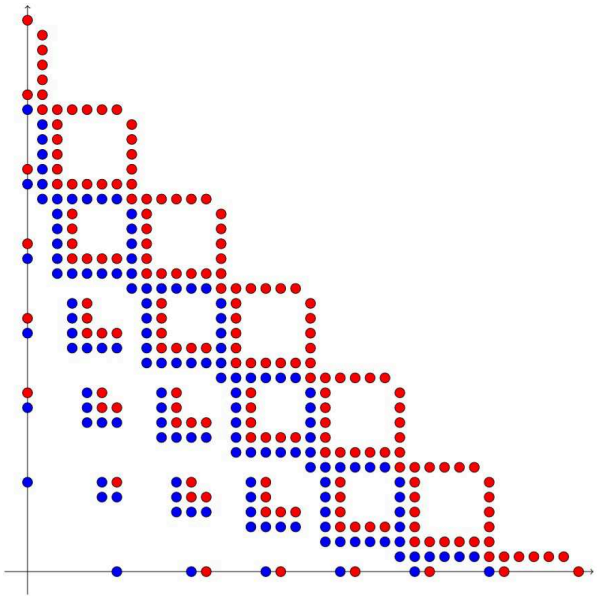

Figura 5.7: Coeficientes dos divisores G que satisfazem as hipóteses do Teorema 5.1 mas não do Teorema 5.12, e que satisfazem as hipóteses do Teorema 5.12 mas não do Teorema 5.17.

Exemplo 5.23. *Mais uma vez, seja $\mathcal{H}$ como no exemplo 5.10. A Figura 5.23 mostra os divisores G para os quais o código $C_\Omega(D, G)$ tem distância mínima maior ou igual ao código $C_\Omega(D', m'P_\infty)$ de mesma dimensão, segundo as análises feitas para os Teoremas 5.1, 5.12 e 5.17.*

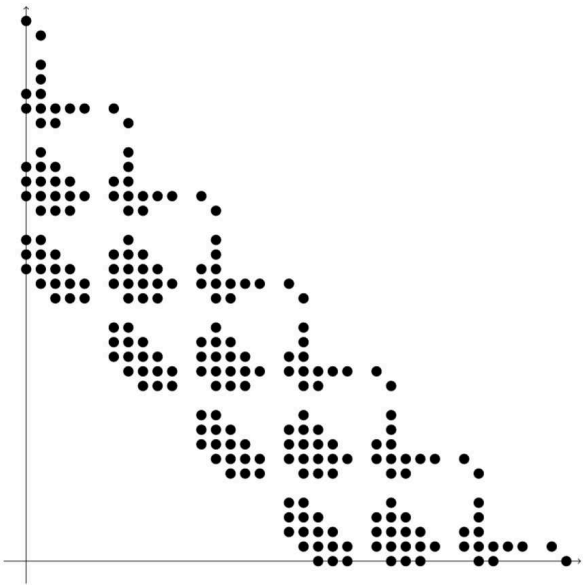

Figura 5.8: Coeficientes dos divisores G para os quais o código $C_\Omega(D, G)$ tem distância mínima maior ou igual ao código $C_\Omega(D', m'P_\infty)$ de mesma dimensão.

Referências Bibliográficas

[1] ARBARELLO, E. e CORNALBA, M. e GRIFFITHS, P. A. e HARRIS, J., *Geometry of Algebraic Curves. Vol I*, Volume 267 de Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematics], Springer-Verlag New York Inc., 1985.

https://doi.org/10.1007/978-1-4757-5323-3

[2] CARVALHO, C. e TORRES, F. *On Goppa codes and Weierstrass gaps at several points*, Designs, Codes and Cryptography 35.2, p. 211-225, 2005.

https://doi.org/10.1007/s10623-005-6403-4

[3] GARCIA, A. e STICHTENOTH, H. e XING, C. P., *On Subfields of the Hermitian Function Field*, Compositio Mathematica 120.2, p. 137-170, 2000.

https://doi.org/10.1023/A:1001736016924

[4] GOLDSCHMIDT, D., *Algebraic Functions and Projective Curves*, Springer Science & Business Media, 2006.

[5] GOPPA, V. D., *Algebraic-Geometric Codes*, Math. USRR-Izv. 21, p. 75-93, 1983.

https://doi.org/10.1070/IM1983v021n01ABEH001641

[6] HEFEZ, A. e VILLELA, M. L. T., *Códigos Corretores de Erros*, Série de Computação e Matemática, IMPA, 2008.

[7] KIM, S. J., *On the Index of the Weierstrass Semigroup of a Pair of Points on a Curve*, Archiv der Mathematik, v. 62, n. 1, p. 73-82, 1994.

https://doi.org/10.1007/BF01200442

[8] MATTHEWS, G. L., *Weierstrass Pairs and Minimum Distance of Goppa Codes*, Designs, Codes and Criptography 22, p. 107 - 121, 2001.

https://doi.org/10.1023/A:1008311518095

[9] *Number Empire - Math Tools*, disponível em https://www.numberempire.com.

[10] ROMAN, S., *Introduction to Coding Theory and Information Theory*, Undergraduate Texts in Mathematics, Springer-Verlag,1997.

[11] STICHTENOTH, H., *A note on Hermitian Codes*, IEEE Trans. Inform. Theory, vol. IT-34, p. 1345-1348, 1988.

https://doi.org/10.1109/18.21267

[12] STICHTENOTH, H., *Algebraic Function Fields and Codes*, Springer Science & Business Media, 2009.

[13] YANG, K. e KUMAR, P. V., *On the True Minimum Distance of Hermitian Codes*, Coding Theory and Algebraic Geometry, Procceddings, Luminy, 1991, Lecture Notes in Mathematics 1518, Springer-Verlag, p. 99-107, 1992.

https://doi.org/10.1007/BFb0087995