Generalização dos Códigos de Goppa

Beatriz Casulari da Motta Ribeiro

UFRJ

Rio de Janeiro

2007

Generalização dos Códigos de Goppa

Beatriz Casulari da Motta Ribeiro

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

Orientadora: Luciane Quoos Conte

Rio de Janeiro

2007

Generalização dos Códigos de Goppa

por

Beatriz Casulari da Motta Ribeiro

Dissertação submetida ao Corpo Docente do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários para a obtenção do grau de Mestre em Matemática.

Área de concentração: Matemática

Aprovada por:

Luciane Quoos Conte - UFRJ-IM

(Presidente)

Arnaldo Garcia - IMPA

Guilherme Leal - UFRJ-IM

Juscelino Bezerra - UERJ-IME

(Suplente)

Rio de Janeiro, 22 de Maro de 2007

Agradecimentos

À professora Luciane Conte, pela orientação e por ser responsável, junto com o professor Adilson Gonçalves, por despertar meu interesse pela Álgebra.

À CAPES, pelo auxílio financeiro.

À minha família, pelo incentivo e por fazer de tudo para que minhas únicas preocupações fossem proposições e Teoremas.

Aos membros da banca, pela disposição demonstrada ao aceitarem ajudar nessa última etapa do mestrado e pelas excelentes sugestões para complementar essa dissertação.

À Raquel Scarpelli, pelos seminários e discussões sobre a Teoria de Corpos de Funções.

Aos meus professores da graduação, do Mestrado e dos Programas de Verão (Walcy Santos na UFRJ em 2005 e Arnaldo Garcia no IMPA em 2006), pelo papel importante que exerceram na minha formação acadêmica.

Aos funcionários da biblioteca e da secretaria de pós-graduação do Instituto de Matemática, em especial à Daniela e ao Eduardo.

À turma de Introdução às Curvas Algébricas do Programa de Verão do IMPA de 2006 – Fred, Anete, Amanda, Rodrigo e Mauro – por todas as horas de estudo e pelos momentos de descontração na sala do café.

Ao Felipe Figueiredo e ao Regis Castijos, pela enorme ajuda com os segredos do LATEX e da dissertação em geral.

Ao André Pereira, pela ajuda com as dúvidas algébricas e pelas caronas.

Aos amigos Fábio Ramos e Rodrigo Neumann pelas longas conversas sobre a vida, o universo e tudo mais, em especial sobre nosso futuro como pesquisadores.

Aos incomparáveis Marcelo Rainha e Marcelo Tavares, pelas horas de estudo na biblioteca e pelos longos almoços seguidos de café no Burguesão.

Aos meus amigos não-matemáticos que entenderam que nem sempre dava para sair no fim de semana. Em especial, à Marina Maia (a responsável pela minha formação cinematográfica nos dias de folga) e ao Bruno Durão (o responsável pela minha calma na reta final).

A todos que ao longo da minha vida perguntaram "você gosta mesmo de matemática?", me fazendo pensar no assunto e concluir que sim.

Não se afobe, não

Que nada é pra já

- Chico Buarque

Resumo

Apresentamos algumas novas construções de códigos geométricos baseados no artigo de Özbudak e Stichtenoth usando resultados básicos sobre códigos lineares e Teoria de Corpos de Funções Algébricas. Nosso principal interesse consiste em estudar a relação dessas novas construções com os Códigos de Goppa Clássicos para saber se são generalizações ou apenas casos especiais que possibilitam novas abordagens para a Teoria de Códigos.

Abstract

We present some new constructions of algebraic-geometry codes based on the work of Özbudak e Stichtenoth using basic results about linear codes and Algebraic Function Fields Theory. Our main interest is to investigate the relation between these new constructions and Goppa's construction to find out if they are generalizations of the classic codes or special cases that provide new points of view for the Coding Theory.

Sumário

Introdução

O interesse pela transmissão de informações de forma segura e correta é um problema abordado desde o início da civilização. A Teoria de Códigos é a área da matemática responsável pelo estudo de processamento de informações através de canais com interferências, de forma que a maior quantidade de erros possa ser corrigida, tendo seu surgimento marcado pelas pesquisas da Bell Lab na década de 1940. As aplicações dessa Teoria estão presentes em diversas ações cotidianas como por exemplo ouvir música via um CD, que utiliza uma classe de Códigos de Reed-Solomon para corrigir problemas devidos a pequenos arranhões e poeira. Nesta dissertação, nos dedicamos ao estudos de uma sub-área da Teoria de Códigos que trata de códigos lineares sobre corpos finitos (subespaços lineares de um determinado espaço vetorial munido de uma métrica).

No primeiro Capítulo, fazemos uma breve introdução às definições básicas e apresentamos alguns resultados essenciais.

A teoria de códigos lineares utiliza ferramentas matemáticas sofisticadas e pode ser abordada a partir de diversas áreas, tais como Geometria Algébrica, Teoria dos Números e Teoria de Grupos. O segundo Capítulo dessa dissertação é dedicado a uma dessas áreas: a Teoria de Corpos de Funções. A escolha dessa arbordagem deve-se ao interesse pelo estudo dos Códigos Geométricos, uma classe dos códigos lineares introduzida por V.D.Goppa em 1981 utilizando ferramentas algebrico-geométricas. Assim, nesse segundo Capítulo, introduzimos os conceitos de lugar,

valoração discreta, divisor aos quais associamos espaços vetoriais de funções, incluindo ferramentas que nos permitem estimar a dimensão de tais espaços para obter os parâmetros dos Códigos Geométricos.

No terceiro Capítulo, começamos o estudo das construções de códigos caso a caso. Na seção 3.1, apresentamos o chamado Códigos de Goppa Clássicos, não da forma como foram introduzidos a princípio, mas como imagem da evaluação de funções em lugares de grau 1. Damos especial atenção ao caso do corpo de funções racionais em exemplos que utilizam os resultados apresentados de forma direta.

A partir daí, nos baseamos nos trabalho de Özbudak e Stichtenoth [4] para estudar cinco novas abordagens dos Códigos Geométricos. As duas primeiras (seções 3.2 e 3.3) foram introduzidas por Xing, Niederreiter e Lam em [7] e se baseiam na expansão de funções em séries de potências em lugares de grau 1. Mostramos que, na verdade, são apenas casos especiais da quarta construção (seção 3.4), a qual é equivalente à construção clássica. Assim, ao fim desse Capítulo, concluímos que as novas construções apresentadas em [7] são importantes apenas por apresentar novos pontos de vista do Códigos de Goppa Clássicos.

No último Capítulo, nos deparamos com a possibilidade de construir códigos geométricos utilizando lugares de grau superior. A seção 4.1 é dedicada a uma generalização natural da construção apresentada em 3.4, que foi introduzida por Niederreiter, Xing e Lam em [3]. Já temos, então, uma generalização do Códigos de Goppa Clássicos. Porém, esses mesmos pesquisadores ainda apresentaram uma generalização ainda melhor em [8]. Mostramos na seção 4.2 como a última construção abrange todas as novas abordagens apresentadas anteriormente e generaliza de forma simples os Códigos de Goppa Clássicos, abrindo assim novos caminhos para a Teoria de Códigos.

Capítulo 1

Introdução à Teoria de Códigos Lineares

Neste Capítulo, introduzimos os conceitos básicos e alguns resultados clássicos da Teoria de Códigos. Para tal vamos considerar $\mathbb{F}_q$ o corpo finito com q elementos.

1.1 Conceitos básicos

Definição 1.1.1. Um código linear C sobre $\mathbb{F}_q$ é um subespaço vetorial não nulo de $\mathbb{F}_q^n$, $n \geq 1$. Dizemos que n é o comprimento de C e $k := \dim C$ é a dimensão de C sobre $\mathbb{F}_q$.

Os elementos de $\mathbb{F}_q$ formam o alfabeto, e os elementos de C são ditos palavras do código.

Uma matriz geradora M para C é uma matriz $k \times n$ sobre $\mathbb{F}_q$ cujas linhas formam uma base para C. Um elemento $y \in \mathbb{F}_q^k$ é codificado como $u = yM \in \mathbb{F}_q^n$, isto é, $C = \{yM \mid y \in \mathbb{F}_q^k\}$.

Uma matriz de checagem H é uma matriz $(n-k) \times n$ tal que $u \in \mathbb{F}_q^n$ é uma palavra do código C se e somente se $Hu^t = 0$, onde u^t denota a transposição de u.

Definição 1.1.2. Sejam $u = (u_1, ..., u_n), v = (v_1, ..., v_n) \in C$. Definimos:

(i) A distância de Hamming entre u e v: $d(u, v) = |\{i;\ u_i \neq v_i\}|$.

(ii) O peso de uma palavra u: $w(u) := d(u, 0) = |\{i;\ u_i \neq 0\}|$.

(iii) A distância mínima de C: $d = d(C) := \min\{d(u, v) \mid u, v \in C,\ u \neq v\}$.

Dizemos que um código com comprimento n, dimensão k e distância mínima d é um código $[n, k, d]$.

Notamos que dadas u e v palavras de C, temos $d(u, v) = d(u-v, 0) = w(u-v)$, donde podemos ver a distância mínima de C como $d = \min\{w(u) \mid 0 \neq u \in C\}$.

Proposição 1.1.3. *Seja C um código linear definido pela matriz de checagem H. Então, a distância mínima d de C é $d \geq s+1$ se e somente se quaisquer s colunas de H são linearmente independentes.*

Demonstração. Suponha que existam s colunas de H linearmente dependentes. Então, é possível tomar $0 \neq u \in \mathbb{F}_q^n$ tal que $Hu^t = 0$ (isto é, u é uma palavra de C) e $w(u) \leq s$, isto é, $d \leq s$. Por outro lado, se quaisquer s colunas de H são linearmente independentes. então não é possível encontrar $0 \neq u \in \mathbb{F}_q^n$ de peso $w(u) \leq s$ tal que $Hu^t = 0$. Assim, $d \geq s + 1$. □

Durante a transmissão de uma informação codificada através de um canal de comunicação, podem ocorrer eventuais erros. Então, é preciso garantir que o código C utilizado seja capaz de identificar e corrigir erros para que possamos recuperar a mensagem original.

Definição 1.1.4. Seja $t \in \mathbb{N}$. Dizemos que um código C corrige t erros se para todo $y \in \mathbb{F}_q^n$ existe no máximo uma palavra u em C tal que $d(y, u) \leq t$.

Sejam $u \in C$ uma palavra transmitida e x a informação recebida com no máximo t erros. Se C corrige t erros, então temos $d(x, u) \leq t$ e $d(x, v) > t$ para toda palavra $v \neq u$ do código. Isto significa que u é a palavra de C mais próxima de x e, portanto, a informação correta.

Proposição 1.1.5. *Seja C um código com distância mínima d. Então, C pode corrigir até $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ erros, onde $\lfloor x \rfloor$ denota a parte inteira de x.*

Demonstração. Sejam $u, v \in C$ e $B_t(u)$ e $B_t(v)$ bolas de raio $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ centradas em u e v respectivamente. Suponhamos que exista $x \in B_t(u) \cap B_t(v)$. Então,

$$d(u, v) \leq d(u, x) + d(x, v) \leq t + t \leq d - 1,$$

o que é uma contradição, já que a distância mínima de C é d.

Dessa forma, se transmitimos a palavra $u \in C$ e recebemos y com $r \leq t$ erros, temos $d(u, y) = r \leq t$ e $d(v, y) > t$ para toda palavra $v \in C$ diferente de u. □

Pelo resultado anterior, uma distância mínima grande representa uma maior capacidade de correção de erros. Então, um dos principais problemas nessa teoria é construir um código com dimensão e distância mínima grandes em relação ao comprimento. Entretanto, há algumas restrições, como a cota de Singleton.

Proposição 1.1.6. *(cota de Singleton) $k + d \leq n + 1$ para C um código $[n, k, d]$.*

Demonstração. Primeiro, notamos que como d é a distância mínima de C, então qualquer palavra $0 \neq c \in C$ é tal que $w(c) \geq d$. Agora, vamos definir o subespaço linear $W := \left\{ u = (u_1, ..., u_n) \in \mathbb{F}_q^n \mid u_i = 0 \ \forall i \geq d \right\}$.Temos que $\dim W = d - 1$ e qualquer elemento $0 \neq u \in W$ possui no máximo $d-1$ coordenadas não-nulas, isto é, $w(u) \leq d - 1$. Assim, $W \cap C = \{0\}$ e $\dim(W \cap C) = 0$.

Portanto, $\dim C + \dim W = \dim(C + W)$, ou seja, $k + (d - 1) \leq n$. □

1.2 Códigos de Reed Solomon

No Capítulo 4, apresentaremos uma generalização dos códigos de Goppa, após estudarmos algumas noções de Corpos de Funções. Uma das razões do interesse

nessa classe de códigos é a existência de diversas cotas inferiores para a distância mínima.

Como motivação para a construção de tal classe de códigos, apresentamos agora os códigos de Reed Solomon, que são obtidos como imagem da função evaluação. Consideramos $\beta \in \mathbb{F}_q$ um gerador do grupo cíclico $\mathbb{F}_q^*$ e definimos o espaço vetorial $\mathscr{L}_k := \{f \in \mathbb{F}_q[T] \mid \deg f \leq k-1\}$, onde $1 \leq k \leq q-1$, e a aplicação $ev : \mathscr{L}_k \to \mathbb{F}_q^n$ dada por $ev(f) := (f(\beta), f(\beta^2), ..., f(\beta^{q-1}))$. Esta aplicação é linear e injetiva (já que um polinômio de grau m possui no máximo m zeros), então podemos definir:

Definição 1.2.1. $C_k := \{(f(\beta), f(\beta^2), ..., f(\beta^{q-1})) \mid f \in \mathscr{L}_k\}$ é dito código de Reed Solomon (ou código RS).

Note que C_k é um código $[q-1, k, d]$.

Proposição 1.2.2. *Seja C_k um código RS, então $d = n + 1 - k$.*

Demonstração. Pela cota de Singleton, temos $d \leq n + 1 - k$.

Seja $0 \neq u \in C_k$. Temos: $w(u) := d(u, 0) = |\{i;\ u_i \neq 0\}| = n - |\{i;\ u_i = 0\}|$. Mas $u_i = f(\beta^i)$, onde $f \in \mathscr{L}_k$ e, então, f tem no máximo $k-1$ zeros. Portanto:

$$w(u) \geq n - \deg f \geq n - (k-1) = n + 1 - k.$$

Como a distância mínima d é igual ao mínimo dentre os pesos das palavras não-nulas do código, temos $d \geq n + 1 - k$.

Logo, $d = n + 1 - k$. □

Capítulo 2

Noções de corpos de funções

Neste Capítulo, estudaremos algumas noções básicas sobre corpos de funções, teoria em que basearemos as construções dos códigos que serão apresentados nos próximos Capítulos. Os resultados não demonstrados podem ser encontrados em [5] e [2].

2.1 Lugares

Definição 2.1.1. Uma extensão de corpos F/K é um corpo de funções algébricas em uma variável sobre K se F é uma extensão algébrica finita de $K(x)$, onde x em F é um elemento transcendente sobre K. O corpo $\widetilde{K}$ dos elementos de F que são algébricos sobre K é chamado o corpo de constantes de F/K.

Vamos sempre supor que $\widetilde{K} = K$, isto é, vamos sempre supor que K é algebricamente fechado em F.

Um corpo de funções F/K é dito racional se $F = K(x)$ para algum $x \in F$ transcendente sobre K. Pelo Teorema da Fatoração Única em $K[x]$, um elemento z não-nulo possue representação única da forma $z = a\prod_i p_i(x)^{n_i}$ com $0 \neq a \in K$, $n_i \in \mathbb{Z}$ e $p_i(x) \in K[x]$ polinômios mônicos irredutíveis distintos.

Freqüentemente, representamos um corpo de funções F/K como uma extensão algébrica simples de um corpo de funções racionais $K(x)$, isto é, $F = K(x, y)$ onde $f(y) = 0$ para algum polinômio irredutível $f(T) \in K(x)[T]$.

Definição 2.1.2. Seja O um anel tal que:

(i) $K \subsetneq O \subsetneq F$;

(ii) $\forall z \in F/$, $z \in O$ ou $z^{-1} \in O$.

O é chamado anel de valoração de F/K.

Seja $O^* := \{z \in O \mid \exists w \in O \text{ tal que } zw = 1\}$ o grupo de unidades de O. Temos que O é um domínio de ideiais principais e possui um único ideal maximal (que é principal) $P := O \backslash O^*$ chamado um lugar de F/K. O conjunto dos lugares de F/K é representado por $\mathbb{P}_F$.

Pela definição 2.1.2, para qualquer $0 \neq z \in F$, temos que $z \in P$ se e somente se $z^{-1} \notin O$. Assim, também podemos caracterizar o anel de valoração a partir do lugar P como $O_P := \{z \in F \mid z^{-1} \notin P\}$.

Definição 2.1.3. Uma valoração discreta de F/K é uma função $v : F \to \mathbb{Z} \cup \{\infty\}$ satisfazendo:

(i) $v(x) = \infty \iff x = 0$;

(ii) $v(xy) = v(x) + v(y)$;

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$ (desigualdade triangular);

(iv) $\exists\ z \in F$ tal que $v(z) = 1$;

(v) $v(a) = 0\ \forall a \in K^*$.

Proposição 2.1.4. *Se $v(x) \neq v(y)$ para $x, y \in F$, então $v(x+y) = \min\{v(x), v(y)\}$.*

Demonstração. Podemos supor $v(x) < v(y)$. Pela desigualdade triangular, temos $v(x + y) \geq \min\{v(x), v(y)\}$. Suponhamos agora que $v(x + y) \neq \min\{v(x), v(y)\}$. Então, $v(x + y) > \min\{v(x), v(y)\} = v(x)$. Assim, obtemos

$$v(x) = v((x + y) - y) \geq \min\{v(x + y), v(y)\} > v(x),$$

uma contradição. □

O resultado a seguir possibilita a definição de uma valoração discreta a partir de um lugar P de F/K.

Proposição 2.1.5. *Sejam P um lugar de F/K, O o seu anel de valoração e $t \in O$ tal que $P = tO$, então para todo $0 \neq z \in F$ existem únicos $n \in \mathbb{Z}$ e $u \in O^*$ tais que $z = t^n u$. Tal t é dito um elemento primitivo em P.*

Proposição 2.1.6. *Considere a aplicação $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ definida por $v_P(z) := n$ e $v_P(0) := \infty$. Então, v_P é uma valoração discreta de F/K.*

Demonstração. A definição da função v_P não depende da escolha do elemento primitivo. De fato, se tomarmos t e l elementos primitivos para P, então $t = lw$, $w \in O_P^*$. Assim, para $0 \neq z \in F$ temos $z = t^n u = l^n w^n u$ e $w^n u \in O_P^*$.

Temos ainda que v_P é realmente uma valoração. Com efeito, sejam $x = t^{n_1} u_1$ e $y = t^{n_2} u_2$, onde $n_1, n_2 \in \mathbb{Z}$ e $u_1, u_2 \in O_P^*$, temos:

(i) $v_P(x) = \infty \Longleftrightarrow x = 0$ por definição;

(ii) $v_P(xy) = v_P(t^{n_1+n_2}(u_1 u_2)) = n_1 + n_2 = v_P(x) + v_P(y)$;

(iii) Suponha $n_1 \leq n_2 < \infty$. Temos: $x + y = t^{n_1}(u_1 + t^{n_2-n_1} u_2) = t^{n_1} w$ com $w \in O_P$. Se $w = 0$, então

$$v_P(x + y) = v_P(0) = \infty > \min\{v_P(x), v_P(y)\}.$$

Se $w \neq 0$, então podemos escrever $w = t^{n_3} u_3$ com $n_3 \geq 0$ e $u_3 \in O_P^*$. Assim:

$$v_P(x + y) = v_P(t^{n_1} w) = v_P(t^{n_1+n_3} u_3) = n_1 + n_3 \geq n_1 = \min\{v_P(x), v_P(y)\}.$$

(iv) Como $K \subseteq O_P^*$, temos $v_P(a) = v_P(t^0 a) = 0$ para todo $a \in K^*$. □

Note que se $t \in O$ é um elemento primitivo, então $v_P(t) = 1$.

Assim, pela Proposição 2.1.6, dado um lugar P de F/K, podemos definir a valoração v_P correspondente e caracterizar P e O_P como $P = \{z \in F \mid v_P(z) > 0\}$ e $O_P = \{z \in F \mid v_P(z) \geq 0\}$. Por outro lado, dada v uma valoração discreta de F/K, o conjunto $P := \{z \in F \mid v(z) > 0\}$ é um lugar de F/K e $O_P := \{z \in F \mid v(z) \geq 0\}$ é o anel de valoração correspondente.

Definição 2.1.7. (i) Sejam P um lugar de F/K e O_P o seu anel de valoração. Como P é um ideal maximal, podemos considerar $F_P := O_P/P$ o seu corpo de classes residuais e a aplicação de classe residual:

$$\begin{aligned} F &\rightarrow F_P \cup \{\infty\} \\ x &\rightarrow x(P) \end{aligned}$$

onde $x(P) = \infty$ para $x \in F \backslash O_P$.

(ii) $\deg P := [F_P : K]$ é o grau de P.

Note que se o grau do lugar P for 1, então o corpo de classes residuais F_P é o próprio corpo de constantes K, fato que será importante para as construções de códigos geométricos que apresentaremos.

Proposição 2.1.8. *Sejam $x \in F \setminus K$ e P um lugar tal que $x \in P$. Então,*

$$\deg P \leq [F : K(x)] < \infty.$$

Demonstração. Sabemos que um elemento x em F é transcendente sobre K se e somente se $[F : K(x)] < \infty$. Assim, temos $[F : K(x)] < \infty$.

Sejam $z_1, ..., z_n$ funções em O_P cujas classes residuais $z_1(P), ..., z_n(P)$ em F_P são linearmente independentes sobre K. Suponha que existam α_i, $1 \leq i \leq n$, funções não todas nulas em $K(x)$ tais que $\sum_{i=1}^{n} \alpha_i z_i = 0$. Podemos supor que, para todo $1 \leq i \leq n$, $\alpha_i = a_i + x g_i$, onde $a_i \in K$ não são todos nulos e $g_i \in K[x]$. Então, como $x \in P$:

$$0 = \sum_{i=1}^{n} \alpha_i(P) z_i(P) = \sum_{i=1}^{n} \left(a_i + x(P) g_i(P)\right) z_i(P) = \sum_{i=1}^{n} a_i z_i(P),$$

que é uma contradição com a independência linear de $z_1(P), ..., z_n(P)$ sobre K. Portanto, as funções $z_1, ..., z_n$ são linearmente independentes sobre $K(x)$ e, assim, $\deg P = [F_P : K] \leq [F : K(x)] < \infty$. □

Exemplo 2.1.9. Vamos estudar os lugares do corpo de funções racionais $K(x)/K$.

Primeiro, considere $p(x) \in K[x]$ um polinômio irredutível e o anel de valoração

$$O_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \text{ e } p(x) \nmid g(x) \right\}$$

cujo ideal maximal é

$$P_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K\left[x\right], p(x) \mid f(x) \text{ e } p(x) \nmid g(x) \right\}.$$

Toda função $z \in K(x)\backslash\{0\}$ pode ser representada de maneira única na forma $z = p(x)^n(\frac{f(x)}{g(x)})$ com $n \in \mathbb{Z}$, $f(x), g(x) \in K[x]$, $p(x) \nmid f(x)$ e $p(x) \nmid g(x)$, então $p(x)$ é um elemento primitivo para $P_{p(x)}$. Assim, a partir da construção feita na Proposição 2.1.5, podemos definir a valoração $v_{P_{p(x)}}(z) = n$. Agora, consideramos o homorfismo de anéis:

$$\begin{aligned} \phi : \ & K[x] \longrightarrow K(x)_{P_{p(x)}} = O_{p(x)}/P_{p(x)} \\ & f(x) \to f(x)(P) \end{aligned}$$

cujo núcleo

$$\ker \phi = \{f(x) \in K[x] \mid f(x)(P_{p(x)}) = 0\} = \{f(x) \in K[x] \mid f(x) \in P_{p(x)}\}$$

é o ideal gerado por $p(x)$ em $K[x]$. Seja $z \in O_{p(x)}$, então $z = \frac{f(x)}{g(x)}$ com $f(x), g(x) \in K[x]$ e $mdc(p(x), g(x)) = 1$, isto é,

$$z = \frac{f(x)}{g(x)} = 1\frac{f(x)}{g(x)} = (a(x)p(x) + b(x)g(x))\frac{f(x)}{g(x)} = \frac{a(x)f(x)}{g(x)}p(x) + b(x)f(x),$$

onde $a(x), b(x) \in K[x]$. Assim, $z(P_{p(x)}) = (b(x)f(x))(P_{p(x)}) \in \Im\phi$, o que significa que ϕ é sobrejetiva e, portanto, induz um isomorfismo

$$\begin{aligned} \varphi : \quad & K[x]/(p(x)) \to K\left(x\right)_{P_{p(x)}} \\ & f(x) mod p(x) \longrightarrow f(x)(P_{p(x)}) \end{aligned} .$$

Logo, $\deg P_{p(x)} = \left[K(x)_{p(x)} : K\right] = [K[x]/(p(x)) : K] = \deg p(x)$.

Em particular, se $p(x) = x - \alpha$, onde $\alpha \in K$, temos para $f(x) \in K[x]$:

$$f(x)(P_{p(x)}) = (f(x) - f(\alpha))(P_{p(x)}) + f(\alpha)(P_{p(x)}) = f(\alpha)(P_{p(x)}) = f(\alpha).$$

Então, para $z \in O_{P_{p(x)}}$, temos $z(P_{p(x)}) = \frac{f(x)}{g(x)}(P_{p(x)}) = \frac{f(\alpha)}{g(\alpha)}$,se $g(\alpha) \neq 0$, e $z(P_{p(x)}) = \infty$, se $g(\alpha) = 0$.

Podemos ainda considerar

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

o anel de valoração cujo ideal maximal

$$P_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \text{ e } \deg f(x) < \deg g(x) \right\}$$

é dito lugar no infinito de $K(x)/K$. Para $x \in K(x)$, temos que $\frac{1}{x} \in P_\infty$, isto é, P_∞ é zero de x. Como $K(\frac{1}{x}) = K(x)$, pela Proposição 2.1.8, temos $\deg P_\infty \leq \left[K(x) : K(\frac{1}{x})\right] = 1$, donde $\deg P_\infty = 1$. Temos ainda que se $z \in P_\infty$, então $z = \frac{f(x)}{g(x)} = \frac{1}{x}\frac{xf(x)}{g(x)}$ com $f(x), g(x) \in K[x]$ e $\deg f(x) < \deg g(x)$. Assim, $\frac{xf(x)}{g(x)} \in O_\infty$ e $z \in \frac{1}{x}O_\infty$, isto é, $\frac{1}{x}$ é elemento primitivo para P_∞. Temos também que a valoração discreta v_{P_∞} é definida por $v_{P_\infty}\left(\frac{f(x)}{g(x)}\right) = \deg g(x) - \deg f(x)$ e, para $z = \frac{f(x)}{g(x)} = \frac{a_n x^n + \ldots + a_1 x + a_0}{b_m x^m + \ldots + b_1 x + b_0}$ onde $a_i, b_j \in K$ e $a_n, b_m \neq 0$, a classe em F_{P_∞} é:

$$z(P_\infty) = z(\infty) = \begin{cases} \frac{a_n}{b_m}, \text{ se } n = m \\ 0, \text{ se } n < m \\ \infty, \text{ se } n > m \end{cases}$$

Por fim, seja $P \neq P_\infty$ um lugar de $K(x)/K$. Se $x \in O_P$, então $K[x] \subseteq O_P$ e como os lugares de $K(x)/K$ correspondem aos ideais maximais de $K[x]$, existe um polinômio $p(x) \in K[x]$ irredutível tal que $O_P = O_{p(x)}$. Assim, os únicos lugares de $K(x)/K$ são $P_{p(x)}$ e P_∞. Portanto, podemos identificar os lugares de $K(x)/K$ de grau 1 com os elementos de $K \cup \{\infty\}$, conjunto que é interpretado como a linha projetiva sobre K.

Definição 2.1.10. Sejam $z \in F$ e $P \in \mathbb{P}_F$, então:

(i) P é um zero de z se e somente se $v_P(z) > 0$ (isto é, $z \in P$).

(ii) P é um pólo de z se e somente se $v_P(z) < 0$ (isto é, $z \notin O_P$).

A ordem do zero ou do pólo de z é $|v_P(z)|$.

Teorema 2.1.11. *Seja F/K um corpo de funções. Qualquer elemento $z \in F$ transcendente sobre K possui pelo menos um pólo e um zero.*

Demonstração. Vamos provar que se R é um subanel de F tal que $K \subseteq R \subseteq F$ e $\{0\} \neq I \subsetneq R$ é um ideal próprio de R, então existe P lugar de F/K tal que $I \subseteq P$ e $R \subseteq O_P$, usando o Lema de Zorn.

Para cada subanel S de F, consideramos o conjunto:

$$IS := \{\sum_{\nu=1}^{\nu_0} a_\nu s_\nu \mid a_\nu \in I,\ s_\nu \in S,\ \nu_0 \in \mathbb{N}\}.$$

Considere $J := \{S \mid S \text{ subanel de } F \text{ com } R \subseteq S \text{ e } IS \neq S\}$ uma família de subanéis de F.

Para $a, b \in IS$, temos $a + b \in IS$. Para $a \in IS$ e $s \in S$, temos $as = \left(\sum_{\nu=1}^{\nu_0} a_\nu s_\nu\right) s = \sum_{\nu=1}^{\nu_0} a_\nu (s_\nu s)$ e $s_\nu s \in S$, pois S é anel. Então, IS é um ideal de S e J é não-vazio já que $R \in J$.

Seja $H \subseteq J$ totalmente ordenado. Temos que o conjunto $T := \cup\{S \mid S \in H\}$ é subanel de F e $R \subseteq T$, já que cada S é subanel de F com $R \subseteq S$. Além disso, $T \neq IT$. De fato, suponha por absurdo que $T = IT$, então $1 \in IT$, donde $1 = \sum_{\nu=1}^{n} a_\nu s_\nu$ com $a_\nu \in I$, $s_\nu \in T$, $n \in \mathbb{N}$. Como H é totalmente ordenado, existe um subanel S_0 tal que $s_1, ..., s_n \in S_0$, isto é, $1 \in IS_0$, o que é um absurdo. Portanto, T é cota superior de H e, pelo Lema de Zorn, J possui elemento maximal O.

Primeiro, como $I \neq \{0\}$ e $IO \neq O$, temos que $O \subsetneq F$ e $I \subseteq O \backslash O^*$.

Agora, suponhamos que exista um elemento $z \in F$ tal que $z \notin O$ e $z^{-1} \notin O$, isto é, $IO[z] = O[z]$ e $IO[z^{-1}] = O[z^{-1}]$. Então, escolhemos $a_0, ..., a_n, b_0, ..., b_m \in IO$,

onde $0 < m \leq n$ e n, m são mínimos, tais que $1 = a_0 + a_1 z + ... + a_n z^n$ e $1 = b_0 + b_1 z^{-1} + ... + b_m z^{-m}$. Multiplicando a primeira equação por $1 - b_0$, a segunda por $a_n z^n$ e somando as equações resultantes, obtemos uma combinação $1 = c_0 + c_1 z + ... + c_{n-1} z^{n-1}$, onde $c_i \in IO$. Como n foi escolhido mínimo, há uma contradição. Então, O é um anel de valoração de F/K.

Para finalizarmos a demonstração, seja $z \in F$ um elemento transcendente sobre K. Considere $R = K[z]$ e $I = zK[z]$. Pelo que acabamos de provar, existe um lugar P tal que $z \in P$, donde P é zero de z, e existe um lugar Q tal que $z^{-1} \in Q$, donde Q é polo de z. □

Em particular, esse Teorema garante que $\mathbb{P}_F \neq \emptyset$. Na verdade, este conjunto é infinito, como mostra o seguinte resultado:

Teorema 2.1.12. *(Teorema da aproximação fraca) Sejam F/K um corpo de funções, $P_1, ..., P_n$ lugares de F/K tais que $P_i \neq P_j$ para $i \neq j$, funções $x_1, ..., x_n \in F$ e números $r_1, ..., r_n \in \mathbb{Z}$. Então, existe $x \in F$ tal que para $i = 1, ..., n$ temos $v_{P_i}(x - x_i) = r_i$.*

Caso $P_1, ..., P_n$ fossem todos os lugares do corpo de funções F/K, escolhendo $x_1 = ... = x_n = 0$ e $r_i \in \mathbb{Z}_+^*$, pelo Teorema da aproximação fraca existiria uma função $x \in F$ tal que $v_{P_i}(x) = r_i > 0$ para todo i. Isto significa que x seria transcendente sobre K e possuiria apenas zeros, contradizendo o Teorema 2.1.11. Assim, $\mathbb{P}_F$ é infinito. Entretanto, cada função $0 \neq x \in F$ possui apenas um número finito de pólos e zeros segundo o próximo resultado que pode ser provado aplicando o Teorema da Aproximação Fraca.

Proposição 2.1.13. *Sejam F/K um corpo de funções e $P_1, ..., P_r$ zeros de $x \in F$. Então, $\sum_{i=1}^{r} v_{P_i}(x) \deg P_i \leq [F : K(x)]$.*

Corolário 2.1.14. *Seja F/K um corpo de funções. Cada função $x \in F$ não nula possui um número finito de zeros e pólos.*

Demonstração. Usando a Proposição 2.1.13 podemos concluir que se $x \in F$ é transcendente sobre K, então o número de zeros de x é limitado por $[F : K(x)]$ (que é finito pela Proposição 2.1.8). Da mesma forma, o número de zeros de x^{-1} é limitado por $[F : K(x^{-1})]$, isto é, o número de pólos de x também é finito. □

Para finalizar a seção, apresentamos um resultado que garante a expansão de toda função f de F em série de potências, e que será importante para a construção das novas abordagens dos códigos de Goppa no Capítulo 3.

Proposição 2.1.15. *Sejam P um lugar de grau 1 de F/K e $\{t_r\}_{-\infty}^{\infty}$ uma seqüência em F tal que $v_P(t_r) = r$ para todo $r \in \mathbb{Z}$. Então, toda função $f \in F$ pode ser escrita como $f = \sum_{r=v}^{\infty} a_r t_r$, onde $a_r \in K$ e $v \leq v_P(f)$.*

Demonstração. Primeiro, note que sempre existe uma seqüência $\{t_r\}_{-\infty}^{\infty}$ em F tal que $v_P(t_r) = r$. De fato, considerando t um uniformizante local em P, basta tomar $t_r := t^r$ para obter $v_p(t_r) = v_P(t^r) = r\ v_P(t) = r$.

Temos ainda que $1 = \deg P = [F_P : K]$, então $F_P = K$.

Agora, sejam $f \in F$ e um inteiro v tal que $v \leq v_P(f)$. Então,

$$v_P(\frac{f}{t_v}) = v_P(f) - v_P(t_v) \geq v - v = 0,$$

isto é, $\frac{f}{t_v} \in O_P$ e definimos $a_v := \left(\frac{f}{t_v}\right)(P)$ a classe de $\frac{f}{t_v}$ em $F_P = K$. Assim, $\left(\frac{f}{t_v} - a_v\right)(P) = 0$, donde $v_P\left(\frac{f}{t_v} - a_v\right) > 0$ e

$$v_P\left(f - a_v t_v\right) = v_P\left(\frac{f}{t_v} - a_v\right) + v_P(t_v) > v.$$

Então, $v_P\left(\frac{f - a_v t_v}{t_{v+1}}\right) = v_P\left(f - a_v t_v\right) - v_P(t_{v+1}) \geq 0$ e, assim, definimos $a_{v+1} := \left(\frac{f - a_v t_v}{t_{v+1}}\right)(P) \in K$. Assim, $\left(\frac{f - a_v t_v}{t_{v+1}} - a_{v+1}\right)(P) = 0$, donde

$$v_P(f - a_v t_v - a_{v+1} t_{v+1}) = v_P\left(\frac{f - a_v t_v}{t_{v+1}} - a_{v+1}\right) + v_P(t_{v+1}) > v + 1.$$

Suponha que obtivemos uma seqüência $\{a_r\}_{r=v}^{m} \subseteq K$ tal que

$$v_P\left(f - \sum_{r=v}^{k} a_r t_r\right) > k, \text{ para todo } v \leq k \leq m.$$

Então, $v_P\left(\frac{f-\sum_{r=v}^{m} a_r t_r}{t_{m+1}}\right) = v_P\left(f - \sum_{r=v}^{m} a_r t_r\right) - v_P(t_{m+1}) \geq 0$ e definimos $a_{m+1} := \left(\frac{f-\sum_{r=v}^{m} a_r t_r}{t_{m+1}}\right)(P) \in K$. Analogamente, temos:

$$v_P\left(f - \sum_{r=v}^{m+1} a_r t_r\right) = v_P\left(\left(\frac{f - \sum_{r=v}^{m} a_r t_r}{t_{m+1}} - a_{m+1}\right) t_{m+1}\right) > m+1.$$

Deste modo, $\{a_r\}_{r=v}^{\infty}$ é uma seqüência em K tal que $v_P\left(f - \sum_{r=v}^{m} a_r t_r\right) > m$, para todo $m \geq v$. Portanto, f pode ser representada como $f = \sum_{r=v}^{\infty} a_r t_r$. □

2.2 Divisores

Até o fim deste Capítulo, F/K representa um corpo de funções algébricas tal que K é o corpo de constantes.

Definição 2.2.1. Um divisor de F/K é uma soma formal $D = \sum_{P \in \mathbb{P}_F} n_P P$, onde $n_P \in \mathbb{Z}$ e $n_P = 0$ para quase todo lugar P de F/K. Se $D = P$, dizemos que D é um divisor primitivo.

Os divisores de F/K são elementos do grupo abeliano livre D_F com elemento neutro $0 := \sum_{P \in \mathbb{P}_F} 0.P$ e operação de adição definida por $D_1 + D_2 := \sum_{P \in \mathbb{P}_F} (n_{P_1} + n_{P_2})P$ se $D_1 = \sum_{P \in \mathbb{P}_F} n_{P_1} P$ e $D_2 = \sum_{P \in \mathbb{P}_F} n_{P_2} P$.

Definição 2.2.2. O suporte de um divisor D é $suppD := \{P \in \mathbb{P}_F \mid n_P \neq 0\}$.

Definição 2.2.3. Seja $D = \sum_{P \in \mathbb{P}_F} n_P P$ um divisor de F/K e Q um lugar de F/K. Definimos a valoração em D como $v_Q(D) := n_Q$.

Usando essa definição, podemos reescrever $suppD = \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\}$ e $D = \sum_{P \in suppD} v_P(D)P$. Além disso, definimos o grau de um divisor D como

$$\deg D := \sum_{P \in suppD} v_P(D) \deg P$$

e uma ordem parcial para D_F dada por:

$$D_1 \leq D_2 \iff v_P(D_1) \leq v_P(D_2)\ \forall P \in \mathbb{P}_F.$$

Definição 2.2.4. Seja $0 \neq x \in F$. Denotamos por Z o conjunto de zeros de x e por N o conjunto de pólos de x. Definimos o divisor de zeros de x como $(x)_0 := \sum_{P \in Z} v_P(x)P$ e o divisor de pólos de x como $(x)_\infty := \sum_{P \in N} (-v_P(x))P$. O divisor principal de x é $(x) = (x)_0 - (x)_\infty$ e definimos $\rho_F := \{(x) \mid 0 \neq x \in F\}$ o grupo dos divisores principais, que é um subgrupo de D_F.

Note que

$$(x) := (x)_0 - (x)_\infty = \sum_{P \in Z} v_P(x)P - \sum_{P \in N} (-v_P(x))P = \sum_{P \in \mathbb{P}_F} v_P(x)P.$$

Se $0 \neq x \in K$, então $v_P(x) = 0\ \forall P \in \mathbb{P}_F$, isto é, $0 \neq x \in K$ se e somente se $(x) = 0$.

Definição 2.2.5. $C_F := D_F/\rho_F$ é o grupo de classes de divisores e, para $D \in D_F$, $[D]$ é a classe correspondente em C_F.

Dizemos que dois divisores D_1 e D_2 são equivalentes e escrevemos $D_1 \backsim D_2$ se $D_1 = D_2 + (x)$, onde $0 \neq x \in F$.

Definição 2.2.6. Seja $D \in D_F$. Definimos $\mathscr{L}(D) := \{x \in F \mid (x) \geq -D\} \cup \{0\}$.

Note que, para $x \in F^*$, $(x) \geq -D$ se e somente se $v_P(x) \geq v_P(-D) = -v_P(D)$ para todo P lugar de F/K e, para $x = 0$, $v_P(x) = \infty \geq -v_P(D)$ para todo $P \in \mathbb{P}_F$.

Então, $\mathscr{L}(D) = \{x \in F \mid v_P(x) \geq -v_P(D)\ \forall P \in \mathbb{P}_F\}$. Assim, considerando um divisor

$$D = \sum_{P \in \mathbb{P}_F} n_P P = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j, \text{ onde } n_i \geq 0 \text{ e } m_j \geq 0,$$

temos que $0 \neq x \in \mathscr{L}(D)$ se e somente se $v_P(x) \geq -v_P(\sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j)$ para todo $P \in \mathbb{P}_F$, isto é, $v_{P_i}(x) \geq -n_i$ para $i = 1, ..., r$ e $v_{Q_j}(x) \geq m_j$ para $j = 1, ..., s$. Portanto, $\mathscr{L}(D)$ é o conjunto de todas as funções $x \in F$ tais que x possui zeros de ordem pelo menos m_j em Q_j ($j = 1, ..., s$) e pode possuir pólos apenas em P_i com ordem no máximo n_i $(i = 1, ..., r)$.

Proposição 2.2.7. *Seja $D \in D_F$.*

(i) $\mathscr{L}(D) \neq \{0\}$ se e somente se existe um divisor D' tal que $D' \backsim D$ e $D' \geq 0$.

(ii) Se $D < 0$, então $\mathscr{L}(D) = \{0\}$.

(iii) $\mathscr{L}(0) = K$.

(iv) $\mathscr{L}(D)$ é espaço vetorial sobre K.

(v) Se D' é um divisor equivalente a D, então $\mathscr{L}(D) \simeq \mathscr{L}(D')$.

(vi) Se D' é um divisor tal que $D' \leq D$, então:

$$\dim(\mathscr{L}(D)/\mathscr{L}(D')) \leq \deg D - \deg D'.$$

Demonstração. (i) Existe divisor $D' \in D'_F$ tal que $D \backsim D$ e $D' \geq 0$ se e somente se existe $D' \in D'_F$ tal que $D' = D + (x)$ e $(x) \geq -D$ com $0 \neq x \in F$, isto é, se e só se $\mathscr{L}(D) \neq \{0\}$.

(ii) Seja $D < 0$. Suponha por absurdo que exista uma função $0 \neq x \in \mathscr{L}(D)$. Por definição, $(x) \geq -D$ e, como $D < 0$, $-D > 0$, donde $(x) > 0$. Isto significa que x possui pelo menos um zero, mas nenhum pólo, o que contradiz o Teorema 2.1.11.

(iii) Seja $x \in K$. Temos que $(x) = 0$, donde $K \subseteq \mathscr{L}(0)$. Por outro lado, seja

$0 \neq x \in \mathscr{L}(0)$. Então, $(x) \geq 0$, isto é, x não possui pólos. Assim, pelo Teorema 2.1.11, $x \in K$, donde $K \supseteq \mathscr{L}(0)$.

(iv) Sejam $x, y \in \mathscr{L}(D)$ e $a \in K$, temos que

$$v_P(x+y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(D) \ \forall P \in \mathbb{P}_F$$

$$\text{e } v_P(ax) = v_P(a) + v_P(x) = v_P(x) \geq -v_P(D) \ \forall P \in \mathbb{P}_F$$

Então, $\mathscr{L}(D)$ é espaço vetorial sobre K.

(v) Se D' é um divisor equivalente a D, então existe x não nulo em F tal que $D = D' + (x)$. Seja $\varphi : (D) \to F$ a aplicação linear dada por $\varphi(z) = xz$. Temos $(xz) = (x) + (z) \geq (x) - D = -D'$, isto é, $\varphi(\mathscr{L}(D)) \subseteq \mathscr{L}(D')$. Analogamente, a aplicação linear $\psi : \mathscr{L}(D') \to F$ dada por $\psi(z) = x^{-1}z$ é tal que $\psi(\mathscr{L}(D')) \subseteq \mathscr{L}(D)$. Como $\varphi \circ \psi(z) = xx^{-1}z = z$ para $z \in \mathscr{L}(D')$ e $\psi \circ \varphi(z) = x^{-1}xz = z$ para $z \in \mathscr{L}(D)$, temos que φ é um isomorfismo entre $\mathscr{L}(D)$ e $\mathscr{L}(D')$.

(vi) Seja $x \in \mathscr{L}(D')$. Temos $v_P(x) \geq -v_P(D')$ para todo P lugar de F/K e $D' \leq D$, então, $v_P(x) \geq -v_P(D') \geq -v_P(D)$ para todo P em $\mathbb{P}_F$, donde $x \in \mathscr{L}(D)$, isto é, $\mathscr{L}(D') \subseteq \mathscr{L}(D)$. Podemos supor $D = D' + P$, onde P é um lugar de F/K, e o caso geral segue por indução (já que apenas um número finito de lugares aparece na soma formal D). Seja $t \in F$ tal que $v_P(t) = v_P(D) = v_P(D') + 1$. Para $x \in \mathscr{L}(D)$, temos

$$v_P(xt) = v_P(t) + v_P(x) \geq v_P(t) - v_P(D) = 0,$$

isto é, $xt \in O_P$. Assim, podemos considerar a aplicação $\Psi : \mathscr{L}(D) \to F_P$ tal que $\Psi(x) = (xt)(P)$. Temos:

$$\begin{aligned} \ker \Psi &= \{x \in \mathscr{L}(D) \mid (xt)(P) = 0\} = \{x \in \mathscr{L}(D) \mid xt \in P\} \\ &= \{x \in \mathscr{L}(D) \mid v_P(xt) > 0\} = \{x \in (D) \mid v_P(x) \geq -v_P(D\prime)\} = \mathscr{L}(D'). \end{aligned}$$

Ou seja, há uma aplicação K-linear injetiva de $(D)/\mathscr{L}(D')$ em F_P, cuja dimensão é $\dim F_P = \deg D - \deg D'$. Assim, $\dim(\mathscr{L}(D)/\mathscr{L}(D')) \leq \deg D - \deg D'$. $\square$

Em particular, o último ítem da Proposição 2.2.7, garante que se D é um divisor de F/K, então a dimensão de $\mathscr{L}(D)$ é finita. De fato, escrevendo $D = D_+ - D_-$, onde $D_+, D_- \geq 0$, temos $D \leq D_+$ e $(D) \subseteq \mathscr{L}(D_+)$. Além disso, considerando a aplicação que leva uma função de $\mathscr{L}(D_+)$ na classe correspondente em $\mathscr{L}(D_+)/\mathscr{L}(0)$, temos $\dim \mathscr{L}(D_+) = \dim(\mathscr{L}(D_+)/\mathscr{L}(0)) + 1$ pelo Teorema do Núcleo e da Imagem, já que $\mathscr{L}(0) = K$. Portanto:

$$\dim \mathscr{L}(D) \leq \dim \mathscr{L}(D_+) = \dim(\mathscr{L}(D_+)/\mathscr{L}(0)) + 1 \leq \deg D_+ + 1.$$

Definição 2.2.8. Seja $D \in D_F$. A dimensão de D é $\dim D := \dim(D)$.

Lema 2.2.9. *Sejam $D \geq 0$ um divisor de F/K e P_i, onde $1 \leq i \leq n$, lugares de grau 1 de F/K. Se α_i são funções em $\mathscr{L}(D + P_i)\backslash\mathscr{L}(D)$ para cada $1 \leq i \leq n$, então $\alpha_1, ..., \alpha_n$ são linearmente independentes sobre K.*

Demonstração. Primeiro, fixando $1 \leq i \leq n$, como $\alpha_i \in \mathscr{L}(D+P_i)\backslash\mathscr{L}(D)$, temos:

$$\begin{aligned} v_{P_i}(\alpha_i) &\geq -v_{P_i}(D + P_i) = -v_{P_i}(D) - 1 \text{ e} \\ v_{P_i}(\alpha_i) &< -v_{P_i}(D), \end{aligned}$$

isto é, $v_{P_i}(\alpha_i) = -v_{P_i}(D) - 1$. Além disso, para $j \neq i$, temos:

$$v_{P_i}(\alpha_j) \geq -v_{P_i}(D + P_j) = -v_{P_i}(D).$$

Suponha que exista uma combinação linear não trivial $\sum_{i=1}^{n} c_i\alpha_i = 0$, onde $c_i \in K$ para todo $1 \leq i \leq n$. Seja $1 \leq k \leq n$ um índice tal que $c_k \neq 0$. Temos que $-c_k\alpha_k = \sum_{i\neq k} c_i\alpha_i$. Assim, $v_{P_k}(-c_k\alpha_k) = v_{P_k}\left(\sum_{i\neq k} c_i\alpha_i\right)$, isto é:

$$-v_{P_i}(D) - 1 = -v_{P_i}(D) - 1 = v_{P_k}\left(\sum_{i\neq k} c_i\alpha_i\right) \geq \min_{i\neq k}\{v_{P_k}(c_i\alpha_i)\} \geq -v_{P_i}(D),$$

uma contradição. Portanto, $c_1 = ... = c_n = 0$, isto é, $\alpha_1, ..., \alpha_n$ são linearmente independentes sobre K. □

Teorema 2.2.10. *Seja $x \in F\backslash K$. Então,* $\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$.

Demonstração. Sejam $P_1, ..., P_r$ os pólos de x (já sabemos que essa quantidade é finita). Definimos $n := [F : K(x)]$ e o divisor $D := (x)_\infty = \sum_{i=1}^{r}(-v_{P_i}(x))P_i$. Pela Proposição 2.1.13, temos:

$$\deg D = \sum_{i=1}^{r}(-v_{P_i}(x)) \deg P_i = \sum_{i=1}^{r}(v_{P_i}(x^{-1})) \deg P_i \leq n.$$

Agora, sejam $\{u_i \mid i = 1, ..., n\}$ uma base de $F/K(x)$ e $A \in D_F$ tal que $A \geq 0$ e $(u_i) \geq -A$, isto é, $\{u_i \mid i = 1, ..., n\} \subseteq \mathscr{L}(A)$. Como os elementos $u_1, ..., u_n$ são linearmente independentes sobre $K(x)$, temos que $x^j u_i$, onde $0 \leq j \leq l$ e $1 \leq i \leq n$, são linearmente independentes sobre K. Além disso, $(x^j u_i) = j(x) + (u_i)$, donde $x^j u_i \in \mathscr{L}(lD + A)$ e, então, $\dim(lD + A) \geq n(l + 1)$ para todo $l \geq 0$. Mas, pela Proposição 2.2.7 (vi), $\dim(lD + A) \leq l \deg D + \deg A + 1$. Comparando as desigualdades, obtemos

$$n(l + 1) \leq \dim(lD + A) \leq l \deg D + \deg A + 1,$$

isto é, $n - \deg A - 1 \leq l(\deg D - n)$ para todo $l \in \mathbb{N}$. Como $n - \deg A - 1$ não depende de l, temos que $\deg D \geq n$.

Assim, $\deg(x)_\infty = n = [F : K(x)]$.

Como $(x)_0 = (x^{-1})_\infty$, temos $\deg(x)_0 = \deg(x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$, o que prova o resultado. □

Isso significa que todo divisor principal tem grau zero e, mais ainda, cada função $0 \neq x \in F$ possui o mesmo número de zeros e pólos se contados com multiplicidade. Além disso, se D_1 e D_2 são divisores equivalentes, então seus graus são iguais, já que $D_1 = D_2 + (x)$ com $0 \neq x \in F$ por definição.

Corolário 2.2.11. *Seja D um divisor de F/K.*

(i) Se $\deg D < 0$, *então* $\dim D = 0$;

(ii) Se $\deg D = 0$ *e* $\dim D = 1$*, então* D *é o divisor principal de alguma função não nula de* F*.*

Demonstração. (i) Suponha que $\dim D > 0$, então pela Proposição 2.2.7 (i) existe $A \geq 0$ um divisor equivalente a D. Logo, $\deg D = \deg A \geq 0$.

(ii) Seja $0 \neq x \in \mathscr{L}(D)$. Temos $(x) \geq -D$, isto é, $D+(x) \geq 0$ e $\deg(D+(x)) = 0$ pela Proposição 2.2.10. Então, $D + (x) = 0$ e, assim, $D = -(x) = (x^{-1})$. □

Lema 2.2.12. *Sejam* $x \in F\backslash K$ *e* $B := (x)_\infty$*. Então, existe um inteiro* γ *tal que para todo* $l \in \mathbb{Z}_+$ *temos* $\deg lB - \dim lB \leq \gamma$*.*

Demonstração. Pelo Teorema 2.2.10, sabemos que $\deg B = [F : K(x)]$. Sejam $A \geq 0$ um divisor de F/K, $\{u_i \mid (u_i) \geq -A,\ 1 \leq i \leq \deg B\}$ uma base para $F/K(x)$ e $l \in \mathbb{Z}_+$. Para $1 \leq i \leq \deg B$ e $0 \leq j \leq l$, temos que as funções $x^j u_i \in \mathscr{L}(lB + A)$ são linearmente independentes sobre K, já que $u_1, ..., u_{\deg B}$ são linearmente independentes sobre $K(x)$. Assim, $\dim(lB + A) \geq (l + 1) \deg B$. Por outro lado, pelo ítem (vi) da Proposição 2.2.7, temos que:

$$\dim(lB + A) - \dim lB \leq \deg(lB + A) - \deg lB = \deg A,$$

isto é, $\dim(lB + A) \leq \dim lB + \deg A$. Comparando as desigualdades, obtemos:

$$(l + 1) \deg B \leq \dim(lB + A) \leq \dim lB + \deg A,$$

ou seja, $\dim lB \geq \deg lB + [F : K(x)] - \deg A$.

Portanto, escolhendo $l = [F : K(x)] - \deg A$, temos que $\deg lB - \dim lB \leq \gamma$, com $\gamma \in \mathbb{Z}$. □

Lema 2.2.13. *Sejam* D *um divisor de* $F\backslash K$*,* $x \in F/K$ *e* $B := (x)_\infty$*. Então, existem* D_1 *e* D_2 *divisores de* F/K *e* $l \in \mathbb{Z}_+$ *tais que* $D \leq D_1$*,* $D_1 \sim D_2$ *e* $D_2 \leq lB$*.*

Demonstração. Seja $D_1 \geq 0$ um divisor de F/K tal que $D_1 \geq D$. Para $l \in \mathbb{Z}_+$, temos $lB - D_1 \leq lB$, donde pela Proposição 2.2.7 (vi) temos:

$$\dim lB - \dim(lB - D_1) \leq \deg lB - \deg(lB - D_1).$$

Assim, pelo Lema 2.2.12, temos:

$$\dim(lB - D_1) \geq \dim lB - \deg D_1 \geq \deg lB - \gamma - \deg D_1.$$

Se l for suficientemente grande, $\deg lB - \gamma - \deg D_1 > 0$, isto é, $\mathscr{L}(lB - D_1) \neq \emptyset$. Portanto, podemos escolher z uma função não nula em $\mathscr{L}(lB - D_1)$ e, definindo $D_2 := D_1 - (z)$, o resultado segue. □

Proposição 2.2.14. *Existe um inteiro γ tal que* $\deg D - \dim D \leq \gamma$ *para todo D divisor de F/K.*

Demonstração. Seja D um divisor de F/K. Pelo Lema 2.2.13, existem D_1 e D_2 divisores de F/K e $l \in \mathbb{Z}_+$ tais que $D \leq D_1$, $D_1 \sim D_2$ e $D_2 \leq lB$, onde $B := (x)_\infty$ para x em F/K. Como $D \leq D_1$, pela Proposição 2.2.7 (vi), temos:

$$\deg D - \dim D \leq \deg D_1 - \dim D_1. \tag{2.1}$$

Como D_1 e D_2 são divisores equivalentes, sabemos que $\deg D_1 = \deg D_2$ e $\dim D_1 = \dim D_2$, isto é:

$$\deg D_1 - \dim D_1 = \deg D_2 - \dim D_2. \tag{2.2}$$

Por fim, como $D_2 \leq lB$, a Proposição 2.2.7 (vi) nos dá novamente:

$$\deg D_2 - \dim D_2 \leq \deg lB - \dim lB. \tag{2.3}$$

Comparando 2.1, 2.2 e 2.3, obtemos:

$$\deg D - \dim D \leq \deg lB - \dim lB$$

e, pelo Lema 2.2.12, segue o resultado. □

Tal cota para a diferença $\deg D - \dim D$, onde D é um divisor de F/K, nos possibilita definir o gênero de um corpo de funções:

Definição 2.2.15. O gênero do corpo de funções F/K é

$$g := \max\{\deg D - \dim D + 1 \mid D \in D_F\}.$$

Escolhendo $D = 0$ na definição do gênero, temos $\deg(0) - \dim(0) + 1 = 0$, donde $g \geq 0$ para qualquer corpo de funções.

Teorema 2.2.16. *(Teorema de Riemann) Seja g o gênero de F/K. Então, existe um inteiro c tal que para todo divisor D com $\deg D \geq c$ temos*

$$\dim D = \deg D + 1 - g.$$

Demonstração. Segue da definição do gênero que $\dim D \geq \deg D + 1 - g$.

Por outro lado, se g é o gênero de F/K, então existe um divisor $A \in D_F$ tal que $g = \deg A - \dim A + 1$. Logo, para D um divisor de F/K tal que $\deg D \geq \deg A + g$, temos:

$$\dim(D - A) \geq \deg D - \deg A + 1 - g \geq \deg A + g - \deg A + 1 - g = 1 > 0.$$

Assim, $\mathscr{L}(D - A) \neq \{0\}$.

Sejam $0 \neq x \in \mathscr{L}(D - A)$ e $D' := D + (x)$. Então, $D' \geq D - (D - A) = A$ e

$$\deg D - \dim D = \deg D' - \dim D' \geq \deg A - \dim A = g - 1,$$

isto é, $\dim D \leq \deg D + 1 - g$.

Portanto, para um divisor D de F/K tal que $\deg D \geq c := \deg A + g$, ocorre a igualdade. □

Determinar o gênero de um corpo de funções é, em geral, um trabalho complicado. Mas é fácil ver que $g = 0$ no corpo de funções racionais $K(x)/K$. De

fato, sejam P_∞ o pólo de x, $r \in \mathbb{Z}_+$ e $\mathscr{L}(rP_\infty)$.Temos que $1, x, ..., x^r$ pertencem a $\mathscr{L}(rP_\infty)$ e são linearmente independentes sobre K, donde para um r suficientemente grande podemos aplicar o Teorema de Riemann e obter:

$$r + 1 \leq \dim \mathscr{L}(rP_\infty) = \deg \mathscr{L}(rP_\infty) + 1 - g = r + 1 - g.$$

Assim, $g \leq 0$. Mas sabemos que $g \geq 0$ para qualquer corpo de funções, donde o gênero do corpo de funções racionais é zero.

Definição 2.2.17. Seja F/K um corpo de funções de gênero g. Dizemos que um divisor W é um divisor Canônico se $\deg W = 2g - 2$ e $\dim W \geq g$.

Todo corpo de funções F/K possui divisor canônico.

Teorema 2.2.18. *(Teorema de Riemann-Roch) Seja W um divisor canônico de F/K. Para qualquer $D \in D_F$ temos* $\dim D = \deg D + 1 - g + \dim(W - D)$.

Corolário 2.2.19. *Seja D um divisor de F/K tal que* $\deg D \geq 2g - 1$. *Então,* $\dim D = \deg D + 1 - g$.

Demonstração. Seja W um divisor canônico de F/K. Como $\deg D \geq 2g - 1$ e $\deg W = 2g-2$, temos $\deg(W - D) = \deg W - \deg D < 0$,isto é, $\dim(W - D) = 0$. Assim, pelo Teorema de Riemann-Roch: $\dim D = \deg D + 1 - g$. □

Definição 2.2.20. Um divisor D de F/K tal que $\dim D = \deg D + 1 - g$ é dito não-especial.

Em particular, o Corolário 2.2.19 garante que qualquer divisor de grau maior ou igual a $2g - 1$ é não-especial. Além disso, se D é um divisor não-especial e D' é um divisor tal que $D' \geq D$, então D' também é não-especial.

No Capítulo 3, veremos que é importante poder estimar a dimensão dos espaços $\mathscr{L}(D)$ para obter os parâmetros do código de Goppa. O que fizemos no fim desse Capítulo, foi determinar a dimensão de $\mathscr{L}(D)$ a partir do grau de D:

(i) Se $\deg D < 0$, então $\dim D = 0$, pela Proposição 2.2.11;

(ii) Se $0 \leq \deg D < 2g - 1$ e W é um divisor canônico de F/K, então $\dim D = \deg D + 1 - g + \dim(W - D)$, pelo Teorema de Riemann-Roch. Em particular, temos que $\dim D \geq \deg D + 1 - g$ sempre;

(iii) Se $\deg D \geq 2g - 1$, então $\dim D = \deg D + 1 - g$, pelo Corolário 2.2.19.

Capítulo 3

Códigos de Goppa Clássicos e novas abordagens

Neste Capítulo, apresentaremos os códigos de Goppa Clássicos utilizando espaços $\mathscr{L}(D)$ e outras três abordagens de códigos sobre curvas algébricas introduzidas por Xing, Niederreiter e Lam em [7] e Özbudak e Stichtenoth em [4], mostrando, em particular, a relação entre as construções. Ao fim do Capítulo, concluiremos que as novas construções apresentadas são apenas abordagens equivalentes do código de Goppa Clássico. No entanto, estas novas construções são importantes por tornar possível o estudo dos códigos clássicos através de uma nova perspectiva.

3.1 Construção I: códigos de Goppa clássicos

Sejam $F/\mathbb{F}_q$ um corpo de funções de gênero g, $P_1, ..., P_n$ lugares distintos de grau 1, D o divisor definido por $D := \sum_{i=1}^{n} P_i$ e G um divisor tal que $P_i \notin suppG$ para todo $1 \leq i \leq n$.

Seja x uma função em $\mathscr{L}(G)$. Para todo $i = 1, ..., n$, temos $v_{P_i}(x) \geq -v_{P_i}(G) = 0$, isto é, $x \in O_{P_i}$. Podemos, então, tomar a classe $x(P_i)$ no corpo residual F_{P_i},

que é igual a $\mathbb{F}_q$, já que $[F_{P_i} : \mathbb{F}_q] = \deg P_i = 1$. Consideramos a seguinte aplicação linear:

$$\begin{aligned} ev_D : \ & \mathscr{L}(G) \to \mathbb{F}_q^n \\ & x \to (x(P_1), ..., x(P_n)). \end{aligned} \tag{3.1}$$

Definição 3.1.1. O código geométrico de Goppa $C_{\mathscr{L}}(D, G)$ é a imagem de $\mathscr{L}(G)$ pela aplicação ev_D, isto é,

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

Teorema 3.1.2. *$C_{\mathscr{L}}(D, G)$ é um código $[n, k, d]$ tal que*

$$k = \dim G - \dim(G - D) \qquad e \qquad d \geq n - \deg G.$$

Se $\deg G < n$, então $k = \dim G \geq \deg G + 1 - g$ e, se $2g - 2 < \deg G < n$ ocorre igualdade.

Demonstração. Seja $x \in \ker(ev_D) = \{x \in \mathscr{L}(G) \mid x(P_i) = 0 \ i = 1, ..., n\}$. Então, $v_{P_i}(x) \geq 1 = -v_{P_i}(G - D)$, para $i = 1, ..., n$, e $v_P(x) \geq -v_P(G) = -v_P(G - D)$ para todo lugar de $F/\mathbb{F}_q$ diferente de $P_1, ..., P_n$, donde $x \in \mathscr{L}(G - D)$. Por outro lado, se $x \in \mathscr{L}(G-D)$, então $v_{P_i}(x) \geq -v_{P_i}(G-D) = 1$, donde $x \in P_i$ e $x(P_i) = 0$, isto é, $x \in \ker(ev_D)$. Logo, $\ker(ev_D) = \mathscr{L}(G - D)$.

Pela construção do código $C_{\mathscr{L}}(D, G)$, temos $k = \dim G - \dim(G - D)$.

Se $\deg G < n = \deg D$, temos $\deg(G - D) = \deg G - \deg D < 0$. Assim, $\dim(G - D) = 0$, isto é, a aplicação ev_D é injetiva. Então, usando o Teorema de Riemann-Roch, temos $k = \dim G \geq \deg G + 1 - g$ e ocorre a igualdade se $2g - 2 < \deg G < n$.

Agora, escolhemos $0 \neq x \in \mathscr{L}(G)$ tal que $w(ev_D(x)) = d$. Temos que d componentes de $ev_D(x)$ são não-nulas e $n - d$ componentes são nulas. Assim, existem $n - d$ lugares no suporte de D que são zeros de x, digamos $P_1, ..., P_{n-d}$. Então, $x \in \mathscr{L}(G - \sum_{i=1}^{n-d} P_i)$, donde $0 \leq \deg(G - \sum_{i=1}^{n-d} P_i) = \deg G - n + d$. □

Nota 3.1.3. Note que, no caso em que $\deg G < n$, o Teorema 3.1.2 nos dá $k+d \geq n+1-g$ e, pela cota de Singleton, já tínhamos $k+d \leq n+1$. Assim,

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

Isso significa que o gênero age como uma medida de quanto os parâmetros do código desviam da cota de Singleton.

Exemplo 3.1.4. Se consideramos $\mathbb{F}_q(x)/\mathbb{F}_q$ o corpo de funções racionais e escolhemos $P_1, ..., P_n$, $1 \leq n \leq q+1$, lugares distintos de grau 1, D o divisor definido por $D := \sum_{i=1}^{n} P_i$ e G um divisor tal que $suppG \cap \{P_1, ..., P_n\} = \emptyset$, o código $C_{\mathscr{L}}(D, G)$ é dito código de Goppa Racional. Note que, nesse caso, sempre podemos calcular a dimensão de $C_{\mathscr{L}}(D, G)$, de fato:

Se $\deg G < 0$, então $k = \dim G - \dim(G - D) = 0$ pela Proposição 2.2.7.

Se $0 < \deg G < n$, como $g = 0$, temos $k + d = n + 1$, donde $k = \deg G + 1$ e $d = n - \deg G$.

Se $\deg G \geq n$, temos $k = n$. De fato, como $\deg(G - D) = \deg G - n \geq 0$ e $g = 0$, o Teorema de Riemann-Roch garante que $\dim(G - D) = \deg G - n + 1$. Assim:

$$k = \dim G - \dim(G - D) = \dim G - \deg G + n - 1 \leq n.$$

Agora, suponha por absurdo que $k = \dim G - \dim(G - D) < n$. Então:

$$\dim G - \deg G + n - 1 < n \Longrightarrow \dim G - \deg G - 1 < 0,$$

que é um absurdo pelo Teorema de Riemann-Roch. Portanto, $k = n$.

No primeiro Capítulo, vimos que outra maneira de definirmos um código é através de sua matriz geradora. Como ev_D é injetiva quando $\deg G < n$, se $\{x_1, x_2, ..., x_k\}$ é uma base para $\mathscr{L}(G)$, então $\{ev_D(x_1), ..., ev_D(x_k)\}$ é uma base

para $C_{\mathscr{L}}(D,G)$. Assim, uma matriz geradora para o código é definida por:

$$M = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ \vdots & \vdots & & \vdots \\ x_k(P_1) & x_k(P_2) & \dots & x_k(P_n) \end{pmatrix}.$$

Isto é, o problema de encontrar uma matriz geradora do código se reduz a determinar uma base para o espaço $\mathscr{L}(G)$.

Exemplo 3.1.5. Voltamos a considerar o código $C_{\mathscr{L}}(D,G)$ definido sobre o corpo de funções racionais $\mathbb{F}_q(x)/\mathbb{F}_q$ de gênero zero. Vamos determinar uma base para o espaço $\mathscr{L}(G)$ no caso em que $\deg G < n$ e outra para $C_{\mathscr{L}}(D,G)$. Separamos em dois casos: $n \leq q$ e $n = q+1$.

Caso $n \leq q$. Existe pelo menos um lugar P de grau 1 que não está no suporte de D. Considere um dos lugares P_i $(1 \leq i \leq n)$ de grau 1, digamos P_1. Como $\deg(P_1 - P) = 0$, o Teorema de Riemann-Roch garante que $\dim(P_1 - P) = 1$ e, pelo Corolário 2.2.11, $P_1 - P$ é o divisor principal de alguma função $0 \neq z \in \mathbb{F}_q(x)$. Então, $1 = \deg P_1 = \deg P = [\mathbb{F}_q(x) : \mathbb{F}_q(z)]$, isto é, z é um elemento primitivo para $\mathbb{F}_q(x)/\mathbb{F}_q$. Pelo Exemplo 3.1.4, temos $\deg G = k-1 \geq 0$ e, assim, o divisor $(k-1)P - G$ tem grau 0 e dimensão 1. Novamente, existe $0 \neq u \in \mathbb{F}_q(x)$ tal que $(k-1)P - G = (u)$.

Sejam $Q \in \mathbb{P}_{\mathbb{F}_q(x)}$ e $0 \leq j \leq k-1$. Temos:

$$v_Q(z^j u) = j v_Q(z) + v_Q(u) = (k-1-j)v_Q(P) + j v_Q(P_1) - v_Q(G) \geq -v_Q(G),$$

isto é, $uz^j \in \mathscr{L}(G)$. Agora, suponhamos que para $j = 0, ..., k-1$ existam $c_j \in \mathbb{F}_q$ não todos nulos tais que $\sum_{j=0}^{k-1} c_j u z^j = 0$. Seja $0 \leq l \leq k-1$ o menor índice tal que $c_l \neq 0$. Então, $\sum_{j=l+1}^{k-1} c_j u z^j = -c_l u z^l$ e

$$l = v_{P_1}(-c_l u z^l) = v_{P_1}\Big(\sum_{j=l+1}^{k-1} c_j u z^j\Big) \geq \min_{l+1 \leq j \leq k-1} \big\{ v_{P_1}(c_j u z^j) \big\} \geq l+1,$$

o que é uma contradição. Assim, $u, uz, ..., uz^{k-1}$são linearmente independentes sobre $\mathbb{F}_q$. Como $\deg G = k-1$, temos $\dim G = \deg G + 1 - g = k$ e, assim, $\{u, uz, ..., uz^{k-1}\}$ é uma base para $\mathscr{L}(G)$. Portanto, basta tomar as classes dessas funções para obter uma base para $C_{\mathscr{L}}(D, G)$. Isto é, uma matriz geradora do código é dada por:

$$M = \begin{pmatrix} u(P_1) & u(P_2) & ... & u(P_n) \\ u(P_1)z(P_1) & u(P_2)z(P_2) & ... & u(P_n)z(P_n) \\ \vdots & \vdots & & \vdots \\ u(P_1)(z(P_1))^{k-1} & u(P_2)(z(P_2))^{k-1} & ... & u(P_n)(z(P_n))^{k-1} \end{pmatrix}.$$

No caso em que $n = q+1$, podemos escolher uma função $z \in \mathbb{F}_q(x)$ tal que P_n é pólo de z. Como no caso anterior, $(k-1)P_n - G = (u)$ para $0 \neq u \in \mathbb{F}_q(x)$ e $\{u, uz, ..., uz^{k-1}\}$ é base para $\mathscr{L}(G)$. Notando que:

$$v_{P_n}(uz^j) = v_{P_n}((k-1)P_n - G) + jv_{P_n}(z) = k-1-j,$$

temos $(uz^j)(P_n) = 0$ para todo $0 \leq j < k-1$ e $(uz^{k-1})(P_n) = \alpha \in \mathbb{F}_q$. Assim, substituindo u por $\alpha^{-1}u$, obtemos

$$M = \begin{pmatrix} u(P_1) & u(P_2) & ... & u(P_{n-1}) & 0 \\ u(P_1)z(P_1) & u(P_2)z(P_2) & ... & u(P_{n-1})z(P_{n-1}) & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ u(P_1)(z(P_1))^{k-1} & u(P_2)(z(P_2))^{k-1} & ... & u(P_{n-1})(z(P_{n-1}))^{k-1} & 1 \end{pmatrix}$$

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

Exemplo 3.1.6. Vamos aplicar o que foi estudado no Exemplo 3.1.5 a um código racional definido sobre o corpo de funções $\mathbb{F}_4(x)/\mathbb{F}_4$.

$\mathbb{F}_4(x)/\mathbb{F}_4$ possui 5 lugares de grau 1, a saber: P_∞ (o pólo de x), P_0 (o zero de x), P_1 (o zero de $x-1$), P_2 e P_3 (os zeros de x^2+x+1 e, para $i = 2, 3$, representamos por α_i a raiz associada a P_i). Vamos considerar o código de Goppa $C_{\mathscr{L}}(D, G)$

sobre $\mathbb{F}_4(x)/\mathbb{F}_4$, onde D e G são os divisores definidos por $D := P_1 + P_2 + P_\infty$ e $G := P_0$. Como $\deg G = 1$, o Exemplo 3.1.4 garante que $k = \deg G + 1 = 2$ e $d = n - \deg G = 2$, isto é, $C_{\mathscr{L}}(D, G)$ é um código $[3, 2, 2]$.

Temos que $\deg(P_1 - P_3) = 0$ e, pelo Teorema de Riemann-Roch, $\dim(P_1 - P_3) = 1$, já que $g = 0$. Assim, pelo Corolário 2.2.11, $P_1 - P_3$ é o divisor principal de alguma função $0 \neq z \in \mathbb{F}_4(x)$. De fato, $P_1 - P_3 = \left(\frac{x-1}{x-\alpha_3}\right)$. Da mesma forma, $P_3 - G$ é o divisor principal de $u = \frac{x-\alpha_3}{x} \in \mathbb{F}_4(x)$.

Como foi feito no Exemplo 3.1.5, temos que $\{u, zu\}$ é uma base para $\mathscr{L}(G)$, já que u e zu são linearmente independentes sobre $\mathbb{F}_4$ e $\dim G = 2$. Então, para determinar uma matriz geradora para $C_{\mathscr{L}}(D, G)$ basta tomar $ev_D(u)$ e $ev_D(zu)$, onde ev_D é a aplicação definida em 3.1. Utilizando os resultados do Exemplo 2.1.9, temos:

$$\begin{aligned}
u(P_1) &= \left(\frac{x-\alpha_3}{x}\right)(P_1) = 1 + \alpha_3 = \alpha_2; \\
(uz)(P_1) &= \left(\frac{x-1}{x}\right)(P_1) = 0; \\
u(P_2) &= \left(\frac{x-\alpha_3}{x}\right)(P_2) = \frac{\alpha_2 + \alpha_3}{\alpha_2} = (\alpha_2)^{-1} = \alpha_3; \\
(uz)(P_2) &= \left(\frac{x-1}{x}\right)(P_2) = \frac{\alpha_2 + 1}{\alpha_2} = \frac{\alpha_3}{\alpha_2} = (\alpha_3)^2 = \alpha_3 + 1 = \alpha_2; \\
u(P_\infty) &= \left(\frac{x-\alpha_3}{x}\right)(P_\infty) = 1; \\
(uz)(P_\infty) &= \left(\frac{x-1}{x}\right)(P_\infty) = 1.
\end{aligned}$$

Portanto, uma matriz geradora para $C_{\mathscr{L}}(D, G)$ é dada por:

$$M = \begin{pmatrix} \alpha_2 & \alpha_3 & 1 \\ 0 & \alpha_2 & 1 \end{pmatrix}.$$

3.2 Construção II

Sejam $F/\mathbb{F}_q$ um corpo de funções de gênero g, $P_\infty, P_1, ..., P_n \in \mathbb{P}_F$ lugares distintos de $F/\mathbb{F}_q$ de grau 1 e $E \geq 0$ um divisor de grau $2g$ tal que $P_\infty \notin suppE$.

Lema 3.2.1. *Existem $g+1$ inteiros $0 = n_0 < n_1 < ... < n_g \leq 2g$ tais que, para todo $0 \leq l \leq g$,*

$$\dim(E - n_l P_\infty) = \dim(E - (n_l + 1)P_\infty) + 1. \tag{3.2}$$

Demonstração. Consideramos a seguinte seqüência de divisores:

$$E - (2g+1)P_\infty \leq E - (2g)P_\infty \leq ... \leq E - P_\infty \leq E,$$

logo $\mathscr{L}(E - (2g+1)P_\infty) \subseteq \mathscr{L}(E - (2g)P_\infty) \subseteq ... \subseteq \mathscr{L}(E - P_\infty) \subseteq \mathscr{L}(E)$.

Temos também que $\deg E = 2g$ e $\deg(E - (2g+1)P_\infty) = 2g - 2g - 1 = -1$. Assim, pelo Teorema de Riemann-Roch, $\dim E = \deg E + 1 - g = g + 1$ e, pela Proposição 2.2.7, $\dim(E - (2g+1)P_\infty) = 0$.

Como para todo $n \in \mathbb{N}$ temos $E - nP_\infty \geq E - (n+1)P_\infty$, ainda pela Proposição 2.2.7, temos:

$$\dim(\mathscr{L}(E - nP_\infty)/\mathscr{L}(E - (n+1)P_\infty) \leq \deg(E - nP_\infty) - \deg(E - (n+1)P_\infty) = 1,$$

isto é, para todo $n \in \mathbb{N}$, $\dim(E - nP_\infty) \leq \dim(E - (n+1)P_\infty) + 1$.

Logo, existem apenas $g+1$ inteiros $0 = n_0 < n_1 < ... < n_g \leq 2g$ tais que ocorre a igualdade em 3.2. □

O Lema 3.2.1 garante que existem exatamente $g+1$ inteiros tais que $\mathscr{L}(E - n_l P_\infty) \backslash \mathscr{L}(E - (n_l + 1)P_\infty) \neq \emptyset$, isto é, para cada $0 \leq l \leq g$, podemos escolher $w_l \in \mathscr{L}(E - n_l P_\infty) \backslash \mathscr{L}(E - (n_l + 1)P_\infty)$. Como $P_\infty \notin suppE$, temos:

$$\begin{aligned} v_{P_\infty}(w_l) &\geq -v_{P_\infty}(E - n_l P_\infty) = n_l \\ v_{P_\infty}(w_l) &< -v_{P_\infty}(E - (n_l + 1)P_\infty) = n_l + 1 \end{aligned}$$

donde $v_{P_\infty}(w_l) = n_l$ para todo $0 \leq l \leq g$.

Lema 3.2.2. *$w_0, w_1, ..., w_g$ formam uma base para $\mathscr{L}(E)$.*

Demonstração. Suponha que existam $a_0, ..., a_g \in \mathbb{F}_q$ não todos nulos tais que $\sum_{l=0}^{g} a_l w_l = 0$ e seja $0 \leq k \leq g$ o menor inteiro tal que $a_k \neq 0$. Então:

$$n_k = v_{P_\infty}(w_k) = v_{P_\infty}(-a_k w_k) = v_{P_\infty}(\sum_{l=k+1}^{g} a_l w_l) \geq \min_{k+1 \leq l \leq g} \{n_l\} = n_{k+1},$$

uma contradição. Logo, $w_0, w_1, ..., w_g$ são linearmente independentes sobre $\mathbb{F}_q$ e, como $\dim E = g + 1$, tais funções formam uma base para o espaço $\mathscr{L}(E)$. □

Agora, para cada $1 \leq i \leq n$, consideramos o espaço $\mathscr{L}(E + P_i)$. Pelo Teorema de Riemann-Roch, como $\deg(E + P_i) = 2g + 1$, temos $\dim(E + P_i) = \dim E + 1$. Assim, $\mathscr{L}(E + P_i) \backslash \mathscr{L}(E) \neq \emptyset$ e podemos tomar $f_i \in \mathscr{L}(E + P_i) \backslash \mathscr{L}(E)$ para todo $1 \leq i \leq n$.

Nota 3.2.3. Na Teoria de Sistemas Lineares, considerando $\mathcal{X}$ a curva associada ao corpo de funções $F/\mathbb{F}_q$, temos que os inteiros $n_0 < n_1 < \cdots < n_g \leq deg(E) = 2g$ são as ordens no P_∞ do morfismo associado ao sistema linear $|E| := \{E + div(f) | f \in L(E) \backslash 0\}$:

$$\begin{aligned} \Phi_{w_0,...,w_g} : \quad & \mathcal{X} \longrightarrow \mathbb{P}^g \\ & P \longmapsto ((t^{e_P} w_0)(P) : \cdots : (t^{e_P} w_g)(P)), \end{aligned}$$

onde $e_P := -min\{v_P(w_0), \ldots, v_P(w_g)\}$ e $\{w_0, \ldots, w_g\}$ é uma base do espaço $mathscr L(E)$. Como referência ao assunto, indicamos [6].

Lema 3.2.4. *$w_0, w_1, ..., w_g, f_1, ..., f_n$ são linearmente independentes sobre $\mathbb{F}_q$.*

Demonstração. Suponha que exista uma combinação linear não trivial tal que

$$\sum_{l=0}^{g} a_l w_l + \sum_{i=1}^{n} b_i f_i = 0,\ a_l, b_i \in \mathbb{F}_q$$

Seja $0 < h \leq n$ tal que $b_h \neq 0$. Então:

$$\begin{aligned} -v_{P_h}(E) - 1 &= v_{P_h}(-b_h f_h) = v_{P_h}(\sum_{l=0}^{g} a_l w_l + \sum_{i \neq h} b_i f_i) \\ &\geq \min\left\{ \min_{0 \leq l \leq g} \{v_{P_h}(a_l w_l)\}, \min_{i \neq h} \{v_{P_h}(b_i f_i)\} \right\} \end{aligned}$$

Como $w_l \in \mathscr{L}(E - n_l P_\infty)$, temos $v_{P_h}(w_l) \geq -v_{P_h}(E) + n_l v_{P_h}(P_\infty) = -v_{P_h}(E)$ e, como $f_i \in \mathscr{L}(E + P_i)$, para $i \neq h$, temos $v_{P_h}(f_i) \geq -v_{P_h}(E) - v_{P_h}(P_i) = -v_{P_h}(E)$. Assim:

$$-v_{P_h}(E) - 1 = v_{P_h}(\sum_{l=0}^{g} a_l w_l + \sum_{i \neq h} b_i f_i) \geq -v_{P_h}(E),$$

o que é uma contradição.

Portanto, $b_1 = ... = b_n = 0$ e, então, $a_0 = ... = a_g = 0$. □

Seja $t \in F$ um uniformizante local em P_∞. Definimos a seqüência:

$$t_r := \begin{cases} t^r, \text{ se } r \in \mathbb{Z} \backslash \{n_0, ..., n_g\} \\ w_l, \text{ se } r = n_l \text{ para algum } 0 \leq l \leq g \end{cases} \tag{3.3}$$

Temos que $v_{P_\infty}(t_r) = r$ para todo $r \in \mathbb{Z}$. De fato:

$$v_{P_\infty}(t_r) = \begin{cases} v_{P_\infty}(t^r) = r v_{P_\infty}(t) = r, \text{ se } r \in \mathbb{N} \backslash \{n_0, ..., n_g\} \\ v_{P_\infty}(w_l) = n_l = r, \text{ se } r = n_l \text{ para algum } 0 \leq l \leq g \end{cases}$$

Pela escolha de f_i, temos ainda que $v_{P_\infty}(f_i) \geq -v_{P_\infty}(E + P_i) = 0$ para todo $1 \leq i \leq n$. Então, pela Proposição 2.1.15, cada função f_i pode ser representada de uma única forma pela expansão $f_i = \sum_{r \geq 0} a_{r,i} t_r$, onde $a_{r,i} \in \mathbb{F}_q$.

Fixando um inteiro positivo $g \leq m < n$, definimos para cada $1 \leq i \leq n$ o vetor $c_i := (\widehat{a_{n_0,i}}, a_{1,i}, ..., \widehat{a_{n_1,i}}, a_{n_1+1,i}, ..., a_{m+g,i})$, onde $\widehat{a_{n,i}}$ representa a entrada omitida. Isto é, omitimos $g + 1$ entradas de um vetor com $m + g + 1$ coordenadas, assim c_i pode ser escrito como

$$c_i = (c_{1,i}, ..., c_{m,i}) \subseteq \mathbb{F}_q^m. \tag{3.4}$$

Definição 3.2.5. O código $C^{II} := C(m, P_\infty; P_1, ..., P_n; E)$ é o código linear associado à matriz de checagem $H := (c_1^T, ..., c_n^T)$. Note que H é matriz $m \times n$ com entradas no corpo finito $\mathbb{F}_q$.

Nota 3.2.6. Observamos que é possível obter uma construção mais geral considerando $E \geq 0$ um divisor de F/K tal que $\dim(E + \sum_{i=1}^{n}) = \dim E + n$ e $P_\infty \notin suppE$. De fato, considerando a cadeia de espaços:

$$\mathscr{L}(E - (\deg E + 1)P_\infty) \subset \mathscr{L}(E - (\deg E)P_\infty) \subset \cdots \subset \mathscr{L}(E - P_\infty) \subset \mathscr{L}(E),$$

pela Proposição 2.2.7, existem $q := \dim E$ inteiros $0 = n_1 < \cdots < n_q \leq \deg E$ tais que $\dim(E - n_l P_\infty) = \dim(E - (n_l + 1)P_\infty) + 1$ para todo $1 \leq l \leq q$. Assim, podemos escolher funções $w_l \in \mathscr{L}(E - n_l P_\infty) \setminus \mathscr{L}(E - (n_l + 1)P_\infty)$ tais que, como $P_\infty \notin suppE$, $v_{P_l}(w_l) = n_l$ e definir a seqüência $\{t_r\}_{r \in \mathbb{Z}}$ como em (3.3). Como $\dim(E + \sum_{i=1}^{n}) = \dim E + n$, podemos ainda considerar as funções $f_i \in \mathscr{L}(E + P_i) \setminus \mathscr{L}(E)$ para todo $1 \leq i \leq n$, que podem ser representadas como $f_i = \sum_{r \geq 0} a_{r,i} t_r$. Por fim, definimos os vetores c_i como em (3.4) e o código linear associado à matriz de checagem $H := (c_1^t, \ldots, c_n^t)$.

A escolha pela construção do código a partir do divisor $E \geq 0$ de grau $2g$ sem P_∞ no suporte é importante, no entanto, para a comparação com as demais construções apresentadas nesse capítulo.

Teorema 3.2.7. *$C^{II} := C(m, P_\infty; P_1, ..., P_n; E)$ é um código $[n, k, d]$ com parâmetros satisfazendo:*

$$\begin{aligned} k &\geq n - m \\ d &\geq m - g + 1. \end{aligned}$$

Demonstração. Temos que a matriz de checagem H associada à C^{II} possui m linhas. Então, pela Definição 1.1.1, temos $k \geq n - m$.

Pela Proposição 1.1.3, para provar que $d \geq m - g + 1$, basta observar que quaisquer $m - g$ colunas de H são linearmente independentes sobre $\mathbb{F}_q$. Sejam $c_{i_1}, ..., c_{i_{m-g}}$, onde $1 \leq i_1 < ... < i_{m-g} \leq n$, $m - g$ colunas de H, isto é, vetores definidos como em (3.4). Suponha que existam $b_1, ..., b_{m-g}$ constantes tais que $\sum_{j=1}^{m-g} b_j c_{i_j} = 0$. Queremos mostrar que então $b_j = 0 \forall j$. Pela definição dos vetores c_{i_j}, isto quer dizer que:

$$\sum_{j=1}^{m-g} b_j a_{r,i_j} = 0 \ \forall r \in \{0, 1, ..., m+g\} \setminus \{n_0, n_1, ..., n_g\}. \tag{3.5}$$

Consideramos a função $f = \sum_{j=1}^{m-g} b_j f_{i_j} - \sum_{j=1}^{m-g} b_j \sum_{l=0}^{g} a_{n_l,i_j} w_l$, onde w_l é uma função em $\mathscr{L}(E - n_l P_\infty) \backslash \mathscr{L}(E - (n_l + 1)P_\infty)$ e $f_{i_j} \in \mathscr{L}(E + P_{i_j}) \backslash \mathscr{L}(E)$ são as funçõ es definidas na construção do código C^{II}. Sabemos que podemos expandir cada função f_{i_j} como $f_{i_j} = \sum_{r=0}^{\infty} a_{r,i_j} t_r$. Assim, temos que:

$$f = \sum_{j=1}^{m-g} b_j \sum_{r=0}^{\infty} a_{r,i_j} t_r - \sum_{j=1}^{m-g} b_j \sum_{l=0}^{g} a_{n_l,i_j} t_{n_l} = \sum_{\substack{r=0 \\ r \notin \{n_0, n_1, ..., n_g\}}}^{\infty} \left(\sum_{j=1}^{m-g} b_j a_{r,i_j} \right) t_r.$$

Usando 3.5, obtemos $f = \sum_{r \geq m+g+1} \left(\sum_{j=1}^{m-g} b_j a_{r,i_j} \right) t_r$. Se f não for nula, temos:

$$v_{P_\infty}(f) = v_{P_\infty} \left(\sum_{r \geq m+g+1} \left(\sum_{j=1}^{m-g} b_j a_{r,i_j} \right) t_r \right) \geq \min_{r \geq m+g+1} \{ v_{P_\infty}(t_r) \} = m+g+1. \tag{3.6}$$

Temos ainda que $f \in \mathscr{L}\left(E + \sum_{j=1}^{m-g} P_{i_j} \right)$ pela definição de f_{i_j} e w_l. Assim:

$$\deg((f)_\infty) \leq \deg\left(E + \sum_{j=1}^{m-g} P_{i_j} \right) = m + g. \tag{3.7}$$

Então, pela definição dos divisores de pólo e de zeros de f, pela Proposição 2.2.10 e usando (3.6) e (3.7), temos:

$$m + g + 1 \leq v_{P_\infty}(f) \leq \deg((f)_0) = \deg((f)_\infty) \leq m + g,$$

uma contradição. Assim, $f \equiv 0$, isto é, $\sum_{j=1}^{m-g} b_j f_{i_j} - \sum_{j=1}^{m-g} b_j \sum_{l=0}^{g} a_{n_l,i_j} w_l = 0$. Então, pelo Lema 3.2.4, concluimos que $b_1 = ... = b_{m-g} = 0$. □

Nota 3.2.8. Assim como na Nota 3.1.3, observamos que os parâmetros do código C^{II} satisfazem as desigualdades:

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

Proposição 3.2.9. *Seja $v = (v_1, ..., v_n) \in \mathbb{F}_q^n$. Temos que $v \in C^{II}$ se e somente se $\sum_{i=1}^{n} v_i f_i = w + u$, onde $w \in \mathscr{L}(E)$ e $v_{P_\infty}(u) \geq m + g + 1$.*

Demonstração. Cada função $f_i \in \mathscr{L}(E + P_i) \backslash \mathscr{L}(E)$ se escreve de forma única como $f_i = \sum_{r \geq 0} a_{r,i} t_r$, onde $a_{r,i} \in \mathbb{F}_q$ e t_r é a seqüência definida em (3.3). Então, para cada $1 \leq i \leq n$, temos:

$$v_i f_i = \sum_{r \geq 0} v_i a_{r,i} t_r = \sum_{r \in S} v_i a_{r,i} t_r + \sum_{\substack{r=1 \\ r \notin S}}^{m+g} v_i a_{r,i} t_r + \sum_{r \geq m+1+g} v_i a_{r,i} t_r,$$

onde $S := \{n_0, ..., n_g\}$. Somando todos os $v_i f_i's$, obtemos:

$$\begin{aligned} \sum_{i=1}^{n} v_i f_i &= \sum_{i=1}^{n} \left(\sum_{r \in S} v_i a_{r,i} t_r + \sum_{\substack{r=1 \\ r \notin S}}^{m+g} v_i a_{r,i} t_r + \sum_{r \geq m+1+g} v_i a_{r,i} t_r \right) = \qquad (3.8) \\ &= \sum_{i=1}^{n} \sum_{r \in S} v_i a_{r,i} t_r + \sum_{i=1}^{n} \sum_{\substack{r=1 \\ r \notin S}}^{m+g} v_i a_{r,i} t_r + \sum_{i=1}^{n} \sum_{r \geq m+1+g} v_i a_{r,i} t_r. \end{aligned}$$

Pela definição do código C^{II}, temos que $v \in C^{II}$ se e somente se $\sum_{i=1}^{n} a_{r,i} v_i = 0$ para todo $r \in \{0, ..., m + g\} \backslash \{n_0, ..., n_g\}$, isto é, o somatório (3.8) torna-se:

$$\sum_{i=1}^{n} v_i f_i = \sum_{i=1}^{n} \sum_{r \in S} v_i a_{r,i} t_r + \sum_{i=1}^{n} \sum_{r \geq m+1+g} v_i a_{r,i} t_r.$$

Temos que $w := \sum_{i=1}^{n} \sum_{r \in S} v_i a_{r,i} t_r \in \mathscr{L}(E)$, já que $t_r = w_l$ se $r = l \in S$ e, pelo Lema 3.2.2, $\{w_0, w_1, ..., w_g\}$ é uma base para $\mathscr{L}(E)$.

Temos ainda que:

$$\begin{aligned} v_{P_\infty}\left(\sum_{i=1}^{n}\sum_{r\geq m+1+g} v_i a_{r,i} t_r\right) &\geq \min_{1\leq i\leq n}\left\{\min_{r\geq m+1+g}\{v_{P_\infty}(v_i a_{r,i} t_r)\}\right\} \\ &= \min_{r\geq m+1+g}\{r\} = m+g+1, \end{aligned}$$

isto é, $u := \sum_{i=1}^{n}\sum_{r\geq m+1+g} v_i a_{r,i} t_r$ é tal que $v_{P_\infty}(u) \geq m+g+1$.

Por fim, observamos que a representação é única. De fato: suponhamos que $w_1+u_1 = \sum_{i=1}^{n} f_i v_i = w_2+u_2$, onde $w_1, w_2 \in \mathscr{L}(E)$ e $v_{P_\infty}(u_i) \geq m+g+1, i = 1, 2$. Então, $w_1 - w_2 = u_2 - u_1$, ou seja, $v_{P_i}(w_1 - w_2) = v_{P_i}(u_2 - u_1) \geq m+g+1$. Dessa forma, teríamos $w_1 - w_2 \in \mathscr{L}(E-(m+g+1)P_\infty)$. Porém, como $m \geq g$, temos que $\deg(E-(m+g+1)P_\infty) = 2g-m-1-g < 0$, donde $\mathscr{L}(E-(m+g+1)P_\infty) = \emptyset$. Portanto, $w_1 = w_2$ e $u_1 = u_2$. □

3.3 Construção III

Sejam $F/\mathbb{F}_q$ um corpo de funções de gênero g, $P_\infty, P_1, ..., P_n$ lugares distintos de $F/\mathbb{F}_q$ de grau 1 e $L \geq 0$ um divisor não-especial de grau g.

Primeiro, precisamos garantir a existência de L. Apresentamos aqui um Lema que garante a existência de um tal divisor L, mas antes precisamos de um resultado auxiliar.

Lema 3.3.1. *Seja* $T \subseteq \{P \in \mathbb{P}_F \mid \deg P = 1\}$ *tal que* $|T| \geq g$. *Se* $P_1, ..., P_g$ *são* g *lugares de* $F/\mathbb{F}_q$ *pertencentes a* T *e* $A \geq 0$ *é um divisor com* $\dim A = 1$ *e* $\deg A \leq g-1$, *então existe um índice* $j \in \{1, ..., g\}$ *tal que* $\dim(A + P_j) = 1$.

Demonstração. Suponha por absurdo que a afirmação seja falsa, isto é, $\dim(A + P_j) > 1$ para todo $j \in \{1, ..., g\}$. Então, para cada $1 \leq j \leq g$, existe $z_j \in \mathscr{L}(A+P_j)\backslash\mathscr{L}(A)$. Temos $v_{P_j}(z_j) = -v_{P_j}(A) - 1$ e $v_{P_i}(z_j) \geq -v_{P_i}(A)$ para $i \neq j$. Assim, se $a_0, ..., a_g$ são constantes não todas nulas tais que $a_0 + \sum_{i=1}^{g} a_i z_i = 0$,

tomando $l > 0$ o menor índice tal que $a_l \neq 0$, temos $-a_l z_l = a_0 + \sum_{i=l+1}^{n} a_i z_i$ e, portanto:

$$\begin{aligned} -v_{P_l}(A) - 1 &= v_{P_l}(z_l) = v_{P_l}(-a_l z_l) \\ &= v_{P_l}\left(a_0 + \sum_{i=l+1}^{n} a_i z_i\right) \geq \min_{l+1 \leq i \leq n} \{v_{P_l}(a_i z_i)\} \geq -v_{P_l}(A), \end{aligned}$$

uma contradição. Logo, $1, z_1, ..., z_g$ são linearmente independentes sobre $\mathbb{F}_q$. Seja D um divisor tal que $D \geq A + P_1 + ... + P_g$ e $\deg D = 2g - 1$. Pelo Teorema de Riemann-Roch, temos $\dim D = g$. Por outro lado, $1, z_1, ..., z_g \in \mathscr{L}(A + P_1 + ... + P_g) \subseteq \mathscr{L}(D)$, donde $\dim D \geq g + 1$, o que é uma contradição. Logo, existe um índice $1 \leq j \leq g$ tal que $\dim(A + P_j) = 1$. □

Lema 3.3.2. *Seja T o conjunto definido no Lema 3.3.1. Então, existe um divisor não-especial $L \geq 0$ tal que $\deg L = g$ e $suppL \subseteq T$.*

Demonstração. Consideramos o divisor $A = 0$, temos $\mathscr{L}(A) = \mathscr{L}(0) = \mathbb{F}_q$. Isto é, A é um divisor tal que $\dim A = 1$ e $\deg A \leq g - 1$. Então, pelo Lema 3.3.1, existe $i_1 \in \{1, ..., g\}$ tal que $\dim(P_{i_1}) = 1$. Da mesma forma, encontramos divisores

$$0 < P_{i_1} < P_{i_1} + P_{i_2} < ... < P_{i_1} + P_{i_2} + ... + P_{i_g} =: L$$

tais que $\dim(P_{i_1} + ... + P_{i_j}) = 1$ para todo $j = 1, ..., g$. Em particular, $\dim L = 1$ e $\deg L = g$. Portanto,

$$\deg L + 1 - g = g + 1 - g = 1 = \dim L,$$

isto é, L é divisor não-especial de grau g. □

Um resultado mais geral sobre a existência de um divisor não-especial de grau g foi apresentado por Ballet e LeBrigand em [1].

Agora, notamos que para cada $1 \leq i \leq n$, $L + P_i$ também é um divisor não-especial, isto é, $\dim(L + P_i) = \deg L + \deg P_i + 1 - g = \dim L + 1$. Assim,

$\mathscr{L}(L+P_i)\backslash\mathscr{L}(L) \neq \emptyset$ e, então, podemos escolher $\alpha_i \in \mathscr{L}(L+P_i)\backslash\mathscr{L}(L)$. Pelo Lema 2.2.9, temos que $1, \alpha_1, ..., \alpha_n$ são linearmente independentes sobre $\mathbb{F}_q$. Como $L + \sum_{i=1}^{n} P_i$ ainda é divisor não-especial, temos $\dim(L + \sum_{i=1}^{n} P_i) = n+1$ e, portanto, $1, \alpha_1, ..., \alpha_n$ formam uma base para $\mathscr{L}(L + \sum_{i=1}^{n} P_i)$.

Sejam $t \in F$ um uniformizante local em P_∞ e $v := v_{P_\infty}(L) \geq 0$. Pela escolha das funções α_i com $1 \leq i \leq n$, temos

$$v_{P_\infty}(\alpha_i) \geq -v_{P_\infty}(L) - v_{P_\infty}(P_i) = -v_{P_\infty}(L) = -v.$$

Então, pela Proposição 2.1.15, podemos expandir cada α_i na forma $\alpha_i = t^{-v} \sum_{r\geq 0} b_{r,i} t^r$, onde $b_{r,i} \in \mathbb{F}_q$. Definimos as constantes

$$c_{r,i} := \begin{cases} b_{r-1,i}, \text{ se } 1 \leq r \leq v \\ b_{r,i}, \text{ se } r \geq v+1 \end{cases}$$

e os vetores $c_i := (c_{1,i}, ..., c_{m,i}) \in \mathbb{F}_q^m$, onde $g \leq m < n$ é um inteiro fixo.

Definição 3.3.3. O código $C^{III} := C(m, P_\infty; P_1, ..., P_n; L)$ é o código associado à matriz de checagem $H = (c_1^T, ..., c_n^T)$. Note que H é matriz $m \times n$ com entradas no corpo finito $\mathbb{F}_q$.

Teorema 3.3.4. *$C^{III} := C(m, P_\infty; P_1, ..., P_n; L)$ é um código $[n, k, d]$ com parâmetros satisfazendo:*

$$\begin{aligned} k &\geq n - m \\ d &\geq m - g + 1. \end{aligned}$$

Demonstração. Como a matriz de checagem H de C^{III}, possui m linhas, temos $k \geq n - m$.

Pela Proposição 1.1.3, precisamos provar que quaisquer $m-g$ colunas da matriz de checagem H são linearmente independentes sobre $\mathbb{F}_q$ para obter a cota para a

distância mínima. Como no Teorema 3.2.7, vamos tomar $m-g$ colunas de H, $c_{i_1}, ..., c_{i_{m-g}}$, onde $1 \leq i_1 < ... < i_{m-g} \leq n$ e supor que existam $a_1, ..., a_{m-g} \in \mathbb{F}_q$ tais que $\sum_{j=1}^{m-g} a_j c_{i_j} = 0$, isto é,

$$\sum_{j=1}^{m-g} a_j b_{r,i_j} = 0 \ \forall r \in \{0, 1, ..., m\} \setminus \{v\}. \tag{3.9}$$

Seja $f = \sum_{j=1}^{m-g} a_j \alpha_{i_j} - \sum_{j=1}^{m-g} a_j b_{v,i_j}$, onde $\alpha_{i_j} \in \mathscr{L}(L + P_{i_j}) \backslash \mathscr{L}(L)$ são as funções definidas na construção do código C^{III}. Sabemos que cada g_{i_j} pode ser expandido de maneira única como $\alpha_i = t^{-v} \sum_{r \geq 0} b_{r,i} t^r$, onde t é um uniformizante local em P_∞. Assim, a função f torna-se:

$$f = t^{-v} \sum_{j=1}^{m-g} a_j \sum_{r \geq 0} b_{r,i_j} t^r - \sum_{j=1}^{m-g} a_j b_{v,i_j} = t^{-v} \sum_{r \neq v} \left(\sum_{j=1}^{m-g} a_j b_{r,i_j} \right) t^r.$$

Usando (3.9), temos $f = t^{-v} \sum_{r \geq m+1} \left(\sum_{j=1}^{m-g} a_j b_{r,i_j} \right) t^r$. Se f não for nula, temos:

$$v_{P_\infty}(f) = v_{P_\infty} \left(t^{-v} \sum_{r \geq m+1} \left(\sum_{j=1}^{m-g} a_j b_{r,i_j} \right) t^r \right) \geq -v + \min_{r \geq m+1} \{ v_{P_\infty}(t^r) \} = m + 1 - v. \tag{3.10}$$

Além disso, $f \in \mathscr{L}\left(L - vP_\infty + \sum_{j=1}^{m-g} P_{i_j} \right)$, já que se P é um lugar de F/K temos:

$$v_P(f) = v_P \left(\sum_{j=1}^{m-g} a_j g_{i_j} - \sum_{j=1}^{m-g} a_j b_{v,i_j} \right) \geq \min_{1 \leq j \leq m-g} \left\{ v_P(a_j g_{i_j}), v_P(a_j b_{v,i_j}) \right\}.$$

Portanto, $\deg((f)_\infty) \leq \deg\left(L - vP_\infty + \sum_{j=1}^{m-g} P_{i_j} \right) = m - v$ e, usando (3.10), obtemos:

$$m + 1 - v \leq v_{P_\infty}(f) \leq \deg((f)_0) = \deg((f)_\infty) \leq m - v,$$

uma contradição. Logo, $f \equiv 0$ e então $a_1 = ... = a_{m-g} = 0$, donde $c_{i_1}, ..., c_{i_{m-g}}$ são linearmente independentes sobre $\mathbb{F}_q$ e obtemos a cota desejada para a distância mínima de C^{III}. □

Nota 3.3.5. Como observamos nas duas primeiras construções (Notas 3.1.3 e 3.2.8 respectivamente), temos que os parâmetros de C^{III} satisfazem:

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

Proposição 3.3.6. *$v=(v_1,...,v_n) \in \mathbb{F}_q^n$ é uma palavra do código C^{III} se e somente se $\sum_{i=1}^{n} v_i\alpha_i = u+w$, onde $u \in \mathbb{F}_q$ e $v_{P_\infty}(w) \geq m+1-v_{P_\infty}(L)$.*

Demonstração. Pela Definição 3.3.3, $v \in C^{III}$ se e somente se $\sum_{i=1}^{n} v_i c_{r,i} = 0$ para todo $1 \leq r \leq m$, isto é, se e somente se $\sum_{i=1}^{n} v_i b_{r,i} = 0$ para todo $r \in \{0,...,m\}\setminus\{v\}$. Para cada $1 \leq i \leq n$ fixado, temos $v_i\alpha_i = t^{-v}\sum_{r\geq 0} v_i b_{r,i} t^r$. Assim:

$$\begin{aligned}
\sum_{i=1}^{n} v_i\alpha_i &= t^{-v}\sum_{i=1}^{n}\sum_{r\geq 0} v_i b_{r,i}t^r = \\
&= t^{-v}\sum_{i=1}^{n}\left(v_i b_{v,i}t^v + \sum_{r\in\{0,...,m\}\setminus\{v\}} v_i b_{r,i}t^r + \sum_{r\geq m+1} v_i b_{r,i}t^r\right) = \\
&= \sum_{i=1}^{n} v_i b_{v,i} + \sum_{i=1}^{n}\sum_{r\geq m+1} v_i b_{r,i}t^{r-v}
\end{aligned}$$

Temos que:

$$\begin{aligned}
v_{P_\infty}\left(\sum_{i=1}^{n}\sum_{r\geq m+1} v_i b_{r,i}t^{r-v}\right) &\geq \min_{1\leq i\leq n}\left\{v_{P_\infty}\left(\sum_{r\geq m+1} v_i b_{r,i}t^{r-v}\right)\right\} \geq \\
&\geq \min_{1\leq i\leq n}\left\{\min_{r\geq m+1}\left\{v_{P_\infty}(v_i b_{r,i}t^{r-v})\right\}\right\} = \\
&= \min_{r\geq m+1}\{r-v\} \geq m+1-v
\end{aligned}$$

isto é, $w := \sum_{i=1}^{n}\sum_{r\geq m+1} v_i b_{r,i}t^{r-v}$ é tal que $v_{P_\infty}(w) \geq m+1-v_{P_\infty}(L)$. Além disso, definimos $u := \sum_{i=1}^{n} v_i b_{v,i} \in \mathbb{F}_q$.

Observamos ainda que a representação é única. Para tal, vamos supor que existam duas representações $u_1+w_1 = \sum_{i=1}^{n} v_i\alpha_i = u_2+w_2$, onde $u_1, u_2 \in \mathbb{F}_q$ e

$v_{P_\infty}(w_i) \geq m + 1 - v_{P_\infty}(L)$ para $i = 1, 2$. Então, $w_1 - w_2 = u_2 - u_1 \in \mathbb{F}_q$, o que é uma contradição. □

Note que os parâmetros obtidos nos Teoremas 3.2.7 e 3.3.4 são parecidos com os dos Códigos de Goppa Clássicos. Com essa motivação, vamos estudar a relação entre as construções II e III e a de Goppa. Para tal, na próxima seção, vamos apresentar um código que engloba C^{II} e C^{III} e é equivalente à construção de Goppa. Em particular, vamos obter os mesmos parâmetros de forma direta como Corolário do Teorema 3.1.2.

3.4 Construção IV

Sejam $F/\mathbb{F}_q$ um corpo de funções de gênero g, $P_1, ..., P_n \in \mathbb{P}_F$ lugares distintos de $F/\mathbb{F}_q$ de grau 1, $B \geq 0$ um divisor não-especial e $A \geq 0$ um divisor tal que $suppA \cap \{P_1, ..., P_n\} = \emptyset$.

Notamos que, para todo $1 \leq i \leq n$, $B + P_i$ ainda é um divisor não-especial, isto é, $\dim(B + P_i) = \dim B + 1$. Então, existe $h_i \in \mathscr{L}(B + P_i) \backslash \mathscr{L}(B)$. Pelo Lema 2.2.9, sabemos que $h_1, ..., h_n$ são linearmente independentes sobre $\mathbb{F}_q$. Além disso, temos que $\dim\left(B + \sum_{i=1}^{n} P_i\right) = \dim B + n$, já que $B + \sum_{i=1}^{n} P_i$ ainda é um divisor não-especial. Então, como $h_i \notin \mathscr{L}(B)$ para todo $1 \leq i \leq n$, qualquer função $h \in \mathscr{L}\left(B + \sum_{i=1}^{n} P_i\right)$ pode ser representada de maneira única como $h = \sum_{i=1}^{n} c_i h_i + w$, onde $w \in \mathscr{L}(B)$ e $c_i \in \mathbb{F}_q$.

Seja α a aplicação definida por

$$\begin{aligned} \alpha : \ \mathscr{L}\left(B + \sum_{i=1}^{n} P_i\right) &\longrightarrow \mathbb{F}_q^n \\ h &\longmapsto (c_1, ..., c_n). \end{aligned} \tag{3.11}$$

Notamos que dados $(c_1, ..., c_n) \in \mathbb{F}_q^n$ e $w \in \mathscr{L}(B)$, então para todo lugar $P \in \mathbb{P}_F$

temos:

$$v_P\left(\sum_{i=1}^{n} c_i h_i + w\right) \geq \min\{v_P(c_i h_i), v_P(w)\} \geq -v_P(B) - v_P(\sum_{i=1}^{n} P_i).$$

Assim, $\sum_{i=1}^{n} c_i h_i + w \in \mathscr{L}\left(B + \sum_{i=1}^{n} P_i\right)$ e, portanto, a aplicação α é sobrejetiva. Notamos também que $\ker \alpha = \left\{h \in \mathscr{L}\left(B + \sum_{i=1}^{n} P_i\right) \mid c_i = 0 \text{ para todo } 1 \leq i \leq n\right\} = \mathscr{L}(B)$.

Agora, tomando $A \geq 0$ um divisor de $F/\mathbb{F}_q$ tal que $suppA \cap \{P_1, ..., P_n\} = \emptyset$, temos $B + \sum_{i=1}^{n} P_i - A \leq B + \sum_{i=1}^{n} P_i$, donde $\mathscr{L}\left(B + \sum_{i=1}^{n} P_i - A\right) \subseteq \mathscr{L}\left(B + \sum_{i=1}^{n} P_i\right)$ e podemos restringir α ao subespaço $\mathscr{L}\left(B + \sum_{i=1}^{n} P_i - A\right)$.

Definição 3.4.1. O código $C^{IV} := C(A; P_1, ..., P_n; B)$ é a imagem do subespaço $\mathscr{L}\left(B + \sum_{i=1}^{n} P_i - A\right)$ pela aplicação α.

Nota 3.4.2. Podemos considerar a construção IV em uma situação mais geral tomando $B \geq 0$ um divisor de F/K tal que $\dim(B + \sum_{i=1}^{n} P_i) = \dim B + n$ (no caso em que B é um divisor não-especial, essa igualdade sempre ocorre) e $A \geq 0$ um divisor arbitrário de F/K. Para cada $1 \leq i \leq n$, temos $\dim(B + P_i) = \dim B + 1$ e, assim, podemos escolher $h_i \in \mathscr{L}(B + P_i) \setminus \mathscr{L}(B)$ como fizemos e definir a aplicação α como em (3.11). Por fim, restrigimos α ao subespaço $\mathscr{L}(B + \sum_{i=1}^{n} P_i - A)$ definindo o código como imagem dessa aplicação. Notamos que aqui não foi necessária a hipótese de que $suppA \cap \{P_1, ..., P_n\} = \emptyset$. Essa condição é importante apenas no Teorema 3.5.3, no qual provaremos a relação entre os códigos IV e de Goppa.

3.5 Relação entre as construções

Nas primeiras seções desse Capítulo, vimos quatro diferentes construções de códigos geométricos que utilizam lugares de grau 1 e divisores com características

apropriadas. É natural, então, procurar uma relação entre tais construções. Nessa seção, vamos esclarecer tal relação.

Teorema 3.5.1. *Os códigos C^{II} e C^{III} são casos particulares da construção C^{IV}.*

Demonstração. Primeiro, consideramos a notação da construção II. Pela Proposição 3.2.9, $(v_1, ..., v_n) \in \mathbb{F}_q^n$ pertence ao código C^{II} se e somente se $\sum_{i=1}^{n} v_i f_i = w + u$, onde $w \in \mathscr{L}(E)$ e $v_{P_\infty}(u) \geq m + g + 1$. Então,

$$u = \sum_{i=1}^{n} v_i f_i - w \in \mathscr{L}\left(E + \sum_{i=1}^{n} P_i - (m + g + 1)P_\infty\right).$$

Agora, notamos que $\dim E = \deg E + 1 - g$, isto é, $E \geq 0$ é um divisor não-especial, $P_1, ..., P_n$ são lugares de grau 1 distintos e $A := (m + g + 1)P_\infty \geq 0$ é tal que $suppA \cap \{P_1, ..., P_n\} = \emptyset$. Assim, C^{II} pode ser obtido como imagem da função:

$$\begin{aligned} \alpha : \quad \mathscr{L}\left(E + \sum_{i=1}^{n} P_i - A\right) &\longrightarrow \mathbb{F}_q^n \quad . \\ u = \sum_{i=1}^{n} v_i f_i - w &\longmapsto (v_1, ..., v_n) \end{aligned}$$

Da mesma forma, considerando a notação da construção III, pela Proposição 3.3.6, sabemos que $(v_1, ..., v_n) \in \mathbb{F}_q^n$ está em C^{III} se e somente se $\sum_{i=1}^{n} v_i \alpha_i = u + w$, onde $u \in \mathbb{F}_q$ e $v_{P_\infty}(w) \geq m + 1 - v_{P_\infty}(L)$. Então,

$$w = \sum_{i=1}^{n} v_i \alpha_i - u \in \mathscr{L}\left(L + \sum_{i=1}^{n} P_i - (m + 1)P_\infty\right).$$

Como $L \geq 0$ é divisor não-especial, $P_1, ..., P_n$ são lugares de grau 1 distintos e $A := (m+1)P_\infty \geq 0$ é tal que $suppA \cap \{P_1, ..., P_n\} = \emptyset$, o código C^{III} é a imagem da função:

$$\begin{aligned} \alpha : \quad \mathscr{L}\left(L + \sum_{i=1}^{n} P_i - A\right) &\longrightarrow \mathbb{F}_q^n \quad . \\ w = \sum_{i=1}^{n} v_i \alpha_i - u &\longmapsto (v_1, ..., v_n) \end{aligned}$$

Assim, concluimos que C^{II} e C^{III} podem ser vistos através da construção C^{IV} se escolhemos os divisores A e B (segundo a notação da construção IV) de forma apropriada. □

Definição 3.5.2. Dizemos que dois códigos $C_1, C_2 \subseteq \mathbb{F}_q^n$ são equivalentes se existem $\lambda_1, ..., \lambda_n \in \mathbb{F}_q \backslash \{0\}$ tais que $C_2 = \{(\lambda_1 u_1, ..., \lambda_n u_n) \mid (u_1, ..., u_n) \in C_1\}$.

Note que códigos equivalentes possuem os mesmos parâmetros, isto é, ambos são códigos $[n, k, d]$.

Teorema 3.5.3. *O código C^{IV} é equivalente ao código de Goppa Clássico $C_{\mathscr{L}}(D; G)$, onde G é um divisor de $F/\mathbb{F}_q$ equivalente a $G_1 := B + \sum_{i=1}^{n} P_i - A$ e $D := \sum_{i=1}^{n} P_i$.*

Demonstração. Consideramos a notação e as funções $h_i \in \mathscr{L}(B+P_i) \backslash \mathscr{L}(B)$ definidas na construção do código C^{IV}. Pelo Teorema da Aproximação Fraca, podemos encontrar uma função $z \in F$ tal que $v_{P_i}(z) = -v_{P_i}(h_i) = v_{P_i}(B) + 1$ para todo $1 \leq i \leq n$. Então, $v_{P_i}(zh_i) = 0$, donde $zh_i \in O_{P_i}$ e podemos tomar as classes $(zh_i)(P_i) \in \mathbb{F}_q^*$ para todo $1 \leq i \leq n$.

Definimos o divisor $G := B + \sum_{i=1}^{n} P_i - A - (z)$ e, como $supp A \cap \{P_1, ..., P_n\} = \emptyset$ por hipótese, notamos que $v_{P_i}(G) = 0$, isto é, $supp G \cap \{P_1, ..., P_n\} = \emptyset$. Como G e G_1 são equivalentes, temos que os espaços $\mathscr{L}(G)$ e $\mathscr{L}(G_1)$ são isomorfos pela aplicação $\varphi(h) := zh$. Consideramos também as aplicações ev_D e α definidas em (3.1) e (3.11) respectivamente. Temos o seguinte diagrama:

$$\begin{array}{ccc} \mathscr{L}(G_1) & \xrightarrow{\varphi} & \mathscr{L}(G) \\ {\scriptstyle \alpha} \searrow & & \swarrow {\scriptstyle ev_D} \\ & \mathbb{F}_q^n & \end{array}$$

Note que, por Definição, o código C^{IV} é a imagem da aplicação α, isto é, $C^{IV} = \alpha(\mathscr{L}(G_1))$.

Para demonstrar a equivalência dos códigos, precisamos provar que qualquer palavra de $C_{\mathscr{L}}(D;G)$ é igual a $(\lambda_1 c_1, ..., \lambda_n c_n)$ onde $(c_1, ..., c_n) \in C^{IV}$ e $\lambda_1, ..., \lambda_n$ são constantes não nulas.

Seja u uma palavra de $C_{\mathscr{L}}(D;G)$, podemos escrever $u = ((zh)(P_1), ..., (zh)(P_n))$ para alguma função $h \in \mathscr{L}(G_1)$. Sabemos que qualquer função $h \in \mathscr{L}(G_1)$ pode ser escrita como $h = \sum_{i=1}^{n} c_i h_i + w$, onde $w \in \mathscr{L}(B)$ e $c_i \in \mathbb{F}_q$. Assim, fixando $1 \leq j \leq n$, temos:

$$(zh)(P_j) = \sum_{i=1}^{n} c_i (zh_i)(P_j) + (zw)(P_j). \tag{3.12}$$

Agora, como $w \in \mathscr{L}(B)$, temos $v_{P_j}(zw) \geq v_{P_j}(B) + 1 - v_{P_j}(B) = 1$, isto é, $(zw)(P_j) = 0$. Assim, a igualdade (3.12) torna-se:

$$(zh)(P_j) = \sum_{i=1}^{n} c_i (zh_i)(P_j). \tag{3.13}$$

Como $h_i \in \mathscr{L}(B + P_i) \backslash \mathscr{L}(B)$, para todo $i \neq j$, temos $v_{P_j}(zh_i) \geq v_{P_j}(B) + 1 - v_{P_j}(B) = 1$, isto é, $(zh_i)(P_j) = 0$. Donde 3.13 torna-se $(zh)(P_j) = c_j (zh_j)(P_j)$ para cada $1 \leq j \leq n$. Definindo $\lambda_j := (zh_j)(P_j) \in \mathbb{F}_q^*$, temos que $u = (\lambda_1 c_1, ..., \lambda_n c_n)$. □

Nesse sentido, as construções I e IV são equivalentes. Em particular, podemos utilizar o Teorema 3.1.2 para estimar os parâmetros de C^{IV}:

Corolário 3.5.4. *Notação como na construção IV. Se* $\deg A > \deg B$*, então* C^{IV} *é um código* $[n, k, d]$ *com parâmetros satisfazendo:*

$$\begin{aligned} k &\geq \deg B - \deg A + n + 1 - g \\ d &\geq \deg A - \deg B. \end{aligned}$$

Demonstração. Se $\deg A > \deg B$, então o grau do divisor $G := B + \sum_{i=1}^{n} P_i - A - (z)$ definido no Teorema 3.5.3 é:

$$\deg G = \deg B + \deg \sum_{i=1}^{n} P_i - \deg A - \deg(z) = \deg B - \deg A + n < n$$

e, então, o Teorema 3.1.2 aplicado ao código $C_{\mathscr{L}}(D;G)$ nos diz que:

$$\begin{aligned} k &\geq \deg G + 1 - g = \deg B - \deg A + n + 1 - g \text{ e} \\ d &\geq n - \deg G = \deg A - \deg B. \end{aligned}$$

Como sabemos que códigos equivalentes possuem os mesmo parâmetros, provamos o Corolário. □

Ainda podemos estimar os parâmetros dos códigos C^{II} e C^{III} utilizando esse resultado e o Teorema 3.5.1.

Corolário 3.5.5. *C^{II} e C^{III} são códigos $[n,k,d]$ com parâmetros:*

$$\begin{aligned} k &\geq n - m \\ d &\geq m - g + 1. \end{aligned}$$

Demonstração. Pelo Teorema 3.5.1, o código C^{II} é caso especial do código C^{IV} escolhendo os divisores $B := E$ e $A := (m+g+1)P_\infty$. Então, pelo Corolário 3.5.4, temos:

$$\begin{aligned} k &\geq \deg B - \deg A + n + 1 - g = 2g - m - g - 1 + n + 1 - g = n - m \text{ e} \\ d &\geq \deg A - \deg B = m + g + 1 - 2g = m - g + 1. \end{aligned}$$

Da mesma forma, o código C^{III} é caso especial do código C^{IV} quando tomamos $B := L$ e $A := (m+1)P_\infty$. Então:

$$\begin{aligned} k &\geq \deg B - \deg A + n + 1 - g = g - m - 1 + n + 1 - g = n - m \text{ e} \\ d &\geq \deg A - \deg B = m - g + 1, \end{aligned}$$

como queríamos demonstrar. □

Capítulo 4

Construções utilizando lugares de grau superior

No Capítulo 3 vimos construções de Códigos Lineares utilizando apenas lugares de grau 1. O problema é que nem sempre é possível encontrar tantos lugares de grau 1 em relação ao gênero do corpo de funções quando o corpo finito é pequeno. Para contornar isso, apresentamos neste Capítulo duas construções de códigos lineares usando lugares de grau arbitrário, mostrando ainda que a primeira é equivalente a um caso particular da segunda e que ambas englobam as construções apresentadas no Capítulo 3.

4.1 Construção V

Sejam $F/\mathbb{F}_q$ um corpo de funções de gênero g, $P_1, ..., P_s$ lugares de $F/\mathbb{F}_q$ tais que $\deg P_i = k_i$, $k_i \in \mathbb{N}$, para $i = 1, ..., s$, B um divisor não-especial e $A \geq 0$ um divisor tal que $suppA \cap \{P_1, ..., P_s\} = \emptyset$.

Nota 4.1.1. Na primeira vez que essa construção foi apresentada por Niederreiter, Xing e Lam em [3], era exigido que B fosse um divisor positivo não-especial de

grau g. A construção apresentada aqui (devida a Özbudak e Stichtenoth em [4]) é, portanto, mais geral.

Para cada $i = 1, ..., s$, temos que o divisor $B + P_i$ ainda é não-especial, assim: $\dim(B + P_i) = \deg B + k_i + 1 - g = \dim B + k_i$. Então, existem k_i elementos distintos $f_{i,1}, ..., f_{i,k_i}$ em $\mathscr{L}(B + P_i) \setminus \mathscr{L}(B)$ linearmente independentes.

Lema 4.1.2. *Cada função* $f \in \mathscr{L}\left(B + \sum_{i=1}^{s} P_i\right)$ *possui representação única na forma* $f = \sum_{i=1}^{s} \sum_{j=1}^{k_i} c_{i,j} f_{i,j} + w$, *onde* $c_{i,j} \in \mathbb{F}_q$ *e* $w \in \mathscr{L}(B)$.

Demonstração. Para cada $1 \leq i \leq s$, seja h_i uma combinação linear de $f_{i,1}, ..., f_{i,k_i}$ de forma que $\sum_{i=1}^{s} h_i = 0$. Seja $1 \leq l \leq s$ um índice tal que $h_l \neq 0$. Então, $-h_l = \sum_{i \neq l} h_i$. Temos que $v_{P_l}(-h_l) = -v_{P_l}(B) - 1$. De fato, caso contrário, teríamos $v_{P_l}(h_l) \geq -v_{P_l}(B)$, donde $h_l \in \mathscr{L}(B)$, o que contradiz a independêcia linear das funções $f_{l,1}, \ldots, f_{l,k_l}$ sobre $\mathbb{F}_q$ (modulo $\mathscr{L}(B)$). Por outro lado, como $h_i \in \mathscr{L}(B + P_i)$ para todo $1 \leq i \leq s$, então:

$$v_{P_l}\left(\sum_{i \neq l} h_i\right) \geq \min_{i \neq l} \{v_{P_l}(h_i)\} \geq -v_{P_l}(B).$$

Assim, obtemos uma contradição. Donde, $f_{1,1}, ..., f_{1,k_1}, ..., f_{s,1}, ..., f_{s,k_s}$ são linearmente independentes sobre $\mathbb{F}_q$.

Agora, definimos $n := \sum_{i=1}^{s} k_i$. Temos que o divisor $B + \sum_{i=1}^{s} P_i$ é não-especial e, assim, $\dim\left(B + \sum_{i=1}^{s} P_i\right) = \deg B + n + 1 - g = \dim B + n$. Então, como $f_{i,j} \in \mathscr{L}(B + P_i) \setminus \mathscr{L}(B)$ para todo $i = 1, ..., s$ e $j = 1, ..., k_i$, obtemos o resultado desejado. □

Definimos a aplicação linear e sobrejetiva:

$$\begin{array}{rccc} \alpha: & \mathscr{L}\left(B + \sum_{i=1}^{s} P_i\right) & \to & \mathbb{F}_q^n \\ & f & \longmapsto & (c_{1,1}, ..., c_{1,k_1}, ..., c_{s,1}, ..., c_{s,k_s}) \end{array} \tag{4.1}$$

cujo núcleo é:

$$\ker \alpha = \left\{ h \in \mathscr{L}\left(B + \sum_{i=1}^{n} P_i\right) \mid c_{i,j} = 0 \text{ para todo } 1 \leq i \leq s,\ 1 \leq j \leq k_i \right\} = \mathscr{L}(B).$$

Como $A \geq 0$, temos que $B + \sum_{i=1}^{n} P_i - A \leq B + \sum_{i=1}^{n} P_i$, donde podemos restringir a aplicação linear α ao subespaç o $\mathscr{L}\left(B + \sum_{i=1}^{n} P_i - A\right)$.

Definição 4.1.3. O código $C^V := C(A; P_1, ..., P_s; B)$ é a imagem de $\mathscr{L}\left(B + \sum_{i=1}^{n} P_i - A\right)$ pela aplicação α.

Claramente, essa é uma generalização da construção IV e, portanto, do código de Goppa clássico. Na próxima seção, apresentaremos a construção do código C^{VI}, que generaliza a construção clássica de forma natural.

4.2 Construção VI

Sejam $F/\mathbb{F}_q$ um corpo de funções de gênero g, $P_1, ..., P_s$ lugares de $F/\mathbb{F}_q$, G um divisor tal que $suppG \cap \{P_1, ..., P_s\} = \emptyset$ e C_i códigos lineares com parâmetros $[n_i, k_i := \deg P_i, d_i]$ para $i = 1, ..., s$.

Fixando $1 \leq i \leq s$, como $k_i := \deg P_i = [F_{P_i} : \mathbb{F}_q]$, temos que existe um isomorfismo $\mathbb{F}_q$-linear entre F_{P_i} e $\mathbb{F}_{q^{k_i}}$. Então, existe também um isomorfismo $\mathbb{F}_q$-linear π_i de F_{P_i} sobre C_i.

Definimos $n := \sum_{i=1}^{s} n_i$ e a aplicação linear:

$$\begin{array}{rccc} \pi: & \mathscr{L}(G) & \to & \mathbb{F}_q^n \\ & f & \longmapsto & (\pi_1(f(P_1)), ..., \pi_s(f(P_s))) \end{array} \tag{4.2}$$

Definição 4.2.1. O código $C^{VI} := C(P_1, ..., P_s; G; C_1, ..., C_s)$ é a imagem de $\mathscr{L}(G)$ pela aplicação π, isto é,

$$C^{VI} = \{(\pi_1(f(P_1)), ..., \pi_s(f(P_s))) \mid f \in \mathscr{L}(G)\}.$$

Note que se $k_i := \deg P_i = 1$ e $n_i = 1$ para todo $1 \leq i \leq s$, então π_i é a aplicação identidade e, assim, a construção VI é exatamente a construção de Goppa neste caso.

Proposição 4.2.2. *Suponha que* $\deg G < \sum_{i=1}^{s} k_i$.

Sejam $Y := \left\{ S \subseteq \{1, ..., s\} \mid \sum_{i \in S} k_i \leq \deg G \right\}$ *e* $\delta := \min \left\{ \sum_{i \notin S} d_i \mid S \in Y \right\}$. *Então,* C^{VI} *é um código* $[n, k, d]$ *com parâmetros*

$$k = \dim G \geq \deg G + 1 - g$$

$$d \geq \delta.$$

Demonstração. Seja f uma função no núcleo da aplicação π, isto é, $f \in \mathscr{L}(G)$ tal que $\pi(f) = 0$. Então, P_i é zero da função f para todo $1 \leq i \leq s$, donde $f \in \mathscr{L}\left(G - \sum_{i=1}^{s} P_i\right)$. Como $\deg G < \sum_{i=1}^{s} k_i$, temos que $\deg\left(G - \sum_{i=1}^{s} P_i\right) < 0$ e isto implica que $\dim\left(G - \sum_{i=1}^{s} P_i\right) = 0$. Assim, $f \equiv 0$, o que significa que π é injetiva e, assim, $k = \dim G$. Por fim, $k = \dim G \geq \deg G + 1 - g$ pelo Teorema de Riemann-Roch.

Sejam d a distância mínima de C^{VI}, f em $\mathscr{L}(G)$ uma função não nula tal que $\pi(f)$ tem peso d e S o conjunto $\{i \in \{1, ..., s\} \mid f(P_i) = 0\}$. Como $f \in \mathscr{L}\left(G - \sum_{i \in S} P_i\right)$, temos $\deg\left(G - \sum_{i \in S} P_i\right) \geq 0$, isto é, $\deg G \geq \sum_{i \in S} k_i$. Assim, $S \in Y$ e, então, $\sum_{i \notin S} d_i \geq \delta$. Portanto, como

$$d = w(\pi(f)) = \sum_{i=1}^{s} w(\pi_i(f(P_i))) = \sum_{i \in S} w(\pi_i(f(P_i))) + \sum_{i \notin S} w(\pi_i(f(P_i))),$$

e $f(P_i) = 0$ para todo $i \in S$, temos

$$d = \sum_{i \notin S} w(\pi_i(f(P_i))) \geq \sum_{i \notin S} d_i \geq \delta,$$

como queríamos demonstrar. □

Nota 4.2.3. Observamos que a demonstração da Proposição 4.2.2 nos dá o seguinte resultado: suponha que $\deg G < \sum_{i=1}^{s} k_i$ e considere f uma função não nula de $\mathscr{L}(G)$. Se $S := \{1 \leq i \leq s \mid f(P_i) = 0\}$, então $w(\pi(f)) \geq \sum_{i \notin S} d_i$, onde w é o peso.

Observamos ainda que podemos ter $S = \emptyset$, ou seja, nenhum P_i é zero da função f. Neste caso, $\sum_{i \notin S} d_i = \sum_{i=1}^{s} d_i$.

4.3 Relação entre as construções

Teorema 4.3.1. *A construção V é um caso particular da construção VI em que* $C_i := \mathbb{F}_q^{k_i}$ *e* $[n_i, k_i, d_i] = [k_i, k_i, 1]$ *para* $1 \leq i \leq s$.

Demonstração. Sejam f_{ij} em $\mathscr{L}(B + P_i) \backslash \mathscr{L}(B)$, $1 \leq i \leq s$ e $1 \leq j \leq k_i$, as funções linearmente independentes sobre $\mathbb{F}_q$ definidas na construção V. Fixando $1 \leq i \leq s$, temos que $v_{P_i}(f_{ij}) = -v_{P_i}(B) - 1$ para todo $1 \leq j \leq k_i$. Então, podemos utilizar o Teorema da Aproximação Fraca, para encontrar uma função $z \in F$ tal que $v_{P_i}(z) = -v_{P_i}(f_{ij})$. Assim, $v_{P_i}(zf_{ij}) = 0$, donde $zf_{ij} \in O_{P_i}$. Agora, fixando $1 \leq i \leq s$ e supondo que existem constantes $c_1, ..., c_{k_i}$ em $\mathbb{F}_q$ não todas nulas tais que $\sum_{j=1}^{k_i} c_j (zf_{ij})(P_i) = 0$, temos que $v_{P_i}\left(\sum_{j=1}^{k_i} c_j (zf_{ij})\right) > 0$, isto é, $v_{P_i}(z) + v_{P_i}\left(\sum_{j=1}^{k_i} c_j f_{ij}\right) > 0$. Então: $v_{P_i}(z) > -v_{P_i}\left(\sum_{j=1}^{k_i} c_j f_{ij}\right)$. Pelo Lema 4.1.2, temos que $v_{P_i}\left(\sum_{j=1}^{k_i} c_j f_{ij}\right) = -v_{P_i} - 1$, donde:

$$v_{P_i}(z) > v_{P_i}\left(\sum_{j=1}^{k_i} c_j f_{ij}\right) = v_{P_i}(B) + 1 = -v_{P_i}(f_{ij}),$$

o que é uma contradição, já que $v_{P_i}(z) = -v_{P_i}(f_{ij})$ por definição. Portanto, $c_1 = ... = c_{k_i} = 0$ e provamos que $\{(zf_{ij})(P_i) \mid 1 \leq j \leq k_i\}$ é uma base para $F_{P_i} := O_{P_i}/P_i$ sobre $\mathbb{F}_q$.

Para cada $1 \leq i \leq s$, definimos a aplicação linear:

$$\begin{array}{rccc} \pi_i: & F_{P_i} & \to & C_i := \mathbb{F}_q^{k_i} \\ & (zf_{ij})(P_i) & \longmapsto & e_j^{(i)} \end{array}$$

onde $e_j^{(i)}$ representa o j-ésimo vetor da base canônica de $\mathbb{F}_q^{k_i}$. Definimos ainda o divisor $G := B + \sum_{i=1}^{s} P_i - A - (z)$, onde $A \geq 0$ é um divisor tal que $suppA \cap \{P_1, ..., P_s\} = \emptyset$ (como assumido na construção V) e notamos que para todo $1 \leq i \leq s$, temos:

$$v_{P_i}(G) = v_{P_i}\left(B + \sum_{i=1}^{s} P_i - A - (z)\right) = v_{P_i}(B) + 1 - v_{P_i}(B) - 1 = 0,$$

isto é $suppG \cap \{P_1, ..., P_s\} = \emptyset$. Consideramos, então, o isomorfismo:

$$\begin{array}{rccc} \varphi: & \mathscr{L}\left(B + \sum_{i=1}^{s} P_i - A\right) & \to & \mathscr{L}(G) \\ & f & \longmapsto & zf \end{array}$$

e as aplicações α e π definidas em (4.1) e (4.2) respectivamente. Assim, construimos o diagrama:

$$\begin{array}{ccc} \mathscr{L}\left(B + \sum_{i=1}^{s} P_i - A\right) & \xrightarrow{\varphi} & \mathscr{L}(G) \\ & \alpha \searrow \quad \swarrow \pi & \\ & \mathbb{F}_q^n & \end{array}$$

Para concluir que os códigos definidos pelas imagens das aplicações α e π são equivalentes, precisamos provar que, para $1 \leq l \leq s$ fixo, temos $\pi_l((zf)(P_l)) = (c_{l,1}, ..., c_{l,k_l})$, onde $(c_{1,1}, ..., c_{1,k_1}, ..., c_{s,1}, ..., c_{s,k_s})$ é uma palavra do código V. Pelo Lema 4.1.2, podemos escrever qualquer função $f \in \mathscr{L}\left(B + \sum_{i=1}^{s} P_i - A\right)$ como $f = \sum_{i=1}^{s}\sum_{j=1}^{k_i} c_{i,j} f_{i,j} + w$, onde $c_{i,j} \in \mathbb{F}_q$ e $w \in \mathscr{L}(B)$.Então:

$$\begin{aligned} \pi_l((zf)(P_l)) &= \pi_l\left(\sum_{i=1}^{s}\sum_{j=1}^{k_i} c_{ij}(zf_{ij})(P_l) + (zw)(P_l)\right) = \\ &= \sum_{i=1}^{s}\sum_{j=1}^{k_i} c_{ij}\pi_l\left((zf_{ij})(P_l)\right) + \pi_l\left((zw)(P_l)\right). \end{aligned}$$

Agora, notamos que

$$v_{P_l}(zf_{ij}) = v_{P_l}(z) + v_{P_l}(f_{ij}) = -v_{P_l}(f_{lj}) + v_{P_l}(f_{ij}) \geq 1 - v_{P_l}(P_i),$$

isto é, se $i \neq l$, então $zf_{ij} \in P_l$ e $(zf_{ij})(P_l) = 0$. Da mesma forma:

$$v_{P_l}(zw) = v_{P_l}(z) + v_{P_l}(w) \geq -v_{P_l}(f_{lj}) - v_{P_l}(B) = 1,$$

donde $zw \in P_l$ e $(zw)(P_l) = 0$. Portanto:

$$\pi_l((zf)(P_l)) = \sum_{j=1}^{k_l} c_{lj}\pi_l\left((zf_{lj})(P_l)\right) = (c_{l,1}, ..., c_{l,k_l}),$$

e, então, os códigos são equivalentes. □

Corolário 4.3.2. *Notação como na construção V. Suponhamos que* $\deg B < \deg A$ *e definamos o conjunto* $Y := \left\{ S \subseteq \{1, ..., s\} \mid \sum_{i \notin S} k_i \geq \deg A - \deg B \right\}$ *e o inteiro* $\delta := \min\{|\{1, ..., s\} \setminus S| \mid S \in Y\}$. *Então,* C^V *é um código* $[n, k, d]$ *com parâmetros:*

$$\begin{aligned} k &\geq \deg B + n - \deg A + 1 - g \\ d &\geq \delta, \end{aligned}$$

Demonstração. Segundo o Teorema 4.3.1, basta tomar $G := B + \sum_{i=1}^{s} P_i - A - (z)$ na Proposição 4.2.2. □

O Teorema 4.3.1 garante que a construção VI é a mais geral dentre as apresentadas nessa dissertação, já que engloba todas as novas abordagens de códigos lineares apresentadas nos capítulos 3 e 4, além de ser uma generalização simples dos Códigos de Goppa Clássicos.

Mais do que isso, se C_1 é um código $[n, k, d]$ qualquer, então é possível escrevê-lo como um código do tipo VI. De fato, considerando $F = \mathbb{F}_q(x)$ o corpo de funções

racionais, P_∞ o pólo de x e $P \neq P_\infty$ um lugar de $\mathbb{F}_q(x)/\mathbb{F}_q$ de grau k. Usando a construção VI, obtemos o código $C(P;(k-1)P_\infty;C_1)$ como imagem da aplicação:

$$\begin{array}{rccc} \mu: & \mathscr{L}((k-1)P_\infty) & \rightarrow & \mathbb{F}_q^n \\ & f & \mapsto & \pi(f(P)) \end{array}$$

onde π é um isomorfismo linear de F_P em C_1. Portanto, $C_1 = C(P;(k-1)P_\infty;C_1)$ e, então, a construção VI é realmente a mais abrangente de todas as apresentadas.

Referências Bibliográficas

[1] Stéphane Ballet and Dominique Le Brigand. On the existence of non-special divisors of degree g and g - 1 in algebraic function fields over fq. *Journal of Number Theory*, 116(2):293–310, 2006.

[2] Harald Niederreiter and Chaoping Xing. *Rational Points on Curves over Finite Fields: Theory and Applications*. London Mathematical Society Lecture Note Series. Cambridge University Press, 2001.

[3] Harald Niederreiter, Chaoping Xing, and Kwok Yan Lam. A new construction of algebraic-geometry codes. *Applicable Algebra in Engineering, Communication and Computing*, 9:373–381, 1999.

[4] Ferruh Özbudak and Henning Stichtenoth. Constructing codes from algebraic curves. *IEEE Transactions on Information Theory*, 45(7):2502–2505, Novembro 1999.

[5] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Spriger-Verlag, 1993.

[6] Karl-Otto Stöhr and José Felipe Voloch. Weierstrass points and curves over finite fields. *Proc. Lond. Math. Soc., III. Ser.*, 52:1–19, 1986.

[7] Chaoping Xing, Harald Niederreiter, and Kwok Yan Lam. Constructions of algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(4):1186–1193, Maio 1999.

[8] Chaoping Xing, Harald Niederreiter, and Kwok Yan Lam. A generalization of algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(7):2498–2501, Novembro 1999.