Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Códigos Lineares Disjuntos e Corpos de Funções Algébricas

por

Pryscilla dos Santos Ferreira Silva
sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Fevereiro/2011
João Pessoa - PB

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Códigos Lineares Disjuntos e Corpos de Funções Algébricas

por

Pryscilla dos Santos Ferreira Silva
sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Fevereiro/2011
João Pessoa - PB

S586c Silva, Pryscilla dos Santos Ferreira.

Códigos lineares disjuntos e corpos de funções algébricas / Pryscilla dos Santos Ferreira Silva. – João Pessoa: [s.n.], 2011.

73f.

Orientador: Antônio de Andrade e Silva.

Dissertação (Mestrado) - UFPB/CCEN.

1.Matemática. 2.Códigos lineares disjuntos. 3.Código algébrico geométrico.

UFPB/BC CDU: 51(043)

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Códigos Lineares Disjuntos e Corpos de Funções Algébricas

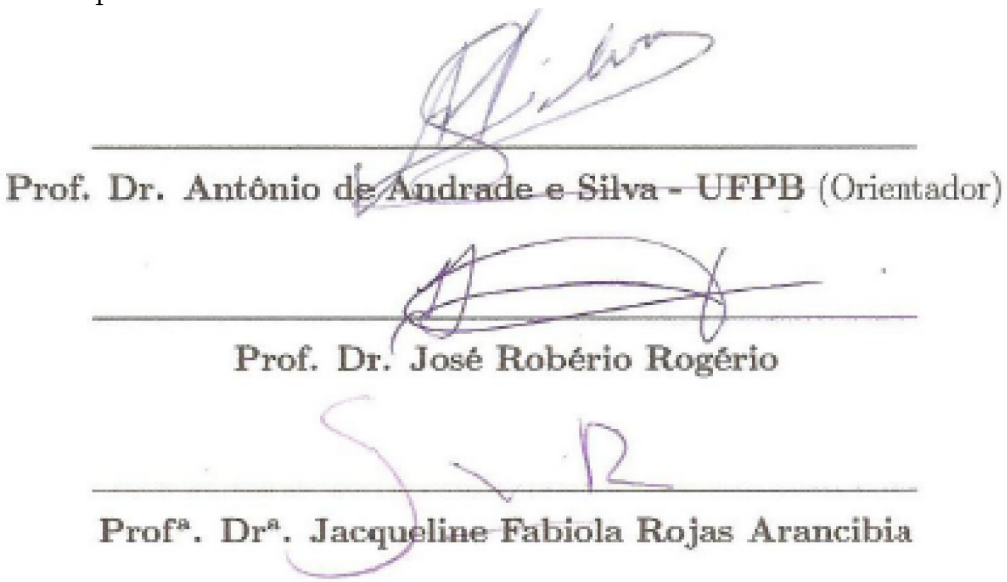
por

Pryscilla dos Santos Ferreira Silva

Dissertação apresentada ao Departamento de Matemática da Universidade Federal da Paraíba, como requisito parcial para a obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:



Dedicatória

Aos meus pais e a minha irmã.

Agradecimentos

A Deus pelo apoio incondicional.

Ao professor Andrade, pelos conselhos para uma vida toda.

Aos meus "irmãos do coração" Maikon, Geraldo, Claudemir e Josué pelos momentos de apoio nos nossos intermináveis grupos de estudo.

A todos os meus professores no mestrado, com atenção especial a professora Jaqueline pela sua paciência e dedicação.

As minhas amigas Taty, Vivi, Cecilia e Andrea. A dona Auta minha "mãe paraibana". Aos meus amigos Marcos, Eduardo, Elano e aos demais colegas do mestrado. Ao meu namorado Henrique pelo seu apoio e boa vontade.

Por fim a Capes pelo apoio financeiro.

Resumo

Neste trabalho, baseados em corpos de funções algébricas, forneceremos construções de códigos lineares disjuntos. Além disso, nós estudaremos comportamentos assintóticos de códigos lineares disjuntos a partir da nossa construção.

Palavras chave- Corpos de funções algébricas, código algébrico geométrico, códigos lineares disjuntos.

Abstract

In this work, based on algebraic function fields, we give constructions of disjoint linear codes. In addition,we study the asymptotic behavior of disjoint linear codes from our constructions.

Key words- Algebraic function fields, algebraic-geometry code, disjoint linear codes.

Notação

- $\mathbb{F}_q$ - corpo finito com q elementos onde q é a potência de um número primo;
- $\lceil x \rceil$ - função maior inteiro aplicada em x, isto é, $\lceil x \rceil := min\{n \in \mathbb{Z};\ x \leq n\}$;
- [ ] - indica referências;
- $\langle v_1, \ \ldots \ , v_n \rangle$ - subespaço gerado por $\{v_1, \ \ldots \ , v_n\}$;
- $A \leq B$ - A é um subespaço vetorial de B;
- $\lfloor x \rfloor$ - função menor inteiro aplicada em x, isto é, $\lfloor x \rfloor := max\{n \in \mathbb{Z};\ n \leq x\}$;
- $|C|$ - cardinalidade de um conjunto C;
- $(m_1, \ldots , m_n)$ - ideal gerado por $m_1, \ldots , m_n$;
- $\deg(p)$ - grau do polinômio p(x);
- $[F : K]$ - dimensão de F como $K-$ espaço vetorial, onde o corpo F é uma extensão do corpo K;
- F/K - considerando que F e K são corpos, significa que F é um corpo de funções sobre K;
- $\deg P$ - grau do divisor P.

Sumário

Introdução

Histórico

O artigo "A teoria matemática da comunicação" de Claude Shannon publicado em 1948 marcou o nascimento da Teoria da Codificação, um campo de estudo relacionado com a transmissão de dados e a recuperação de mensagens corrompidas. Em pouco mais de meio século, a Teoria da Codificação viveu um crescimento fenomenal, com ampla aplicação em áreas que vão desde sistemas de comunicação para leitores de discos compactos a tecnologia de armazenamento.

Apesar dos problemas da Teoria da Codificação surgirem frequentemente das aplicações da engenharia, é fascinante observar a relação íntima entre a matemática e o desenvolvimento da teoria. A importância da álgebra, geometria e combinatória na área de codificação é um fato geralmente reconhecido, com profundidade de muitos resultados matemáticos.

Mas, não só a matemática auxilia diretamente no estudo dos códigos como a Teoria da Codificação também traz grandes contribuições para a matemática. Um exemplo disso é o estudo das funções *resilient,* que necessitam da existência de Códigos Lineares Disjuntos para a veracidade de alguns resultados. Logo, os recursos dos códigos não são apenas para engenheiros e cientistas da computação mas também para os matemáticos.

Dentre os muitos códigos estudados sem dúvida os mais importantes para esta dissertação são os Códigos de Goppa e os Códigos Concatenados. Os Códigos Concatenados têm criação atribuída a Forney cuja primeira aparição foi no artigo de mesmo autor "Codigos Concatenados" de 1966. Os Códigos de Goppa são atribuídos a Goppa e surgiram pela primeira vez no seu artigo "Códigos associados com divisores" publicado em 1977.

O estudo de Códigos de Goppa está diretamente ligado aos estudos de Corpos de Funções Algébricas, afinal foi justamente Goppa que utilizou corpos de funções algébricas na construção dos códigos que levam o seu nome. Os corpos de funções algébricas são tipos especiais de extensões de corpos e ocorrem naturalmente em vários ramos da matemática como a geometria algébrica, teoria dos números e a teoria das superfícies compactas de Riemann. Daí pode-se estudar corpos de funções algébricas a partir de pontos de vista muito diferentes.

Entretanto, a exposição puramente algébrica da teoria dos corpos de funções algébricas é que irá nortear todo o trabalho desenvolvido nesse texto. E essa abordagem aliada aos códigos mencionados anteriormente nos permitirá, considerando corpos de funções algébricas sobre corpos finitos, obter códigos lineares disjuntos e cotas para o número de códigos lineares disjuntos.

Descrição do trabalho

Esta dissertação é constituída de quatro capítulos.

No Capítulo 1, apresentamos os conceitos básicos relativos a Teoria de Corpos de Funções Algébricas, pois esses conceitos permeiam a maioria dos resultadaos abordados. Além da definição de corpos de funções algébricas, vamos estudar temas como: divisores,corpos de funções racionais e espaços de Riemann-Roch.

No Capítulo 2, fazemos uma breve discussão sobre Extensões Algébricas de Corpos de Funções Algébricas juntamente com o Teorema e a Cota de Hasse-Weil.

No Capítulo 3, fornecemos alguns resultados básicos da Teoria da Codificação. Em seguida, definiremos Códigos de Goppa e Códigos Concatenados expondo alguns resultados e exemplos.

Finalmente, no Capítulo 4,com base no artigo "Disjoint Linear Codes From Algebraic Function Fields", construiremos Códigos Lineares Disjuntos sobre corpos finitos. Além disso vamos estimar a quantidade de códigos dessa natureza bem como fazer análises de.comportamentos assintóticos obtidos a partir de uma família de códigos cuja existência é devida a essa construção.

Capítulo 1

Corpos de Funções Algébricas

Definições e resultados básicos da teoria de corpos de funções algébricas como valorizações, lugares, gênero de um corpo de funções, são fundamentais ao estudo de códigos algébricos geométricos, um dos temas principais do nosso trabalho. Considerando essas noções básicas veremos o conceito de Divisores bem como o Teorema de Riemann.

1.1 Noções Preliminares

Como já havíamos mencionado a definição de lugar é fundamental para o nosso estudo, mas antes apresentaremos algumas definições e resultados relativos a extensões de corpos. O leitor interessado em mais detalhes pode consultar [3].

Seja K um corpo. Uma *extensão* de K é um corpo F que contém K. Note que podemos considerar F como um espaço vetorial sobre K. Assim, o *grau* de F sobre K é a dimensão de F como espaço vetorial sobre K. Notação: $[F : K]$. Se $[F : K]$ é finita, dizemos que F é uma *extensão finita* de K. Se $K \subseteq F \subseteq L$ é uma torre de corpos, então verifica-se que

$$[L : K] = [L : F][F : K].$$

Além disso, se $[L : K] < \infty$, então $[L : F] < \infty$ e $[F : K] < \infty$.

Seja F uma extensão de K. Um elemento $a \in F$ é chamado *algébrico* sobre K se existir $f \in K[X]$, não nulo, tal que $f(a) = 0$. Note que dentre todos os polinômios não nulos $f \in K[X]$ tal que $f(a) = 0$ existe um único polinômio de menor grau mônico e irredutível p tal que $p(a) = 0$ e será denotado por

$$p = \mathrm{irr}(a, K).$$

Um elemento que não é algébrico é chamado *transcendente*. Se todo elemento de F for algébrico sobre K, dizemos que F é uma *extensão algébrica* de K. Verifica-se que toda extensão finita é algébrica e que o conjunto dos elementos de F que são algébricos sobre K é um subcorpo de F.

Proposição 1.1 *Sejam K um corpo e $f \in K[x]$. Então o anel quociente*

$$F = \frac{K[x]}{(f)} = \{g + (f) : g \in K[x]\}$$

é um corpo se, e somente se, f é um polinômio irredutível sobre K. Em particular, se $\deg f = n$, *então*

$$F = \{r + (f) : r \in K[x], \ \textit{com } r = 0 \ \textit{ou } \deg r < n\}.$$

Nesse caso, F é um espaço vetorial (extensão) sobre K de grau n, pois

$$\{1 + (f), x + (f), \ldots, x^{n-1} + (f)\}$$

é uma base para F.

Sejam F uma extensão de K e $a \in F$. A interseção de todos os subcorpos de F que contém K e a (e, portanto, o menor subcorpo de F que contém K e a) será denotada por $K(a)$. Pode ser provado que

$$K(a) = \left\{ \frac{p(a)}{q(a)} : p, q \in K[X] \text{ e } q(a) \neq 0 \right\},$$

e que se $a \in F$ é algébrico sobre K, então

$$[K(a) : K] < \infty.$$

Um *corpo de funções algébricas de uma variável* sobre K é uma extensão F de K tal que F é uma extensão finita de $K(x)$, para algum elemento $x \in F$ que é transcendente sobre K. Denotamos por F/K o corpo de funções algébricas de uma variável sobre K. Se K é um corpo finito, dizemos que F/K é um *corpo de funções global*. Com o objetivo de simplicar a notação vamos nos referir a F/K como um corpo de funções.

Proposição 1.2 *Os elementos de F que são transcendentes sobre K podem ser caracterizados como segue: $z \in F$ é transcendente sobre K se, e somente se, a extensão F de $K(z)$ é de grau finito.*

Prova. Por definição, existe $x \in F$ transcendente sobre K tal que

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

Logo, F é uma extensão algébrica sobre $K(x)$. Assim, para qualquer $z \in F$, existe

$$p(X) = \text{irr}(z, K(x)) \in K(x)[X]$$

tal que $p(z) = 0$. Portanto,

$$z^n + r_{n-1}z^{n-1} + \cdots + r_0 = 0, \ \text{onde } r_i = \frac{a_i(x)}{b_i(x)} \in K(x), \ \text{com } b_i(x) \neq 0, \ \forall \ i = 0, \ldots, n-1.$$

Pondo $b(x) = b_0(x) \cdots b_{n-1}(x) \in K(x)^*$, obtemos

$$b(x)p(z) = b(x)z^n + b(x)a_{n-1}(x)z^{n-1} + \cdots + b(x)a_0(x) = 0. \tag{1.1}$$

Note que essa expressão pode ser considerada como um polinômio com coeficientes em $K(z)$ aplicado em x. Além disso, esse polinômio é não nulo, pois seu termo constante é

$$b(0)z^n + b(0)a_{n-1}(0)z^{n-1} + \cdots + b(0)a_0(0)$$

desde que z é transcendente sobre K. Assim, pela equação (1.1), x é algébrico sobre $K(z)$. Nesse caso,

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

de modo que F é uma extensão algébrica sobre $K(z, x)$, pois

$$K(x) \subseteq K(x, z) \subseteq F.$$

Portanto,

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

Reciprocamente, suponhamos, por absurdo que z seja algébrico sobre K. Então

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

o que é uma contradição. ■

O conjunto

$$\widetilde{K} = \{z \in F : z \text{ é algébrico sobre } K\}$$

é um subcorpo de F. O corpo $\widetilde{K}$ é chamado o *corpo de constantes* de F/K.

Proposição 1.3 *Seja F um corpo de funções sobre K. Então $\widetilde{K}$ é algebricamente fechado em F, isto é, qualquer elemento de $F - \widetilde{K}$ é transcendente sobre $\widetilde{K}$.*

Prova. Seja $z \in F$ algébrico sobre $\widetilde{K}$. Então existe $p \in \widetilde{K}[X]$ tal que $p(z) = 0$, onde

$$p = \text{irr}(z, \widetilde{K}) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1} + X^n.$$

Logo, z é algébrico sobre $K(c_0, \ldots, c_{n-1})$. Assim,

$$[K(c_0, \ldots, c_{n-1}, z) : K(c_0, \ldots, c_{n-1})] < \infty$$

e

$$[K(c_0, \ldots, c_{n-1}) : K] < \infty,$$

pois os $c_0, \ldots, c_{n-1}$ são algébricos sobre K. Portanto,

$$[K(c_0, \ldots, c_{n-1}, z) : K] = [K(c_0, \ldots, c_{n-1}, z) : K(c_0, \ldots, c_{n-1})][K(c_0, \ldots, c_{n-1}) : K] < \infty.$$

Neste caso, z é algébrico sobre K, ou seja, $z \in \widetilde{K}$. ■

Observação 1.4 *Se $z \in F$ é transcendente sobre K, então z é transcendente sobre $\widetilde{K}$. Além disso,*

$$K \subseteq \widetilde{K} \subseteq F$$

e F é um corpo de funções sobre $\widetilde{K}$ e $\widetilde{K} \neq F$. De fato, seja $x \in F$ transcendente sobre K. Então segue da Proposição 1.2

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

Como

$$K(x) \subseteq \widetilde{K}(x) \subseteq F.$$

Temos

$$[F : \widetilde{K}(x)] < \infty.$$

Dizemos que K é *algebricamente fechado* em F ou K é todo o corpo de constantes se $\widetilde{K} = K$.

Um corpo de funções algébricas F/K é dito um *corpo de funções racionais* se $F = K(x)$, para algum $x \in F$, que é transcendente sobre K.

Exemplo 1.5 *Se F/K é um corpo de funções racionais, então $K = \widetilde{K}$. De fato, seja*

$$z = \frac{f}{g} \in K(x), \ \ com \ \ \mathrm{mdc}(f, g) = 1,$$

algébrico sobre K. Então existem $a_0, \ldots, a_n \in K$ tais que

$$a_0 + a_1 z + \cdots + a_n z^n = 0 \Rightarrow a_0 g^n + a_1 f g^{n-1} + \cdots + a_n f^n = 0.$$

Assim,

$$f | a_0 \ \ e \ \ g | a_n.$$

Portanto, $f, g \in K$ e $z \in K$. ■

Um *anel de valorização* sobre um corpo de funções F/K é um subanel $\mathcal{O} \subseteq F$ que satisfaz as seguintes propriedades:

1. $K \subset \mathcal{O} \subset F$
2. Para qualquer $z \in F$, se $z \notin \mathcal{O}$ então, $z^{-1} \in \mathcal{O}$.

Essa definição é motivada pela seguinte observação: dado um polinômio mônico e irredutível $p \in K[x]$ o conjunto

$$\mathcal{O}_p = \left\{ \frac{f}{g} : f, g \in K[x], \ p \nmid g \ \text{ e } \ g \neq 0 \right\}$$

é um anel de valorização de $K(x)/K$. De fato, é claro que $K \subset \mathcal{O}_p \subset K(x)$. Além disso, se

$$z = \frac{f}{g} \in K(x), \ \ \text{com} \ \ \mathrm{mdc}(f, g) = 1,$$

então podemos supor que

$$p \nmid f \ \ \text{ou} \ \ p \nmid g,$$

de modo que se $z \notin \mathcal{O}_p$, então, $z^{-1} \in \mathcal{O}_p$. Note que se p e q são polinômios irredutíveis sobre K, então $\mathcal{O}_p \neq \mathcal{O}_q$.

Proposição 1.6 *Seja $\mathcal{O}$ um anel de valorização do corpo das funções F/K. Então as seguintes afirmações são satisfeitas*:

1. *$\mathcal{O}$ é um anel local, isto é, $\mathcal{O}$ possui um único ideal maximal $P = \mathcal{O} - \mathcal{O}^\bullet$, onde $\mathcal{O}^\bullet$ é o grupo das unidades de $\mathcal{O}$.*

2. *Seja $x \in F^*$, $x \in P$ se, e somente se, $x^{-1} \notin \mathcal{O}$.*

3. *Para o corpo $\widetilde{K}$ das constantes de F/K, obtemos $\widetilde{K} \subseteq \mathcal{O}$ e $\widetilde{K} \cap P = \{0\}$. Neste caso, $[F : K(x)] < \infty$, para todo $x \in P$.*

Prova. Confira [10, p.2, Proposition 1.1.5]. ■

Teorema 1.7 *Sejam $\mathcal{O}$ um anel de valorização do corpo de funções F/K e P seu único ideal maximal. Então*:

1. *P é um ideal principal.*

2. *Se $P = t\mathcal{O}$, então qualquer $z \in F^*$ pode ser escrito de modo única sob a forma*

$$z = t^n u,$$

para algum $n \in \mathbb{Z}$ e $u \in \mathcal{O}^\bullet$.

Prova. Confira [10, p.3, Theorem 1.1.6]. ■

Um *lugar* (*place*) P de um corpo de funções F/K é o ideal maximal de algum anel de valorização $\mathcal{O}$ de F/K. Neste caso, qualquer elemento $t \in P$ tal que $P = t\mathcal{O}$ chama-se *elemento primitivo* para P. Vamos denotar por $\mathbb{P}_F$ o conjunto de todos os lugares de F/K, em símbolos,

$$\mathbb{P}_F = \{P : P \text{ é um lugar de } F/K\}.$$

Note que existe uma correspodência biunívoca $\mathcal{O} \leftrightarrow P = t\mathcal{O}$. Como veremos a seguir

Observação 1.8 *Se $\mathcal{O}$ é um anel de valorização de F/K e P é o seu ideal maximal, então $\mathcal{O}$ é unicamente determinado por P. De fato, pelo item 2 da Proposição* 1.6*,*

$$\mathcal{O} = \{z \in F : z^{-1} \notin P\} \cup \{0\}.$$

Nesse caso, $\mathcal{O} = \mathcal{O}_P$ chama-se o anel de valorização associado ao lugar *P.*

Para darmos uma segunda descrição de lugar, vamos estender o domínio $\mathbb{Z}$ adjuntando um elemento ∞ que não pertence a $\mathbb{Z}$, isto é, o domínio estendido de $\mathbb{Z}$ é o conjunto $\mathbb{Z} \cup \{\infty\}$ munido com a adição e a multiplicação de $\mathbb{Z}$ estendida a $\mathbb{Z} \cup \{\infty\}$ por

$$\infty + \infty = \infty + m = m + \infty = \infty \text{ e } \infty > n, \ \forall \ m, n \in \mathbb{Z}.$$

Uma *valorização discreta* sobre F/K é uma função $v : F \to \mathbb{Z} \cup \{\infty\}$ satisfazendo as seguintes propriedades:

1. $v(x) = \infty$ se, e somente se, $x = 0$.

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

3. $v(x + y) \geq \min\{v(x),\ v(y)\}$, para todos $x, y \in F$. (**Desigualdade Triangular**)

4. Existe um elemento $z \in F$ tal que $v(z) = 1$.

5. $v(a) = 0$, para todo $a \in K^*$.

Note que as propriedades 2 e 4 garantem que v é sempre sobrejetora. Além disso, a propriedade 2 prova que v é um homomorfismo de grupos do grupo multiplicativo F^* no grupo aditivo de $\mathbb{Z}$.

Observação 1.9 *Sejam v uma valorização discreta sobre F/K e $c \in \mathbb{R}$, com $0 < c < 1$. Então a função $|\cdot|_v : F \to \mathbb{R}$ definida como*

$$|x|_v = \begin{cases} c^{v(x)}, & se\ x \neq 0 \\ 0, & se\ x = 0 \end{cases}$$

satisfaz as seguintes propriedades:

1. $|x|_v > 0$ *e* $|x|_v = 0$ *se, e somente se,* $x = 0$.

2. $|xy|_v = |x|_v\,|y|_v$, *para todos* $x, y \in F$.

3. $|x + y|_v \leq |x|_v + |y|_v$, *para todos* $x, y \in F$.

Neste caso, a função $|\cdot|_v$ satisfaz as propriedades semelhantes do valor absoluto usual. Além disso, uma função $|\cdot|_v$ que satisfaz as propriedades 1, 2 *e* $3'$ *a seguir*

3' $|x + y|_v \leq \max\{|x|_v, |y|_v\}$, *para todos* $x, y \in F$.

Também satisfaz a propriedade 3. *Portanto, é uma valorização discreta sobre F/K. Uma valorização satisfazendo as propriedades* 1, 2 *e* $3'$ *chama-se* não Arquimediana.

Lema 1.10 (Desigualdade Triangular Estrita) *Sejam F/K um corpo de funções, v uma valorização discreta sobre F/K e $x, y \in F$, com $v(x) \neq v(y)$. Então*

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

Prova. Pelas propriedades 2 e 5 da definição de valorização discreta, obtemos

$$v(ay) = v(a) + v(y) = 0 + v(y) = v(y),\ \ \forall\ a \in K^*.$$

Em particular, $v(-y) = v(y)$. Sendo $v(x) \neq v(y)$, podemos assumir que $v(x) < v(y)$. Suponhamos, por absurdo, que

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

Assim, pela propriedade 3 da definição de valorização discreta, obtemos

$$v(x+y) > v(x).$$

Portanto,

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

o que é um absurdo ■

Para qualquer $P \in \mathbb{P}_F$ associamos uma função $v_P : F \to \mathbb{Z} \cup \{\infty\}$ definida como segue: Escolha um elemento primitivo t para P. Então qualquer $z \in F^*$ pode ser escrito de modo único sob a forma

$$z = t^n u,$$

para algum $n \in \mathbb{Z}$ e $u \in \mathcal{O}_P^\bullet$. Agora, defina

$$v_P(z) = \begin{cases} n, & \text{se } z \neq 0 \\ \infty, & \text{se } z = 0. \end{cases}$$

Observe que a unicidade da representação garante que v_P é uma função e que esta depende apenas de P e não da escolha de t. De fato, se t_1 é um outro elemento primitivo para P, então

$$P = t\mathcal{O}_P = t_1\mathcal{O}_P.$$

Logo, existe $w \in \mathcal{O}_P^\bullet$ tal que $t = wt_1$. Portanto,

$$t^n u = (wt_1)^n u = t_1^n(uw^n),$$

para algum $uw^n \in \mathcal{O}_P^\bullet$.

Teorema 1.11 *Seja F/K um corpo de funções.*

1. *Para qualquer $P \in \mathbb{P}_F$, a função v_P é uma valorização discreta sobre F/K. Além disso,*

$$\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\},\ \mathcal{O}_P^\bullet = \{z \in F : v_P(z) = 0\} \text{ e } P = \{z \in F : v_P(z) > 0\}.$$

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

3. *Todo anel de valorização $\mathcal{O}$ de F/K é um subanel próprio maximal de F.*

4. *Se v é uma valorização discreta sobre F/K. Então o conjunto*

$$P = \{z \in F : v(z) > 0\}$$

é um lugar de F/K e

$$\mathcal{O}_P = \{z \in F : v(z) \geq 0\}$$

é o anel de valorização correspondente.

Prova. Vamos provar apenas o item 3, para os demais itens confira [10, p.5, Theorem 1.1.13]. Seja M um subanel de F tal que $\mathcal{O} \subseteq M \subseteq F$ e $M \neq F$. Suponhamos, por absurdo, que $M \neq \mathcal{O}$. Então existe $z \in M$ tal que $z \notin \mathcal{O}$.

Afirmação. $F = \mathcal{O}[z]$.

De fato, como $z \notin \mathcal{O}$ temos que $z^{-1} \in P$. Logo, $v_P(z^{-1}) > 0$. Assim, dado $y \in F$, existe, pela Lei Arquimediana, um $k \in \mathbb{N}$ tal que

$$kv_P(z^{-1}) > -v_P(y).$$

Donde

$$v_P(yz^{-k}) = kv_P(z^{-1}) + v_P(y) > -v_P(y) + v_P(y) = 0,$$

isto é, $w = yz^{-k} \in \mathcal{O}$ e $y = wz^k \in \mathcal{O}[z]$ Portanto, $F \subseteq \mathcal{O}[z]$ Neste caso, $F = M$, o que é uma contradição. ■

Sejam F/K um corpo de funções, $P \in \mathbb{P}_F$ e $\mathcal{O}_P$ seu anel de valorização. Então o anel de classes residuais

$$F_P = \frac{\mathcal{O}_P}{P} = \{x + P : x \in \mathcal{O}_P\} = \{x(P) : x \in \mathcal{O}_P\}$$

é um corpo. Estendendo F_P para $F_P \cup \{\infty\}$ definimos rara qualquer $x \in F - \mathcal{O}_P$, $x(P) = \infty$. Note que a função $\pi_P : \mathcal{O}_P \to F_P$ definida como $\pi_P(x) = x(P)$ é um epimorfismo de anéis tal que

$$\varphi = \pi_P|_{\widetilde{K}} : \widetilde{K} \to F_P$$

é injetor, pois

$$x \in \ker \varphi \Leftrightarrow x(P) = P \Leftrightarrow x \in P \Leftrightarrow x \in P \cap \widetilde{K} = \{0\}.$$

Assim, podemos considerar $\widetilde{K}$ (K) como um subcorpo de F_P. Nesse caso, a função de F em $F_P \cup \{\infty\}$ definida como, $x \mapsto x(P)$, chama-se *função de classes residuais* em relação ao lugar P. O número

$$\deg P = [F_P : K]$$

chama-se o *grau* de P. Um lugar de grau 1 é chamado um *lugar racional* de F/K.

Proposição 1.12 *Sejam F/K um corpo de funções, $P \in \mathbb{P}_F$ e $x \in P$, com $x \neq 0$. Então*

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

Prova. Segue da Proposição 1.6 que $[F : K(x)] < \infty$. Assim, basta provar que quaisquer $z_1, \ldots, z_n \in \mathcal{O}_P$ cujas classes residuais $z_1(P), \ldots, z_n(P) \in F_P$ sejam LI sobre K sejam LI sobre $K(x)$. Suponhamos, por absurdo, que existam $\varphi_i(x) \in K(x)$, não todos nulos, tais que

$$\sum_{i=1}^{n} \varphi_i(x) z_i = 0, \tag{1.2}$$

Podemos supor, sem perda de generalidade, que os $\varphi_i(x)$ são polinômios em x e que nem todos eles sejam divisíveis por x, isto é,

$$\varphi_i(x) = a_i + xg_i(x), \text{ onde } a_i \in K \text{ e } g_i(x) \in K[x],$$

e os a_i não todos nulos. Como $x \in P$ e $g_i(x) \in \mathcal{O}_P$ temos que

$$\varphi_i(x)(P) = a_i(P) = a_i, \;\; i = 1, \ldots, n.$$

Aplicando a função classe residual na equação (1.2), obtemos:

$$0 = 0(P) = \sum_{i=1}^{n} \varphi_i(x)(P) z_i(P) = \sum_{i=1}^{n} a_i z_i(P),$$

que contradiz a independência linear de $z_1(P), \ldots, z_n(P)$ sobre K. ■

Corolário 1.13 *Seja F/K um corpo de funções. Então*

$$[\widetilde{K} : K] < \infty.$$

Prova. Vamos admitir que $\mathbb{P}_F \neq \emptyset$, confira Corolário 1.16. Assim, existe $P \in \mathbb{P}_F$, de modo que

$$[F_P : K] = [F_P : \widetilde{K}][\widetilde{K} : K] \Rightarrow [\widetilde{K} : K] \leq [F_P : K] < \infty,$$

que é o resultado desejado. ■

Observação 1.14 *Sejam F/K um corpo de funções e $P \in \mathbb{P}_F$ com* $\deg P = 1$. *Então $F_P = K$, pois*

$$1 = \deg P = [F_P : K].$$

Sejam F/K um corpo de funções, $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um *zero* de z se $v_p(z) > 0$ e P é um *polo* de z se $v_P(z) < 0$. Sejam $m, n \in \mathbb{N}$. Se

$$v_P(z) = m > 0,$$

então P é um zero de z de ordem m e se

$$v_P(z) = -n < 0,$$

então P é um polo de z de ordem n,

Teorema 1.15 *Sejam F/K um corpo de funções e R um subanel de F, com $K \subseteq R \subseteq F$. Se $\{0\} \neq I \subset R$ é um ideal próprio de R, então existe $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $K \subseteq P$.*

Prova. Confira [10, p.7, Theorm 1.1.19]. ■

Corolário 1.16 *Sejam F/K um corpo de funções e $z \in F$ transcendente sobre K. Então existem $P, Q \in \mathbb{P}_F$ tal que P é um zero de z e Q é um polo de z. Em particular, $\mathbb{P}_F \neq \emptyset$.*

Prova. Consideremos o anel $R = K[z]$ e o ideal $I = zK[z]$. Note que se z é transcendente sobre K, então

$$K[z] \simeq K[X].$$

Assim, podemos identifcar $I = zK[z]$ com $XK[X]$. Logo, pelo Teorema 1.15, existe $P \in \mathbb{P}_F$ tal que $I \subseteq P$. Portanto, $z \in P$ e P é um zero de z. De modo análogo, prova-se que z^{-1} tem um zero em $Q \in \mathbb{P}_F$. Portanto, z tem um polo em Q. ■

Proposição 1.17 *Sejam F/K um corpo de funções e $P_1, \ldots, P_r$ zeros do elemento $x \in F$. Então*

$$\sum_{i=1}^{r} v_{P_i}(x) \deg P_i \leq [F : K(x)].$$

Prova. Confira [10, p.13, Proposition 1.3.3]. ■

Corolário 1.18 *Seja F/K um corpo de funções. Então qualquer $x \in F$, com $x \neq 0$, possui uma quantidade finita de zeros e de polos.*

Prova. Se x é algébrico sobre K, então $x \in \widetilde{K} \subset \mathcal{O}_P^{\bullet}$. Assim, $v_P(x) = 0$, isto é, x não possui zeros nem polos. Se x é trancendente sobre K, então pela Proposição 1.17

$$\sum_{i=1}^{r} v_{P_i}(x) \deg P_i \leq [F : K(x)].$$

Como $P_1, \ldots, P_r$ são zeros de x temos que $v_{P_i}(x) \geq 1$. Portanto,

$$r \leq [F : K(x)],$$

pois

$$\deg P_i = \dim_K(F_{P_i}) \geq 1.$$

De modo análogo, temos que o números de zeros de x^{-1} (e, portanto, o número de polos de x) é menor do que ou igual a $[F : K(x^{-1})]$. Portanto, x possui finitos zeros e polos. ■

1.2 O Corpo das Funções Racionais

Vamos investigar os conceitos de valorização e lugares no caso de um corpo de funções racionais $F = K(x)$, onde x é transcendente sobre K.

Dado um polinômio mônico e irredutível $p \in K[x]$, consideremos o anel de valorização

$$\mathcal{O}_p = \left\{ \frac{f}{g} : f, g \in K[x],\ p \nmid g \text{ e } g \neq 0 \right\}$$

Para obtermos o lugar associado a $\mathcal{O}_p$ basta determinar os elementos que não são invertíveis. De fato, como

$$\left(\frac{f}{g}\right)^{-1} = \frac{g}{f}$$

temos que esse elemento não possui inverso em $\mathcal{O}_p$ se p divide f, Portanto, o ideal maximal de $\mathcal{O}_p$, em símbolos P_p, é dado por

$$P_p = \left\{ \frac{f}{g} : f, g \in K[x],\ p \mid f,\ p \nmid g \text{ e } g \neq 0 \right\}.$$

Neste caso,

$$\mathcal{O}_p^{\bullet} = \left\{ \frac{f}{g} : f, g \in K[x],\ p \nmid f,\ p \nmid g \text{e } g \neq 0 \right\}.$$

Em particular, se $p = x - \alpha$, então escreveremos $P_\alpha = P_{x-\alpha} \in \mathbb{P}_F$.

Existe outro anel de valorização de F/K, a saber,

$$\mathcal{O}_\infty = \left\{ \frac{f}{g} : f, g \in K[x],\ \ g \neq 0 \ \text{ e } \ \deg f \leq \deg g \right\}.$$

Onde o grau do polinômio nulo é $-\infty$, com

$$-\infty + -\infty = -\infty,\ \ -\infty + n = -\infty \ \text{ e } \ -\infty < n,\ \ \forall\ n \in \mathbb{Z}.$$

Logo,

$$0 = \frac{0}{1} \in \mathcal{O}_\infty.$$

Os elementos não invertíveis de $\mathcal{O}_\infty$ são

$$\frac{f}{g},\ \text{ com } \ \deg f < \deg g,$$

desse modo o lugar correspondente a $\mathcal{O}_\infty$, chamado de *lugar infinito*, é dado por

$$P_\infty = \left\{ \frac{f}{g} : f, g \in K[x],\ \ g \neq 0 \ \text{ e } \ \deg f < \deg g \right\}.$$

A seguir apresentamos alguns resultados com o intuito de descrever melhor algumas características de $K(x)$. Um desses resultados, cuja demonstração vamos omitir, é

$$K(x) = K\left(\frac{1}{x}\right).$$

Lema 1.19 *Sejam A um anel noetheriano. Se A é um domínio de fatoração única, $a \in A^*$ e p um elemento primo em A, então existe um único $n_p \in \mathbb{Z}_+$ tal que*

$$p^{n_p} \mid a,\ \ \textit{mas}\ \ p^{n_p+1} \nmid a.$$

Prova. Suponhamos, por absurdo, que o resultado seja falso. Então, para qualquer $n = n_p \in \mathbb{Z}_+$ fixado, existe $b_n \in A$ tal que $a = p^n b_n$. Logo,

$$b_n = p b_{n+1},$$

pois $a = p^{n+1} b_{n+1}$, de modo que

$$(b_0) \subset (b_1) \subset (b_2) \subset \cdots$$

é uma cadeia estritamente crescente de ideais em A, o que é uma contradição. ■

Sejam A um domínio de fatoração única, $a \in A$ e p um elemento primo em A. A *multiplicidade* de p em a, em símbolos $v_p(a)$, é o único elemento $n_p \in \mathbb{Z}_+$ tal que

$$p^{n_p} \mid a,\ \ \text{mas}\ \ p^{n_p+1} \nmid a,$$

com $v_p(a) = \infty$ se $a = 0$. Quando $v_p(a) = 1$ ($v_p(a) > 1$), dizemos que p é um *fator simples* (*múltiplo*) do elemento a.

Proposição 1.20 *Seja F/K o corpo de funções racionais.*

1. *Seja $P = P_p \in \mathbb{P}_F$, onde $p \in K[x]$ é um polinômio mônico e irredutível sobre K. Então p é um elemento primitivo de P e sua valorização associada é definida como*

$$v_P(z) = \begin{cases} n, & se\ z = p^n \frac{f}{g} \\ \infty, & se\ z = 0, \end{cases}$$

onde $n \in \mathbb{Z}$ e $\frac{f}{g} \in \mathcal{O}_P^{\bullet}$. Além disso, o corpo das classes residuais

$$F_p = \frac{\mathcal{O}_P}{P} \simeq \frac{K[x]}{(p)},$$

$f(x) + (p) \mapsto f(x)(P)$. Consequentemente, $\deg P = \deg p$.

2. *Se $p = x - \alpha$, então $\deg P = 1$ e a função de classe residual é definida como*

$$z(P) = z(\alpha),\ \forall\ z = \frac{f}{g} \in F$$

onde $z(\alpha)$ é definido como

$$z(\alpha) = \begin{cases} \frac{f(\alpha)}{g(\alpha)}, & se\ g(\alpha) \neq 0 \\ \infty, & se\ g(\alpha) = 0, \end{cases}$$

3. *Se $P = P_\infty$, então $\deg P_\infty = 1$. Um elemento primitivo para P_∞ é*

$$t = \frac{1}{x}$$

e a valorização discreta correspondente v_∞ é definida como

$$v_\infty \left(\frac{f}{g} \right) = \deg g - \deg f.$$

A função de classe residual associada a P_∞ é definida como

$$z(P_\infty) = z(\infty),$$

onde $z(\infty)$ é definido como

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

sendo

$$z = \frac{f}{g} = \frac{a_0 + a_1 x + \cdots + a_n x^n}{b_0 + b_1 x + \cdots + b_m x^m},\ \ com\ a_n, b_m \neq 0,$$

Prova. Vamos provar apenas os itens 1 e 3, para mais informações consulte [10, p.9, Proposition 1.2.1]: 1 Note que o ideal P_p é gerado por p, pois se

$$z = \frac{f}{g} \in P_p,$$

então existe $u \in K[x]$ tal que $f = up$. Assim,

$$z = \frac{f}{u} \cdot \frac{u}{g} = p\frac{u}{g} \Rightarrow z \in p\mathcal{O}_P \Rightarrow P_p = p\mathcal{O}_P.$$

Logo, p é um elemento primitivo de P. Como $K[x]$ é um domínio de fatoração única e F é seu corpo quociente temos que qualquer elemento $z \in F$ pode ser escrito de modo único sob a forma

$$z = p^n \frac{f}{g},$$

onde $n \in \mathbb{Z}$ e $\frac{f}{g} \in \mathcal{O}_P^{\bullet}$. Assim, por definição,

$$v_P(z) = \begin{cases} n, & \text{se } z = p^n \frac{f}{g} \\ \infty, & \text{se } z = 0, \end{cases}$$

possui as propriedades desejadas.

3 Sabemos que

$$\frac{1}{x} \in P_\infty \text{ e } K(x) = K\left(\frac{1}{x}\right) \Rightarrow \left[K(x) : K\left(\frac{1}{x}\right)\right] = 1,$$

Logo, pela Proposição 1.12,

$$\deg P_\infty \leq \left[K(x) : K\left(\frac{1}{x}\right)\right] = 1 \Rightarrow \deg P_\infty = 1.$$

Note que $\frac{1}{x}$ é um elemento primitivo para P_∞, pois se

$$z = \frac{f}{g} \in P_\infty,$$

então

$$z = \frac{1}{x} \cdot \frac{xf}{g} \Rightarrow z \in \frac{1}{x}\mathcal{O}_\infty \Rightarrow P_\infty = \frac{1}{x}\mathcal{O}_\infty.$$

Os resultados que restam seguem diretamente da afirmação anterior. ■

Teorema 1.21 *Seja F/K o corpo de funções racionais. Então os únicos lugares de F/K são P_p e P_∞ com $p \in K[x]$ mônico e irredutível.*

Prova.Seja $\mathcal{O}_P$ um anel de valorização de F/K.

CASO 1

Assuma que $x \in \mathcal{O}_P$. Então $K[x] \subseteq \mathcal{O}_P$. Prova-se que o conjunto $I := K[x] \cap P$ é um ideal primo de $K[x]$.

Temos também que a aplicação de classes residuais induz o seguinte homomorfismo:

$$\begin{array}{rcl} \gamma : K[x] & \to & K(x)_P \\ f(x) & \mapsto & f(x)(P) \end{array}$$

Note que, $ker\gamma = I$. Assim, pelo Teorema do Isomorfismo: $K[x]/I \simeq Im\gamma \leq K(x)_P$.

Observe que $I \neq \{0\}$, pois se $I = \{0\}$, então $K[x]/I = K[x]$ e $Im\gamma$ teria dimensão infinita,um absurdo. Isso signfica que existe um polinômio irredutível e mônico (unicamente determinado) $p(x) \in K[x]$ tal que $I = p(x)K[x]$. Todo elemento $g(x) \in K[x]$ com $p(x) \nmid g(x)$ não está em I, assim, pela Proposição 1.6,

$$g(x) \notin P \text{ e } \frac{1}{g(x)} \in \mathcal{O}_P.$$

Logo, nós concluímos que

$$\mathcal{O}_p = \left\{ \frac{f(x)}{g(x)} : p(x) \nmid g(x) \right\} \subseteq \mathcal{O}_P$$

Segue do Teorema 1.11 que todo anel de valorização é um subanel próprio maximal de $K(x)$, logo nós temos que $\mathcal{O}_P = \mathcal{O}_p$.

CASO 2

Suponhamos agora que $x \notin \mathcal{O}_P$, então, pela Proposição 1.6, $x^{-1} \in P$, logo

$$K[x^{-1}] \subseteq \mathcal{O}_P \text{ e } x^{-1} \in P \cap K[x^{-1}].$$

Assim, como no caso anterior, temos o ideal primo $P \cap K[x^{-1}] = p(x^{-1})K[x^{-1}]$ onde $p(x^{-1}) \in K[x^{-1}]$ é um polinômio mônico e irredutível. Entretanto $p(x^{-1}) = x^{-1}$, desse modo $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$ e mais uma vez como no **CASO 1** obtemos:

$$\begin{array}{rcl} \mathcal{O}_P \supseteq \left\{ \frac{f}{g} : f,\ g \in K[x^{-1}],\ g \neq 0 \text{ e } x^{-1} \nmid g(x^{-1}) \right\} & = & \\ \left\{ \frac{a_0 \ + \ ... \ + a_n x^{-n}}{b_0 \ + \ ... \ + b_m x^{-m}},\ b_0 \neq 0 \right\} & = & \\ \left\{ \frac{a_0 x^{m+n} \ + \ ... \ + a_n x^m}{b_0 x^{m+n} \ + \ ... \ + b_m x^n},\ b_0 \neq 0 \right\} & = & \\ \left\{ \frac{u}{v} : u,\ v \in K[x],\ v \neq 0 \text{ e } \deg u \leq \deg v \right\} & = & \mathcal{O}_\infty. \end{array}$$

Assim, $\mathcal{O}_P = \mathcal{O}_\infty$. ■

Observação 1.22 *Note que se K é um corpo finito com q elementos, então, pelo teorema anterior, K possui $q+1$ lugares racionais. A saber, q lugares da forma P_α e o lugar P_∞.*

1.3 Divisores

O corpo $\widetilde{K}$ de constantes de um corpo de funções algébricas F/K é uma extensão finita do corpo K. Desde que F pode ser considerado um corpo de funções sobre $\widetilde{K}$, salvo menção

explícita em contrário, o corpo de funções F/K é tal que K é o corpo de constantes completo de F/K.

O *grupo de divisores* de F/K é definido como o grupo abeliano livre (com notação aditiva) que é gerado pelos lugares de F/K, em símbolos $\mathrm{div}(F)$. Os elementos de $\mathrm{div}(F)$ são chamados *divisores* de F/K. Em outras palavras, um divisor é a soma da forma

$$D = \sum_{P \in \mathbb{P}_F} n_P P,$$

onde $n_P \in \mathbb{Z}$ e $n_P = 0$, exceto para uma quantidade finita de $P \in \mathbb{P}_F$. O *suporte* de D é definido por:

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

Escreveremos com frequência

$$D = \sum_{P \in S} n_P P,$$

onde $S \subseteq \mathbb{P}_F$ é um conjunto finito com $\operatorname{supp} D \subseteq S$. Um divisor da forma $D = P$, onde $P \in \mathbb{P}_F$, é chamado de *divisor primo*. Dois divisores

$$D = \sum n_P P \ \text{ e } \ D' = \sum n'_P P$$

são somados da seguinte forma

$$D + D' = \sum (n_P + n'_P) P.$$

O *elemento neutro* de $\mathrm{div}(F)$ é o divisor

$$0 = \sum_{P \in \mathbb{P}_F} n_P P$$

tal que $n_P = 0$, para todo $P \in \mathbb{P}_F$. Para $Q \in \mathbb{P}_F$ e

$$D = \sum_{P \in \mathbb{P}_F} n_P P,$$

definimos $v_Q(D) = n_Q$. Assim,

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

Uma *ordem parcial* sobre $\mathrm{div}(F)$ é definida por

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

Se $D_1 \leq D_2$ e $D_1 \neq D_2$, então também escreveremos $D_1 < D_2$. Um divisor $D \geq 0$ é chamado *positivo* ou *eficaz*. Note que essa ordem não é total, pois os divisores

$$D_1 = P_1 + 2P_2 \ \text{ e } \ D_2 = 2P_1 + P_2$$

não são comparáveis.

O *grau* de um divisor $D \in \mathrm{div}(F)$ é definido como

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

Portanto, existe um homomorfismo de grupos $\varphi : \mathrm{div}(F) \longrightarrow \mathbb{Z}$ definido como $\varphi(D) = \deg D$.

Sabemos, pelo Corolário 1.18, que qualquer $x \in F$, com $x \neq 0$, transcendente sobre K possui uma quantidade finita de zeros e de polos em $\mathbb{P}_F$, o que fornece sentido as seguintes definições:

Sejam $x \in F$, com $x \neq 0$ e denote por $\mathcal{Z}$ (respectivamente $\mathcal{N}$) o conjunto de zeros (respectivamente polos) de x em $\mathbb{P}_F$. Definimos

$$(x)_0 = \sum_{P \in \mathcal{Z}} v_P(x) P$$

o *divisor zero* de x e

$$(x)_\infty = \sum_{P \in \mathcal{N}} (-v_P)(x) P$$

o *divisor polo* de x. Finalmente,

$$(x) := (x)_0 - (x)_\infty$$

o *divisor principa*l de x. Note que $(x)_0 \geq 0$, $(x)_\infty \geq 0$ e

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

Os elementos $x \in F$, com $x \neq 0$ que são algébricos (constantes) sobre K serão caracterizados por

$$x \in K \Leftrightarrow (x) = 0.$$

Nesse caso, $(x)_\infty = (x)_0 = 0$.

O conjunto de divisores

$$\mathcal{P}_F = \{(x) : x \in F^*\}$$

é chamado o *grupo de divisores principais* de F/K. Denominamos o grupo quociente

$$Cl(F) := \frac{\mathrm{div}(F)}{\mathcal{P}_F}$$

de *grupo das classes de divisores* de F/K. Para um divisor $D \in \mathrm{div}(F)$, o elemento correspondente no grupo quociente será denotado por $[D]$, a classe do divisor D. Assim, obtemos a seguinte relação de equivalência:

$$D \sim D' \Leftrightarrow [D] = [D'],$$

isto é, $D = D' + (x)$, para algum $x \in F^*$.

Lema 1.23 *Sejam K um corpo, V um espaço vetorial sobre K e W um subespaço de V. Então*

$$\dim\left(\frac{V}{W}\right) = \dim V - \dim W.$$

Prova. A função

$$\pi : V \to \frac{V}{W}$$

definida como $\pi(\mathbf{v}) = \mathbf{v}+W$ é linear e sobrejetora. Logo, pelo Teorema do Núcleo e da Imagem,

$$\dim\left(\frac{V}{W}\right) = \dim V - \dim W,$$

pois $\ker \pi = W$. ■

Para um divisor $A \in \mathrm{div}(F)$ fixado, definimos o *espaço de Riemman-Roch* associado a A como

$$\mathcal{L}(A) = \{x \in F^* : (x) \geq -A\} \cup \{0\}.$$

Observe que

$$x \in \mathcal{L}(A) \Leftrightarrow v_P(x) \geq -v_P(A), \ \forall \ P \in \mathbb{P}_F.$$

Além disso, $\mathcal{L}(A) \neq \{0\}$ se, e somente se, existe $D \in \mathrm{div}(F)$ tal que $D \sim A$, com $D \geq 0$. De fato,

$$\mathcal{L}(A) \neq \{0\} \Leftrightarrow \ \exists \ x \in F^*; \ (x) \geq -A \Leftrightarrow A + (x) \geq 0 \Leftrightarrow D = A + (x) \geq 0 \Leftrightarrow D \sim A.$$

Lema 1.24 *Sejam F/K um corpo de funções e $A \in \mathrm{div}(F)$.*

1. *$\mathcal{L}(A)$ é um K subespaço vetorial de* F.
2. *Se D é um divisor equivalente a A, então $\mathcal{L}(A) \simeq \mathcal{L}(D)$.*
3. *$\mathcal{L}(0) = K$ e $\mathcal{L}(A) = \{0\}$ se $A < 0$.*
4. *Se B é um divisor com $A \leq B$, então nós temos $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ e*

$$\dim\left(\frac{\mathcal{L}(B)}{\mathcal{L}(A)}\right) \leq \deg B - \deg \ A.$$

Prova. Confira [10, p.17 and 18, Lemmas 1.4.6, 1.4.7 and 1.4.8]. ■

Proposição 1.25 *Seja F/K um corpo de funções. Então para cada divisor $A \in \mathrm{div}(F)$ $\mathcal{L}(A)$ é um espaço vetorial sobre K de dimensão finita. Mais precisamente, se $A = A_+ - A_-$ onde os divisores A_+ e A_- são positivos, então*

$$\dim \mathcal{L}(A) \leq \deg A_+ + 1.$$

Prova. Confira [10, p.19, Proposition 1.4.9]. ■

Para cada divisor $A \in \mathrm{div}(F)$, o inteiro

$$\ell(A) = \dim \mathcal{L}(A)$$

é chamado a *dimensão* do divisor A.

Teorema 1.26 *Seja F/K um corpo de funções. Para todo $x \in F - K$, obtemos*

$$\deg(x)_0 = \deg(x)_\infty = [F : K(x)].$$

Em particular qualquer divisor principal possui grau zero.

Prova. Sejam

$$n = [F : K(x)] \text{ e } B = (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x)P_i,$$

em que $P_1, \ldots, P_r$ são todos polos de x. Então, pela Proposição 1.17,

$$\deg B = \sum_{i=1}^{r} v_{P_i}(x^{-1}) \deg P_i \leq [F : K(x^{-1})] = [F : K(x)] = n,$$

pois o polo de x é o zero de x^{-1} Por outro lado, vamos provar que $\deg B \geq n$. Escolha uma base

$$u_1, \ldots, u_n$$

para $F/K(x)$. Como os zeros e os polos de um elemento formam um conjunto finito temos que o conjunto

$$T = \{v_P(u_i) : i = 1, \ldots, n \text{ e } P \in S\}$$

é finito, em que

$$S = \bigcup_{i=1}^{n} \mathrm{supp}(u_i).$$

Assim, existe um $n_0 \in \mathbb{N}$ tal que $-n_0 < \min T$. Considere o divisor

$$C = n_0 \sum_{P \in S} P \geq 0,$$

obtemos $(u_i) \geq -C$, $i = 1, \ldots, n$.

Agora, seja o conjunto

$$A = \{x^j u_i : 0 \leq j \leq t \text{ e } 1 \leq i \leq n\}$$

com $t \in \mathbb{Z}$, $t \geq 0$.Os elementos de A são LI sobre K e $A \subseteq \mathcal{L}(tB + C)$, pois

$$v_P(x^j u_i) = j v_P(x) + v_P(u_i) \geq -j v_P(B) - v_P(C) \geq -t v_P(B) - v_P(C) = -v_P(tB + C).$$

Assim, $\langle A\rangle$ é um subespaço de $\mathcal{L}(tB+C)$ e

$$\dim\langle A\rangle \leq \ell(tB+C) \Rightarrow (t+1)n \leq \ell(tB+C). \tag{1.3}$$

Como $C \geq 0$ e $t \geq 0$ temos $(tB+C) \geq 0$. Logo, pela Proposição 1.25,

$$\ell(tB+C) \leq \deg(tB+C)+1 = t\deg B + \deg C + 1,$$

isto é,

$$(t+1)n \leq t\deg B + \deg C + 1.$$

Tomando $c = \deg C$, obtemos

$$(t+1)n \leq t\deg B + c + 1 \Rightarrow n - c - 1 \leq t(\deg B - n).$$

Portanto, $\deg B - n \geq 0$. ■

Corolário 1.27 *Seja F/K um corpo de funções.*

1. *Se A e A' são divisores com $A \sim A'$, então*

$$\ell(A) = \ell(A') \;\; e \;\; \deg A = \deg A'.$$

2. *Se $\deg A < 0$, então $\ell(A) = 0$.*

3. *Para um divisor A de grau zero as seguintes afirmações são equivalentes*:

a. A é principal;

b. $\ell(A) \geq 1$;

c. $\ell(A) = 1$.

Prova. Confira [10, p.19, Corollary 1.4.12]. ■

Proposição 1.28 *Seja F/K um corpo de funções. Então existe $\gamma \in \mathbb{Z}$ tal que*

$$\deg(A) - \ell(A) \leq \gamma, \;\; \forall \;\; A \in \operatorname{div}(F).$$

Note que γ independe do divisor A e depende apenas do corpo de funções F/K.

Prova. Confira [10, p.21, Proposition 1.4.14]. ■

Consideremos o conjunto

$$X = \{\deg(A) - \ell(A) + 1 : A \in \operatorname{div}(F)\}.$$

Então, pela Proposição 1.28, existe $\gamma \in \mathbb{Z}$ tal que

$$\deg(A) - \ell(A) + 1 \leq \gamma + 1, \;\; \forall \;\; A \in \operatorname{div}(F).$$

Assim, X é limitado superiormente. Portanto, X possui um elemento máximo. O *gênero* de F/K é definido como

$$g = \max X.$$

Corolário 1.29 *Seja F/K um corpo de funções. Então o gênero de F/K é um inteiro não negativo.*

Prova. Tomando $A = 0$, obtemos pelo Lema 1.24,

$$g \geq \deg 0 - \ell(0) + 1 = 0,$$

que é o resultado desejado. ■

Teorema 1.30 (Teorema de Riemann) *Seja F/K um corpo de funções de gênero g.*

1. *$\ell(A) \geq \deg A + 1 - g$, para todo $A \in \mathrm{div}(F)$.*
2. *Existe um inteiro c dependendo somente de F/K tal que*

$$\ell(A) = \deg A + 1 - g,$$

quando $\deg A \geq c$.

Prova. 1 Por definição de gênero, obtemos

$$g \geq \deg A - \ell(A) + 1 \Rightarrow \ell(A) \geq \deg A + 1 - g,$$

para todo $A \in \mathrm{div}(F)$.

2 Existe um divisor A_0 tal que

$$g = \deg A_0 - \ell(A_0) + 1.$$

Assim, pelo item 1,

$$\ell(A - A_0) \geq \deg(A - A_0) + 1 - g.$$

Pondo $c = \deg\ A_0 + g$ e se $\deg A\ \geq c$, então

$$\begin{aligned} \deg(A - A_0) + 1 - g &= \deg A - \deg A_0 + 1 - g \\ &\geq c - \deg A_0 + 1 - g \\ &= \deg A_0 + g - \deg A_0 + 1 - g \\ &= 1. \end{aligned}$$

Logo, $\ell(A - A_0) \geq 1$ de onde concluímos que $\mathcal{L}(A - A_0) \neq \{0\}$. Assim, existe $z \in \mathcal{L}(A - A_0)$, com $z \neq 0$. Consideremos o divisor $A' := A + (z)$, então $A' \geq A_0$, pois

$$z \in \mathcal{L}(A - A_0) \Rightarrow (z) \geq -A + A_0 \Rightarrow A' = (z) + A \geq A_0.$$

Pelo Lema 1.24 e Corolário 1.27,

$$\deg A - \ell(A) = \deg A' - \ell(A') \geq \deg\ A_0 - \ell(A_0) = g - 1.$$

Portanto,

$$\ell(A) \leq \deg A + 1 - g$$

e pelo item 1 temos a igualdade. ■

Exemplo 1.31 *Seja F/K um corpo de funções racionais, então F/K possui gênero $g = 0$.*

Solução. Sabemos, pelo Teorema de Riemann, que existe $c \in \mathbb{Z}$ tal que

$$\ell(A) = \deg A + 1 - g,$$

quando $\deg A \geq c$. Seja $r > 0$ tal que $r > c$ e consideremos $P_\infty = (x)_\infty$ e $\mathcal{L}(rP_\infty)$. Então, pelo Teorema 1.26,

$$\deg(rP_\infty) = r \deg P_\infty = r[F : K(x)] = r$$

Logo,

$$\ell(rP_\infty) = \deg(rP_\infty) + 1 - g = r + 1 - g.$$

Afirmação. $1, x, \ldots, x^r \in \mathcal{L}(rP_\infty)$.
De fato,

$$-v_P(rP_\infty) \leq 0, \ \forall \ P \in \mathbb{P}_F,$$

pois

$$v_P(rP_\infty) = \begin{cases} r > 0, & \text{se } P = P_\infty \\ 0, & \text{se } P \neq P_\infty \end{cases}$$

Logo,

$$0 = v_P(1) \geq -v_P(rP_\infty), \ \forall \ P \in \mathbb{P}_F.$$

Além disso, sendo P_∞ um polo de x, obtemos

$$v_{P_\infty}(x^i) = iv_{P_\infty}(x) < 0 \Rightarrow iv_{P_\infty}(x) > rv_{P_\infty}(x) = -rv_{P_\infty}(P_\infty).$$

Como

$$v_P(x) \geq 0, \ \forall \ P \in \mathbb{P}_F - \{P_\infty\}.$$

Temos

$$v_P(x^i) \geq -v_P(rP_\infty), \ \forall \ P \in \mathbb{P}_F,$$

ou seja, $x^i \in \mathcal{L}(rP_\infty)$, $i = \ 0, \ldots, r$. Portanto, $\ell(rP_\infty) = r + 1$ e $g = 0$. ■

Teorema 1.32 *Seja F/K um corpo de funções. Se A é um divisor, com $\deg A \geq 2g-1$, então*

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

Prova. Confira [10, p.31, Theorem 1.5.17]. ■

Proposição 1.33 *Seja $P \in \mathbb{P}_F$. Então para cada $n \in \mathbb{N}$, com $n \geq 2g$, existe $x \in F$, com divisor polo*

$$(x)_\infty = nP.$$

Prova. Confira [10, p.34, Proposition 1.6.6]. ■

Capítulo 2

Extensões de Corpos de Funções

A depender do corpo de funções F/K é possível estimar o número de lugares racionais que ele possui.Visando obter essa estimativa apresentaremos os conceitos básicos de extensões algébricas, extensões de lugares, índice de ramificação e o Teorema de Hasse-Weil. Vamos considerar os corpos de funções algébricas F/K e F'/K', com K o corpo de constantes completo de F, K' o corpo de constantes completo de F'. Denotaremos por $\mathbb{F}_q$ o corpo finito com q elementos, onde q é a potência de um número primo. O leitor interessado em mais detalhes pode consultar [10].

2.1 Extensões Algébricas

Um corpo de funções algébricas F'/K' é chamado uma *extensão algébrica* de F/K se F'/F é uma extensão algébrica e $K \subseteq K'$. A extensão algébrica F'/K' de F/K é chamada *corpo constante* se $F' = FK'$ é o corpo compósito de F e K', em que FK' é o menor subcorpo de F' gerado por F e K', onde

$$FK' = F(K') = K'(F).$$

Finalmente, a extensão algébrica F'/K' de F/K é chamada uma *extensão finita* se $[F' : F] < \infty$.

Lema 2.1 *Seja F'/K' uma extensão algébrica de F/K. Então verifica-se que:*

1. *K'/K é uma extensão algébrica e $F \cap K' = K$.*
2. *$[F' : F] < \infty$ se, e somente se, $[K' : K] < \infty$.*

Prova. Confira [10, p.69, Lemma 3.1.2]. ■

Seja F'/K' uma extensão algébrica de F/K. Dizemos que um lugar $P' \in \mathbb{P}_{F'}$ *está acima de* (*lies over*) $P \in \mathbb{P}_F$ ou que P *está abaixo de* (*lies under*) P', em símbolos $P' \mid P$, se $P \subseteq P'$. Também dizemos que P' é uma *extensão* de P.

Proposição 2.2 *Seja F'/K' uma extensão algébrica de F/K. Suponhamos que P (P') é um lugar de F/K (F'/K'), $\mathcal{O}_P \subseteq F$ ($\mathcal{O}_{P'} \subseteq F'$) e v_P ($v_{P'}$) é a correspondente valorização discreta. Então as seguintes afirmações são equivalentes*:

1. $P' \mid P$;

2. $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$;

3. *Existe um inteiro* $e \geq 1$ *tal que* $v_{P'}(x) = ev_P(x)$, *para todo* $x \in F$.

Além disso, se $P' \mid P$, *então*

$$P = P' \cap F \ \ e \ \ \mathcal{O}_P = \mathcal{O}_{P'} \cap F.$$

Por esta razão, P *é também chamado de* restrição *de* P' *a* F.

Prova. Confira [10, p.69, Proposition 3.14]. ■

Observação 2.3 *Pela Proposição* 2.2, *concluímos que o homomorfismo de corpos de classes residuais de* F_P *em* $F'_{P'}$ *definido como*

$$x(P) \mapsto x(P'), \ \ \forall \ x \in \mathcal{O}_P,$$

está bem definido e é injetor, de modo que obtemos uma imersão de F_P *em* $F'_{P'}$. *Portanto, podemos identificar* F_P *com um subcorpo de* $F'_{P'}$. *Neste caso,* $F'_{P'}$ *pode ser visto como uma extensão de* F_P.

Sejam F'/K' uma extensão algébrica de F/K e $P' \in \mathbb{P}_{F'}$ um lugar de F'/K' acima de $P \in \mathbb{P}_F$. Dizemos que o inteiro $e = e(P' \mid P)$, com

$$v_{P'}(x) = ev_P(x), \ \ \forall \ x \in F,$$

é o *índice de ramificação* de P' sobre P. O inteiro

$$f = f(P' \mid P) = [F_{P'} : F_P]$$

é chamado o *grau relativo* de P' sobre P. Note que f pode ser finito ou infinito, enquanto e é sempre um número natural.

Proposição 2.4 *Sejam* F'/K' *uma extensão algébrica de* F/K *e* $P' \in \mathbb{P}_{F'}$ *um lugar de* F'/K' *acima de* $P \in \mathbb{P}_F$. *Então*

$$f = f(P' \mid P) < \infty \Leftrightarrow [F' : F] < \infty.$$

Prova. Confira [10, p.71, Proposition 3.1.6]. ■

Proposição 2.5 *Seja* F'/K' *uma extensão algébrica de* F/K.

1. *Para cada* $P' \in \mathbb{P}_{F'}$ *existe exatamente um lugar* $P \in \mathbb{P}_F$ *tal que* $P' \mid P$, *a saber,* $P = P' \cap F$.

2. Qualquer lugar $P \in \mathbb{P}_F$ possui no mínimo um, mas apenas finitas extensões $P' \in \mathbb{P}_{F'}$.

Prova. 1 Vamos primeiro provar que existe um $z \in F$, com $z \neq 0$, tal que $v_{P'}(z) \neq 0$. De fato, suponhamos, por absurdo, que seja falso. Então escolha $t \in F'$ tal que $v_{P'}(t) > 0$. Como F'/F é um extensão algébrica temos que existem $c_0, \ldots, c_n \in F$, com $c_0 \neq 0$ e $c_n \neq 0$, tais que

$$c_n t^n + c_{n-1} t^{n-1} + \cdots + c_1 t + c_0 = 0.$$

Note que,

$$v_{P'}(c_i) = 0 \;\; i = 0, \ldots, n \;\text{ e }\; v_{P'}(c_i t^i) = v_{P'}(c_i) + i v_{P'}(t) > 0, \;\; i = 1, \ldots, n.$$

Assim,

$$v_{P'}(c_0) = 0 \;\text{ e }\; v_{P'}(c_n t^n + \cdots + c_1 t) \geq \min\{v_{P'}(c_n t^n), \ldots, v_{P'}(c_1 t)\} > 0$$

Portanto, pela Desigualdade Triangular Estrita,

$$v_{P'}((c_n t^n + c_{n-1} t^{n-1} + \cdots + c_1 t) + c_0) = \min\{v_{P'}(c_n t^n + c_{n-1} t^{n-1} + \cdots + c_1 t), v_{P'}(c_0)\} = 0.$$

Mas

$$\infty = v_{P'}(0) = v_{P'}(c_n t^n + c_{n-1} t^{n-1} + \cdots + c_1 t + c_0) = 0,$$

o que é uma contradição. Consequentemente, existe $\omega \in F$ tal que $v_{P'}(\omega) > 0$. Logo, $P' \cap F \neq \emptyset$ e $\mathcal{O}_{P'} \cap F \neq \emptyset$.

Afirmação. $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$ e $P = P' \cap F$.
De fato, como $K \subseteq K' \subset \mathcal{O}_{P'}$ temos que $K \subset \mathcal{O}_P$. Note que se $\mathcal{O}_P = F$, então $F \subseteq O_{P'}^{\bullet}$ e $v_{P'}(z) = 0$, para todo $z \in F$, o que é impossível. Assim, existe $z \in F$ tal que $z \notin \mathcal{O}_P$. Logo, $z \notin \mathcal{O}_{P'}$ o que implca $z^{-1} \in \mathcal{O}_{P'}$, isto é, $z^{-1} \in F \cap \mathcal{O}_{P'}$. Portanto, $z^{-1} \in \mathcal{O}_P$. Neste caso, $\mathcal{O}_P$ é um anel de valorização e P é o seu único ideal maximal, pois $P = \mathcal{O}_P - \mathcal{O}_P^{\bullet}$

A unicidade segue da Proposição 2.2.

2 Seja P um lugar qualquer de F/K. Então, pela Proposição 1.33, existe $x \in F$ cujo único zero é P.

Afirmação. $P' \mid P$ se, e somente se, $v_{P'}(x) > 0$.
De fato, se $P' \mid P$, então

$$v_{P'}(x) = e(P' \mid P) v_P(x) > 0, \;\text{ pois }\; e(P' \mid P) \geq 1.$$

Por outro lado, se $v_{P'}(x) > 0$ e Q é o lugar de F/K que está abaixo de P', então $v_Q(x) > 0$. Assim $Q = P$, pois P é o único zero de x em F/K.

Finalmente, como x tem no mínimo um e no máximo finitos zeros em F'/F temos o resultado. ■

Seja F'/K' uma extensão algébrica de F/K. Para um lugar $P \in \mathbb{P}_F$ fixado, definimos sua *conorma* com respeito a F'/F como

$$\text{Con}_{F'/F}(P) = \sum_{P'|P} e(P' \mid P) P',$$

em que a soma percorre todos os lugares $P' \in \mathbb{P}_{F'}$ que estão acima de P.

Teorema 2.6 *Sejam F'/K' uma extensão finita de F/K, P um lugar de F/K e $P_1, \ldots, P_m$ todos os lugares de F'/K' que estão acima de P. Seja $e_i = e(P_i|P)$ o índice de ramificação e $f_i = f(P_i|P)$ o grau relativo de $P_i|P$. Então*

$$\sum_{i=1}^{m} e_i f_i = [F' : F].$$

Prova. Confira [10, p. 74, Theorem 3.1.11]. ■

Corolário 2.7 *Sejam F'/K' uma extensão finita de F/K e $P \in \mathbb{P}_F$. Então*

$$|\{P' \in \mathbb{P}_{F'} : P' \mid P\}| \leq [F' : F].$$

Prova. Para cada i, $1 \leq i \leq m$, obtemos

$$1 \leq e_i f_i \Rightarrow m \leq \sum_{i=1}^{m} e_i f_i = [F' : F],$$

que é o resultado desejado. ■

Proposição 2.8 *Se $F' = FK'$ é uma extensão algébrica corpo constante de F/K, então F'/K' possui o mesmo gênero de F/K.*

Prova. Confira [10, p. 114, Theorem 3.6.3]. ■

2.2 Teorema de Hasse-Weil e a Cota de Hasse-Weil

Nesta seção F é um corpo de funções algébricas cujo corpo de constantes é $\mathbb{F}_q$. O próximo resultado é de fundamental importância em todo o desenvolvimento desta seção.

Lema 2.9 *Para cada $n \geq 0$ existe uma quantidade finita divisores positivos de grau n.*

Prova. Basta provar que o conjunto

$$S = \{P \in \mathbb{P}_F : \deg P \leq n\}$$

é finito, pois qualquer divisor positivo é a soma de divisores primos. Escolhendo $x \in F - \mathbb{F}_q$, consideremos o conjunto

$$S_0 = \{P_0 \in \mathbb{P}_{\mathbb{F}_q(x)} : \deg P_0 \leq n\}$$

e a extensão algébrica finita $F/\mathbb{F}_q$ de $\mathbb{F}_q(x)/\mathbb{F}_q$. Então

$$P \cap \mathbb{F}_q(x) \in S_0, \ \forall \ P \in S.$$

Pois,

$$\frac{\mathcal{O}_{P \cap \mathbb{F}_q(x)}}{P \cap \mathbb{F}_q(x)}$$

é um subespaço vetorial de

$$\frac{\mathcal{O}_P}{P}$$

logo temos que $\deg(P \cap \mathbb{F}_q(x)) \leq n$. Além disso, pela Proposição 2.5, cada $P_0 \in S_0$ possui apenas uma quantidade finita de extensões em F. Assim, resta provar que S_0 é finito. De fato, como os lugares de $\mathbb{F}_q(x)$, exceto o polo de x, correspondem a polinômios mônicos e irredutíveis $\mathbb{F}_q[x]$ e $\mathbb{F}_q$ é um corpo finito temos que S_0 é finito. ■

Teorema 2.10 *Seja F um corpo finito contendo um subcorpo $\mathbb{F}_q$. Então F possui q^r elementos, em que $r = [F : \mathbb{F}_q]$. Em particular,* $\dim(F) = r = \log_q |F|$.

Prova. Note que F é um espaço vetorial sobre $\mathbb{F}_q$ de dimensão r, pois F é um corpo finito. Seja

$$\beta = \{\mathbf{u}_1, \ldots, \mathbf{u}_r\}$$

uma base para F. Então para cada $\mathbf{u} \in F$ existem únicos $x_1, \ldots, x_r \in \mathbb{F}_q$ tais que

$$\mathbf{u} = \sum_{i=1}^{r} x_i \mathbf{u}_i.$$

Vamos definir a função $T_\beta : \mathbb{F}_q^r \to F$ como

$$T_\beta(x_1, \ldots . x_r) = \mathbf{u}.$$

É fácil verificar que T_β está bem definida, é linear e injetora. Portanto, F é isomorfo a $\mathbb{F}_q^r$. Como para cada x_i existem q possibilidades, temos que $|F| = q^r$ e

$$\dim(F) = r = \log_q |F| \quad \text{ou} \quad |F| = q^{\dim(F)},$$

que é o resultado desejado. ■

Observação 2.11 *A transformação linear $T_\beta : \mathbb{F}_q^r \to F$ é chamada a* parametrização *de F dada pela base β e T_β^{-1} é chamada de* isomorfismo de base canônica *de F associada com a base β.*

Vamos denotar o corpo finito F do Teorema 2.10 por $\mathbb{F}_{q^r}$. Assim, para cada $r \in \mathbb{N}$ existe exatamente uma extensão $\mathbb{F}_{q^r}/\mathbb{F}_q$ de grau r. Note que

$$\mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^s} \Leftrightarrow r \mid s.$$

Além disso, pode ser provado que o fecho algébrico $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$ é

$$\overline{\mathbb{F}}_q = \bigcup_{r \in \mathbb{N}} \mathbb{F}_{q^r}.$$

O leitor interessado em mais detalhes sobre corpos finitos pode consultar [1] e [3].

No que segue consideremos a extensão corpo constante (composito) $\overline{F} = F\overline{\mathbb{F}}_q$ de $F/\mathbb{F}_q$ e

$$F_r = F\mathbb{F}_{q^r} \subseteq \overline{F}.$$

Proposição 2.12 *Seja $F/\mathbb{F}_q$ um corpo de funções. Verifica-se que:*

1. *$\mathbb{F}_{q^r}$ é o corpo de constantes completo de F_r.*
2. *Seja $P \in \mathbb{P}_F$ um lugar de grau m. Então*

$$\mathrm{Con}_{F_r/F}(P) = P_1 + \cdots + P_d,$$

onde $d = \mathrm{mdc}(m, r)$, $P_i \in \mathbb{P}_{F_r}$ $i = 1, \ldots, d$ são lugares distintos dois a dois de grau $\frac{m}{d}$.

Prova. Confira [10, p.190, Lemma 5.1.9]. ■

Seja $F/\mathbb{F}_q$ um corpo de funções, definimos

$$A_n = |\{A \in \mathrm{div}(F) : A \geq 0 \text{ e } \deg A = n\}|.$$

Por exemplo, $A_0 = 1$ e A_1 é o número de lugares de grau 1. A série de potências

$$Z(t) := Z_F(t) = \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}$$

é chamada a *função Zeta* de $F/\mathbb{F}_q$. Observe que t é uma variável complexa e que $Z(t)$ é uma série de potências sobre os complexos. A proposição a seguir garante que ela converge em uma vizinhança de zero.

Proposição 2.13 *A série de potências $Z(t)$ converge, quando $|t| < q^{-1}$.*

Prova. Confira [10, p.188, Proposition 5.1.6]. ■

A partir de $Z(t)$ vamos poder obter uma expressão para o número de lugares de grau 1 de $F/\mathbb{F}_q$ e de F_r. Para $|t| < q^{-1}$, os resultados a seguir nos ajudarão nesse processo.

Proposição 2.14 *Seja $F/\mathbb{F}_q$ um corpo de funções.*

1. *Se $F/\mathbb{F}_q$ é de gênero 0, então $F/\mathbb{F}_q$ é um corpo de funções racional e a função Zeta é*

$$Z(t) = \frac{1}{(1-t)(1-qt)}.$$

2. *Se $F/\mathbb{F}_q$ é de gênero $g \geq 1$, então sua função Zeta pode ser escrita sob a forma $Z(t) = F(t) + G(t)$, com*

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg[C] \leq 2g-2} q^{\ell([C])} t^{\deg[C]}$$

e

$$G(t) = \frac{h}{q-1}\left(q^g t^{2g-1} \frac{1}{1-qt} - \frac{1}{1-t}\right).$$

Onde, $h = |\{[A] \in Cl(F) : \deg[A] = 0\}|$.

Prova. Confira [10, p.192, Corollary 5.1.12]. ■

Seja $F/\mathbb{F}_q$ um corpo de funções. O polinômio

$$L(t) = L_F(t) = (1-t)(1-qt)Z(t)$$

é chamado o *L-polinômio* de $F/\mathbb{F}_q$. Note, pela Proposição 2.14, que

$$L(t) = (1-t)(1-qt)F(t) + \frac{h}{q-1}(q^g t^{2g-1}(1-t) - (1-qt)) \text{ ou } L(t) = 1$$

Logo, $L(t)$ é de fato um polinômio. Além disso, $L(t)$ contém todas as informações sobre os números A_n, pois

$$L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n.$$

Teorema 2.15 *Seja $F/\mathbb{F}_q$ um corpo de funções. Então verifica-se que:*

1. $\deg(L(t)) = 2g$.
2. *Pondo*
$$L(t) = a_0 + a_1 t + \cdots + a_n t^{2g},$$
obtemos $a_0 = 1$ e $a_1 = N - (q+1)$, onde N é o número de lugares $P \in \mathbb{P}_F$ de grau 1.
3. *$L(t)$ se fatora em $\mathbb{C}[t]$ na forma*
$$L(t) = \prod_{i=1}^{2g}(1-\alpha_i t). \tag{2.1}$$
4. *Se $L_r(t) := (1-t)(1-q^r t)Z_r(t)$ denota o L-polinômio do corpo extensão constante F_r, então*
$$L_r(t) = \prod_{i=1}^{2g}(1-\alpha_i^r t),$$
onde α_i são dados na equação (2.1).

Prova. Confira [10, p.193, Theorem 5.1.15]. ■

Seja $F/\mathbb{F}_q$ um corpo de funções, definimos:

$$N(F) = N = |\{P \in \mathbb{P}_F : \deg P = 1\}|$$

e para $r \geq 1$ o número

$$N_r = N(F_r) = |\{P \in \mathbb{P}_{F_r} : \deg P = 1\}|$$

onde F_r é a extensão corpo constante de $F/\mathbb{F}_q$.

Corolário 2.16 *Seja $F/\mathbb{F}_q$ um corpo de funções, então para qualquer $r \in \mathbb{N}$,*

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r,$$

onde $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ são os inversos das raízes de $L(t)$. Em particular, como $N_1 = N(F)$ temos que

$$N(F) = q + 1 - \sum_{i=1}^{2g} \alpha_i.$$

Prova. Pelo Teorema 2.15,

$$N_r - (q^r + 1)$$

é o coeficiente de t no polinômio $L_r(t)$. Novamente, pelo Teorema 2.15, obtemos

$$L_r(t) = \prod_{i}^{2g} (1 - \alpha_i^r t).$$

Como o coeficiente de t no produtório acima é igual a

$$-\sum_{i=1}^{2g} \alpha_i^r$$

temos o resultado. ■

Pondo

$$S_r = -\sum_{i=1}^{2g} \alpha_i^r,$$

temos, pelo Corolário 2.16, que

$$N_r = q^r + 1 + S_r, \tag{2.2}$$

em que $S_r = 0$, se $g = 0$, pela Observação 1.22.

Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g, definimos:

$$B_\tau = B_\tau(F) = \left|\{P \in \mathbb{P}_F : \deg P = \tau\}\right|.$$

Observe que $B_1 = N(F)$.

Proposição 2.17 *Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g. Então*

$$N_r = \sum_{i|r} i B_i.$$

Prova. Sejam $P \in \mathbb{P}_F$; $\deg P = i$, com $i \mid r$. Então, pela Proposição 2.12,

$$\text{Con}_{F_r/F}(P) = P_1 + \cdots + P_i,$$

onde $P_j \in \mathbb{P}_{F_r}$, com $\deg P_j = 1$, $j = 1, \ldots, i$. Ainda pela mesma proposição, temos que se $\deg P$ não divide r então $\deg Q > 1$ para todo Q que está acima de P. Desse modo, como cada $Q \in \mathbb{P}_{F_r}$ está acima de um único $P \in \mathbb{P}_F$, temos que lugares de $\mathbb{P}_{F_r}$ de grau um estão sempre acima de lugares de $\mathbb{P}_F$ cujo grau divide r. Portanto,

$$N_r = \sum_{i|r} iB_i,$$

pois para cada $P \in \mathbb{P}_F$, com $\deg P = i$, existem exatamente i lugares Q acima de P. ■

Antes de enunciar os próximos resultados vamos lembrar a definição da função de Möbius $\mu : \mathbb{N} \to \{-1, 0, 1\}$

$$\mu(n) = \begin{cases} 1, & \text{se } n = 1 \\ 0, & \text{se existe um inteiro } k > 1 \text{ com } k^2 | n, \\ (-1)^k, & \text{se } n \text{ é o produto de } k \text{ primos distintos.} \end{cases}$$

e a fórmula de inversão de Möbius

$$N_r = \sum_{i|r} iB_i \Leftrightarrow rB_r = \sum_{i|r} \mu\left(\frac{r}{i}\right) N_i. \tag{2.3}$$

Para mais informações sobre a função de Möbius consulte [6].

Teorema 2.18 (Teorema de Hasse-Weil) *Os inversos das raízes de $L_F(t)$ satisfazem a seguinte propriedade*:

$$|\alpha_i| = q^{\frac{1}{2}}, \;\; i = 1, \ldots, 2g.$$

Prova. Confira [10, p.197, Theorem 5.2.1]. ■

Corolário 2.19 (Cota de Hasse-Weil) *O número $N = N(F)$ de lugares de grau 1 de $F/\mathbb{F}_q$ satisfaz*

$$|N - (q+1)| \leq 2gq^{\frac{1}{2}}.$$

Prova. Segue Corolário 2.16, que

$$N - (q+1) = -\sum_{i=1}^{2g} \alpha_i \Rightarrow |N - (q-1)| = \left| -\sum_{i=1}^{2g} \alpha_i \right| \leq \sum_{i=1}^{2g} |\alpha_i| \,.$$

Assim, pelo Teorema de Hasse-Weil, obtemos

$$|N - (q-1)| = \left| -\sum_{i=1}^{2g} \alpha_i \right| \leq \sum_{i=1}^{2g} |\alpha_i| \leq 2gq^{\frac{1}{2}},$$

que é o resultado desejado. ■

Note que o corolário acima aplicado a $F_r/\mathbb{F}_{q^r}$ nos fornece

$$|N_r - (q^r + 1)| \leq 2gq^{\frac{1}{2}},$$

para todo $r \geq 1$.

Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g. Dizemos que $F/\mathbb{F}_q$ é *maximal* se

$$N = q + 1 + 2gq^{\frac{1}{2}}.$$

Proposição 2.20 *Se $F/\mathbb{F}_q$ é um corpo de funções maximal, então*

$$\alpha_i = -q^{\frac{1}{2}}, \ \ i = 1, \ldots, 2g.$$

Prova. Pelo Corolário 2.16 e o Teorema 2.18, obtemos

$$N = q + 1 - \sum_{i=1}^{2g} \alpha_i \ \text{ e } \ |\alpha_i| = q^{\frac{1}{2}}, \ \ i = 1, \ldots, 2g.$$

Como $F/\mathbb{F}_q$ é maximal temos que

$$q + 1 - \sum_{i=1}^{2g} \alpha_i = q + 1 + 2gq^{\frac{1}{2}} \Rightarrow \sum_{i=1}^{2g} \alpha_i = -2gq^{\frac{1}{2}}.$$

Logo,

$$\left| \sum_{i=1}^{2g} \alpha_i \right| = |\alpha_1| + \cdots + |\alpha_{2g}| \Rightarrow \alpha_k = b_{kl}\alpha_l, \ \text{ onde } \ b_{kl} \in \mathbb{R} \ \text{ e } \ 1 \leq k, l \leq 2g.$$

Assim, para cada α_t fixo,

$$\sum_{i=1}^{2g} \alpha_i = \left(1 + \sum_{i=2}^{2g} b_{it}\right) \alpha_t = -2gq^{\frac{1}{2}} \Rightarrow \alpha_t \in \mathbb{R} \Rightarrow \alpha_i \in \mathbb{R}, \ \ 2 \leq i \leq 2g,$$

de modo que

$$|\alpha_i| = q^{\frac{1}{2}} \Rightarrow \alpha_i = \pm q^{\frac{1}{2}}, \ \ i = 1, \ldots, 2g.$$

Desde que

$$\sum_{i=1}^{2g} \alpha_i = -2gq^{\frac{1}{2}},$$

obtemos $\alpha_1 = \cdots = \alpha_{2g} = -q^{\frac{1}{2}}$. ■

Capítulo 3

Códigos Lineares

Neste capítulo vamos fazer uma introdução ao estudo dos Códigos Lineares, fornecendo alguns exemplos, principalmente os de códigos utilizados no capítulo subsequente. O leitor interessado em mais detalhes pode consultar [8] e [7].

3.1 Códigos

Um *alfabeto* é qualquer conjunto não vazio A. Um *código* C sobre um alfabeto A é qualquer subconjunto não vazio do conjunto $A^{\mathbb{I}}$ de todas as sequências

$$\mathbf{c} = \{c_i : i \in \mathbb{I}\} = (c_i)_{i \in \mathbb{I}},$$

onde $c_i \in A$ e $\mathbb{I} \subseteq \mathbb{N}$. Quando

$$\mathbb{I} = \{i : 1 \leq i \leq n\}$$

temos que $A^n = A^{\mathbb{I}}$.

Um *código de bloco* C de comprimento n sobre um alfabeto A é qualquer subconjunto não vazio do conjunto A^n de todas as palavras (ou sequências)

$$\mathbf{c} = \{c_i : i \in \mathbb{I}\}.$$

Durante os nossos estudos vamos trabalhar apenas com alfabetos finitos. Um exemplo particular de alfabeto finito é $A = \mathbb{F}_q$, onde $\mathbb{F}_q$ é um corpo finito, com q elementos e $q = p^m$, para algum número primo p e $m \in \mathbb{N}$.

Sejam $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in A^n$. A *distância de Hamming* entre $\mathbf{x}$ e $\mathbf{y}$ é definida como

$$d(\mathbf{x}, \mathbf{y}) = |\{i \in \mathbb{I} : x_i \neq y_i\}|.$$

Note que quando um código C está definido sobre um alfabeto finito é comum utilizar uma denominação especial a depender da cardinalidade do alfabeto A. Se $|A| = q$, então dizemos que C é um código q-ário. Em particular, para $q = 2$ binário, $q = 3$ ternário e $q = 4$ quaternário, etc. Além disso, se $|C| = 1$ ou $C = A^n$, dizemos que C é um *código trivial*.

A *distância mínima* de um código C, com $|C| \neq 1$, é definida como

$$d = d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}.$$

O *peso* de $\mathbf{x} \in C$, denotado por $\omega_l(x)$, é definido como

$$\omega_H(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$$

e o *peso mínimo* de um código C é definido como

$$\min\{\omega_H(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}.$$

Um *código linear* é qualquer subespaço C de $\mathbb{F}_q^n$, onde as palavras código são os elementos de C. Chamam-se n o comprimento de C e $\dim(C)$ a dimensão de C. Um *código* $[n, k]$ é um código de comprimento n e dimensão k. Se a distância mínima d é conhecida denotamos por $[n,\ k,\ d]$ o código de comprimento n, dimensão k e distância mínima d. Também denotaremos por $[n,\ k,\ \geq\ d]$ o código de comprimento n, dimensão k e distância mínima no mínimo d. Prova-se que a distância mínima em um código linear é igual ao peso mínimo.

Sejam C um código linear $[n,\ k]$ sobre $\mathbb{F}_q$ e

$$\{\mathbf{c}_1, \ldots, \mathbf{c}_k\}$$

uma base para C. Então a função $\Phi : \mathbb{F}_q^k \to \mathbb{F}_q^n$ definida como

$$\Phi(x_1, \ldots, x_k) = x_1\mathbf{c}_1 + \cdots + x_k\mathbf{c}_k$$

é claramente linear e injetora, com $C = \operatorname{Im}\Phi$. Portanto, a cada código linear C podemos associar uma transformação linear injetora $\Phi : \mathbb{F}_q^k \to \mathbb{F}_q^n$, com $C = \operatorname{Im}\Phi$, e vice versa.

Seja C um código linear $[n,\ k]$ sobre $\mathbb{F}_q$ Uma *matriz geradora* $\mathbf{G}$ para C é uma matriz $k \times n$ cujas linhas são as coordenadas de uma base para C.

Sejam $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$. O *produto interno* $\langle \mathbf{x}, \mathbf{y} \rangle$ é definido como

$$\sum_{i=1}^{n} x_i y_i.$$

Considere o código linear C . O subespaço de $\mathbb{F}_q^n$,

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

chama-se *código dual* de C. A matriz geradora $\mathbf{H}$ para $C^{\perp}$ chama-se *matriz de verificação de paridade* de C. Pode ser provado que $C^{\perp}$ é um código $[n,\ n-k]$ e

$$\mathbf{G}\mathbf{H}^t = O.$$

Note que

$$C = \{\mathbf{c} \in \mathbb{F}_q^n : \mathbf{H}\mathbf{c}^t = \mathbf{0}\}.$$

Assim, a matriz de verificação de paridade $\mathbf{H}$ nos diz se um vetor $u \in \mathbb{F}_q^n$ é uma palavra código ou não.

Salvo menção explícita em contrário, todos os códigos considerados nesta dissertação serão lineares. Por isso, para simplificar, dizemos apenas códigos.

Um dos problemas básicos em teoria dos códigos é construir, sobre um alfabeto fixo $\mathbb{F}_q$, códigos cuja dimensão e a distância mínima sejam grandes em comparação com o comprimento. Entretanto, existem algumas restrições. A grosso modo, se a dimensão de um código é grande (com relação ao seu comprimento), então a sua distância mínima é pequena. A cota mais simples é a seguinte:

Proposição 3.1 (Cota do Singleton) *Para qualquer código q-ários linear $[n, k, d]$ temos que*

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

Prova. Consideremos o subespaço vetorial $E \subseteq \mathbb{F}_q^n$ definido como

$$E = \{(x_1, \ldots, x_{d-1}, x_d, \ldots, x_n) \in \mathbb{F}_q^n : x_i = 0, \ \forall \ i \geq d\}$$

Como o peso mínimo de C é igual d temos que $E \cap C = \{\mathbf{0}\}$. Portanto,

$$k + d - 1 = \dim(C) + \dim(E) = \dim(E + C) + \dim(E \cap C) = \dim(E + C) \leq n,$$

que é o resultado desejado. ■

Os códigos em que $k + d = n + 1$ são considerados ótimos, estes códigos são chamados de *códigos MDS (códigos separáveis de máxima distância)*.

Proposição 3.2 (Cota de Hamming) *Seja C um código q-ários linear $[n, k, d]$. Então*

$$q^k \left(\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \right) \leq q^n \ \ com \ t = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

e

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \leq x\}.$$

Prova. Sejam $\mathbf{c}_1, \mathbf{c}_2 \in C$, com $\mathbf{c}_1 \neq \mathbf{c}_2$, para cada $t \in \mathbb{N}$ defina

$$S_t(\mathbf{c}) = \{\mathbf{x} \in \mathbb{F}_q^n : d(\mathbf{x}, \mathbf{c}) < t\}$$

Então $S_t(\mathbf{c}_1) \cap S_t(\mathbf{c}_2) = \emptyset$, pois se $\mathbf{x} \in S_t(\mathbf{c}_1)$ e $\mathbf{x} \in S_t(\mathbf{c}_2)$, então

$$d \leq d(\mathbf{c}_1, \mathbf{c}_2) \leq d(\mathbf{x}, \mathbf{c}_1) + d(\mathbf{x}, \mathbf{c}_2) < 2t = d - 1,$$

o que é impossível. Além disso, cada uma das q^k esferas $S_t(\mathbf{c})$, com $c \in C$,contém

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i$$

palavras em $\mathbb{F}_q^n$, por exemplo, se $\mathbf{x}_i \in \mathbb{F}_q^n$ é uma palavra com apenas uma componente não nula, então ela pode ser escolhida de

$$\binom{n}{1}$$

maneiras, mas cada componente não nula é um elemento de $\mathbb{F}_q^*$. Portanto, existem

$$\binom{n}{1}(q-1)$$

palavras com uma componente não nula. Como existem q^n palavras em $\mathbb{F}_q^n$ temos que

$$q^k\left(\sum_{i=0}^{t}\binom{n}{i}(q-1)^i\right) \leq q^n,$$

que é o resultado desejado. ■

3.2 Códigos Concatenados

Concatenação é um método para se obter códigos longos a partir de códigos curtos, veremos mais adiante o que vem a ser um código concatenado bem como algumas de suas propriedades.

É conveniente construirmos códigos sobre uma extensão $\mathbb{F}_{q^t}$ de $\mathbb{F}_q$. Nesse caso, obtemos pelo Teorema 2.10,

$$[\mathbb{F}_{q^t} : \mathbb{F}_q] = t.$$

Proposição 3.3 (Código Concatenado) *Seja C um código $[n,k,d]$ sobre $\mathbb{F}_{q^t}$, onde $\mathbb{F}_{q^t}$ é uma extensão de $\mathbb{F}_q$. Se existir um código A $[m,t,s]$ sobre $\mathbb{F}_q$, então existe um código C' $[nm, kt, \geq ds]$ sobre $\mathbb{F}_q$.*

Prova. Como A e $\mathbb{F}_{q^t}$ são espaços vetoriais sobre $\mathbb{F}_q$, existe um isomorfismo $\Phi : \mathbb{F}_{q^t} \longrightarrow A$. Consideremos a aplicação

$$\begin{array}{rccc} \Phi^* : & \mathbb{F}_{q^t}^n & \to & \mathbb{F}_q^{mn} \\ & (\mathbf{v}_1, \ldots, \mathbf{v}_n) & \mapsto & (\Phi(\mathbf{v}_1), \ldots, \Phi(\mathbf{v}_n)) \end{array}$$

Então Φ^* é linear e injetora, pois Φ é linear e injetora. Como o código C é um subespaço de $\mathbb{F}_{q^t}^n$ temos que $C' = \Phi^*(C)$ é um subespaço de $\mathbb{F}_q^{nm}$. Assim, pelo Teorema 2.10, obtemos

$$\dim(C') = \log_q |C'| = \log_q |C| = \log_q((q^t)^k) = \log_q q^{kt} = kt.$$

Finalmente, seja

$$\mathbf{c} = (\mathbf{c}_1, \ldots, \mathbf{c}_n)$$

uma palavra código não nula de C. Se $\mathbf{c}_i \neq \mathbf{0}$, para algum i, então $\Phi(\mathbf{c}_i)$ é uma palavra código não nula de A. Assim,

$$\omega_H(\Phi(\mathbf{c}_i)) \geq s.$$

Como $\mathbf{c}$ possui no mínimo d posições não nulas temos que o número de posições não nulas de

$$(\Phi(\mathbf{c}_1), \ldots, \Phi(\mathbf{c}_n))$$

é no mínimo ds. Portanto, C' é um código $[nm, kt, \geq ds]$ sobre $\mathbb{F}_q$. ■

O código C' chama-se *código concatenado* e o método para obtê-lo é conhecido como *concatenação*. O código C é normalmente denominado de *código externo* e o código A é denominado *código interno.*

Exemplo 3.4 *Seja*

$$\mathbb{F}_2 = \{0, 1\}$$

um corpo finito com dois elementos. Note que

$$p = x^2 + x + 1 \in \mathbb{F}_2[x]$$

é irredutível sobre $\mathbb{F}_2$*. Assim, o corpo*

$$\mathbb{F}_4 = \frac{\mathbb{F}_2[x]}{(p)} = \{0, 1, \alpha, 1 + \alpha\},$$

onde $0 = (p), 1 = 1 + (p)$ *e* $\alpha = x + (p) \in \mathbb{F}_4$ *é uma raiz de* p*, é uma extensão finita de* $\mathbb{F}_2$*. Observe que* $\{1, \alpha\}$ *é uma base para* $\mathbb{F}_4$ *sobre* $\mathbb{F}_2$*. Agora, consideremos o código* $[2, 1, 2]$

$$C = \langle (1, \alpha) \rangle = \{(0, 0), (1, \alpha), (\alpha, 1 + \alpha), (1 + \alpha, 1)\}$$

sobre $\mathbb{F}_4$*. Escolha o código* $[3, 2, 2]$

$$A = \langle (1, 1, 0), (1, 0, 1) \rangle = \{(0, 0, 0), (1, 1, 0), (1, 0, 1), (0, 1, 1)\}$$

sobre $\mathbb{F}_2$*. Um isomorfismo* Φ *de* $\mathbb{F}_4$ *sobre* A *é completamente determinado por* $\Phi(1)$ *e* $\Phi(\alpha)$*, por exemplo,*

$$\Phi(1) = (1, 1, 0) \ \ e \ \ \Phi(\alpha) = (1, 0, 1).$$

Nesse caso,

$$\Phi(a + b\alpha) = (a + b, a, b).$$

Finalmente,

$$\begin{aligned} C' &= \Phi^*(C) = \{(\Phi(\mathbf{v}_1), \Phi(\mathbf{v}_2)) : (\mathbf{v}_1, \mathbf{v}_2) \in C\} \\ &= \{(0, 0, 0, 0, 0, 0), (1, 1, 0, 1, 0, 1), (1, 0, 1, 0, 1, 1), (0, 1, 1, 1, 1, 0)\} \\ &= \langle (1, 1, 0, 1, 0, 1), (1, 0, 1, 0, 1, 1) \rangle. \end{aligned}$$

Portanto, C' *é um código* $[6, 2, 4]$ *sobre* $\mathbb{F}_2$*.*

3.3 Códigos Algébricos Geométricos

Os Códigos Algébricos Geométricos (Códigos AG) foram introduzidos por V. D. Goppa. Por isso, às vezes, os chamamos de códigos de Goppa geométricos. Como uma motivação para a construção desses códigos vamos considerar primeiro os códigos Reed-Solomon (ou códigos RS) sobre $\mathbb{F}_q$. Essa classe importante de códigos é bem conhecida em Teoria dos Códigos há bastante tempo. Sob certas condições, os códigos Algébricos Geométricos são uma generalização natural dos códigos RS.

Teorema 3.5 (Códigos de Reed-Solomon) *Sejam $\mathbb{F}_q$ um corpo e $n \leq q+1$. Então existe um código linear $[n,k,d]$ MDS sobre $\mathbb{F}_q$, com $1 \leq k \leq n$.*

Prova. Inicialmente assuma que $n = q+1$.Considere,

$$\mathcal{L}_k = \{f \in \mathbb{F}_q[X] : \deg f \leq k-1\}$$

e $\varphi : \mathcal{L}_k \longrightarrow \mathbb{F}_q^n$ a função (avaliação) definida como

$$\varphi(f) = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_q), a_{k-1}), \tag{3.1}$$

onde $\alpha_1, \alpha_2, \ldots, \alpha_q$ são todos os q elementos de $\mathbb{F}_q$ e

$$f = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} \in \mathbb{F}_q[X].$$

Observe que $\mathcal{L}_k$ é um espaço vetorial sobre $\mathbb{F}_q$ de dimensão k, logo verifica-se que φ é linear e injetora, pois. Assim, $C = \varphi(\mathcal{L}_k)$ é um código linear com comprimento n e dimensão k. Se $a_{k-1} \neq 0$, então pelo Teorema Fundamental da Álgebra, f possui no máximo $k-1$ raízes. Assim, o peso de Hamming de qualquer palavra código não nula $\mathbf{c}$ é

$$w_H(\mathbf{c}) \geq n - (k-1).$$

Assim, pela Proposição 3.1,

$$w_H(\mathbf{c}) = n - k + 1.$$

Se $a_{k-1} = 0$, então, pelo Teorema Fundamental da Álgebra, f possui no máximo $k-2$ raízes. Logo,

$$w_H(\mathbf{c}) \geq n - [(k-2)+1] = n - k + 1.$$

Novamente, pela Proposição 3.1,

$$w_H(\mathbf{c}) = n - k + 1.$$

Portanto, C é um código MDS. Se $n < q+1$, então obtemos este código simplesmente omitindo componentes no código acima. ■

No caso em que $n < q$, observe que os códigos RS são mais curtos em comparação com o tamanho do alfabeto.

Observação 3.6 *Não existe código (linear ou não)* $[4,2,3]$ *sobre* $\mathbb{F}_2$*. De fato, suponhamos, por absurdo, que exista um* $[4,2,3]$*-código* C *sobre* $\mathbb{F}_2$*. Sendo*

$$d(C) = d(C + \mathbf{a})$$

para todo $\mathbf{a} \in \mathbb{F}_2^4$ *podemos supor, sem perda de generalidade, que* $(0,0,0,0) \in C$*. Sendo* C *um código* MDS *temos, que cada par de posições é um conjunto de informação. Assim, existe uma palavra código com* $(0,1)$ *nas duas primeiras posições, a qual deve ser* $(0,1,1,1)$*, pois caso contrário,* $d(C) < 3$*. Similarmente,* C *contém*

$$(1,0,1,1), (1,1,0,1) \quad e \quad (1,1,1,0).$$

Mas a distância de Hamming entre qualquer duas palavras é igual a 2*, o que é uma contradição. Portanto, concluímos que não existe um código* $[4,2,3]$ *sobre* $\mathbb{F}_2$*, no entanto, o Teorema* 3.5*, prova que existe um código linear* $[4,2,3]$ *sobre* $\mathbb{F}_q$ *com* $q \geq 3$*. Assim, podemos notar que sobre corpos grandes temos bons parâmetros de códigos.*

Antes de apresentarmos a noção de código algébrico geométrico, vamos introduzir as seguintes notações:

- $F/\mathbb{F}_q$ um corpo de funções algébricas de gênero g.
- $P_1, \ldots, P_n$ lugares distintos aos pares de $F/\mathbb{F}_q$ de grau 1.
- $D = P_1 + \cdots + P_n$.
- G um divisor de $F/\mathbb{F}_q$ tal que

$$\operatorname{supp} G \cap \operatorname{supp} D = \emptyset.$$

O código algébrico geométrico (ou código AG) $C_{\mathcal{L}}(D,G)$ associado aos divisores D e G é definido por

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

Note que a definição acima faz sentido, pois

$$\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$$

implica que

$$v_{P_i}(x) \geq -v_{P_i}(G) = 0, \ \forall \ x \in \mathcal{L}(G) \text{ e } i = 1, \ldots, n.$$

Logo,

$$x \in \mathcal{O}_{P_i}, \ \forall \ i = 1, \ldots, n.$$

Além disso, como $\deg P_i = 1$ temos que seu corpo de classes residual pode ser identificado com

$$\mathbb{F}_q \text{ e } x(P_i) \in \frac{\mathcal{O}_{P_i}}{P_i} = \mathbb{F}_q, \ \forall \ i = 1, \ldots, n,$$

confira Observação 1.14.

Como na equação (3.1) podemos considerar a função $\varphi : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n$ definida como

$$\varphi(x) = (x(P_1), \ldots, x(P_n)),$$

Então verifica-se que φ é uma aplicação linear e sua imagem é $C_{\mathcal{L}}(D, G)$, pois $\mathcal{L}(G)$ é um espaço vetorial sobre $\mathbb{F}_q$. Logo, $C_{\mathcal{L}}(D, G) = \varphi(\mathcal{L}(G))$ é um código linear sobre $\mathbb{F}_q$ de comprimento n.

Teorema 3.7 *$C_{\mathcal{L}}(D, G)$ é um $[n, k, d]$-código sobre $\mathbb{F}_q$ com parâmetros*

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

Prova. Primeiro vamos provar que

$$\ker \varphi = \{x \in \mathcal{L}(G) : v_{P_i}(x) > 0, \ \forall \ i = 1, \ldots, n\} = \mathcal{L}(G - D).$$

Dado $x \in \ker \varphi$, obtemos

$$(x(P_1), \ldots, x(P_n)) = (0, \ldots, 0).$$

Logo, $x(P_i) = 0$, para todo $i = 1, \ldots, n$. Neste caso, $v_{P_i}(x) > 0$, para todo $i = 1, \ldots, n$. Como $v_Q(x) \geq -v_Q(G)$, para todo $Q \in \mathbb{P}_F$, e

$$\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$$

temos que

$$v_Q(x) \geq -v_Q(G) = -v_Q(G) + v_Q(D), \ \forall \ Q \notin \{P_1, \ldots, P_n\},$$

e

$$v_Q(x) \geq 1 = -v_Q(G) + v_Q(D), \ \forall \ Q \in \{P_1, \ldots, P_n\}.$$

Portanto, $\ker \varphi \subseteq \mathcal{L}(G - D)$. Por outro lado, dado $x \in \mathcal{L}(G - D)$, obtemos

$$v_Q(x) \geq -v_Q(G) + v_Q(D) \geq -v_Q(G), \ \forall \ Q \in \mathbb{P}_F.$$

Logo $x \in \mathcal{L}(G)$, isto é,

$$\mathcal{L}(G - D) \subseteq \mathcal{L}(G).$$

Como

$$v_Q(x) \geq 1 = -v_Q(G) + v_Q(D) > 0, \ \forall \ Q \in \{P_1, \ldots, P_n\}.$$

temos que

$$x \in \mathcal{L}(G) \ \text{ e } \ x \in P_i, \ \forall \ i = 1, \ldots, n,$$

isto é, $x \in \ker \varphi$. Portanto, $\mathcal{L}(G - D) \subseteq \ker \varphi$. Assim, pelo Primeiro Teorema de Isomorfismo, obtemos

$$\frac{\mathcal{L}(G)}{\ker \varphi} \simeq \operatorname{Im} \varphi = C_{\mathcal{L}}(G, D) \ \text{ e } \ \ell(G) - \dim \ker \varphi = \dim C_{\mathcal{L}}(G, D) = k.$$

Como

$$\ker \varphi = \mathcal{L}(G - D),$$

temos

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

Suponhamos que $C_{\mathcal{L}}(G, D) \neq \{0\}$, caso contrário, não faria sentido falarmos em distância mínima. Então escolha um elemento $0 \neq x \in \mathcal{L}(G)$, com

$$\omega_H(\varphi(x)) = d.$$

Logo,

$$|\{i : x(P_i) = 0\}| = n - d,$$

ou seja, existem exatamente $n - d$ lugares $P_{i_1}, \ldots, P_{i_{n-d}}$ em $\operatorname{supp} D$ que são zeros de x. Uma vez que $\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$,

$$v_Q(x) \geq -v_Q(G) = -v_Q(G) + v_Q(D), \ \forall \ Q \notin \{P_{i_1}, \ldots, P_{i_{n-d}}\},$$

$$v_Q(x) \geq 1 = -v_Q(G) + v_Q(D), \ \forall \ Q \in \{P_{i_1}, \ldots, P_{i_{n-d}}\}.$$

Assim,

$$0 \neq x \in \mathcal{L}(G - (P_{i_1} + \cdots + P_{i_{n-d}})) \text{ e } \ell(G - (P_{i_1} + \cdots + P_{i_{n-d}})) \neq 0$$

Logo, pelo Corolário 1.27, obtemos

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

Portanto, $d \geq n - \deg G$. ■

Corolário 3.8 *Suponhamos que* $\deg G < n$. *Então* $\varphi : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n$ *é injetora. Neste caso,* $C_{\mathcal{L}}(G, D)$ *é um* $[n, k, d]$*-código, em que*

$$d \geq n - \deg G, \ \ k = \ell(G) \geq \deg G + 1 - g$$

e a matriz geradora é

$$\mathbf{G} = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \ldots & x_1(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ x_k(P_1) & x_k(P_2) & \ldots & x_k(P_n) \end{pmatrix},$$

onde $\{x_1, \ldots x_k\}$ *é uma base para* $\mathcal{L}(G)$.

Prova. Sendo

$$\deg(G - D) = \deg G - n < 0$$

temos, pelo Corolário 1.27), que $\mathcal{L}(G - D) = \{0\}$. Assim, $\ker \varphi = \{0\}$, ou seja, φ é injetora. Pelo Teorema 3.7,

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

Como $\ell(G - D) = 0$ temos, pelo Teorema de Riemann, que

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

Além disso, se $\{x_1, \ \ldots, \ x_k\}$ é uma base para $\mathcal{L}(G)$, então

$$\{(x_i(P_1), \ldots, x_i(P_n))\}, \ \ i = 1, \ldots, k,$$

é uma base de $C_{\mathcal{L}}(G, \ D)$, pois φ é injetora. Portanto, $\mathbf{G}$ é a matriz geradora de $C_{\mathcal{L}}(G, D)$. ■

3.4 Códigos Algébricos Geométricos Racionais

Nesta seção vamos investigar códigos AG associados a divisores de um corpo de funções racionais. Mais a frente vamos perceber que tais códigos podem ser encarados como uma generalização natural dos códigos Reed-Solomon e por isso são denominados de códigos Reed-Solomon Generalizados.

Um código algébrico geométrico $C_{\mathcal{L}}(D,\, G)$ associado com os divisores G e D de um corpo de funções racionais $\mathbb{F}_q(z)/\mathbb{F}_q$ é chamado de *código algébrico geométrico racional* ou um *código AG racional*.

Observe que o comprimento de um código AG racional é no máximo $q+1$, pois pelo Teorema 1.21 $\mathbb{F}_q(z)$ possui somente $q+1$ lugares de grau um, a saber, o polo P_∞ de z e para cada $\alpha \in \mathbb{F}_q$, P_α o zero de $z-\alpha$. Lembremos que o Exemplo 1.31 nos garante que o corpo de funções racionais possui gênero $g = 0$.

Proposição 3.9 *Seja $C = C_{\mathcal{L}}(D, G)$ um código AG racional $[n, k, d]$ sobre $\mathbb{F}_q$. Então:*

1. *$k = n \Leftrightarrow \deg G > n - 2$.*
2. *Se $0 \leq \deg G \leq n - 2$, então*

$$k = 1 + \deg G \;\; e \;\; d = n - \deg G.$$

3. *Se $n = q + 1$, então C possui a matriz geradora*

$$\mathbf{G} = \begin{pmatrix} v_1 & v_2 & \dots & v_{n-1} & 0 \\ \alpha_1 v_1 & \alpha_2 v_2 & \dots & \alpha_{n-1} v_{n-1} & 0 \\ {\alpha_1}^2 v_1 & {\alpha_2}^2 v_2 & \dots & {\alpha_{n-1}}^2 v_{n-1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ {\alpha_1}^{k-1} v_1 & {\alpha_2}^{k-1} v_2 & \dots & {\alpha_{n-1}}^{k-1} v_{n-1} & 1 \end{pmatrix}$$

onde $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_{n-1}\}$ e $v_1, \dots, v_{n-1} \in \mathbb{F}_q^*$.

Prova. 1 Se $k = n$, então pela Proposição 3.1

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

Assim, pelo Teorema 3.7, obtemos

$$1 \geq d \geq n - \deg G \Rightarrow 1 - n \geq -\deg G \Rightarrow \deg G \geq n - 1 \Rightarrow \deg G > n - 2.$$

Reciprocamente, como $n \geq 1$ temos, pelo Teorema 1.32, que

$$\deg G > n - 2 \geq 1 - 2 = -1 = 2g - 1 \Rightarrow \ell(G) = \deg G + 1.$$

Analogamente,

$$\begin{aligned} \deg G - n &> -2 \Rightarrow \deg(G-D) = \deg G - \deg D = \deg G - n > -2 \\ &\Rightarrow \deg(G-D) \geq -1 \Rightarrow \ell(G-D) = deg\ G - n + 1. \end{aligned}$$

Portanto, pelo Teorema 3.7,

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

2 Note que, pelo e o ,

$$\begin{aligned} 0 &\leq \deg G \leq n-2 \Rightarrow -2 < 0 \leq \deg G \leq n-2 < n \\ &\Rightarrow -2 + 2g < \deg G < n. \end{aligned}$$

Agora, segue do Corolário 3.8 que $k = \ell(G)$ e do Teorema 1.32 $k = \ell(G) = \deg G + 1$. Assim, pela Proposição 3.1,

$$k + d \leq n + 1 \Rightarrow \deg G + 1 + d \leq n + 1 \Rightarrow d \leq n - \deg G.$$

Mas, pelo Teorema 3.7,

$$d \geq n - \deg G \Rightarrow d = n - \deg G.$$

3 Não há perda de generalidade em supor que $1 < k < n$, pois se $k = n$ a base canônica de $\mathbb{F}_q^n$ é uma base para o código e se $k = 1$ qualquer elemento não nulo do código serve como base, consequentemente em ambos os casos a matriz do código é conhecida.

Pondo z, o elemento gerador de $\mathbb{F}_q(z)$, e consideremos

$$D = P_1 + \cdots + P_n \text{ e } P_n = P_\infty.$$

Pelos itens (1) e (2) vamos considerar

$$k = \deg G + 1,$$

de modo que

$$0 \leq \deg G \leq n - 2,$$

pois se $\deg G < 0$,então $\mathcal{L}(G) = \{0\}$ pelo Corolário 1.27. Note que o divisor

$$(k-1)P_\infty - G$$

satisfaz as seguintes condições:

$$\deg((k-1)P_\infty - G) = \deg((k-1)P_\infty) - \deg G = k - 1 - k + 1 = 0 \geq -1 = 2g - 1$$

e, pelo Teorema 1.32,

$$\ell((k-1)P_\infty - G) = \deg((k-1)P_\infty - G) + 1 = 1.$$

Assim, pelo Corolário 1.27,

$$(k-1)P_\infty - G = (u), \text{ onde } 0 \neq u \in \mathbb{F}_q(z).$$

Agora, consideremos o conjunto

$$\{u, zu, \ldots, z^{k-1}u\}.$$

Note que $z^i u \in \mathcal{L}(G)$, $i = 0, \ldots, k-1$, pois

$$(z^i u) = i(P_0 - P_\infty) + (k-1)P_\infty - G = iP_0 + (k-1-i)P_\infty - G.$$

Como

$$iP_0 + (k-1-i)P_\infty \geq 0 \Rightarrow iP_0 + (k-1-i)P_\infty - G \geq -G$$

temos que

$$(z^i u) \geq -G \Rightarrow z^i u \in \mathcal{L}(G).$$

Afirmação. $\{u, zu, \ldots, z^{k-1}u\}$ é LI sobre.$\mathbb{F}_q$
De fato, seja

$$\sum_{i=1}^{k-1} a_i(z^i u) = 0.$$

Então

$$\sum_{i=0}^{k-1} a_i(z^i u) = u\sum_{i=0}^{k-1} a_i z^i \Rightarrow \sum_{i=0}^{k-1} a_i z^i = 0 \Rightarrow a_i = 0, \text{ para todo } i,$$

pois z um elemento transcendente sobre $\mathbb{F}_q$. Portanto,

$$\{u, zu, \ldots, z^{k-1}u\}$$

é uma base para $\mathcal{L}(G)$ e pelo Teorema 1.32 $k = \ell(G)$. Além disso, os elementos $\alpha_j = z(P_j) \in \mathbb{F}_q$ são distintos aos pares, pois se $\alpha_i = \alpha_j$, então $P_i = P_j$. Observe que $u(P_j) \in \mathbb{F}_q^*$, $j = 1, \ldots, n-1$, uma vez que $P_j \notin \text{supp}(u)$.

Finalmente, vamos analisar o comportamento das classes em $P_n = P_\infty$. De fato, se $i = 0, \ldots, k-2$, então

$$v_{P_n}(uz^i) = v_{P_n}(u) + iv_{P_n}(z) = k-1-i \geq 1 \Rightarrow (uz^i)(P_n) = 0(P_n).$$

Se $i = k-1$, então

$$v_{P_n}(uz^i) = 0 \Rightarrow (uz^i)(P_n) = \gamma \in \mathbb{F}_q^*.$$

Portanto,

$$((uz^i)(P_1), \ldots, (uz^i)(P_n)) = (\alpha_1^i u(P_1), \ldots, \alpha_{n-1}^i u(P_{n-1}), 0), \;\; i = 1, \ldots, k-2$$

e

$$((uz^i)(P_1), \ldots, (uz^i)(P_n)) = (\alpha_1^i u(P_1), \ldots, \alpha_{n-1}^i u(P_{n-1}), \gamma), \;\; i = k-1$$

Assim, substituindo u por $\gamma^{-1}u$ e considerando $v_i = \gamma^{-1}u(P_i)$, obtemos pelo Corolário 3.8 a matriz desejada. ■

Observação 3.10 *Note que*

$$\mathcal{L}(G) = \{uf(z) : f \in \mathbb{F}_q[z] \ \ e \ \ \deg f \leq k-1\}$$

e

$$C = \{(v_1 f(\alpha_1), \ldots, v_{n-1} f(\alpha_{n-1}), \theta) : \deg f \leq k-1 \ \ e \ \ \theta \in \mathbb{F}_q\},$$

o que justifica a denominação de código de RS generalizado.

Com base na proposição anterior, exibiremos o exemplo de um código AG sobre o corpo de funções racionais.

Exemplo 3.11 *Seja*

$$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$$

um corpo finito com cinco elementos. Nosso objetivo é determinar uma matriz geradora, a distância mínima e a dimensão do código $C_{\mathcal{L}}(G, D)$, com

$$D = P_0 + P_1 + P_2 + P_3 + P_4 + P_\infty.$$

Note que $p = z^2 - 3$ é um polinômio irredutível sobre $\mathbb{F}_5$. Pondo

$$G = P_{z^2-3},$$

obtemos, pela Proposição 1.20*,*

$$\deg G = 2 < 6 - 2 = 4.$$

Portanto, $k = 3$ e $d = 4$. Note que o elemento

$$\frac{1}{z^2 - 3}$$

tem zero apenas em P_∞ e polo apenas em P_{z^2-3}, logo

$$v_\infty\left(\frac{1}{z^2-3}\right) = 2 \ \ e \ \ v_{P_{z^2-3}}\left(\frac{1}{z^2-3}\right) = -1,$$

de modo que

$$\left(\frac{1}{z^2-3}\right) = 2P_\infty - G.$$

Assim, o conjunto

$$\left\{\frac{1}{z^2-3}, \frac{z}{(z^2-3)}, \frac{z^2}{(z^2-3)}\right\}$$

é uma base para $\mathcal{L}(G)$. Logo, pela Proposição 1.20*,*

$$\frac{1}{z^2-3}(P_1) = \frac{1}{1^2-3} = -\frac{1}{2}, \ \ \frac{z^2}{z^2-3}(P_\infty) = 1.$$

Analogamente, obtemos os outros valores para as demais classes em cada lugar racional que compõe D. Portanto, a matriz de $C_{\mathcal{L}}(G, D)$ é dada por

$$\begin{pmatrix} -\frac{1}{3} & -\frac{1}{2} & 1 & \frac{1}{6} & \frac{1}{13} & 0 \\ 0 & -\frac{1}{2} & 2 & \frac{1}{2} & \frac{4}{13} & 0 \\ 0 & -\frac{1}{2} & 4 & \frac{3}{2} & \frac{16}{13} & 1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{3} & -\frac{1}{2} & 1 & 1 & \frac{1}{3} & 0 \\ 0 & -\frac{1}{2} & 2 & \frac{1}{2} & \frac{4}{3} & 0 \\ 0 & -\frac{1}{2} & 4 & \frac{3}{2} & \frac{1}{3} & 1 \end{pmatrix}.$$

Capítulo 4

Códigos Lineares Disjuntos

Em [4, p.499, Teorema 2], Johansson e Pasalic, mostraram que a existência de uma classe de funções, as funções *resilient* definidas de $\mathbb{F}_2^n$ em $\mathbb{F}_2^m$ onde $m, n \in \mathbb{N}$, está condicionada à existência de um conjunto de códigos lineares sobre $\mathbb{F}_2$ cuja interseção aos pares contenha apenas o vetor nulo. Motivados pela necessidade de obter uma estimativa para a quantidade de códigos lineares com essas características, é que Niederreiter e Xing apresentam em seu artigo *Disjoint Linear Codes From Algebraic Function Fields*, [9] não só uma estimativa para a quantidade, como também um método para obter tais códigos sobre um corpo finito qualquer $\mathbb{F}_q$ e a análise de alguns comportamentos assintóticos. O objetivo deste capítulo é apresentar o estudo feito por Niederreiter e Xing no artigo supra citado.

4.1 Códigos Lineares Disjuntos

Dois códigos lineares q-ários de mesmo comprimento são ditos *disjuntos* se sua interseção consiste apenas do vetor nulo. Estamos interessados na seguinte questão: dados o comprimento, a dimensão e a distância mínima, quantos códigos lineares q-ários disjuntos podemos determinar? Quando falamos de um conjunto de códigos q-ários disjuntos, nos referimos a códigos de mesmo comprimento que são disjuntos aos pares.

Lema 4.1 *Sejam $\mathbb{F}_q$ um corpo finito e $V(k,q)$ um espaço vetorial de dimensão k sobre $\mathbb{F}_q$. Então o número de bases distintas para $V(k,q)$ é igual a*:

$$\prod_{i=0}^{k-1}(q^k - q^i).$$

Prova. Note que qualquer base para $V(k,q)$ pode ser construída como segue: qualquer vetor $\mathbf{v}_1 \in V(k,q)$, $\mathbf{v}_1 \neq \mathbf{0}$, pode ser escolhido para ser o primeiro vetor de uma base para $V(k,q)$. Como $V(k,q) \simeq \mathbb{F}_q^k$ temos que $|V(k,q)| = q^k$, de modo que existem $q^k - 1$ escolhas para $\mathbf{v}_1$. Qualquer $\mathbf{v}_2 \in V(k,q)$; $\mathbf{v}_2$ não pertence ao espaço gerado por $\mathbf{v}_1$, é linearmente independente com $\mathbf{v}_1$, de modo que podemos escolher $\mathbf{v}_2$ para o segundo vetor de uma base para $V(k,q)$. Como

$$V(1,q) = \{x\mathbf{v}_1 : x \in \mathbb{F}_q\} \simeq \mathbb{F}_q$$

temos que $|V(1,q)| = q$. Assim, existem $q^k - q$ escolhas para $\mathbf{v}_2$ Continuando com esse processo, obtemos

$$(q^k-1)(q^k-q)\cdots(q^k-q^{k-1}) = \prod_{i=0}^{k-1}(q^k-q^i),$$

que é o resultado desejado. ■

Corolário 4.2 *Sejam $\mathbb{F}_q$ um corpo finito e $V(n,q)$ o espaço vetorial de dimensão n sobre $\mathbb{F}_q$.*

1. *O número de subespaços distintos de dimensão k contidos em $V(n,q)$ é igual a:*

$$N_q(k,n) = \prod_{i=0}^{k-1}\frac{q^{n-i}-1}{q^{k-i}-1}.$$

2. *Para um subespaço de dimensão l fixado em $V(n,q)$, o número de subespaços distintos de dimensão k de $V(n,q)$ contendo $V(l,q)$ é igual a $N_q(k-l,n-l)$.*

Prova. (1) Como os conjuntos

$$\{\mathbf{u}_1,\ldots,\mathbf{u}_k\} \text{ e } \{\mathbf{v}_1,\ldots,\mathbf{v}_k\}$$

geram $V(k,q)$ se, e somente se, eles são bases para $V(k,q)$ temos, pelo Lema 4.1, que

$$N_q(k,n) = \frac{\prod_{i=0}^{k-1}(q^n-q^i)}{\prod_{i=0}^{k-1}(q^k-q^i)} = \prod_{i=0}^{k-1}\frac{q^{n-i}-1}{q^{k-i}-1}.$$

(2) Consideremos o espaço quociente

$$W(n-l,q) = \frac{V(n,q)}{V(l,q)} \simeq \mathbb{F}_q^{n-l}.$$

Se $V(k,q)$ é qualquer subespaço de $V(n,q)$ contendo $V(l,q)$, então

$$W(k-l,q) = \frac{V(k,q)}{V(l,q)} \simeq \mathbb{F}_q^{k-l}.$$

é um subespaço de dimensão $k-l$ de $W(n-l,q)$. Assim, pelo item (1), o número de subespaços de dimensão $k-l$ de $W(n-l,q)$ é igual a $N_q(k-l,n-l)$. Como

$$\frac{W(n-l,q)}{W(k-l,q)} \simeq \frac{V(n,q)}{V(k,q)}$$

temos que o número de subespaços distintos de dimensão k de $V(n,q)$ contendo $V(l,q)$ é igual a $N_q(k-l,n-l)$. ■

Para números inteiros positivos fixados n, k e d, considere $S = \{C \leq \mathbb{F}_q^n : C \text{ é de tipo } [n,\ k,\ \geq d] \text{ disjuntos aos pares}\}$. Denotaremos por $M_q(n,k,d) = |S|$.

Proposição 4.3 *Para números inteiros positivos fixados n, k e d, obtemos*

$$M_q(n,k,d) \leq \frac{q^n-1}{q^k-1}$$

Prova. Seja S o conjunto de todos os códigos q-ários lineares $[n,k,\geq d]$ disjuntos aos pares, com

$$|S| = M_q(n,k,d).$$

Então é claro que os conjuntos $C-\{\mathbf{0}\}$ são disjuntos, para todo $C \in S$, e

$$\bigcup_{\mathcal{C}\in S}(C-\{\mathbf{0}\}) \subseteq \mathbb{F}_q^n - \{\mathbf{0}\}.$$

Como $|C| = q^k$ temos

$$q^n - 1 = \left|\mathbb{F}_q^n - \{\mathbf{0}\}\right| \geq \left|\bigcup_{\mathcal{C}\in S}(C-\{\mathbf{0}\})\right| = \sum_{\mathcal{C}\in S}(|C|-1) = |S|\,(q^k-1),$$

que é o resultado desejado. ■

Lema 4.4 *Seja $\mathcal{C}$ o conjunto de todos os códigos lineares q-ários disjuntos, com comprimento n, dimensão pelo menos k e distância mínima pelo menos d. Então*

$$|\mathcal{C}| \leq M_q(n,k,d).$$

Prova. Para cada $C \in \mathcal{C}$, tome um único código D_C tal que $D_C \subseteq C$ e $\dim D_C = k$. Então o conjunto

$$\mathcal{D} = \{D_C : C \in \mathcal{C}\}$$

é tal que $|\mathcal{C}| = |\mathcal{D}|$. Como os códigos em D são disjuntos temos, pela Proposição 4.3, que $|\mathcal{D}| \leq M_q(n,k,d)$. Portanto, $|\mathcal{C}| \leq M_q(n,k,d)$. ■

Observação 4.5 *Considerando um código* A *fixo sobre $\mathbb{F}_q$ e a aplicação linear injetora*

$$\begin{array}{rccc} \Phi^*: & \mathbb{F}_{q^t}^n & \to & \mathbb{F}_q^{mn} \\ & (\mathbf{v}_1,\ldots,\mathbf{v}_n) & \mapsto & (\Phi(\mathbf{v}_1),\ldots,\Phi(\mathbf{v}_n)) \end{array}$$

definida na prova da Proposição 3.3. *Para qualquer família $\{C_i\}_{i\in I}$ de códigos lineares disjuntos aos pares sobre $\mathbb{F}_{q^t}$, a família*

$$\{\Phi^*(C_i)\}_{i\in I}$$

é de códigos concatenados disjuntos, pois Φ^* é injetora.

Lema 4.6 *Seja S um conjunto de códigos q^t-ários lineares $[n,k,\geq d]$ disjuntos. Se existir um A código linear* q*-ário $[m,t,\geq s]$, então*

$$M_q(nm,kt,ds) \geq |S|.$$

Prova. Seja $S := \{C_i\}_{i\in I}$. Então, pela Observação 4.5,

$$\{\Phi^*(C_i)\}_{i\in I}$$

é uma família de $[nm, kt, \geq ds]$-códigos concatenados disjuntos. Logo, pela injetividade de Φ^* e a Proposição 4.3, obtemos

$$|\{C_i\}_{i\in I}| = |\{\Phi^*(C_i)\}_{i\in I}| \leq M_q(nm, kt, ds),$$

que é o resultado desejado. ■

Sejam R e δ dois número reais no intervalo $(0, 1)$, definimos

$$A_q(R, \delta) = \sup_{\sigma} \left\{ \limsup_{n\to\infty} \frac{\log_q M_q(n, k_n, d_n)}{n} \right\},$$

onde o supremo é estendido sobre todas as sequências σ de ternos ordenados $(n, k_n, d_n) \in \mathbb{N}^3$ e $n \in \mathbb{N}$, com

$$\lim_{n\to\infty} \frac{k_n}{n} = R \text{ e } \lim_{n\to\infty} \frac{d_n}{n} = \delta.$$

Note, pela Proposição 4.3, que

$$M_q(n, k_n, d_n) \leq \frac{q^n - 1}{q^{k_n} - 1}.$$

Portanto, $A_q(R,\, \delta) \leq 1 - R$. De fato,

$$\frac{q^n - 1}{q^{k_n} - 1} \leq \frac{q^n}{q^{k_n} - 1} = \frac{q^{n-k_n+1}}{q - \left(\frac{1}{q}\right)^{k_n-1}},$$

entretanto

$$\begin{aligned} q \;\geq\; 2 \text{ e } \left(\frac{1}{q}\right)^{k_n-1} \leq 1 &\Rightarrow q - \left(\frac{1}{q}\right)^{k_n-1} \geq 1 \\ \Rightarrow \quad \frac{1}{q - \left(\frac{1}{q}\right)^{k_n-1}} \leq 1 &\Rightarrow \frac{q^{n-k_n+1}}{q - \left(\frac{1}{q}\right)^{k_n-1}} \leq q^{n-k_n+1}. \end{aligned}$$

Assim,

$$\begin{aligned} \frac{\log_q M_q(n, k_n, d_n)}{n} &\leq \frac{\log_q q^{n-k_n+1}}{n} = 1 - \frac{k_n}{n} + \frac{1}{n} \Rightarrow \\ \limsup_{n\to\infty} \frac{\log_q M_q(n, k_n, d_n)}{n} &\leq \limsup_{n\to\infty} \left(1 - \frac{k_n}{n} + \frac{1}{n}\right) = 1 - R. \end{aligned}$$

Portanto,

$$A_q(R, \delta) = \sup_{\sigma} \left\{ \limsup_{n\to\infty} \frac{\log_q M_q(n, k_n, d_n)}{n} \right\} \leq 1 - R.$$

A proposição a seguir é o resultado da generalização do caso particular $q = 2$ apresentado por Pasalic e Johanson em [4, Teorema 3, p. 500].

Proposição 4.7 *Para $k, n \in \mathbb{N}$ fixados, com $n > k \geq 2$, obtemos*

$$M_q(n,k,d) \geq B_q(n,k,d) = \left\lceil \frac{N_q(k,n) - \left(\frac{S_q(n,d)}{q-1}\right) N_q(k-1,n-1)}{(q^k-1)(N_q(k-1,n-1)-1)} \right\rceil,$$

onde

$$\lceil x \rceil = \min\{n \in \mathbb{Z} : x \leq n\} \;\; e \;\; S_q(n,\, d) = \left|\{\mathbf{x} \in \mathbb{F}_q^n : 1 \leq \omega_H(\mathbf{x}) \leq d-1\}\right|.$$

Prova. Sejam $\mathcal{C}$ o conjunto de todos os códigos lineares q-ários com comprimento n, dimensão k e a esfera

$$S_d = \{\mathbf{x} \in \mathbb{F}_q^n : 1 \leq \omega_H(\mathbf{x}) \leq d-1\}.$$

Então $C \cap S_d = \emptyset$, para todo $C \in \mathcal{C}$, com distância mínima igual a d. Como qualquer palavra em S_d gera um espaço vetorial de dimensão 1 sobre $\mathbb{F}_q$ temos, pelo item (2) do Corolário 4.2, que o número de códigos em $\mathcal{C}$ contendo uma palavra $\mathbf{x} \in S_d$ é igual a $N_q(k-1,n-1)$. Assim, existem pelo menos

$$N_q(k,n) - N_q(k-1,n-1)\frac{S_q(n,d)}{q-1} \tag{4.1}$$

códigos em $\mathcal{C}$ S_d. Logo, a expressão (4.1) é uma cota superior para o número de códigos de $\mathcal{C}$ interseptando S_d, pois alguns códigos podem conter mais de uma palavra de S_d. Seja C_1 qualquer dos códigos restantes de $\mathcal{C}$. Então

$$|\{C \in \mathcal{C} : C \cap C_1 \neq \{\mathbf{0}\}\}| \leq (q^k-1)(N_q(k-1,n-1)-1),$$

pois qualquer das q^k-1 palavras de C_1 pode estar em no máximo $N_q(k-1,n-1)-1$ códigos. Continuando com esse processo escolhendo um novo código C_2 em $\mathcal{C}$ e removendo todos os códigos que interseptam C_2.Assim, um M-ésimo código $[n,k,d]$ pode ser adicionado ao conjunto de códigos que não interseptam esses códigos se a seguinte desigualdade vale

$$N_q(k,n) - N_q(k-1,n-1)\frac{S_q(n,d)}{q-1} - [(M-1)(q^k-1)(N_q(k-1,n-1)-1)] \geq 0.$$

Portanto,

$$M_q(n,k,d) \geq \left\lceil \frac{N_q(k,n) - \left(\frac{S_q(n,d)}{q-1}\right) N_q(k-1,n-1)}{(q^k-1)(N_q(k-1,n-1)-1)} \right\rceil,$$

que é o resultado desejado. ■

Com base na Proposição 4.7 podemos definir, para R e δ fixados no intervalo $(0,1)$,

$$B_q(R,\delta) = \sup_{\sigma} \left\{ \limsup_{n\to\infty} \frac{\log_q B_q(n,k,d)}{n} \right\},$$

onde o supremo é estendido sobre todas as sequências σ de ternos ordenados $(n,k_n,d_n) \in \mathbb{N}^3$ e $n \in \mathbb{N}$, com

$$\lim_{n\to\infty} \frac{k_n}{n} = R \;\text{ e }\; \lim_{n\to\infty} \frac{d_n}{n} = \delta.$$

Note que

$$B_q(R,\delta) \leq \sup_{\sigma}\left\{\limsup_{n\to\infty}\frac{1}{n}\log_q\frac{N_q(k_n,\,n)}{q^{k_n}N_q(k_n-1,\,n-1)}\right\}.$$

De fato, observe que $n > k_n \geq 2$ implica que

$$\frac{q^{n-1}-1}{q^{k_n-1}-1} \geq \frac{q^{n-1}}{q^{k_n-1}} = q^{n-k_n} \geq q.$$

Assim,

$$N_q(k_n-1,n-1) = \frac{q^{n-1}-1}{q^{k_n-1}-1}\prod_{i=1}^{k_n-2}\frac{q^{(n-1)-i}-1}{q^{(k_n-1)-i}-1} \Rightarrow N_q(k_n-1,n-1) \geq q. \tag{4.2}$$

Para simplificar a notação vamos denotar por $N = N_q(k_n,n)$, $S = S_q(n,d_n)$ e $N_1 = N_q(k_n - 1, n-1)$. Logo,

$$\begin{aligned}\left\lceil\frac{N-\left(\frac{S}{q-1}\right)N_1}{(q^{k_n}-1)(N_1-1)}\right\rceil &\leq 2\left(\frac{N-\left(\frac{S}{q-1}\right)N_1}{(q^{k_n}-1)(N_1-1)}\right)\\ &\leq \frac{2N}{(q^{k_n}-1)(N_1-1)} = \frac{\frac{2q^2N}{q^{k_n}N_1}}{\left(q-\left(\frac{1}{q}\right)^{k_n-1}\right)\left(q-\frac{q}{N_1}\right)}\end{aligned}$$

Utilizando a inequação (4.2), obtemos

$$\frac{\frac{2q^2N}{q^{k_n}N_1}}{\left(q-\left(\frac{1}{q}\right)^{k_n-1}\right)\left(q-\frac{q}{N_1}\right)} \leq \frac{2q^2N}{q^{k_n}N_1}.$$

Portanto,

$$\begin{aligned}\frac{\log_q B_q(n,k_n,d_n)}{n} &\leq \frac{1}{n}\log_q\left(\frac{2q^2N_q(k_n,n)}{q^{k_n}N_q(k_n-1,n-1)}\right)\\ &= \frac{1}{n}\log_q\left(\frac{N_q(k_n,n)}{q^{k_n}N_q(k_n-1,n-1)}\right)+\frac{2}{n}+\frac{1}{n}\log_q 2\end{aligned}$$

e

$$\sup_{\sigma}\left\{\limsup_{n\to\infty}\frac{\log_q B_q(n,k_n,d_n)}{n}\right\} \leq \sup_{\sigma}\left\{\limsup_{n\to\infty}\left(\frac{1}{n}\log_q\frac{N_q(k_n,n)}{q^{k_n}N_q(k_n-1,n-1)}\right)\right\},$$

isto é,

$$B_q(R,\delta) \leq \sup_{\sigma}\left\{\limsup_{n\to\infty}\left(\frac{1}{n}\log_q\frac{N_q(k_n,n)}{q^{k_n}N_q(k_n-1,n-1)}\right)\right\}.$$

Proposição 4.8 *Com as notações acima, obtemos*

$$B_q(R,\delta) \leq 1-2R.$$

Prova. Primeiro note que

$$\frac{N_q(k_n, n)}{N_q(k_n - 1, n-1)} = \frac{q^n - 1}{q^{k_n} - 1}$$

e

$$\frac{q^n - 1}{q^{k_n}(q^{k_n} - 1)} \leq \frac{q^n}{q^{k_n}(q^{k_n} - 1)} = \frac{\frac{qq^n}{q^{2k_n}}}{\left(q - \left(\frac{1}{q}\right)^{2k_n - 1}\right)} \leq \frac{qq^n}{q^{2k_n}} = q^{n+1-2k_n}.$$

Assim,

$$\sup_{\sigma}\left\{\limsup_{n\to\infty}\left(\frac{1}{n}\log_q \frac{N_q(k_n, n)}{q^{k^n} N_q(k_n - 1, n-1)}\right)\right\} \leq \lim_{n\to\infty}\left(\frac{1}{n}\log_q(q^{n+1-2k_n})\right) = 1 - 2R.$$

Portanto, $B_q(R, \delta) \leq 1 - 2R$. ■

Proposição 4.9 *Se existir um código linear q-ário $[m, t, \geq s]$, então*

$$A_q\left(\frac{Rt}{m}, \frac{\delta s}{m}\right) \geq \frac{t}{m} A_{q^t}(R, \delta).$$

Prova. Já vimos que

$$A_{q^t}(R, \delta) = \sup_{\sigma}\left\{\limsup_{n\to\infty} \frac{\log_{q^t} M_{q^t}(n, k_n, d_n)}{n}\right\},$$

onde o supremo é estendido sobre todas as sequências σ de ternos ordenados $(n, k_n, d_n) \in \mathbb{N}^3$ e $n \in \mathbb{N}$, com

$$\lim_{n\to\infty} \frac{k_n}{n} = R \text{ e } \lim_{n\to\infty} \frac{d_n}{n} = \delta.$$

Assim, dado um número real $\epsilon > 0$ existe uma sequência σ tal que

$$\limsup_{n\to\infty} \frac{\log_{q^t} M_{q^t}(n, k_n, d_n)}{n} > A_{q^t}(R, \delta) - \epsilon$$

Pelo Lema 4.6, obtemos

$$M_q(nm, k_n t, d_n s) \geq M_{q^t}(n, k_n, d_n),$$

para todo $n \in \mathbb{N}$. Mas,

$$\frac{1}{nm}\log_q M_q(nm, k_n t, d_n s) \geq \frac{t}{nm}\log_{q^t} M_{q^t}(n, k_n, d_n),$$

Logo,

$$\begin{aligned} A_q\left(\frac{Rt}{m}, \frac{\delta s}{m}\right) &\geq \limsup_{n\to\infty} \frac{\log_q M_q(mn, k_n t, d_n s)}{mn} \\ &\geq \frac{t}{m}\limsup_{n\to\infty} \frac{\log_{q^t} M_{q^t}(n, k_n, d_n)}{n} \\ &> \frac{t}{m}\left(A_{q^t}(R, \delta) - \epsilon\right). \end{aligned}$$

Como $\epsilon > 0$ é arbitrário temos que

$$A_q\left(\frac{Rt}{m}, \frac{\delta s}{m}\right) \geq \frac{t}{m} A_{q^t}(R, \delta),$$

que é o resultado desejado. ■

4.2 Construções de Códigos Lineares Disjuntos

Nesta seção vamos apresentar uma construção de códigos lineares disjuntos via corpos de funções algébricas. Através dessa construção vamos obter parâmetros R e δ para os quais $A_q(R,\ \delta) > B_q(R,\ \delta)$.

Para auxiliar na nossa construção, vamos considerar as seguintes definições: sejam

$$D_1 = \sum_{P \in \mathbb{P}_F} m_P P \text{ e } D_2 = \sum_{P \in \mathbb{P}_F} n_P P$$

dois divisores de $F/\mathbb{F}_q$. Então

$$D_1 \vee D_2 = \sum_{P \in \mathbb{P}_F} \max\{m_P, n_P\} P \text{ e } D_1 \wedge D_2 = \sum_{P \in \mathbb{P}_F} \min\{m_P, n_P\} P.$$

Proposição 4.10 *Para quaisquer divisores D_1 e D_2 de $F/\mathbb{F}_q$. obtemos*

1. $\mathcal{L}(D_1) + \mathcal{L}(D_2) \subseteq \mathcal{L}(D_1 \vee D_2)$.
2. $\mathcal{L}(D_1) \cap \mathcal{L}(D_2) = \mathcal{L}(D_1 \wedge D_2)$.

Prova. 1 Dado $g \in \mathcal{L}(D_1) + \mathcal{L}(D_2)$, existem $f_1 \in \mathcal{L}(D_1)$ e $f_2 \in \mathcal{L}(D_2)$ tal que $g = f_1 + f_2$. Já vimos que

$$v_P(f_1 + f_2) \geq \min\{v_P(f_1), v_P(f_2)\}.$$

Suponhamos que $\min\{v_P(f_1), v_P(f_2)\} = v_P(f_1)$. Então

$$\begin{aligned} v_P(f_1) &\geq -v_P(D_1) \geq -\max\{v_P(D_1), v_P(D_2)\} \Rightarrow v_P(g) \geq -v_P(D_1 \vee D_2) \\ &\Rightarrow g \in \mathcal{L}(D_1 \vee D_2), \end{aligned}$$

ou seja, $\mathcal{L}(D_1) + \mathcal{L}(D_2) \subseteq \mathcal{L}(D_1 \vee D_2)$.

2 Dado $f \in \mathcal{L}(D_1) \cap \mathcal{L}(D_2)$, obtemos $v_P(f) \geq -v_P(D_1)$ e $v_P(f) \geq -v_P(D_2)$. Assim,

$$v_P(f) \geq -\min\{v_P(D_1), v_P(D_2)\} \Rightarrow v_P(f) \geq -v_P(D_1 \wedge D_2) \Rightarrow f \in \mathcal{L}(D_1 \wedge D_2),$$

ou seja, $\mathcal{L}(D_1) \cap \mathcal{L}(D_2) \subseteq \mathcal{L}(D_1 \wedge D_2)$.

Reciprocamente, dado $f \in \mathcal{L}(D_1 \wedge D_2)$, obtemos

$$\begin{aligned} v_P(f) &\geq -v_P(D_1 \wedge D_2) = -\min\{v_P(D_1), v_P(D_2)\} \\ &\Rightarrow v_P(f) \geq -v_P(D_1) \text{ e } v_P(f) \geq -v_P(D_2) \\ &\Rightarrow f \in \mathcal{L}(D_1) \cap \mathcal{L}(D_2), \end{aligned}$$

ou seja, $\mathcal{L}(D_1 \wedge D_2) \subseteq \mathcal{L}(D_1) \cap \mathcal{L}(D_2)$. ■

Verifica-se que $\mathbb{F}_q \subseteq \mathcal{L}(D)$, quando D é um divisor positivo de $F/\mathbb{F}_q$. Assim,

$$\langle (1, \ldots, 1) \rangle \subseteq C_{\mathcal{L}}(\mathcal{P}, D),$$

onde $\mathcal{P} = P_1 + \cdots + P_n$; $\deg P_1 = \cdots = \deg P_n = 1$; $P_1, \ldots,\ P_n$ disjuntos aos pares e

$$\operatorname{supp} D \cap \operatorname{supp} \mathcal{P} = \emptyset.$$

Lema 4.11 *Sejam $F/\mathbb{F}_q$ um corpo de funções algébricas e $x \in F$ um elemento transcendente sobre $\mathbb{F}_q$ tal que $F/\mathbb{F}_q$ seja uma extensão algébrica finita de $\mathbb{F}_q(x)/\mathbb{F}_q$. Suponhamos que P' está acima P, onde $P' \in \mathbb{P}_F$ e $P \in \mathbb{P}_{\mathbb{F}_q(x)}$. Se* $\deg P' = 1$, *então* $\deg P = 1$.

Prova. Se P' está acima P, então $(\mathbb{F}_q(x))_P$ é um subcorpo de $F_{P'}$. Sendo $(\mathbb{F}_q(x))_P$ e $F_{P'}$ espaços vetoriais sobre $\mathbb{F}_q$, podemos considerar $(\mathbb{F}_q(x))_P$ como um subespaço vetorial de $F_{P'}$. Assim,

$$\deg P' = 1 \Leftrightarrow [F_{P'} : \mathbb{F}_q] = 1 \Rightarrow [(\mathbb{F}_q(x))_P : \mathbb{F}_q] = 1 \Leftrightarrow \deg P = 1,$$

que é o resultado desejado. ■

Teorema 4.12 *Seja $\mathcal{P} = P_1 + \cdots + P_n$ um divisor, com $P_1, \ldots, P_n$ lugares racionais distintos aos pares de $F/\mathbb{F}_q$. Sejam D_1 e D_2 divisores positivos de $F/\mathbb{F}_q$, com*

$$\operatorname{supp} D_j \cap \operatorname{supp} \mathcal{P} = \emptyset, \;\; j = 1, 2.$$

Se $\deg(D_1 \vee D_2) < n$ *e* $\deg(D_1 \wedge D_2) < \frac{n}{q}$, *então* $C_1 \cap C_2 = \{\mathbf{0}\}$, *onde C_j é o subespaço de $C_{\mathcal{L}}(\mathcal{P}, D_j)$ tal que*

$$C_j \oplus \langle (1, \ldots, 1) \rangle = C_{\mathcal{L}}(\mathcal{P}, D_j), \;\; j = 1, 2.$$

Prova. Primeiro vamos provar que $\mathcal{L}(D_1) \cap \mathcal{L}(D_1) = \mathbb{F}_q$. Suponhamos, por absurdo, que $\mathcal{L}(D_1) \cap \mathcal{L}(D_1) \neq \mathbb{F}_q$. Então existe um

$$x \in \mathcal{L}(D_1) \cap \mathcal{L}(D_1) = \mathcal{L}(D_1 \wedge D_2)$$

tal que $x \notin \mathbb{F}_q$. Assim, $x \in F$ é um elemento transcendente sobre $\mathbb{F}_q$. Note que

$$\begin{aligned} x \;\; &\in \;\; \mathcal{L}(D_1) \cap \mathcal{L}(D_2) \Rightarrow v_P(x) \geq -v_P(D_1 \wedge D_2) \Rightarrow -v_P(x) \leq v_P(D_1 \wedge D_2) \\ &\Rightarrow \;\; -v_P(x) \deg P \leq v_P(D_1 \wedge D_2) \deg P. \end{aligned}$$

Em particular, se $P \in \mathbb{P}_F$ é um divisor de polo de x, então pelo Teorema 1.26

$$\deg((x)_\infty) \leq \deg(D_1 \wedge D_2) \Rightarrow [F : \mathbb{F}_q(x)] = r = \deg((x)_\infty) \leq \deg(D_1 \wedge D_2).$$

Consideremos a extensão algébrica finita $F/\mathbb{F}_q$ de $\mathbb{F}_q(x)/\mathbb{F}_q$. Pelo Corolário 2.7, obtemos no máximo r lugares de grau 1 que estão acima de P_α, onde $\alpha \in \mathbb{F}_q$. Sendo P_∞ o único zero de

$$\frac{1}{x},$$

e $x \in \mathcal{L}(D_1 \wedge D_2)$, obtemos

$$v_{Pi}(x) \geq 0, \;\; 1 \leq i \leq n, \;\; \Rightarrow -v_{Pi}(x) \leq 0 \Rightarrow v_{Pi}\left(\frac{1}{x}\right) = -v_{Pi}(x) \leq 0 \Rightarrow P_i \nmid P_\infty,$$

onde a última implicação segue da prova da Proposição 2.5. Portanto, existem no máximo $N - n$ lugares de grau 1 que estão acima de P_∞, com $N = N(F)$ o número de lugares racionais

de $F/\mathbb{F}_q$. Pela Proposição 2.5 qualquer lugar de $\mathbb{P}_F$ está acima de um único lugar de $\mathbb{P}_{\mathbb{F}_q(x)}$ e pelo Lema 4.11 qualquer lugar que está abaixo de um lugar de grau 1 tem grau 1. Portanto,

$$N = \left(\sum_{\alpha \in \mathbb{F}_q} \nu_\alpha \right) + \nu_\infty,$$

onde ν_α denota o número de lugares de grau 1 que estão acima de P_α e ν_∞ o número de lugares de grau 1 que estão acima de P_∞. Além disso, como $\nu_\alpha \leq r$ e $\nu_\infty \leq N - n$ temos que

$$N = \left(\sum_{\alpha \in \mathbb{F}_q} \nu_\alpha \right) + \nu_\infty \leq qr + N - n \Rightarrow r \geq \frac{n}{q}.$$

Portanto,

$$\deg(D_1 \wedge D_2) \geq \frac{n}{q},$$

o que é uma contradição.

Finalmente, seja $\mathbf{c} \in C_1 \cap C_2$. Então existe $f_j \in \mathcal{L}(D_j) \;\; j = 1, 2$, tal que

$$\mathbf{c} = (f_1(P_1), \ldots, f_1(P_n)) = (f_2(P_1), \ldots, f_2(P_n)) \Rightarrow (f_1 - f_2)(P_i) = 0(P_i).$$

Neste caso,

$$v_{Pi}(f_1 - f_2) \geq 1, \;\; 1 \leq i \leq n,$$

pois $f_1 - f_2 \in P_i$. Além disso,

$$f_1 - f_2 \in \mathcal{L}(D_1) + \mathcal{L}(D_2) \subseteq \mathcal{L}(D_1 \vee D_2).$$

Assim,

$$v_P(f_1 - f_2) \geq -v_P((D_1 \vee D_2) - \mathcal{P}) \Rightarrow f_1 - f_2 \in \mathcal{L}((D_1 \vee D_2) - \mathcal{P}).$$

Entretanto,

$$\deg((D_1 \vee D_2) - \mathcal{P}) = \deg((D_1 \vee D_2) - n < 0,$$

pois $\deg(D_1 \vee D_2) < n$. Logo, pelo Lema 1.24,

$$\mathcal{L}((D_1 \vee D_2) - \mathcal{P}) = 0 \Rightarrow f_1 - f_2 = 0.$$

Portanto,

$$f_1 = f_2 \in \mathcal{L}(D_1) \cap \mathcal{L}(D_2) = \mathbb{F}_q,$$

isto é, $\mathbf{c} = (\beta, \ldots, \beta)$, para algum $\beta \in \mathbb{F}_q$. Donde $\mathbf{c} = \mathbf{0}$ e $C_1 \cap C_2 = \{\mathbf{0}\}$. ■

Observação 4.13 *Se D_1 e D_2 são divisores disjuntos de $F/\mathbb{F}_q$, então*

$$v_P(D_1) = 0, \;\; \forall \;\; P \in \operatorname{supp} D_2 \;\; e \;\; v_P(D_2) = 0, \;\; \forall \;\; P \in \operatorname{supp} D_1.$$

Logo,

$$\min\{v_P(D_1), v_P(D_2)\} \leq 0, \;\; \forall \;\; P \in \operatorname{supp} D_1 \cup \operatorname{supp} D_2.$$

Portanto,

$$\deg(D_1 \wedge D_2) \leq 0.$$

Em particular se os divisores forem positivos, então $D_1 \wedge D_2 = \{0\}$.

Desse modo,

$$\deg(D_1 \wedge D_2) \leq 0 < \frac{n}{q}$$

e portanto a condição

$$\deg(D_1 \wedge D_2) < \frac{n}{q}$$

é sempre satisfeita.

Teorema 4.14 *Seja* $F/\mathbb{F}_q$ *um corpo de funções algébricas com gênero* g *e* n *lugares racionais. Denotaremos por* B_r *o número de lugares de* F *de grau* r. *Se*

$$\max\{1, g\} < r < \frac{n}{2},$$

então:

1. *Para* $r = 2$ *e* 3,
$$M_q(n, r-g, n-r) \geq B_r.$$

2. *Para* $r \geq 4$,
$$M_q(n, r-g, n-r) \geq B_r + \sum_{j=2}^{\lfloor \frac{r}{2} \rfloor} \min\{B_j, B_{r-j}\}.$$

Prova. (1) Para $r \geq 2$, existem B_r códigos lineares disjuntos com dimensão pelo menos $r-g$ e distância mínima pelo menos $n-r$. De fato, sejam

$$D_1, \ldots, D_{B_r}$$

os lugares distintos de F de grau r. Note que cada lugar é um divisor e os divisores são positivos e disjuntos aos pares. Além disso,

$$\begin{aligned} \deg(D_i \vee D_j) &= \deg\left(\sum_{P \in \mathbb{P}_F} \max\{v_P(D_i), v_P(D_j)\}P\right) \leq \deg(D_i + D_j) \\ &= r + r < \frac{n}{2} + \frac{n}{2} = n, \ \forall \ i, j \in \{1, \ldots, B_r\}, \ \text{com} \ i \neq j. \end{aligned}$$

Agora, consideremos $P_1, \ldots, P_n$ os n lugares de grau 1 de F e

$$\mathcal{P} = P_1 + \cdots + P_n.$$

Como o grau de cada lugar D_i é igual a r temos que

$$\operatorname{supp} D_i \cap \operatorname{supp} \mathcal{P} = \emptyset.$$

Seja C_i um subespaço do código $C_{\mathcal{L}}(\mathcal{P}, D_i)$ tal que

$$C_i \oplus \langle (1, \ldots, 1) \rangle = C_{\mathcal{L}}(\mathcal{P}, D_i), \;\; i = 1, 2, \ldots, B_r.$$

Então, pela Observação 4.13 e o Teorema 4.12,

$$C_1, \ldots, C_{B_r}$$

são códigos lineares q-ários disjuntos aos pares, pelo Corolário 3.8

$$\dim(C_i) = \dim\left(C_{\mathcal{L}}(\mathcal{P}, D_i)\right) - 1 = \ell(D_i) - 1 \geq r - g,$$

$$d(C_i) \geq n - r.$$

Portanto, pelo Lema 4.4,

$$M_q(n, r - g, n - r) \geq B_r.$$

(2) Além dos B_r códigos lineares disjuntos obtidos no item (1), vamos determinar mais

$$\sum_{j=2}^{\lfloor \frac{r}{2} \rfloor} \min\{B_j, B_{r-j}\}.$$

códigos lineares disjuntos. De fato, se $r \geq 4$, então existem pelo menos

$$M = \sum_{j=2}^{\lfloor \frac{r}{2} \rfloor} \min\{B_j, B_{r-j}\}.$$

lugares de grau r da forma $E+G$, com E um lugar de grau j e G um lugar de grau $r-j$ disjuntos aos pares e positivos. Considerando os geradores de cada divisor temos que a interseção do suporte dos divisores da forma $E + G$, com $\mathcal{P}$ é igual ao vazio. De modo análogo à prova do item (1), obtemos M códigos q-ários lineares disjuntos. Assim, pelo Lema 4.4,

$$M_q(n, r - g, n - r) \geq B_r + \sum_{j=2}^{\lfloor \frac{r}{2} \rfloor} \min\{B_j, B_{r-j}\},$$

que é o resultado desejado. ■

Exemplo 4.15 *Seja F um corpo de funções racionais sobre $\mathbb{F}_q$, com $q \geq 8$, N_i o número de lugares racionais de $F_i = F\mathbb{F}_{q^i}$. Se $F/\mathbb{F}_q$ possui gênero 0, então pela Proposição 2.8 $F_i/\mathbb{F}_{q^i}$ possui gênero 0. Portanto, pela Proposição 2.14, $F_i/\mathbb{F}_{q^i}$ é um corpo de funções racionais. Pondo $r = 4$, $n = q + 1 > 8$ e usando as identidades (2.3), obtemos*

$$B_2 = \frac{1}{2}\left(\mu\left(\frac{2}{1}\right) N_1 + \mu\left(\frac{2}{2}\right) N_2\right) = \frac{1}{2}((-1)(q+1) + 1(q^2+1)) = \frac{q^2 - q}{2}$$

e

$$B_4 = \frac{1}{4}\left(\mu\left(\frac{4}{1}\right) N_1 + \mu\left(\frac{4}{2}\right) N_2 + \mu\left(\frac{4}{4}\right) N_4\right) = \frac{1}{4}(0 + (-1)(q^2+1) + 1(q^4+1)) = \frac{q^4 - q^2}{4}.$$

Como

$$1 < r < \frac{n}{2}$$

temos, pelo Teorema 4.14*, que*

$$M_q(q+1, 4, q-3) \geq B_4 + B_2 = \frac{q^4 + q^2 - 2q}{4}.$$

Note que assintoticamente a principal contribuição para uma cota inferior de

$$M_q(n, r-g, n-r)$$

dada no Teorema 4.14 é o termo B_r, como pode ser visto na prova do teorema a seguir.

Teorema 4.16 *Seja q o quadrado de um número primo, com $q \geq 16$. Então para qualquer*

$$\frac{1}{\sqrt{q}-1} < \lambda < \frac{1}{2},$$

obtemos

$$A_q\left(\lambda - \frac{1}{\sqrt{q}-1}, 1-\lambda\right) \geq \lambda.$$

Em particular, se

$$q \geq 49 \;\; e \;\; \frac{1}{3} + \frac{2}{3(\sqrt{q}-1)} < \lambda < \frac{1}{2},$$

então

$$A_q(R, 1-\lambda) > 1 - 2R,$$

com

$$R = \lambda - \frac{1}{\sqrt{q}-1}.$$

Prova. Seja $\{F/\mathbb{F}_q\}$ uma família de corpos de funções com gêneros crescentes $g = g(F)$ tal que

$$\lim_{g\to\infty} \frac{N(F)}{g} = \sqrt{q} - 1,$$

onde $N(F)$ é o número de lugares racionais de $F/\mathbb{F}_q$ (veja em [2] a construção dessa família). Sejam $n = N(F)$ e B_r o número de lugares de F de grau $r = \lfloor n\lambda \rfloor$. Verifica-se que

$$g < r < \frac{n}{2},$$

para n suficientemente grande. Pelo Teorema 4.14, temos

$$M_q(n, r-g, n-r) \geq B_r.$$

Seja N_i o número de lugares q^i-racionais de $F\mathbb{F}_{q^i}$. Então, pela Cota Hasse-Weil, obtemos

$$q^i + 1 - 2gq^{\frac{i}{2}} \leq N_i \leq q^i + 1 + 2gq^{\frac{i}{2}}.$$

Em particular,

$$q^r + 1 - 2gq^{\frac{r}{2}} \leq N_r \leq q^r + 1 + 2gq^{\frac{r}{2}}.$$

Como

$$N_r = \sum_{i|r} iB_i \Rightarrow rB_r \leq \sum_{i|r} iBi = N_r \Rightarrow B_r \leq \frac{N_r}{r}.$$

Temos que

$$B_r \leq \frac{N_r}{r} \leq \frac{q^r + 1 + 2gq^{\frac{r}{2}}}{r} \leq \frac{2q^r(1+g)}{r}.$$

Assim,

$$\log_q B_r \leq \log_q \frac{N_r}{r} \leq \log_q \frac{2q^r(1+g)}{r} \leq \log_q \frac{q^{r+1}(1+g)}{g} \Rightarrow$$

$$\frac{\log_q B_r}{n} \leq \left(\frac{\log_q \left(\frac{N_r}{r}\right)}{n} \right) \leq \frac{1}{n} + \frac{r}{n} + \log_q \left(1 + \frac{1}{g}\right).$$

Considerando que, quando $g \to \infty$, segue-se que $n \to \infty$

$$\limsup_{g\to\infty} \left(\frac{\log_q B_r}{n} \right) \leq \limsup_{g\to\infty} \left(\frac{\log_q \left(\frac{N_r}{r}\right)}{n} \right) \leq \lim_{g\to\infty} \left(\frac{r}{n}\right).$$

Por outro lado,

$$\liminf_{g\to\infty} \left(\frac{\log_q B_r}{n} \right) \geq \liminf_{g\to\infty} \left(\frac{\log_q \left(\frac{1}{r} \left(N_r - \sum_{i=1}^{\lfloor \frac{r}{2} \rfloor} N_i \right) \right)}{n} \right) \geq \lim_{g\to\infty} \left(\frac{r}{n}\right).$$

Portanto,

$$\lim_{g\to\infty} \left(\frac{\log_q B_r}{n} \right) = \lim_{g\to\infty} \left(\frac{r}{n}\right).$$

Note que,

$$\frac{n\lambda - 1}{n} \leq \frac{\lfloor n\lambda \rfloor}{n} \leq \frac{n\lambda + 1}{n} \Rightarrow \lim_{g\to\infty} \left(\frac{r}{n}\right) = \lambda.$$

Assim,

$$A_q\left(\lambda - \frac{1}{\sqrt{q}-1}, 1 - \lambda\right) \geq \lambda,$$

pois

$$\lim_{g\to\infty} \left(\frac{r-g}{n}\right) = \lambda - \frac{1}{\sqrt{q}-1} \text{ e } \lim_{g\to\infty} \left(\frac{n-r}{n}\right) = 1 - \lambda$$

implicam que

$$A_q(\lambda - \frac{1}{\sqrt{q}-1}, 1-\lambda) = \sup_{\sigma} \left\{ \lim_{n\to\infty} \frac{M_q(n, r-g, n-r)}{n} \right\} \geq \sup_{\sigma} \left\{ \lim_{n\to\infty} \left(\frac{\log_q B_r}{n} \right) \right\}.$$

Finalmente, como

$$\lambda - \left(\frac{1}{3} + \frac{2}{3(\sqrt{q}-1)} \right) > 0 \Rightarrow 3\lambda - 1 - \frac{2}{\sqrt{q}-1} > 0$$

temos que

$$\lambda - (1 - 2R) = \lambda - 1 + 2\left(\lambda - \frac{1}{\sqrt{q}-1}\right) = 3\lambda - 1 - \frac{2}{\sqrt{q}-1} > 0$$

Portanto, $A_q(R, 1-\lambda) > 1 - 2R$. ■

4.3 Códigos Lineares Binários Disjuntos

Nesta seção vamos considerar o caso especial em que $q = 2$ por causa da conexão entre conjuntos de códigos lineares binários disjuntos e as funções *resilient wiht hight nonlinearity.*

Teorema 4.17 *Sejam $F/\mathbb{F}_{2^t}$ um corpo de funções de gênero* g, *com* n *lugares racionais e B_r o número de lugares de F de grau* r. *Se existe um código $[m, t, \geq s]$ linear binário e*

$$\max\{1, g\} < r < \frac{n}{2},$$

então

$$M_2(mn, (r-g)t, (n-r)s) \geq B_r + \sum_{j=2}^{\lfloor \frac{r}{2} \rfloor} \min\{B_j, B_{r-j}\}.$$

Prova. Já vimos, no Teorema 4.14, que

$$M_{2^i}(n, r-g, n-r) \geq B_r + \sum_{j=2}^{\lfloor \frac{r}{2} \rfloor} \min\{B_j, B_{r-j}\}.$$

Mas, pelo Lema 4.6,

$$M_2(mn, (r-g)t, (n-r)s) \geq M_{2^t}(n, r-g, n-r).$$

Portanto,

$$M_2(mn, (r-g)t, (n-r)s) \geq B_r + \sum_{j=2}^{\lfloor \frac{r}{2} \rfloor} \min\{B_j, B_{r-j}\},$$

que é o resultado desejado. ■

Exemplo 4.18 *Seja $F/\mathbb{F}_4$ um corpo de funções de gênero* 1, *com nove lugares racionais. Logo ele é um corpo de funções maximal.e assim, pela Proposição* 2.20,

$$\alpha_i = -\sqrt{4} \Rightarrow N_3 = 4^3 + 1 - \sum_{i=1}^{2} \alpha_i = 4^3 + 1 - 2(-2)^3 = 81.$$

Logo,

$$B_3 = \frac{1}{3} \sum_{d|3} \mu\left(\frac{3}{d}\right) N_d = \frac{1}{3}\left(N_3 - N_1\right) = \frac{1}{3}(81 - 9) = 24.$$

Portanto, tomando $r = 3$ e os códigos binários

$$[2, 2, 1] \ \ e \ \ [3, 2, 2],$$

temos, pelo Teorema 4.17, *que*

$$M_2(18\ 4, 6) \geq 24 \ \ e \ \ M_2(27, 4, 12) \geq 24.$$

Teorema 4.19 *Seja $t \geq 2$ um inteiro qualquer. Então para qualquer*

$$\frac{1}{2^t - 1} < \lambda < \frac{1}{2},$$

obtemos

$$A_2\left(\lambda - \frac{1}{2^t - 1}, \frac{1-\lambda}{2t}\right) \geq \lambda.$$

Em particular, se

$$t \geq 3 \ \ e \ \ \frac{1}{3} + \frac{2}{3(2^t - 1)} < \lambda < \frac{1}{2},$$

então

$$A_2(R, \frac{1-\lambda}{2t}) > 1 - 2R,$$

com

$$R = \lambda - \frac{1}{2^t - 1}.$$

Prova. Considerando o código $[2t, 2t, 1]$ binário temos, pela Proposição 4.9

$$A_2\left(\lambda - \frac{1}{2^t - 1}, \frac{1-\lambda}{2t}\right) \geq A_{2^{2t}}\left(\lambda - \frac{1}{2^t - 1}, 1 - \lambda\right).$$

Pondo $q = 2^{2t}$, o resultado segue do Teorema 4.16. ■

Observação 4.20 *Considerando outros códigos binários lineares diferentes do código $[2t, 2t, 1]$, podemos obter outros limitantes inferiores para $A_2(R, \delta)$ para diferentes parâmetros R e δ. Por exemplo, se usarmos o código linear binário*

$$[2t + 1, 2t, 2],$$

então para $t \geq 2$ e

$$\frac{1}{2^t - 1} < \lambda < \frac{1}{2},$$

obtemos

$$A_2\left(\frac{2t}{2t+1}\left(\lambda - \frac{1}{2^t - 1}\right), \frac{2(1-\lambda)}{2t+1}\right) \geq \frac{2t\lambda}{2t+1}.$$

Para os parâmetros da segunda parte do Teorema 4.19 nós temos

$$A_q(R, \delta) > 1 - 2R,$$

e assim, pela Proposição 4.8,

$$A_q(R, 1 - \lambda) > B_q(R, 1 - \lambda).$$

Referências Bibliográficas

[1] Dummit D.; Foote R. **Abstract Algebra**. 3 ed. Danvers: John Wiley and Sons, 2004.

[2] Garcia A.; Stichtenoth A. "A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound", **Invent. Math.**, vol. 121, 1995, p. 211 − 222 .

[3] Herstein I. **Topics in Algebra**. London: Ginn and Company, 1964.

[4] Johansson, T. ; Pasalic, E. "A construction of resilient functions with high nonlinearity," **IEEE Trans. Inform. Theory**, vol. 49, (2003), p. 494 - 501.

[5] Lang S. **Algebra**. 3 ed. New York: Springer, 2002.

[6] Lidl R.; Niederreiter H. **Finite Fields**. 2 ed. Cambridge: Cambridge Univ. Press, 1997.

[7] Ling S.; Xing C. **Coding Theory: A First Course.** New York: Cambridge University Press, 2004.

[8] Lint J. H. **Introduction to Coding Theory.** 3ed. Berlin: Springer, 1999.

[9] Niederreiter H.; Xing, C. "Disjoint Linear Codes From Algebraic Function Fields", **IEEE Trans. Inform. Theory**, vol. 50, (2004), p. 2174 − 2177.

[10] Stichtenoth, H. **Algebraic Function Fields and Codes**. 2 ed. Berlin: Springer, 2009.