LEANDRO CRUVINEL LEMES

Códigos de Goppa e Distâncias Generalizadas de Hamming

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2009

LEANDRO CRUVINEL LEMES

Códigos de Goppa e Distâncias Generalizadas de Hamming

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

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria algébrica.

Orientador: Prof. Dr. Cícero Fernandes de Carvalho.

UBERLÂNDIA - MG
2009

Dados Internacionais de Catalogação na Publicação (CIP)

L552e Lemes, Leandro Cruvinel, 1985-
Códigos de Goppa e distâncias generalizadas de Hamming / Leandro Cruvinel Lemes. - 2009.
58 f.

Orientador: Cicero Fernandes de Carvalho.

Dissertação (mestrado) – Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Inclui bibliografia.

1. Códigos de Goppa - Teses. I. Carvalho, Cicero Fernandes de. II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III. Título.

CDU: 519.718

Elaborado pelo Sistema de Bibliotecas da UFU / Setor de Catalogação e Classificação

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

ALUNO: Leandro Cruvinel Lemes.

NÚMERO DE MATRÍCULA: 86187.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Códigos de Goppa e Distâncias Generalizadas de Hamming.

ORIENTADOR: Prof. Dr. Cícero Fernandes de Carvalho.

A dissertação foi **APROVADA**, em reunião pública, realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 06 de março de 2009, às 16:00 horas, com a seguinte Banca Examinadora:

NOME	**ASSINATURA**
Prof. Dr. Cícero Fernandes de Carvalho UFU - Universidade Federal de Uberlândia	
Prof. Dr. Fernando Eduardo Torres Orihuela UNICAMP - Universidade Estadual de Campinas - SP	
Prof. Dr. Victor Gonzalo Lopez Neumann UFU - Universidade Federal de Uberlândia	

Uberlândia, 06 de março de 2009.

Dedicatória

Dedico este trabalho a todos que fizeram parte dele.

Agradecimentos

Agradeço a agência FAPEMIG pela bolsa de pesquisa a mim oferecida durante o programa de pós-graduação, aos professores Fernando Eduardo Torres Orihuela e Victor Gonzalo Lopez Neumann por terem aceitado o convite para participar da banca e ao professor Cícero Fernandes de Carvalho por me orientar nesse trabalho. Agradeço ainda à Beatriz Casulari da Motta Ribeiro e ao Professor Alonso Sepúlveda Castellanos pela leitura da tese e por várias sugestões.

LEMES, L. C. *Códigos de Goppa e Distâncias Generalizadas de Hamming.* 2009. 80 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho estudamos códigos de Goppa e apresentamos diversos resultados sobre as assim chamadas distâncias generalizadas de Hamming. No caso particular de códigos Hermitianos, apresentamos resultados exatos para a primeira, segunda e terceira distâncias generalizadas de Hamming, considerando quase todos os códigos suportados em um ponto.

Palavras-chave: Códigos de Goppa, Distâncias generalizadas de Hamming, Gonalidade, Corpos de funções Hermitianos.

LEMES, L. C. *Goppa Codes and Generalized Hamming Weights.* 2009. 80 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work, we study geometric Goppa codes and present several results on the so-called generalized Hamming distances. In the particular case of Hermitian codes we present precise results for the first, second and third generalized distances, for almost all Goppa codes supported on one point.

Key-words: Goppa Codes, Generalized Hamming Weights, Gonality, Hermitian Function Field.

Sumário

Resumo **vii**

Abstract **viii**

Introdução **1**

1 Conceitos Básicos **2**
1.1 Corpos de funções, anéis de valorização, lugares e divisores 2
1.2 Adeles, diferenciais de Weil, divisores canônicos e o teorema de Riemann-Roch . 12
1.3 Derivações e diferenciais 18
1.4 Extensões de corpos de funções 25

2 Códigos e distâncias generalizadas de Hamming **27**
2.1 Códigos lineares e distâncias generalizadas de Hamming 27
2.2 Códigos de Goppa e distâncias generalizadas de Hamming 32
2.3 Códigos Hermitianos e distâncias generalizadas de Hamming 39

Referências Bibliográficas **52**

Índice Remissivo **53**

Introdução

Esta dissertação trata de códigos de Goppa, estudando, em particular, resultados relacionados com o conceito de distância generalizada de Hamming. Este conceito foi introduzido por Wei em [10]; além dos resultados de Wei apresentaremos também resultados encontrados em [9]. Tal conceito, além da importância teórica, tem também importância em aplicações práticas, como por exemplo, o estudo de transmissões sujeitas a escuta, que aliás, foi a motivação do trabalho de Wei; veja mais detalhes sobre essa aplicação em [10]. Outra aplicação prática desse conceito está na área de decodificação, especialmente a "decodificação em listas"; para mais detalhes sobre essa aplicação veja o artigo [3] de V. Guruswami.

Este trabalho está dividido em dois capítulos. No primeiro capítulo, veremos alguns conceitos e resultados fundamentais para o entendimento do que mostraremos no segundo capítulo, dentre eles os conceitos de corpos de funções algébricas de uma variável, valorizações, lugares, divisores, adeles, diferenciais de Weil e o Teorema de Riemann-Roch. No primeiro capítulo, várias demonstrações serão omitidas, as mesmas podem ser encontradas em [7]. No segundo capítulo apresentaremos definições e resultados básicos sobre códigos de Goppa e estudaremos as distâncias generalizadas de Hamming, apresentando alguns resultados sobre esse conceito. Na última seção estudaremos o caso particular dos códigos Hermitianos suportados em um ponto, apresentando resultados específicos, por exemplo, calcularemos a primeira, a segunda e a terceira distância generalizada de Hamming para esses códigos. Todos os resultados do segundo e terceiro capítulo serão demonstrados e estão baseados nas referências [9] e [10].

Leandro Cruvinel Lemes
Uberlândia-MG, 06 de março de 2009

Capítulo 1

Conceitos Básicos

1.1 Corpos de funções, anéis de valorização, lugares e divisores

Definição 1.1.1 *Um corpo de funções algébricas F/K de uma variável sobre K é uma extensão de corpos $K \subseteq F$ onde existe um elemento $x \in F$ transcendente sobre K tal que F é uma extensão algébrica finita de $K(x)$.*

Por simplicidade iremos nos referir a F/K apenas como um corpo de funções. Notaremos por $\tilde{K}$ ao conjunto

$$\tilde{K} := \{z \in F;\ z \text{ é algébrico sobre K}\}.$$

O conjunto $\tilde{K}$ é um subcorpo de F, pois, a soma, o produto e os inversos de elementos algébricos são ainda algébricos. O subcorpo $\tilde{K}$ é chamado de corpo de constantes de F/K. Temos que $K \subseteq \tilde{K} \subsetneq F$ e, facilmente, pode se verificar que $F/\tilde{K}$ é um corpo de funções sobre $\tilde{K}$. Nós dizemos que K é algebricamente fechado em F (ou K é o corpo de constantes de F) se $\tilde{K} = K$.

Observação 1.1.2 *Os elementos de F, transcendentes sobre K, podem ser caracterizados pela seguinte propriedade:*

$$z \in F \text{ é transcendente sobre } K \Leftrightarrow [F : K(z)] < \infty.$$

Definição 1.1.3 *Sejam F/K um corpo de funções e $x \in F$ transcendente sobre K tal que F é uma extensão algébrica finita de $K(x)$. Dizemos que F/K é um corpo de funções racionais se $F = K(x)$.*

Os corpos de funções racionais são o caso mais simples de corpos de funções, porém várias vezes recorremos a eles para resolver casos particulares e, assim, obter idéias de provas para casos gerais.

Definição 1.1.4 *Um anel de valorização de um corpo de funções F/K é um anel $\mathcal{O} \subseteq F$ com as seguintes propriedades:*

(i) $K \subsetneq \mathcal{O} \subsetneq F$;

(ii) Para todo $z \in F$, tem-se $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.

Vejamos algumas propriedades dos anéis de valorização.

Proposição 1.1.5 *Seja $\mathcal{O}$ um anel de valorização do corpo de funções F/K. Então*

(i) $\mathcal{O}$ *é um anel local, ou seja,* $\mathcal{O}$ *tem um único ideal maximal* $P = \mathcal{O} \setminus \mathcal{O}^*$*, onde* $\mathcal{O}^* = \{z \in \mathcal{O};$ *existe* $a \in \mathcal{O}$*com* $za = 1\}$ *é o grupo de unidades de* $\mathcal{O}$*.*

(ii) Para todo $0 \neq x \in F$*, temos* $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$*.*

(iii) Dado $\tilde{K}$ *o corpo de constantes de* F/K*, então* $\tilde{K} \subseteq \mathcal{O}$ *e* $\tilde{K} \cap P = \{0\}$*.*

Demonstração

(i) Seja $P := \mathcal{O}/\mathcal{O}^*$. Se $x \in P$ e $z \in \mathcal{O}$, então $xz \notin \mathcal{O}^*$, caso contrário, existiria $y \in \mathcal{O}^*$ tal que $(xz)y = 1$, isto é, $x(zy) = 1$ com $zy \in \mathcal{O}$, o que é absurdo, pois $x \in P = \mathcal{O}/\mathcal{O}^*$. Se $x, y \in P$, como $x/y \in \mathcal{O}$ ou $y/x \in \mathcal{O}$, podemos supor sem perda de generalidade que $x/y \in \mathcal{O}$. Logo $1 + x/y \in \mathcal{O}$ e $x + y = y(1 + x/y) \in P$, pelo que já mostramos. Logo P é uma ideal. Seja J ideal de $\mathcal{O}$ com $P \subseteq J \subsetneq \mathcal{O}$. Suponhamos por absurdo que $J \neq P$, então existe $0 \neq x \in J$ tal que $x \notin P$, isto é, $x \in J$ e $x \in \mathcal{O}^*$. Logo $x^{-1} \in \mathcal{O}$ e, como J é ideal e $x \in J$, $xx^{-1} = 1 \in J$, isto é, $J = \mathcal{O}$, o que contradiz a hipótese. Logo P é maximal. Mostraremos, por fim, que P é o único ideal maximal de $\mathcal{O}$. Seja Q ideal maximal de $\mathcal{O}$. Como $Q \neq \mathcal{O}$, então $\mathcal{O}^* \cap Q = \emptyset$. Logo $Q \subseteq P$. Como Q é maximal, $P = Q$.

(ii) Óbvio.

(iii) Mostremos que $\tilde{K} \subset \mathcal{O}$. Seja $z \in \tilde{K}$. Suponha por absurdo que $z \notin \mathcal{O}$, logo $z^{-1} \in \mathcal{O}$. Como z^{-1} também é algébrico sobre K, existem elementos $a_1, a_2, \ldots, a_r$ em K tais que

$$1 + a_1(z^{-1}) + a_2(z^{-1})^2 + \cdots + a_r(z^{-1})^r = 0,$$

ou seja,

$$(z^{-1})(-a_1 - a_2(z^{-1}) - \cdots - a_r(z^{-1})^{r-1}) = 1.$$

Logo $z = -a_1 - a_2(z^{-1}) - \cdots - a_r(z^{-1})^{r-1} \in K[z^{-1}] \subseteq \mathcal{O}$, o que é absurdo. Segue que $\tilde{K} \subseteq \mathcal{O}$.

□

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

(i) P *é um ideal principal.*

(ii) Se $P = t\mathcal{O}$*, então todo elemento* $0 \neq z \in F$ *tem uma única representação da forma* $z = t^n u$ *para algum* $n \in \mathbb{Z}$*, com* $u \in \mathcal{O}^*$*.*

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

No teorema 1.1.6 o inteiro n não depende do elemento t escolhido tal que $P = t\mathcal{O}$. De fato, se t e l são tais que $P = t\mathcal{O} = l\mathcal{O}$, então existem $a, b \in \mathcal{O}$ com $t = la$ e $l = tb$, assim $t = tab$ e, portanto, $ba = 1$, ou ainda, $a = b^{-1} \in \mathcal{O}$. Assim $b \in \mathcal{O}^*$. Sejam $n \in \mathbb{Z}$ e $u \in \mathcal{O}^*$, então

$$l^n u = (tb)^n u = t^n(b^n u),$$

com $b^n u \in \mathcal{O}^*$. Essa observação dá sentido à definição de valorização associada a P que veremos mais adiante.

Definição 1.1.7 *Seja F/K um corpo de funções*

(i) Um lugar P de F/K é o ideal maximal de algum anel de valorização $\mathcal{O}$ de F/K. Todo elemento $t \in P$ tal que $P = t\mathcal{O}$ é chamado de elemento primo para P.

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

Se $\mathcal{O}$ é um anel de valorização do corpo de funções F/K e P seu ideal maximal, vimos que $\mathcal{O}$ é unicamente determinado por P, a saber $\mathcal{O} = \{z \in F;\ z^{-1} \notin P\}$. Logo, denotaremos $\mathcal{O}_P := \mathcal{O}$ e chamaremos de anel de valorização do lugar P.

Definição 1.1.8 *Uma valorização discreta de F/K é uma função $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:*

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

(ii) $v(xy) = v(x) + v(y)$, *para todos* $x, y \in F$;

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$, *para todos* $x, y \in F$;

(iv) existe $z \in F$ *com* $v(z) = 1$;

(v) $v(a) = 0$ *para todo* $0 \neq a \in K$.

Neste contexto, o símbolo ∞ significa algum elemento que não pertence a $\mathbb{Z}$ tal que $\infty+\infty = \infty + n = n + \infty = \infty$ e $\infty > m$ para todos $m, n \in \mathbb{Z}$.

Proposição 1.1.9 (Desigualdade Triangular Estrita) *Sejam v uma valorização discreta do corpo de funções F/K e $x, y \in F$ com $v(x) \neq v(y)$. Então $v(x + y) = \min\{v(x), v(y)\}$.*

Demonstração
Dados $x, y \in F$ com $v(x) < v(y)$, suponha por absurdo que $v(x+y) \neq v(x)$. Logo $v(x+y) > v(x)$ e $v(x) = v((x + y) - y) \geq \min\{v(x + y), v(y)\} > v(x)$, o que é absurdo. Logo $v(x + y) = \min\{v(x), v(y)\}$. □

Definição 1.1.10 *Para todo lugar $P \in \mathbb{P}_F$ nós associamos uma função $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ (que é uma valorização discreta de F/K) da seguinte maneira: escolha um elemento primo t para P. Então, todo $0 \neq z \in F$ tem uma única representação $z = t^n u$ com $u \in \mathcal{O}_P^*$ e $n \in \mathbb{Z}$. Definimos $v_P(z) := n$ e $v_P(0) := \infty$.*

Dado um anel de valorização $\mathcal{O}$ e seu ideal maximal P, podemos caracterizá-los usando a valorização discreta v_P associada a P.

Teorema 1.1.11 *Seja F/K um corpo de funções. Então:*

(i) Para todo lugar $P \in \mathbb{P}_F$, a função v_P da definição 1.1.10 *é uma valorização de F/K. Mais ainda, temos*

$$\mathcal{O}_P = \{z \in F;\ v_P(z) \geq 0\};$$

$$\mathcal{O}_P^* = \{z \in F;\ v_P(z) = 0\};$$

$$P = \{z \in F;\ v_P(z) > 0\}.$$

Um elemento $x \in F$ é um elemento primo para P se, e somente se, $v_P(x) = 1$.

(ii) Reciprocamente, suponha que v é uma valorização discreta de 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.

(iii) Todo anel $\mathcal{O}$ de F/K é um subanel maximal próprio de F.

Definição 1.1.12 *Seja $P \in \mathbb{P}_F$.*

(i) $F_P := \mathcal{O}_P/P$ é o corpo de classes de resíduo de P. A aplicação $x \mapsto x(P)$ de F em $F_P \cup \{\infty\}$ é chamada de aplicação de classes residuais com respeito a P. Às vezes, nós também denotamos $x + P := x(P)$, com $x \in P$.

(ii) $K \subseteq \mathcal{O}_P$, então a aplicação $x \mapsto x(P)$ mergulha K em F_P e, daí, K pode ser considerado subcorpo de F_P. Definimos $\deg P := [F_P : K]$ o grau do lugar P.

Proposição 1.1.13 *Se P é um lugar de F/K e $0 \neq x \in P$, então*

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

A proposição 1.1.13 dá sentido à definição 1.1.12.

Corolário 1.1.14 *O corpo de constantes $\tilde{K}$ de F/K é uma extensão de corpos finita de K.*

Demonstração
Usaremos que $\mathbb{P}_F \neq \emptyset$ (mostraremos tal afirmação no corolário 1.1.17). Seja $P \in \mathbb{P}_F$. Como $\tilde{K}$ é mergulhado em F_P pela aplicação de classes de resíduo $\mathcal{O}_P \longrightarrow F_P$, temos que

$$[\tilde{K} : K] \leq [F_P : K] < \infty.$$

□

Para o caso em que $\deg P = 1$, nós temos $F_P = K$, e a aplicação de classes de resíduo leva F em $K \cup \{\infty\}$. Em particular, se K é um corpo algebricamente fechado, então todo lugar é de grau um e $\tilde{K} = K$, logo nós podemos ver um elemento $z \in F$ como uma função

$$z : \begin{cases} \mathbb{P}_F \longrightarrow K \cup \{\infty\} \\ P \longmapsto z(P) \end{cases}$$

Este é o motivo pelo qual F/K é chamado de corpo de funções. Os elementos de K, interpretados como funções no sentido acima, são funções constantes. Por essa razão K é chamado de corpo de constantes de F.

Definição 1.1.15 *Sejam $z \in F$ e $P \in \mathbb{P}_F$. Nós dizemos que P é um zero de z se $v_P(z) > 0$; P é um pólo de z se $v_P(z) < 0$. Se $v_P(z) = m > 0$, então P é um zero de z de ordem m; se $v_P(z) = -m < 0$, então P é um pólo de z de ordem m.*

Observe que se P é um zero de $z \in F$, com $z \neq 0$, temos que $v_P(z) > 0$. Como $v_P(1) = 0$, temos $v_P(zz^{-1}) = 0$, logo $v_P(z^{-1}) = -v_P(z) < 0$, e P é pólo de z^{-1}.

Teorema 1.1.16 *Sejam F/K um corpo de funções e R um subanel de F com $K \subseteq R \subseteq F$. Suponha que $\{0\} \neq I \subsetneq R$ é um ideal próprio de R. Então existe um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$.*

Corolário 1.1.17 *Sejam F/K um corpo de funções e $z \in F$ transcendente sobre K. Então z tem pelo menos um zero e um pólo. Em particular, $\mathbb{P}_F \neq \emptyset$.*

Demonstração
Considere o anel $R = K[z]$ e o ideal $I = zK[z]$. O teorema 1.1.16 garante que existe um lugar $P \in \mathbb{P}_F$ com $z \in P$, isto é, $v_P(z) > 0$. Logo P é um zero de z. De maneira análoga provamos que z^{-1} tem um zero $Q \subseteq \mathbb{P}_F$ e, logo, Q é pólo de z. □

Veremos a seguir algumas propriedades dos corpos de funções racionais. Seja F/K um corpo de funções racionais, isto é, existe $x \in F$ transcendente sobre K tal que $F = K(x)$. Dado um polinômio mônico e irredutível $p(x) \in K[x]$, considere o anel

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

É fácil verificar que $\mathcal{O}_{p(x)}$ é anel de valorização de $K(x)/K$ com ideal maximal

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

Em particular, quando $p(x)$ é da forma $p(x) = x - \alpha$ com $\alpha \in K$, nós usaremos a seguinte notação

$$P_\alpha := P_{x-\alpha} \in \mathbb{P}_{K(x)}.$$

Outro anel de valorização de $K(x)/K$ é dado por

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

com ideal maximal

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

Este é chamado de lugar infinito de $K(x)$. Observe que estas notações dependem do elemento x de $K(x)/K$.

Proposição 1.1.18 *Seja F/K um corpo de funções racionais onde $F = K(x)$.*

(i) Seja $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ tal que $p(x) \in K[x]$ é um polinômio irredutível. Então $p(x)$ é um elemento primo para P e sua valorização discreta v_P pode ser descrita como segue: Se $z \in K(x) \setminus \{0\}$ é escrito na forma $z = p(x)^n.(f(x)/g(x))$ com $n \in \mathbb{Z}$, $f(x), g(x) \in K[x]$, $p(x) \nmid f(x)$ e $p(x) \nmid g(x)$, então $v_P(z) = n$. A classe residual $K(x)_P = \mathcal{O}_P/P$ é isomorfa a $K[x]/(p(x))$; um isomorfismo é dado por

$$\phi : \begin{cases} K[x]/(p(x)) \longrightarrow K(x)_P \\ f(x) \ mod\ p(x) \longmapsto f(x)(P). \end{cases}$$

Conseqüentemente, $\deg P = \deg p(x)$.

(ii) No caso especial em que $p(x) = x - \alpha$ com $\alpha \in K$, o grau de $P = P_\alpha$ é um e a aplicação de classes residuais é dada por

$$z(P) = z(\alpha),\ \textit{para } z \in K(x),$$

onde $z(\alpha)$ é definido como segue: escrevendo $z = f(x)/g(x)$ com $f(x), g(x) \in K[x]$ polinômios primos entre si, temos

$$z(\alpha) = \begin{cases} f(\alpha)/g(\alpha),\ \textit{se } g(\alpha) \neq 0, \\ \infty,\ \textit{se } g(\alpha) = 0. \end{cases}$$

(iii) Seja $P = P_\infty$ o lugar infinito de $K(x)/K$, então $\deg P_\infty = 1$. Um elemento primo para P_∞ é $t = 1/x$. A valorização discreta correspondente v_∞ é dada por

$$v_\infty(f(x)/g(x)) = \deg g(x) - \deg f(x),$$

onde $f(x), g(x) \in K[x]$. A classe residual correspondente para P_∞ é determinada por $z(P_\infty) = z(\infty)$ para $z \in K(x)$, onde $z(\infty)$ é definido usualmente da seguinte maneira: se

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

então

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

(iv) K é o corpo de constantes de $K(x)/K$.

Teorema 1.1.19 *Não existe lugar de um corpo de funções racionais $K(x)/K$ diferente de $P_{p(x)}$ e P_∞.*

Corolário 1.1.20 *Existe uma bijeção entre os lugares de grau um de $K(x)/K$ e $K \cup \{\infty\}$.*

Demonstração
Segue da proposição 1.1.18 e do teorema 1.1.19. □

Teorema 1.1.21 (Teorema da aproximação fraca) *Sejam F/K um corpo de funções, $P_1, \ldots, P_n \in \mathbb{P}_F$ lugares dois a dois distintos de F/K; $x_1, \ldots, x_n \in F$ e $r_1, \ldots, r_n \in \mathbb{Z}$. Então, existe um elemento $x \in F$ tal que*

$$v_{P_i}(x - x_i) = r_i, \text{ para } i = 1, \ldots, n.$$

Corolário 1.1.22 *Todo corpo de funções tem infinitos lugares.*

Demonstração
Suponha por absurdo que exista apenas um número finito de lugares, a saber $P_1, \ldots, P_n$. No teorema 1.1.21 tome x_i primo para P_i e $r_i = 1$, $i = 1, \ldots, n$. Logo, existe $x \in F$ tal que

$$v_{P_i}(x - x_i) = 1, \text{ para } i = 1, \ldots, n.$$

Se $v_{P_i}(x) < v_{P_i}(x_i)$, pela desigualdade triangular estrita

$$1 = v_{P_i}(x - x_i) = v_{P_i}(x) < v_{P_i}(x_i) = 1.$$

Assim $v_{P_i}(x) \geq v_{P_i}(x_i) = 1$. Logo $v_{P_i}(x) > 0$, para $i = 1, \ldots, n$, ou seja, x só tem pólos, o que é absurdo. □

Proposição 1.1.23 *Sejam F/K um corpo de funções e $P_1, \ldots, P_r$ zeros do elemento $x \in F$. Então:*

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

Corolário 1.1.24 *Em um corpo de funções F/K, todo elemento $0 \neq x \in F$ tem apenas um número finito de zeros e de pólos.*

Demonstração
Se x é constante, então x não tem zeros nem pólos. Se x é transcendente, o número de zeros de x é menor ou igual à $[F : K(x)]$ pela proposição 1.1.23. O mesmo argumento mostra que x^{-1} tem somente uma quantidade finita de zeros e, portanto, x tem, também, uma quantidade finita de pólos. □

Já observamos que o corpo $\tilde{K}$ de constantes de um corpo de funções algébricas F/K é uma extensão finita sobre K e F pode ser considerado como um corpo de funções sobre $\tilde{K}$. A partir de agora e até o final desse trabalho, assumiremos $K = \tilde{K}$.

Definição 1.1.25 *O grupo abeliano livre gerado pelos lugares de F/K e denotado por $\mathcal{D}_F$ é chamado de grupo de divisores de F/K. Os elementos de $\mathcal{D}_F$ são chamados de divisores de F/K. Em outras palavras, um divisor é uma soma formal*

$$D = \sum_{P \in \mathbb{P}_F} n_P P, \text{ com } n_P \in \mathbb{Z} \text{ e quase todos } n_P \text{ são iguais a } 0.$$

O suporte de D é definido por

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

Escreveremos, às vezes, D da forma

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

onde $S \subseteq \mathbb{P}_F$ é um conjunto finito tal que supp $D \subseteq S$.
Um divisor da forma $D = P$ com $P \in \mathbb{P}_F$ é chamado de divisor primo. A soma de dois divisores $D = \sum n_P P$ e $D' = \sum n'_P P$ é dada por

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

O elemento zero do grupo de divisores $\mathcal{D}_F$ é o divisor

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

Para $Q \in \mathbb{P}_F$ e $D = \sum n_P P \in \mathcal{D}_F$ nós definimos $v_Q(D) := n_Q$, logo

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

Uma ordem parcial em $\mathcal{D}_F$ é definida por

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

Um divisor $D \geq 0$ é chamado positivo (ou efetivo). O grau de um divisor é definido por

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

e esta expressão fornece um homomorfismo $\deg : \mathcal{D}_F \longrightarrow \mathbb{Z}$.

Pelo corolário 1.1.24, todo elemento $0 \neq x \in F$ tem apenas um número finito de zeros e de pólos em $\mathbb{P}_F$, logo a definição abaixo faz sentido.

Definição 1.1.26 *Seja $0 \neq x \in F$ e denotaremos por Z (respectivamente N) o conjunto de zeros (respectivamente pólos) de $x \in \mathbb{P}_F$. Então definimos*

$$(x)_0 := \sum_{P \in Z} v_P(x)P, \text{ o divisor de zeros de } x,$$

$$(x)_\infty := \sum_{P \in N} (-v_P(x))P, \text{ o divisor de pólos de } x,$$

$$(x) := (x)_0 - (x)_\infty, \text{ o divisor de } x.$$

Claramente $(x)_0 \geq 0, (x)_\infty \geq 0$ e

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

Os elementos $x \in F$ constantes e não nulos são caracterizados por

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

Definição 1.1.27 *O conjunto*

$$\mathcal{P}_F := \{(x);\ 0 \neq x \in F\}$$

é chamado de grupo de divisores principais de F/K. Este é um subgrupo de $\mathcal{D}_F$, pois para $0 \neq x, y \in F$, $(xy) = (x) + (y)$. O grupo quociente

$$\mathcal{C}_F := \mathcal{D}_F/\mathcal{P}_F$$

é chamado de grupo das classes de divisores. Para um divisor $D \in \mathcal{D}_F$, o elemento correspondente no grupo quociente $\mathcal{C}_F$ é denotado por $[D]$. Dois divisores $D, D' \in \mathcal{D}_F$ são ditos equivalentes e escrevemos

$$D \sim D',$$

se $[D] = [D']$, ou seja, $D = D' + (x)$ para algum $x \in F \setminus \{0\}$. Pode se verificar que $\sim$ é uma relação de equivalência.

Definição 1.1.28 *Para um divisor $A \in \mathcal{D}_F$, definimos*

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

Observação 1.1.29 *Seja $A \in \mathcal{D}_F$, então:*

(i) $x \in \mathcal{L}(A)$ *se, e somente se,* $v_P(x) \geq -v_P(A)$, *para todo* $P \in \mathbb{P}_F$.

(ii) $\mathcal{L}(A) \neq \{0\}$ *se, e somente se, existe um divisor* $A' \sim A$ *com* $A' \geq 0$.

De fato, (i) e (ii) são conseqüências diretas das definições 1.1.27 e 1.1.28.

Lema 1.1.30 *Seja $A \in \mathcal{D}_F$. Então temos:*

(i) $\mathcal{L}(A)$ *é um espaço vetorial sobre* K.

(ii) Se A' *é um divisor equivalente à* A *então* $\mathcal{L}(A) \simeq \mathcal{L}(A')$ *(isomorfismo de espaços vetoriais sobre* K*).*

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

(iv) Se $A < 0$ então $\mathcal{L}(A) = \{0\}$.

Demonstração

(i) Sejam $x, y \in \mathcal{L}(A)$ e $a \in K$. Então, para todo $P \in \mathbb{P}_F$, $v_P(ax+y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(A)$, pela observação 1.1.29.

(ii) Se A é equivalente a A', então existe $z \in F$ tal que $A = A' + (z)$. Considere as aplicações

$$\phi : \begin{cases} \mathcal{L}(A) \longrightarrow F \\ x \longmapsto xz \end{cases}$$

e

$$\phi' : \begin{cases} \mathcal{L}(A') \longrightarrow F \\ x \longmapsto xz^{-1}. \end{cases}$$

Temos que ϕ e ϕ' são K-lineares, $\phi(\mathcal{L}(A)) \subseteq \mathcal{L}(A')$ e $\phi(\mathcal{L}(A')) \subseteq \mathcal{L}(A)$, logo existe um isomorfismo entre $\mathcal{L}(A)$ e $\mathcal{L}(A')$.

(iii) É claro que $0 \in K \cap \mathcal{L}(0)$. Suponhamos que $x \neq 0$. Sabemos que

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

Logo se $x \in K$, então $x \in \mathcal{L}(0)$. Portanto $K \subseteq \mathcal{L}(0)$. Se $x \in \mathcal{L}(0)$, então $(x) \geq 0$. Logo x não tem pólos. Pelo corolário 1.1.17, $x \in K$. Daí $\mathcal{L}(0) \subseteq K$.

(iv) Se $A < 0$, então $\mathcal{L}(A) = \{0\}$. Suponha por absurdo que existe um elemento $x \in \mathcal{L}(A)$ não nulo. Então $(x) \geq -A > 0$, logo x tem pelo menos um zero, o que é absurdo, pois x não tem pólos. Portanto $\mathcal{L}(A) = \{0\}$.

□

Nosso próximo objetivo é encontrar a dimensão de $\mathcal{L}(A)$ para um divisor $A \in \mathcal{D}_F$. Este resultado será apresentado na próxima seção pelo teorema de Riemann-Roch.

Lema 1.1.31 *Sejam A, B divisores de F/K com $A \leq B$. Então temos que $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ e*

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg B - \deg A.$$

Proposição 1.1.32 *Para todo divisor $A \in \mathcal{D}_F$, o espaço $\mathcal{L}(A)$ é um espaço vetorial sobre K de dimensão finita. Mais precisamente: Se $A = A_+ - A_-$, com A_+ e A_- divisores positivos, então*

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

Demonstração
Como $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$, pelo lema 1.1.31, é suficiente mostrar que

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

Agora $0 \leq A_+$ e temos que $\dim \mathcal{L}(A_+) = \dim(\mathcal{L}(A_+)/\mathcal{L}(0))+1$ uma vez que a aplicação K-linear

$$\phi : \begin{cases} \mathcal{L}(A_+) \longrightarrow \mathcal{L}(A_+)/\mathcal{L}(0) \\ x \longmapsto \bar{x} \end{cases}$$

é sobrejetora e tem núcleo $\mathcal{L}(0) = K$ (ver lema 1.1.30). Novamente, pelo lema 1.1.31

$$\dim \mathcal{L}(A_+) = \dim(\mathcal{L}(A_+)/\mathcal{L}(0)) + 1 \leq \deg A_+ - \deg 0 + 1 = \deg A_+ + 1.$$

□

Definição 1.1.33 *Dado um divisor $A \in \mathcal{D}_F$, o inteiro $\dim A := \dim \mathcal{L}(A)$ é chamado de dimensão do divisor A.*

Teorema 1.1.34 *Todo divisor principal tem grau zero, isto é, dado $x \in F/K$ e $(x)_0$ (respectivamente, $(x)_\infty$) denota o divisor de zeros de x (respectivamente, denota o divisor de pólos de x), então*

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

ou seja, $\deg(x) = \deg(x_0) - \deg(x_\infty) = 0$.

Corolário 1.1.35 *As seguintes propriedades são satisfeitas:*

(a) Sejam A, A' divisores com $A \sim A'$. Então, temos $\dim A = \dim A'$ e $\deg A = \deg A'$.

(b) Se $\deg A < 0$, então $\dim A = 0$.

(c) Dado um divisor A de grau zero. Então são equivalentes:

(i) A é principal.

(ii) $\dim A \geq 1$.

(iii) $\dim A = 1$.

Demonstração

(a) Que $\dim A = \dim A'$ segue do lema 1.1.30, item (ii). Como $A \sim A'$, existe $z \in F$ tal que $A = A' + (z)$. Como $\deg(z) = 0$, temos

$$\deg A = \deg(A' + (z)) = \deg A' + \deg(z) = \deg A'.$$

(b) Se $\dim A > 0$, então $\mathcal{L}(A) \neq \{0\}$. Pela observação 1.1.29, existe um divisor $A \sim A'$ com $A' \geq 0$. Logo $\deg A' \geq 0$, o que é absurdo. Portanto $\dim A = 0$.

(c) Mostremos as três implicações:

(i) $\Rightarrow$ (ii) Se $A = (x)$ para algum $x \in F$, então $x^{-1} \in \mathcal{L}(A)$, logo $\dim A \geq 1$.

(ii) $\Rightarrow$ (iii) Se $\dim A \geq 1$ e $\deg A = 0$, então $A \sim A'$ para algum $A' \geq 0$, pela observação 1.1.29. As condições $A' \geq 0$ e $\deg A' = 0$ implicam que $A' = 0$ e, portanto, $\dim A = \dim A' = 1$.

(iii) $\Rightarrow$ (i) Se $\dim A = 1$ e $\deg A = 0$, para todo $0 \neq z \in \mathcal{L}(A)$ temos que $(z) + A \geq 0$. Como $\deg((z) + A) = \deg A = 0$, segue que $(z) + A = 0$, logo $A = (z^{-1})$ é principal.

□

Proposição 1.1.36 *Existe uma constante $\gamma \in \mathbb{Z}$ tal que, para todo divisor $A \in \mathcal{D}_F$, vale a seguinte desigualdade:*

$$\deg A - \dim A \leq \gamma.$$

Definição 1.1.37 *O gênero g de F/K é definido por*

$$g := max\{\deg A - \dim A + 1;\ A \in \mathcal{D}_F\}.$$

Observação 1.1.38 *O gênero de F/K é um inteiro não negativo.*

De fato, basta notar que $\deg 0 - \dim 0 + 1 = 0$.

Teorema 1.1.39 (Teorema de Riemann) *Seja F/K um corpo de funções de gênero g, então:*

(i) Para todo divisor $A \in \mathcal{D}_F$, tem-se que

$$\dim A \geq \deg A + 1 - g.$$

(ii) Existe um inteiro c, dependendo de F/K, tal que

$$\dim A = \deg A + 1 - g$$

sempre que $\deg A \geq c$.

O teorema de Riemann encontra a dimensão de todos os divisores A tais que $\deg A$ é maior que uma certa constante c que depende de F/K e limita inferiormente a dimensão de todos os divisores em $\mathcal{D}_F$. Na próxima seção determinaremos precisamente esta dimensão.

Definição 1.1.40 *Dado um divisor $A \in \mathcal{D}_F$, o inteiro*

$$i(A) := \dim A - \deg A + g - 1$$

é chamado de índice de especialidade do divisor A.

1.2 Adeles, diferenciais de Weil, divisores canônicos e o teorema de Riemann-Roch

Os próximos conceitos serão fundamentais na demonstração do teorema de Riemman-Roch.

Definição 1.2.1 *Um adele de F/K é uma aplicação*

$$\alpha = \begin{cases} \mathbb{P}_F \longrightarrow F, \\ P \longmapsto \alpha_P, \end{cases}$$

tal que $\alpha_P \in \mathcal{O}_P$ para quase todos $P \in \mathbb{P}_F$. Podemos, assim, considerar um adele como um elemento da produto direto $\prod_{P \in \mathbb{P}_F} F$ e usar a notação $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$, ou ainda, por simplicidade, $\alpha = (\alpha_P)$. O conjunto

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

é chamado de espaço de adeles de F/K. Podemos considerar $\mathcal{A}_F$ como um espaço vetorial sobre K da seguinte maneira: sejam $\alpha, \beta \in \mathcal{A}_F$, então o adele $\alpha + \beta : \mathbb{P}_F \longrightarrow F$ é definido por

$$(\alpha + \beta)_P = \alpha_P + \beta_P,\ \forall P \in \mathbb{P}_F.$$

Seja $\lambda \in K$, então o adele $\lambda\alpha : \mathbb{P}_F \longrightarrow F$ é definido por

$$(\lambda\alpha)_P = \lambda\alpha_P,\ \forall P \in \mathbb{P}_F.$$

Note que as definições fazem sentido, pois $v_P(\alpha_P + \beta_P) \geq \min\{v_P(\alpha_P), v_P(\beta_P)\} \geq 0$ para quase todos $P \in \mathbb{P}_F$. Da mesma forma $v_P(\lambda\alpha_P) = v_P(\alpha_P) \geq 0$, também, para quase todos $P \in \mathbb{P}_F$.

O adele principal de um elemento $x \in F$ é o adele no qual todas suas componentes são iguais a x, o que dá uma aplicação $F \hookrightarrow \mathcal{A}_F$. A valorização v_P de F/K é estendida naturalmente a $\mathcal{A}_F$ tomando-se $v_P(\alpha) := v_P(\alpha_P)$ (onde α_P é a P-componente do adele α).

Definição 1.2.2 *Dado um divisor $A \in \mathcal{D}_F$, definimos*

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

É fácil ver que este conjunto é K-subespaço de $\mathcal{A}_F$.

Teorema 1.2.3 *Para todo divisor A o índice de especialidade é*

$$i(A) = \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)).$$

Note que os K-espaços vetoriais $\mathcal{A}_F$, $\mathcal{A}_F(A)$ e F possuem dimensão finita. O teorema fala que o espaço quociente $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ tem dimensão finita sobre K.

Corolário 1.2.4 *Se g é o gênero de um corpo de funções F/K, então*

$$g = \dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F)).$$

Basta notar que $i(0) = \dim(0) - \deg(0) + g - 1 = 1 - 0 + g - 1 = g$.

Definição 1.2.5 *Uma diferencial de Weil de F/K é uma aplicação K-linear $\omega : \mathcal{A}_F \longrightarrow K$ que se anula em $\mathcal{A}_F(A) + F$ para algum divisor $A \in \mathcal{D}_F$. Nós chamamos o conjunto*

$$\Omega_F := \{\omega;\ \omega \text{ é uma diferencial de Weil de } F/K\}$$

de o módulo de diferenciais de Weil de F/K. Dado $A \in \mathcal{D}_F$, denotamos

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

Podemos considerar Ω_F como um K-espaço vetorial de maneira óbvia (de fato, sempre que w_1 anula-se em $\mathcal{A}_F(A_1) + F$ e w_2 anula-se em $\mathcal{A}_F(A_2) + F$, $w_1 + w_2$ anula-se em $\mathcal{A}_F(A_3) + F$ para todos divisores A_3 com $A_3 \leq A_1$ e $A_3 \leq A_2$; e aw_1 anula-se em $\mathcal{A}_F(A_1) + F$, onde $a \in K$). É fácil ver que $\Omega_F(A)$ é um subespaço de Ω_F.

Proposição 1.2.6 *Dado um divisor $A \in \mathcal{D}_F$ temos que* $\dim \Omega_F(A) = i(A)$.

Definição 1.2.7 *Sejam $x \in F$ e $\omega \in \Omega_F$, definimos $x\omega : \mathcal{A}_F \longrightarrow K$ por*

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

É fácil ver que se $\omega \in \Omega_F$ se anula em $\mathcal{A}_F(A) + F$ e $x \in F$, então $x\omega$ se anula em $\mathcal{A}_F(A + (x)) + F$. Assim a definição 1.2.7 dá ao conjunto Ω_F uma estrutura de espaço vetorial sobre F.

Proposição 1.2.8 *Ω_F é um espaço vetorial de dimensão um sobre F.*

Nosso próximo objetivo é definir um divisor de uma diferencial de Weil. Para isso consideraremos o seguinte conjunto:

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

Lema 1.2.9 *Seja $0 \neq \omega \in \Omega_F$. Então existe um divisor unicamente determinado $W \in M(\omega)$ tal que $A \leq W$, para todo $A \in M(\omega)$.*

Definição 1.2.10 *(a) O divisor (ω) de uma diferencial de Weil $\omega \neq 0$ é o divisor de F/K unicamente determinado pelas seguintes propriedades:*

(i) ω *anula-se em* $\mathcal{A}_F((\omega)) + F$*;*

(ii) se ω *anula-se em* $\mathcal{A}_F(A) + F$*, então* $A \leq (\omega)$*.*

(b) Dados $0 \neq \omega \in \Omega_F$ *e* $P \in \mathbb{P}_F$ *definimos* $v_P(\omega) := v_P((\omega))$*.*

(c) Um lugar P *é dito ser um zero (respectivamente, um pólo) de* ω *se* $v_P(\omega) > 0$ *(respectivamente, se* $v_P(\omega) < 0$*). Uma diferencial* ω *é dito ser regular em* P *se* $v_P(\omega) \geq 0$ *e* ω *é dito regular (ou holomorfo) se é regular em todo* $P \in \mathbb{P}_F$*.*

(d) Um divisor W *é um divisor canônico de* F/K *se* $W = (\omega)$ *para todo* $\omega \in \Omega_F$*.*

A definição 1.2.10 faz sentido devido ao lema 1.2.9.
As seguintes caracterizações seguem imediatamente da definição:

$$\Omega_F(A) = \{\omega \in \Omega_F;\ \omega = 0 \text{ ou } (\omega) \geq A\},$$

$$\Omega_F(0) = \{\omega \in \Omega_F;\ \omega \text{ é regular}\}.$$

É fácil ver que:

$$\dim \Omega_F(0) = g.$$

Proposição 1.2.11 *(i) Dados* $0 \neq x \in F$ *e* $0 \neq \omega \in \Omega_F$*, temos* $(x\omega) = (x) + (w)$*.*

(ii) Dois divisores canônicos quaisquer de F/K *são equivalentes.*

Demonstração

(i) Se ω se anula em $\mathcal{A}_F(A) + F$, então $x\omega$ se anula em $\mathcal{A}_F(A + (x)) + F$, tomando $A = (x)$ temos

$$(\omega) + (x) \leq (x\omega) \text{ (ver definição 1.2.10, item } (a)).$$

Como $x\omega$ se anula em $\mathcal{A}_F((x\omega)) + F$, $x^{-1}(x\omega)$ se anula em $\mathcal{A}_F((x\omega) + (x^{-1}))$, logo

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

Combinando as desigualdades obtemos

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

(ii) Segue da proposição 1.2.8 e do item (i) acima.

□

Teorema 1.2.12 *Sejam* A *um divisor arbitrário e* $W = (\omega)$ *um divisor canônico de* F/K*. Então a aplicação*

$$\mu = \begin{cases} \mathcal{L}(W - A) \longrightarrow \Omega_F(A), \\ x \longmapsto x\omega \end{cases}$$

é um isomorfismo de K*-espaços vetoriais. Em particular,*

$$i(A) = \dim(W - A).$$

Temos agora todos os resultados necessários para apresentar o teorema de Riemann-Roch.

Teorema 1.2.13 (Teorema de Riemann-Roch) *Seja W um divisor canônico de F/K. Então, para todo $A \in \mathcal{D}_F$, temos*

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

Demonstração
Pelo teorema 1.2.12

$$i(A) = \dim(W - A),$$

Por outro lado, $i(A) = \dim A - \deg A + g - 1$. Logo

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

□

Vejamos algumas conseqüências do Teorema de Riemann-Roch.

Corolário 1.2.14 *Para um divisor canônico W, temos*

$$\deg W = 2g - 2 \ e \ \dim W = g.$$

Demonstração
Para $A = 0$, o teorema de Riemann-Roch e o lema 1.1.30, item (iii), garantem

$$1 = \dim 0 = \deg 0 + 1 - g + \dim (W - 0).$$

Logo $\dim W = g$. Fazendo $A = W$ temos

$$g = \dim W = \deg W + 1 - g + \dim(W - W) = \deg W + 2 - g.$$

Logo $\deg W = 2g - 2$. □

Teorema 1.2.15 *Se A é um divisor de F/K de grau $\geq 2g - 1$, então*

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

Demonstração
Temos que $\dim A = \deg A + 1 - g + \dim(W - A)$, onde W é um divisor canônico. Como $\deg A \geq 2g - 1$ e $\deg W = 2g - 2$, então $\deg(W - A) < 0$. Logo $\dim(W - A) = 0$. □

Observe que o limitante $2g - 1$ do teorema 1.2.15 é o melhor possível, pois para um divisor canônico W temos

$$\dim W = \deg W + 1 - g + \dim(W - W) > \deg W + 1 - g.$$

Proposição 1.2.16 *Suponha que $g_0 \in \mathbb{Z}$ e $W_0 \in \mathcal{D}_F$ satisfaçam*

$$\dim A = \deg A + 1 - g_0 + \dim(W_0 - A),$$

para todo $A \in \mathcal{D}_F$. Então $g_0 = g$ e W_0 é um divisor canônico.

Demonstração
Fazendo $A = 0$, respectivamente $A = W_0$, por hipótese nós obtemos que $\dim W_0 = g_0$ e $\deg W_0 = 2g_0 - 2$ (conferir prova do corolário 1.2.14). Seja W um divisor canônico de F/K. Escolhemos um divisor A com $\deg A > max\{2g - 2, 2g_0 - 2\}$. Então $\dim A = \deg A + 1 - g$ pelo teorema 1.2.15 e $\dim A = \deg A + 1 - g_0$ por hipótese. Logo $g = g_0$.

Fazendo $A = W$ temos

$$g = (2g - 2) + 1 - g + \dim(W_0 - W),$$

logo $\dim(W_0 - W) = 1$. Como $\deg(W_0 - W) = 0$, temos que $W_0 - W$ é principal, logo $W_0 \sim W$.
□

Proposição 1.2.17 *Um divisor B é canônico se, e somente se,* $\deg B = 2g-2$ *e* $\dim B \geq g$.

Demonstração
Suponha que $\deg B = 2g-2$ e $\dim B \geq g-1+\dim(W-B)$. Logo $\dim(W-B) \geq 1$. Como $\deg(W-B)=0$, segue do corolário 1.1.35 que $W \sim B$. □

Proposição 1.2.18 *Seja F/K um corpo de funções. Então são equivalentes:*

(i) F/K é racional.

(ii) F/K tem gênero 0 e existe um divisor $A \in \mathcal{D}_F$ com $\deg A = 1$.

O próximo teorema é um melhoramento do teorema da aproximação fraca.

Teorema 1.2.19 (Teorema da Aproximação Forte) *Sejam $S \subsetneq \mathbb{P}_F$ um subconjunto próprio de $\mathbb{P}_F$ e $P_1, \ldots, P_r \in S$. Sejam ainda $x_1, \ldots, x_r \in F$ e $n_1, \ldots, n_r \in \mathbb{Z}$. Então existe um elemento $x \in F$ tal que*

$$v_{P_i}(x - x_i) = n_i \quad (i = 1, \ldots, r) \text{ e}$$
$$v_P(x) \geq 0 \quad \text{para todo } P \in S \setminus \{P_1, \ldots, P_r\}.$$

Proposição 1.2.20 *Seja $P \in \mathbb{P}_F$. Então, para todo $n \geq 2g$, existe um elemento $x \in F$ com divisor de pólos $(x)_\infty = nP$.*

Demonstração
Pelo teorema 1.2.15 nós sabemos que $\dim((n-1)P) = (n-1)\deg P + 1 - g$ e $\dim(nP) = n\deg P + 1 - g$, logo $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$. Todo elemento $x \in \mathcal{L}(nP) \setminus \mathcal{L}((n-1)P)$ tem divisor de pólo nP. □

Definição 1.2.21 *Seja $P \in \mathbb{P}_F$. Um inteiro $n \geq 0$ é uma ordem de pólo de P se existe um elemento $x \in F$ com $(x)_\infty = nP$. Caso contrário, n é chamado de lacuna de P.*

Observação 1.2.22 *Seja $P \in \mathbb{P}_F$. O conjunto das ordens de pólo de P é um sub-semigrupo do semigrupo $\mathbb{N} \cup \{0\}$.*

Teorema 1.2.23 (Teorema das lacunas de Weiertrass) *Suponha que F/K tem gênero $g > 0$ e P é um lugar de grau um. Então existem exatamente g lacunas $i_1 < \cdots < i_g$ de P. Temos ainda*

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

Para um divisor A com $\deg A < 0$, temos $\dim A = 0$. Se $\deg A > 2g-2$, então $\dim A = \deg A + 1 - g$ pelo teorema 1.2.15. Vamos agora estudar um pouco mais o caso em que $0 < \deg A \leq 2g-2$.

Definição 1.2.24 *Um divisor $A \in \mathcal{D}_F$ é chamado de divisor não especial se $i(A) = 0$. Caso contrário A é chamado de divisor especial.*

Observação 1.2.25 *(i) A é um divisor não especial* $\Leftrightarrow \dim A = \deg A + 1 - g$.

(ii) $\deg A > 2g-2 \Rightarrow$ *A é um divisor não especial.*

(iii) A propriedade de um divisor A ser, ou não, especial depende apenas de sua classe de equivalência $[A]$ no grupo de classes de divisores.

(iv) Todo divisor canônico é especial.

(v) Seja A um divisor com $\dim A > 0$ e $\deg A < g$. Então A é um divisor especial.

(vi) Se A é um divisor não especial e $B \geq A$, então B é um divisor não especial.

Todas essas observações são conseqüências imediatas da definição.

Proposição 1.2.26 *Suponha que $T \subseteq \mathbb{P}_F$ é um conjunto de lugares de grau um tal que $|T| \geq g$. Então existe um divisor não especial $B \geq 0$ com $\deg B = g$ e supp $B \subseteq T$.*

Lema 1.2.27 *Suponha que A e B sejam divisores tais que $\dim A > 0$ e $\dim B > 0$. Então*

$$\dim A + \dim B \leq 1 + \dim(A + B).$$

Teorema 1.2.28 (Teorema de Clifford) *Para todo divisor A com $0 \leq \deg A \leq 2g - 2$ vale*

$$\dim A \leq 1 + \frac{1}{2} \deg A.$$

Demonstração
O caso em que $\dim A = 0$ é trivial. Por outro lado, se $\dim(W - A) = 0$ (onde W é um divisor canônico), então

$$\dim A = \deg A + 1 - g = 1 + \frac{1}{2} \deg A + \frac{1}{2}(\deg A - 2g) < 1 + \frac{1}{2} \deg A,$$

pois $\deg A \leq 2g - 2$. Consideraremos agora o caso em que $\dim A > 0$ e $\dim(W - A) > 0$. Usando o lema 1.2.27 obtemos

$$\dim A - \dim(W - A) \leq 1 + \dim W = 1 + g.$$

Por outro lado,

$$\dim A - \dim(W - A) = \deg A + 1 - g$$

pelo teorema de Riemann-Roch. Juntando as duas últimas expressões obtemos os resultado desejado.

□

Definição 1.2.29 *Seja $P \in \mathbb{P}_F$.*

(i) Dado $x \in F$, seja $\iota_P(x) \in \mathcal{A}_F$ o adele cuja P-componente é x e todas as outras componentes são nulas.

(ii) Dada uma diferencial de Weil $\omega \in \Omega_F$, definimos sua componente local $\omega_P : F \longrightarrow K$ por

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

É fácil ver que ω_P é uma aplicação K-linear.

Proposição 1.2.30 *Sejam $\omega \in \Omega_F$ e $\alpha = (\alpha_P) \in \mathcal{A}_F$. Então $\omega_P(\alpha_P) \neq 0$ para uma quantidade finita de lugares P e*

$$\omega(\alpha) = \sum_{P \in \mathbb{P}_F} \omega_P(\alpha_P).$$

Em particular,

$$\sum_{P \in \mathbb{P}_F} \omega_P(1) = 0.$$

Proposição 1.2.31 *(i) Sejam $\omega \neq 0$ uma diferencial de Weil de F/K e $P \in \mathbb{P}_F$. Então*

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

Em particular, $\omega_P \neq 0$.

(ii) Se $\omega, \omega' \in \Omega_F$ e $\omega_P = \omega'_P$ para algum $P \in \mathbb{P}_F$, então $w = w'$.

Proposição 1.2.32 *Seja F/K com $F = K(x)$ um corpo de funções racionais. Então:*

(i) O divisor $-2P_\infty$ é canônico.

(ii) Existe uma única diferencial de Weil $\eta \in \Omega_{K(x)}$ com $(\eta) = -2P_\infty$ e $\eta P_\infty(x^{-1}) = -1$.

(iii) A componente local ηP_∞ (respectivamente, ηP_a) da diferencial de Weil η acima satisfaz

$$\eta P_\infty((x-a)^n) = \begin{cases} 0, & \text{se } n \neq -1, \\ -1, & \text{se } n = -1, \end{cases}$$

$$\eta P_a((x-a)^n) = \begin{cases} 0, & \text{se } n \neq -1, \\ 1, & \text{se } n = -1. \end{cases}$$

1.3 Derivações e diferenciais

Definição 1.3.1 *Sejam L/K uma extensão algébrica, $\alpha \in L$, $f(x) \in K[x]$ o minimal de α e E um corpo de fatoração de $f(x)$. Dizemos que α é separável sobre K se $f(x)$ não possui raízes múltiplas no corpo de fatoração E. Uma extensão algébrica L/K é uma extensão separável se todo $\alpha \in L/K$ é separável sobre K.*

Definição 1.3.2 *Um corpo K é perfeito se toda extensão algébrica L/K é separável.*

A partir desta seção consideramos que o corpo de constantes K é perfeito.

Definição 1.3.3 *Seja M um módulo sobre F, isto é, um F-espaço vetorial. Uma aplicação $\delta : F \longrightarrow M$ é dita ser uma derivação de F/K se δ é K-linear e a regra do produto*

$$\delta(uv) = u\delta(v) + v\delta(u)$$

vale para todos $u, v \in F$.

Nosso objetivo nesta seção é estabelecer um isomorfismo entre diferenciais (que definiremos posteriormente) e diferenciais de Weil.

Lema 1.3.4 *Seja δ uma derivação de um corpo de funções F/K, então:*

(a) $\delta(a) = 0$, para todo $a \in K$;

(b) $\delta(z^n) = nz^{n-1}\delta(z)$, para todo $z \in F$;

(c) Se char $K = p > 0$, então $\delta(z^p) = 0$, para todo $z \in F$;

(d) $\delta(x/y) = \frac{y\delta(x) - x\delta(y)}{y^2}$, para $x, y \in F$ e $y \neq 0$.

Demonstração

(a) Note que $\delta(1) = \delta(1.1) = 1\delta(1) + 1\delta(1)$, logo $2\delta(1) = \delta(1)$, ou seja, $\delta(1) = 0$. Seja $a \in K$, como δ é K-linear, temos $\delta(a) = a\delta(1) = 0$.

(b) Seja $n \in \mathbb{N} \setminus \{0\}$. Faremos indução sobre n.

Se $n = 1$, então a igualdade é óbvia. Suponha que $\delta(z^n) = nz^{n-1}\delta(z)$, então

$$\delta(z^{n+1}) = \delta(z^n z) = z\delta(z^n) + z^n\delta(z) =$$

$$z[nz^{n-1}\delta(z)] + z^n\delta(z) = (n+1)z^n\delta(z).$$

Logo a igualdade é válida para $n+1$. Segue que (b) é válido para todo $n \in \mathbb{N}_0$. Por outro lado, $0 = \delta(1) = \delta(yy^{-1}) = y\delta(y^{-1}) + y^{-1}\delta(y)$, logo $\delta(y^{-1}) = (-1)y^{-2}\delta(y)$. Assim, dado $z \in F$ e $n \in \mathbb{N} \setminus \{0\}$ temos

$$\delta(z^{-n}) = \delta((z^n)^{-1}) = (-1)(z^n)^{-2}\delta(z^n) = (-1)z^{-2n}nz^{n-1}\delta(z) = (-n)z^{-(n+1)}\delta(z).$$

Logo a igualdade em (b) vale para todo $n \in \mathbb{Z}$.

(c) Pelo item (b), $\delta(z^p) = pz^{p-1}\delta(z) = 0$.

(d) Basta notar que $\delta(xy^{-1}) = x\delta(y^{-1}) + y^{-1}\delta(x) = -xy^{-2}\delta(y) + y^{-1}\delta(x) = y^{-2}(y\delta(x) - x\delta(y))$.

□

Definição 1.3.5 *Considere uma extensão algébrica L/K onde char $L = p > 0$. Um elemento $\gamma \in L$ é dito puramente inseparável sobre K se $\gamma^{p^r} \in K$ para algum $r \geq 0$. A extensão L/K é puramente inseparável se todos elementos $\gamma \in L$ são puramente inseparáveis sobre K.*

Para os próximos resultados, assumiremos que K é um corpo perfeito de característica $p > 0$.

Definição 1.3.6 *Um elemento $x \in F$ é dito separante sobre F/K se $F/K(x)$ é um extensão algébrica separável. Um corpo de funções F/K é dito separavelmente gerado se existe um elemento separante sobre F/K.*

A proposição seguinte apresenta várias propriedades a respeito de elementos separantes e uma caracterização desses elementos.

Proposição 1.3.7 *As seguintes sentenças são verdadeiras:*

(a) Suponha que $z \in F$ satisfaça $v_P(z) \not\equiv 0 \ mod\ p$ para algum $P \in \mathbb{P}_F$. Então z é um elemento separante para F/K. Em particular, F/K é separavelmente gerado.

(b) Existe $x, y \in F$ tal que $F = K(x, y)$.

(c) Para todo $n \geq 1$, o conjunto $F^{p^n} := \{z^{p^n};\ z \in F\}$ é um subcorpo de F. Mais ainda,

(1) $K \subseteq F^{p^n} \subseteq F$ e F/F^{p^n} é puramente inseparável de grau p^n.

(2) A aplicação de Frobenius $\phi_n : F \longrightarrow F$, definida por $\phi_n(z) := z^{p^n}$, é um isomorfismo de F em F^{p^n}. Logo o corpo de funções F^{p^n}/K tem o mesmo gênero de F/K.

(3) Suponha que $K \subseteq F_0 \subseteq F$ e F/F_0 é puramente inseparável de grau $[F : F_0] = p^n$, então $F_0 = F^{p^n}$.

(d) Um elemento $z \in F$ é separante para F/K se, e somente se, $z \in F^p$.

Os elementos separantes têm propriedades interessantes relacionadas à derivações.

Lema 1.3.8 *Suponha que x é separante sobre F/K e que $\delta_1, \delta_2 : F \longrightarrow M$ são derivações de F/K com $\delta_1(x) = \delta_2(x)$. Então $\delta_1 = \delta_2$.*

Proposição 1.3.9 *Valem as seguintes afirmações sobre derivações:*

(a) Sejam E/F uma extensão finita e separável de F e $\delta_0 : F \longrightarrow N$ uma derivação de F/K em algum corpo $N \subseteq E$. Então δ_0 pode ser estendida a uma derivação $\delta : E \longrightarrow N$. Essa extensão é unicamente determinada por δ_0.

(b) Se $x \in F$ é um elemento separante de F/K e $N \supseteq F$ é algum corpo, então existe uma única derivação $\delta : F \longrightarrow N$ de F/K tal que $\delta(x) = 1$.

A proposição anterior dá sentido a próxima definição.

Definição 1.3.10 *(a) Seja x um elemento separante do corpo de funções F/K. A única derivação $\delta_x : F \longrightarrow F$ tal que $\delta_x(x) = 1$ é chamada de derivação com respeito a x.*

(b) Seja

$$Der_F := \{\eta : F \longrightarrow F;\ \eta \text{ é uma derivação de } F/K\}.$$

Para $\eta_1, \eta_2 \in Der_F$ e $z, u \in F$ definimos

$$(\eta_1 + \eta_2)(z) := \eta_1(z) + \eta_2(z) \text{ e}$$

$$(u.\eta_1)(z) := u\eta_1(z).$$

Com essas operações Der_F é um F-módulo chamado de módulo das derivações de F/K.

Lema 1.3.11 *Seja x um elemento separante de F/K. Então:*

(a) $\forall \eta \in Der_F$, temos que $\eta = \eta(x)\delta_x$.

(b) (Regra da Cadeia) Seja y outro elemento separante de F/K. Então:

$$\delta_y = \delta_y(x)\delta_x.$$

(c) Para $t \in F$, temos

$$\delta_x(t) \neq 0 \Leftrightarrow t \text{ é um elemento separante.}$$

Demonstração

(a) Considere as duas derivações η e $\eta(x)\delta_x$ de F/K em F.Como $(\eta(x)\delta_x)(x) = \eta(x)\delta(x) = \eta(x)$ e x é separante, pelo lema 1.3.8 temos que $\eta(x)\delta_x = \eta$.

(b) Segue de (a).

(c) Se t é separante, $1 = \delta_t(t) = \delta_t(x)\delta_x(t)$ (pela definição de δ_t e pela regra da cadeia). logo $\delta_x(t) \neq 0$. Suponha agora que t é não separante. Se $char\ K = 0$, então $t \in K$ e $\delta_x(t) = 0$, pois todas as derivações de F/K zeram em K. Se $char\ K = p$, então $t = u^p$ para algum $u \in F$ (ver proposição 1.3.7 e $\delta_x(t) = \delta_x(u^p) = 0$, pelo lema 1.3.4.

□

Agora podemos introduzir a definição de diferencial.

Definição 1.3.12 *(a) Seja* $Z := \{(u,x) \in F \times F;\ x \text{ é separante}\}$. *Definimos a relação* $\sim$ *por*

$$(u,x) \sim (v,y) :\Leftrightarrow v = u\delta_y(x).$$

É fácil verificar que esta é uma relação de equivalência.

(b) Denotaremos por udx *a classe de equivalência de* $(u,x) \in Z$ *com respeito a* $\sim$. *Chamamos* udx *de uma diferencial de* F/K. *A classe de equivalência de* $(1,x)$ *é simplesmente denotada por* dx. *Observe que*

$$udx = vdy \Leftrightarrow v = u\delta_y(x).$$

(c) $\Delta_F := \{udx;\ u,x \in F \text{ com } x \text{ separante}\}$ *é o conjunto de todas diferenciais de* F/K. *Definimos a soma de duas diferenciais* $udx, vdy \in \Delta_F$ *como segue: Seja* z *separante, então*

$$udx = (u\delta_z(x))dz \text{ e } vdy = (v\delta_z(y))dz$$

e

$$udx + vdy := (u\delta_z(x) + v\delta_z(y))dz.$$

Esta definição independe da escolha de z *pela regra da cadeia. Nós, também definimos,*

$$w(udx) := (wu)dx \in \Delta_F.$$

Com esta definição Δ_F *torna-se um* F*-módulo.*

(d) Para um elemento $t \in F$ *não separável, definimos* $dt := 0$. *Logo, obtemos a aplicação*

$$d = \begin{cases} F \longrightarrow \Delta_F \\ t \longmapsto dt, \end{cases}$$

O par (Δ_F, d) *é chamado de módulo de diferenciais de* F/K *(por simplicidade notaremos apenas por* Δ_F*).*

Proposição 1.3.13 *(a) Seja* $z \in F$ *separante. Então* $dz \neq 0$ *e toda diferencial* $w \in \Delta_F$ *pode ser escrita de maneira única na forma* $w = udz$ *com* $u \in F$. *Logo* Δ_F *é um* F*-módulo unidimensional.*

(b) A aplicação $d : F \longrightarrow \Delta_F$ *da definição* 1.3.12*, item* (d)*, é uma derivação de* F/K.

(c) Para $t \in F$*, temos:*

$$dt \neq 0 \Leftrightarrow t \text{ é separante.}$$

(d) Seja $\delta : F \longrightarrow M$ *uma derivação de* F/K *em algum* F*-módulo* M. *Então existe uma única aplicação* $\mu : \Delta_F \longrightarrow M$ *tal que* $\delta = \mu \circ d$.

Como as diferenciais de Weil também são um F-módulo unidimensional (ver proposição 1.2.8), existe um isomorfismo F-linear entre diferenciais e diferenciais de Weil.

Definição 1.3.14 *(a) A diferencial da forma* $w = dx$ *é dita exata. As diferenciais exatas formam um* K*-subespaço de* Δ_F.

(b) *Como Δ_F é um F-módulo unidimensional, podemos definir $w_1/w_2 \in F$ para $w_1, w_2 \in \Delta_F$ e $w_2 \neq 0$ sendo*

$$u = \frac{w_1}{w_2} \Leftrightarrow w_1 = uw_2.$$

Em particular, se z é separante e $y \in F$, o quociente dy/dz é definido e nós temos

$$\delta_z(y) = \frac{dy}{dz},$$

Mais ainda, se x, z são separantes vale

$$udx = vdy \Leftrightarrow v = u\frac{dx}{dy} \Leftrightarrow u = \frac{dy}{dx} \text{ e}$$

$$\frac{dy}{dx} = \frac{dy}{dz}\frac{dz}{dx}.$$

Definição 1.3.15 *Uma valorização de um corpo T é uma aplicação sobrejetiva $v : T \longrightarrow \mathbb{Z} \cup \{\infty\}$ que satisfaz*

(1) $v(x) = \infty \Leftrightarrow x = 0$;

(2) $v(xy) = v(x) + v(y), \forall x, y \in T$;

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

Dizemos que uma seqüência $(x_n)_{n\geq 0} \subseteq T$ é convergente se existe $x \in T$ tal que, $\forall c \in \mathbb{R}$, existe um índice $n_0 \in \mathbb{N}$ tal que

$$v(x - x_n) \geq c, \text{ sempre que } n \geq n_0.$$

Dizemos que $(x_n)_{n\geq 0}$ é uma seqüência de Cauchy se vale a seguinte propriedade: Dado $c \in \mathbb{R}$, existe um índice $n_0 \in \mathbb{N}$, tal que, para todos $n, m \geq n_0$, temos $v(x_n - x_m) \geq c$.

Neste contexto também valem as propriedades:

(i) O limite de uma seqüência convergente é único.

(ii) Toda seqüência de Cauchy é convergente.

Definição 1.3.16 *Seja $v : T \longrightarrow \mathbb{Z} \cup \{\infty\}$ uma valorização de um corpo T. Ao par (T, v) chamamos de corpo com valorização.*

Definição 1.3.17 *(a) Um corpo com valorização (T, v) é completo se toda seqüência de Cauchy é convergente em T.*

(b) Suponha que (T, v) é um corpo com valorização. Um completamento de T é um corpo com valorização $(\tilde{T}, \tilde{v})$ com as seguintes propriedades:

(1) $T \subseteq \tilde{T}$ e v é restrição de $\tilde{v}$ a T;

(2) T é completo com respeito à valorização $\tilde{v}$;

(3) T é denso em $\tilde{T}$, i.e., $\forall z \in \tilde{T}$, existe $(x_n)_{n\geq 0} \subseteq T$ convergindo para z.

Proposição 1.3.18 *Para todo corpo com valorização (T, v) existe um completamento. Este é único no seguinte sentido: Sejam $(\tilde{T}, \tilde{v})$ e $(\hat{T}, \hat{v})$ completamentos de (T, v), então existe um isomorfismo $f : \tilde{T} \longrightarrow \hat{T}$ tal que $\tilde{v} = \hat{v} \circ f$. Logo $(\hat{T}, \hat{v})$ é chamado de completamento de (T, v).*

Proposição 1.3.19 *Seja $(z_n)_{n\geq 0}$ uma seqüência em (T, v). Então a série $\sum_{i=0}^{\infty} z_i$ é convergente se, e somente se, $(z_n)_{n\geq 0}$ converge para 0.*

Demonstração
Suponha que $(z^n)_{n\geq 0}$ converge para zero. Considere a m-ésima soma parcial $s_m := \sum_{i=0}^{m} z_i$. Para $n > m$ nós temos

$$v(s_n - s_m) = v(\sum_{i=m+1}^{n})z_i \geq \min\{v(z_i); m < i \leq n\} \geq \{v(z_i; i > m\}.$$

Como $v_{z_i} \to \infty$, para $i \to \infty$, isto mostra que $(s_n)_{n\geq 0}$ é uma seqüência de de Cauchy em T. Logo convergente. A recíproca é feita de maneira análoga a demonstração feita para séries de números reais em análise. □

Agora estudaremos as diferenciais no contexto de corpo de funções.

Definição 1.3.20 *Seja P um lugar de F/K. O completamento de F com respeito a valorização v_P é chamado o completamento P-ádico de F. Denotamos este completamento por $\hat{F}_P$ e a valorização de $\hat{F}_P$ por v_P.*

Teorema 1.3.21 *Seja $P \in \mathbb{P}_F$ um lugar de grau um e $t \in F$ um elemento P-primo. Então todo elemento $z \in \hat{F}_P$ tem uma única representação da forma*

$$z = \sum_{i=n}^{\infty} a_i t^i, \ \text{com } n \in \mathbb{Z} \text{ e } a_i \in K.$$

Esta representação é chamada de expansão P-ádica de z em séries de potências com respeito a t. Por outro lado, se $(c_i)_{i\geq n}$ é uma seqüência em K, então a série $\sum c_i t^i$ converge em $\hat{F}_P$ e temos

$$v_P(\sum_{i=n}^{\infty} c_i t^i) = \min\{i; \ c_i \neq 0\}.$$

Continuaremos a considerar um lugar P de F/K de grau um e um elemento t primo para P. Pela proposição 1.3.7, t é um elemento separante de F/K e logo, podemos falar na derivação $\delta_t : F \to F$ com respeito a t. Usando uma expansão P-ádica de z em séries de potências com respeito a t, podemos calcular $dz/dt = \delta(z)$ para $z \in F$.

Proposição 1.3.22 *Seja $P \in \mathbb{P}_F$ de grau um e $t \in F$ um elemento P-primo. Se $z \in F$ tem a expansão P-ádica $z = \sum_{\infty}^{i=n} a_i t^i$ com coeficientes $a_i \in K$, então*

$$\frac{dz}{dt} = \sum_{i=n}^{\infty} i a_i t^{n-1}.$$

Também gostaríamos de introduzir o conceito de resíduo de uma diferencial $\omega \in \Delta_F$ em relação a um lugar P em F/K.

Definição 1.3.23 *Suponha que P é um lugar de grau um e $t \in F$ é um elemento P-primo. Se $z \in F$ tem sua expansão P-ádica da forma $z = \sum_{i=n}^{\infty} a_i t_i$, com $n \in \mathbb{Z}$ e $a_i \in K$, nós definimos o resíduo com respeito a P e t por*

$$res_{P,t}(z) = a_{-1}.$$

Claramente, $res_{P,t} : F \longrightarrow K$ é uma aplicação K-linear e

$$res_{P,t}(z) = 0, \ \text{se } v_P(z) \geq 0.$$

Proposição 1.3.24 *Seja $s, t \in F$ elementos P-primos (onde P é um lugar de grau um). Então*

$$res_{P,s}(z) = res_{P,t}(z\frac{ds}{dt}),$$

para todo $z \in F$.

Definição 1.3.25 *Seja $w \in \Delta_F$ uma diferencial e $P \in \mathbb{P}_F$ um lugar de grau um. Escolha um elemento P-primo $t \in F$ e escreva $w = udt$, com $u \in F$. Então definimos o resíduo de w em P por*

$$res_P(w) := res_{P,t}(u).$$

Teorema 1.3.26 *Suponha que F/K é um corpo de funções algébricas sobre um corpo perfeito K e seja $x \in F$ um elemento separante.*

(a) A aplicação $\delta : F \longrightarrow \Omega_F$ é uma derivação de F/K;

(b) Para qualquer $y \in F$, nós temos

$$\delta(y) = \frac{dy}{dx}\delta(x);$$

(c) A aplicação

$$\mu = \begin{cases} \Delta_F \longrightarrow \Omega_F \\ zdx \longmapsto z\delta(x) \end{cases}$$

é um isomorfismo do módulo de diferenciais Δ_F em Ω_F. Este isomorfismo é compatível com as derivações $d : F \longrightarrow \Delta_F$ e $\delta : F \longrightarrow \Omega_F$, isso significa que $\mu \circ d = \delta$.

(d) Se $P \in \mathbb{P}_F$ é um lugar de F/K de grau um e $\omega = z\delta(x) \in \Omega_F$, a componente local de ω em P é dada por

$$(z\delta(x))_P(u) = res_P(uzdx).$$

Em particular

$$(z\delta(x))_P(1) = res_P(zdx).$$

(e) Se $\omega = z\delta(t) \in \Omega_F$ e t é primo do lugar P, então temos $v_P(\omega) = v_P(z)$.

Definição 1.3.27 *Como conseqüência do teorema anterior, nós identificamos o módulo de diferenciais Δ_F com o módulo de diferenciais de Weil de F/K. Isto significa que uma diferencial $\omega = zdx \in \Delta_F$ é a mesma diferencial de Weil $\omega = z\delta(x) \in \Omega_F$ (onde $x \in F$ é separante e $z \in F$). Em outras palavras,*

$$\Delta_F = \Omega_F \text{ e } zdx = z\delta(x).$$

Se $0 \neq \omega \in \Delta_F$ e t é um elemento primo para o lugar $P \in \mathbb{P}_F$, nós podemos escrever $\omega = zdt$, com $z \in F$, e definimos

$$v_P(\omega) := v_P(z) \text{ e } (\omega) := \sum_{P \in \mathbb{P}_F} v_P(\omega)P.$$

O teorema 1.3.26 e a definição 1.3.27 concluem objetivo dessa seção.

Observação 1.3.28 *Como uma importante conseqüência do teorema* 1.3.26*, temos a seguinte fórmula para o divisor de uma diferencial $\omega = zdx \neq 0$:*

$$(zdx) = (z) + (dx).$$

1.4 Extensões de corpos de funções

Nessa seção consideraremos o corpo de funções F'/K' (onde K' é o corpo de constantes de F') tal que F'/F é uma extensão algébrica e $K \subseteq K'$. Por conveniência fixaremos um fecho algébrico $\Phi \supseteq F$ e consideraremos apenas extensões $F' \supseteq F$ com $F' \subseteq \Phi$.

Começaremos com as definições básicas.

Definição 1.4.1 *Um corpo de funções algébricas F'/K' é chamado de extensão algébrica de F/K se $F' \supseteq F$ é uma extensão algébrica e $K' \supseteq K$. Se $[F' : F]$ é finita, então dizemos que F'/K' é uma extensão algébrica finita de F/K.*

Definição 1.4.2 *Considere uma extensão algébrica F'/K' de F/K. Dizemos que um lugar $P' \in \mathbb{P}_{F'}$ está sobre $P \in \mathbb{P}_F$ se $P \subseteq P'$. Também dizemos que P' é uma extensão de P, ou ainda, P está sob P' e denotamos $P'|P$.*

Proposição 1.4.3 *Seja F'/K' uma extensão algébrica de F/K. Suponha que P (resp. P') é um lugar de F/K (resp. F'/K') e seja $\mathcal{O}_P \subseteq F$ (resp. $\mathcal{O}_{P'} \subseteq F'$) denota o correspondente anel de valorização, v_P (resp. $v_{P'}$) a correspondente valorização discreta. Então são equivalentes:*

(i) $P'|P$;

(i) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$;

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

Uma conseqüência da proposição acima é que para $P'|P$ existe um mergulho canônico do corpo de classes de resíduo $F_P = \mathcal{O}_P/P$ no corpo de classes de resíduos $F'_P = \mathcal{O}_{P'}/P'$, dado por

$$x(P) \mapsto x(P') \text{ para } x \in \mathcal{O}_P.$$

Logo nós podemos considerar F_P como subcorpo de $F'_{P'}$. Este fato e a proposição 1.4.3 motivam a próxima definição.

Definição 1.4.4 *Seja F'/K' uma extensão algébrica de F/K e seja $P' \in \mathbb{P}_{F'}$ um lugar de F'/K' sobre $P \in \mathbb{P}_F$.*

(i) O inteiro $e(P'|P) := e$ com

$$v_{P'}(x) = ev_P(x), \text{ para todo } x \in F$$

é chamado de índice de ramificação de P' sobre P. Dizemos que $P'|P$ é ramificado se $e(P'|P) > 1$ e $P'|P$ é não é ramificado se $e(P'|P) = 1$.

(ii) $f(P'|P) := [F'_{P'} : F_P]$ é chamado de grau relativo de P' sobre P.

Note que $f(P'|P)$ pode ser finito ou infinito, no entanto o índice de ramificação é sempre um número natural.

Proposição 1.4.5 *Seja F'/K' uma extensão de F/K e P' um lugar de F'/K' sobre $P \in \mathbb{P}_F$. Então*

(i) $f(P'|P) < \infty \Leftrightarrow [F' : F] < \infty$;

(ii) Se F''/K'' é uma extensão algébrica de F'/K' e $P'' \in \mathbb{P}_{F''}$ é uma extensão de P', então

$$e(P''|P) = e(P''|P').e(P'|P);$$

$$f(P''|P) = f(P''|P').f(P'|P).$$

Iremos agora apresentar alguns resultados sobre a existência de lugares em corpos de funções.

Proposição 1.4.6 *Seja F'/K' uma extensão algébrica de F/K.*

(i) Para todo lugar $P' \in \mathbb{P}_F$ existe exatamente um lugar $P \in \mathbb{P}_F$ tal que $P'|P$, a saber $P = P' \cap F$.

(ii) Reciprocamente, todo lugar $P \in \mathbb{P}_F$ tem pelo menos uma, mas somente uma quantidade finita, extensão $P' \in \mathbb{P}_{F'}$.

Gostaríamos de ter um limitante para o número de extensões $P' \in \mathbb{P}_{F'}$ de um lugar P de F/K. Isso pode ser obtido, para o caso de extensões finitas de corpos de funções, como conseqüência do próximo teorema.

Teorema 1.4.7 *Seja F'/K' uma extensão finita de F/K. P uma lugar de F/K e $P_1, \ldots, P_m$ todos os lugares de F'/K' sobre 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*

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

Demonstração
Ver [7], teorema III.1.11. □

Nas condições do teorema acima, o número de lugares $P' \in \mathbb{P}_{F'}$ sobre $P \in \mathbb{P}_F$ não ultrapassa $[F' : F]$. Se $P' \in \mathbb{P}_{F'}$ está sobre P, então $e(P'|P) \leq [F' : F]$ e $f(P'|P) \leq [F' : F]$.

Capítulo 2

Códigos e distâncias generalizadas de Hamming

2.1 Códigos lineares e distâncias generalizadas de Hamming

Essa seção é baseada, em parte, nas referências [9] e [10].

Seja $\mathbb{F}_q$ um corpo finito com q elementos. Consideraremos o espaço vetorial $\mathbb{F}_q^n$ de dimensão n cujos elementos são n-uplas da forma $a = (a_1, \ldots, a_n)$ com $a_i \in \mathbb{F}_q$.

Definição 2.1.1 *Sejam $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$. A função $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{N}_0$ definida por*

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

é chamada de distância de Hamming em $\mathbb{F}_q^n$. O peso de um elemento $a \in \mathbb{F}_q^n$ é definido por

$$w(a) := d(a, 0) = |\{i;\ a_i \neq 0\}|.$$

É fácil ver que a distância de Hamming satisfaz os axiomas de métrica em $\mathbb{F}_q^n$.

Definição 2.1.2 *Dizemos que C é um código $[n, k]$ se C é um $\mathbb{F}_q$-subespaço linear de $\mathbb{F}_q^n$ e $\dim(C) = k$. Aos elementos de C, chamaremos de palavras do código. Um subconjunto $D \subseteq C$ é dito subcódigo de C se D é um $\mathbb{F}_q$-subespaço linear de C. Chamamos de n o comprimento de C e à $k = \dim C$ chamamos de dimensão do código C. Assim um código $[n, k]$ é um código de comprimento n e dimensão k.*

A distância mínima $d(C)$ de um código $C \neq 0$ é definida por

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

Note que, como $d(a, b) = d(a - b, 0) = w(a - b)$ e C é um espaço linear, a distância mínima é igual a

$$d(C) = \min\{w(c);\ 0 \neq c \in C\}.$$

Um código $[n, k]$ com distância mínima d será chamado de código $[n, k, d]$.
A distribuição de peso de um código $[n, k]$ é a $(n + 1)$-upla $(A_0, \ldots, A_n) \in \mathbb{N}_0^{n+1}$ dada por

$$A_i := |\{c \in C;\ w(c) = i\}|.$$

É fácil ver que $A_0 = 1$ e $A_i = 0$ para $1 \leq i \leq d(C) - 1$. O polinômio

$$W_C(X) := \sum_{i=0}^{n} A_i X^i \in \mathbb{Z}[X]$$

é chamado de polinômio enumerador de peso do código C.

Definição 2.1.3 *Sejam C um código $[n,k]$, $I_n = \{1,\ldots,n\}$ e D um subcódigo de C. Chamamos de suporte de D ao conjunto*

$$\chi(D) := \{i \in I_n;\ \exists (x_1,\ldots,x_n) \in D \text{ com } x_i \neq 0\}.$$

Definição 2.1.4 *Sejam C um código $[n,k]$ e $r \in \{1,\ldots,k\}$. O r-ésimo peso generalizado de Hamming de C, denotado por $d_r(C)$, é o menor número de elementos que um suporte de um subcódigo D de C, com $\dim(D) = r$, pode assumir, ou seja,*

$$d_r(C) := min\{|\chi(D)|;\ D \text{ é um subcódigo de } C \text{ com } \dim(D) = r\}.$$

Ao conjunto $\{d_r(C);\ 1 \leq r \leq k\}$ chamamos de hierarquia de pesos do código C.

Note que $d_1(C)$ coincide com $d(C)$.

Definição 2.1.5 *Seja C um código $[n,k]$. Então:*

(i) Uma matriz cujas linhas formam uma base para C é dita matriz geradora de C.

(ii) Notaremos por $C^{\perp}$ o conjunto

$$C^{\perp} = \{x \in \mathbb{F}_q^n;\ < x,y >= 0 \text{ para todo } y \in C\},$$

onde $<,>$ denota o produto interno em $\mathbb{F}_q^n$ definido por

$$< a,b >:= \sum_{i=1}^{n} a_i b_i$$

para $a = (a_1,\ldots,a_n)$ e $b = (b_1,\ldots,b_n) \in \mathbb{F}_q^n$. Chamaremos a esse conjunto de espaço ortogonal à C.

(iii) Uma matriz cujas linhas formam uma base para $C^{\perp}$ é dita matriz de checagem de paridade de C. Sejam $H_i, i \in I \subseteq \{1,\ldots,n\}$, respectivamente o i-ésimo vetor coluna da matriz H de checagem de paridade de C. Denotaremos por $< H_i;\ i \in I >$ como o espaço gerado pelos vetores colunas H_i, com $i \in I$.

Uma matriz de checagem de paridade de um código $[n,k]$ é uma $(n-k) \times n$ matriz H de posto $n-k$ e, mais ainda, temos

$$C = \{u \in \mathbb{F}_q^n;\ Hu^t = 0\}$$

(onde u^t denota o transposto do vetor u). Logo, uma matriz de checagem de paridade verifica se um vetor $u \in \mathbb{F}_q^n$ é uma palavra código ou não.

Proposição 2.1.6 *Sejam C um código $[n,k]$ e D um subcódigo de C. Então*

(i) Se $\dim(D) = r$, $0 \leq r \leq k$, então $|\chi(D)| \geq r$.

(ii) Se $|\chi(D)| = r$, $0 \leq r \leq n$, então $\dim(D) \leq r$.

(iii) Seja $E \subset D$ um subcódigo de D, então $\chi(E) \subseteq \chi(D)$ e, portanto, $|\chi(E)| \leq |\chi(D)|$.

Demonstração:

(i) Suponha por absurdo que $|\chi(D)| = s < r$, isto é, $\chi(D) = \{i_1, \ldots, i_s\} \subseteq \{1, \ldots, n\}$. Dado $x := (x_1, \ldots, x_n) \in D$, então $x_i = 0$ para todo $i \notin \chi(D)$. Seja $\phi : D \longrightarrow \mathbb{F}_q^s$ uma função definida por $\phi(x_1, \ldots, x_n) = (x_{i_1}, \ldots, x_{i_s})$. A função ϕ é obviamente linear e, mais ainda,

$$\ker(\phi) = \{x \in D;\ \phi(x) = 0\} = \{x \in D;\ x_i = 0, \forall i \in \chi(D)\} = \{0\}.$$

Pelo Teorema do Núcleo e Imagem,

$$r = \dim D = \dim(\ker(\phi)) + \dim(Im(\phi)) = \dim(Im(\phi)) \leq s,$$

ou seja, $r \leq s$, o que é absurdo. Logo $|\chi(D)| \geq r$.

(ii) Suponha por absurdo que $\dim(D) = s > r$. Como $|\chi(D)| = r$, podemos escrever $\chi(D) = \{i_1, \ldots, i_r\}$. Considere a função $\phi : D \longrightarrow \mathbb{F}_q^r$, tal que $\phi(x_1, \ldots, x_n) = (x_{i_1}, \ldots, x_{i_r})$. Uma vez mais, ϕ é linear e $\ker(\phi) = 0$. Pelo Teorema do Núcleo e Imagem,

$$r \geq \dim(Im(\phi)) = \dim(\ker(\phi)) + \dim(Im(\phi)) = \dim(D) = s,$$

isto é, $r \geq s$, o que é absurdo. Portanto, $\dim(D) \leq r$.

(iii) De fato, se $i \in \chi(E)$, então existe $x = (x_1, \ldots, x_n) \in E$ *com* $x_i \neq 0$, logo existe $x = (x_1, \ldots, x_n) \in D$ *com* $x_i \neq 0$ e, daí, $i \in \chi(D)$. Assim, $\chi(E) \subset \chi(D)$ e, portanto, $|\chi(E)| \leq |\chi(D)|$.

Um dos teoremas que mais serão usados é o seguinte:

Teorema 2.1.7 (Monotonicidade) *Seja C um código $[n, k]$ com $k > 0$. Então*

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

Demonstração
Seja D um subcódigo de C tal que $|\chi(D)| = d_r(C)$ e $\dim(D) = r$. Sejam ainda $i \in \chi(D)$ e $D_i := \{x \in D;\ x_i = 0\}$. É claro que $D_i \subsetneq D$. Assim, existe $y \in D \backslash D_i$. Note que fazendo $y = (y_1, \ldots, y_n)$, temos $y_i \neq 0$. Mostremos agora que $D = D_i \oplus < y >$. De fato, se $x := (x_1, \ldots, x_n) \in D$, então existe $\lambda \in \mathbb{F}_q$ tal que $x_i = \lambda y_i$. Assim $x = (x - \lambda y) + \lambda y$ com $(x - \lambda y) \in D_i$ e $\lambda y \in < y >$. Além disso, se $x \in D_i \cap < y >$, então $x_i = 0$ e existe $\lambda \in \mathbb{F}_q^n$ tal que $x = \lambda y$, assim, $0 = x_i = \lambda y_i$ com $y_i \neq 0$. Logo $\lambda = 0$ e, portanto, $x = 0$, ou seja, $D_i \cap < y >= \{0\}$. Segue então que $D = D_i \oplus < y >$. Logo $\dim(D_i) = \dim(D) - 1$. Daí,

$$d_{r-1}(C) \leq |\chi(D_i)| = |\chi(D)| - 1 = d_r(C) - 1 < d_r(C).$$

Falta mostrar que $d_1(C) \geq 1$ e $d_k(C) \leq n$. Mas, se D é subcódigo de C de dimensão um, $D \neq \{0\}$, logo existe $x \in D$ tal que $x \neq 0$, isto é, $\chi(D) \neq \emptyset$, ou ainda, $|\chi(D)| \geq 1$. Assim, como D foi tomado arbitrariamente, $d_1(C) \geq 1$. Como os elementos de C têm no máximo n coordenadas, $|\chi(C)| \leq n$. Daí, $d_k(C) \leq |\chi(C)| \leq n$. □

Corolário 2.1.8 *Sejam C um código $[n, k]$, $r \in \{1, \ldots, k\}$ e $t \in \{0, \ldots, k - r\}$. Então $d_r(C) + t \leq d_{r+t}(C)$.*

Demonstração
Utilizaremos indução sobre t. Fixado $r \in \{1, \ldots, k\}$, é claro que $d_r(C) + 0 \leq d_{r+0}(C)$. Suponha que $d_r(C) + t \leq d_{r+t}(C)$ com $t \in \{0, \ldots, k - r - 1\}$. Pelo Teorema 2.1.7, $d_{r+t}(C) < d_{r+t+1}(C)$. Assim, $d_{r+t+1}(C) \geq d_{r+t}(C) + 1 \geq d_r(C) + t + 1$. □

Corolário 2.1.9 (Cota de Singleton Generalizada) *Sejam C um código $[n,k]$ e $r \in \{1,\ldots,k\}$. Então $d_r(C) \leq n-k+r$.*

Demonstração
Basta tomar $t = k-r$ no corolário 2.1.8. Assim, de $d_r(C) + k - r \leq d_{r+(k-r)}(C) = d_k(C)$ e $d_k(C) \leq n$, segue que

$$d_r(C) \leq d_k(C) - k + r \leq n - k + r.$$

□

Códigos com $k + d = n + 1$ são chamados de códigos MDS (maximum distance separable codes). Em particular a distância mínima de um código não pode ser maior que $n - k + 1$.

Teorema 2.1.10 *Sejam C um código $[n,k]$ e $1 \leq r \leq k$. Então*

$$d_r(C) = \min\{|X|;\ |X| - \dim(< H_i;\ i \in X >) \geq r\},$$

onde $X \subseteq \{1,\ldots,n\}$.

Demonstração
Dado $I \subseteq \{1,\ldots,n\}$, definimos $S(I) :=< H_i;\ i \in I >$ e $S^{\perp}(I) := \{x \in \mathbb{F}_q^n;\ x_i = 0\ para\ todo\ i \notin I\ e\ \sum_{i\in I} x_i H_i = 0\}$. Mostremos que $\dim(S(I)) + \dim(S^{\perp}(I)) = |I|$. Suponhamos $I = \{i_1,\ldots,i_s\}$. Considere a aplicação

$$\phi = \begin{cases} \mathbb{F}_q^{|I|} \longrightarrow M_{(n-k)\times 1}(\mathbb{F}_q), \\ (x_{i_1},\ldots,x_{i_s}) \longmapsto H_{i_1}x_{i_1} + \cdots + H_{i_s}x_{i_s}. \end{cases}$$

É fácil ver que ϕ está bem definida e é linear. Considere também a aplicação

$$\psi = \begin{cases} S^{\perp}(I) \longrightarrow \ker(\phi), \\ (x_1,\ldots,x_n) \longmapsto (x_{i_1},\ldots,x_{i_s}). \end{cases}$$

A aplicação ψ está, também, bem definida e é linear. Note que, dado $x = (x_1,\ldots,x_n) \in S^{\perp}(I)$, temos $x_i = 0, \forall i \notin I$. Se $\psi(x) = 0$, então $x_i = 0$ também para todo $i \in I$. Logo $\ker(\psi) = \{0\}$, ou seja, ψ é injetora. Seja agora $y = (y_{i_1},\ldots,y_{i_s}) \in \ker(\phi)$. Tome $x = (x_1,\ldots,x_n)$ com $x_i = y_i, \forall i \in I$ e $x_i = 0, \forall i \notin I$. Assim $x \in S^{\perp}(I)$ e $\psi(x) = y$. Portanto ψ é sobrejetora. Segue que $S^{\perp}(I)$ é isomorfo ao núcleo de ϕ. Como $S(I) = Im\ (\phi)$, pelo Teorema do Núcleo e imagem

$$|I| = \dim \mathbb{F}_q^{|I|} = \dim(\ker(\phi)) + \dim(Im\ (\phi)) = \dim(S^{\perp}(I)) + \dim(S(I)).$$

Sejam $d = min\{|X|;\ |X| - \dim(< H_i; i \in X >) \geq r\}$ e $I \subseteq \{1,\ldots,n\}$, tal que $|I| = d$ e $|I| - \dim(S(I)) = r$. Vamos mostrar que existe I nessas condições. Seja $a := \dim < H_i; i \in I >$, onde $|I| = d$ (a existência do mínimo é óbvia). Suponhamos por absurdo que $|I| - \dim(S(I)) > r$. Então existem $j_1, j_2, \ldots, j_a \in I$ tais que $\{H_{j_1},\ldots,H_{j_a}\}$ é um conjunto linearmente independente. Como $|I| > a$ (se $|I| \leq a$, então $|I| - \dim(< H_i; i \in I >) \leq 0 < r$, o que é absurdo), defina $h := |I| - a > 0$ e tome $l_1, l_2, \ldots, l_h \in I \setminus \{j_1,\ldots,j_a\}$. Então $I = \{j_1,\ldots,j_a,l_1,\ldots,l_h\}$. Por hipótese ao absurdo $|I| - \dim(S(I)) = a + h - a = h > r$. Seja $J = \{j_1,\ldots,j_a,l_1,\ldots,l_r\}$. Então $|J| = a + r < a + h = |I|$ e $|J| - \dim < H_i; i \in J >= a + r - a = r$, o que é absurdo pois $|I| = d = \min\{|X|; |X| - \dim < H_i; i \in X > \geq r\} \leq |J|$.

Nas condições acima temos que $\dim(S^{\perp}(I)) = |I| - \dim(S(I)) = r$. Sabendo que $C = \{u \in \mathbb{F}_q^n;\ Hu^t = 0\}$, temos que, se $x := (x_1,\ldots,x_n) \in S^{\perp}(I)$, então $Hx^t = \sum_{i\in I} H_i x_i + \sum_{i\notin I} H_i x_i = 0$, logo $x \in C$. Daí $S^{\perp}(I) \subseteq C$. Portanto, $d_r(C) \leq |\chi(S^{\perp}(I))| \leq |I| = d$. Portanto, $d_r(C) \leq d$.

Para demonstrarmos o Teorema 2.1.10, basta provar a desigualdade $d \leq d_r(C)$. Sejam, então, D subcódigo de C com $\dim(D) = r$, $|\chi(D)| = d_r(C)$ e $I = \chi(D)$. Então $D \subseteq S^{\perp}(I)$. De

fato, basta notar que, se $x \in D$, então $x_i = 0, \forall i \notin \chi(D)$ e, como $D \subseteq C$, então $Hx^t = 0$, ou seja, $0 = \sum_{i\in I} H_i x_i + \sum_{i\notin I} H_i x_i = \sum_{i\in I} H_i x_i$. Mas, $\dim(S(I)) = |I| - \dim(S^\perp(I)) \leq |I| - \dim(D) = |I| - r$, logo $|I| - \dim(S(I)) \geq r$. Mostremos que a igualdade vale. Suponha por absurdo que $|I| - \dim(S(I)) = r' > r$, então $D \neq S^\perp(I)$ (pois, se $D = S^\perp(I)$, então $|I| - \dim(S(I)) = r = r'$, o que não acontece por hipótese), logo $d_{r'}(C) \leq |\chi(S^\perp(I))| \leq |I| = |\chi(D)| = d_r(C)$. Mas, novamente, por hipótese $r < r'$ e, pelo Teorema 2.1.7, $d_r(C) < d_{r'}(C)$. Absurdo. Temos assim que $|I| - \dim(S(I)) = r$. Daí $d_r(C) = |\chi(D)| = |I| \geq |I| - \dim(S(I)) \geq d$. Resumindo, $d_r(C) \geq d$. Portanto $d_r(C) = d$. □

Apesar de não ser fácil determinar o $\min\{|X|; |X| - \dim(< H_i; i \in I >) \geq r\}$, este é o primeiro resultado que determina a r-ésima distância generalizada de forma precisa.

Teorema 2.1.11 *Seja C um código $[n, k]$. Então* $\{d_r(C);\ 1 \leq r \leq k\} = \{1, \ldots, n\} \backslash \{n + 1 - d_r(C^\perp);\ 1 \leq r \leq n - k\}$.

Demonstração
Seja $r \in \{1, \ldots, n-k\}$. Pelo teorema 2.1.7, $d_r(C^\perp) \leq n$, logo

$$n + 1 - d_r(C^\perp) \geq 1.$$

Também, pelo teorema 2.1.7, $d_r(C^\perp) \geq 1$, logo

$$n + 1 - d_r(C^\perp) \leq n.$$

Assim $n + 1 - d_r(C^\perp) \in \{1, \ldots, n\}$, para todo $r \in \{1, \ldots, n-k\}$. Portanto basta mostrar que $n + 1 - d_r(C^\perp) \notin \{d_t(C);\ 1 \leq t \leq k\}$.

Definimos $d_0(C) := 0$. Façamos $t = k + r - d_r(C^\perp)$. Usando a Cota de Singleton Generalizada

$$d_r(C^\perp) \leq n - (n - k) + r = k + r,$$

logo $t \geq 0$. Pelo teorema da monotonicidade $d_r(C^\perp) \geq r$, e logo $t \leq k$. Isso prova que $d_t(C)$ está definido para todo r com $1 \leq r \leq k$. Então provemos que $d_t(C) \leq n - d_r(C^\perp)$.

Seja D um subcódigo de $C^\perp$ com $\dim D = r$ e $|\chi(D)| = d_r(C^\perp)$. Então existe uma matriz de checagem de paridade para C onde as r primeiras linhas são vetores em D e as últimas $n - k - r$ não são. Os vetores colunas $\{H_i;\ i \notin \chi(D)\}$ tem suas r primeiras coordenadas zero. Logo $dim(< H_i;\ i \notin \chi(D) >) =$ posto coluna de $(< H_i;\ i \notin \chi(D) >) \leq$ posto linha de $(< R_i;\ r + 1 \leq i \leq n - k >) = n - k - r$ (onde R_i é a i-ésima linha de H). Pelo teorema 2.1.10, fazendo $I = \{1, \ldots, n\} \setminus \chi(D)$, temos $d_t(C) \leq |I| = n - d_r(C^\perp)$, uma vez que $|I| - \dim(< H_i;\ i \in I >) \geq n - d_r(C^\perp) - (n - k - r) = k + r - d_r(C^\perp) = t$.

Agora, provemos que $d_{t+\Delta} \neq n - d_r(C^\perp) + 1$, para todo $\Delta \geq 1$. Suponhamos por absurdo que $d_{t+\Delta}(C) = n - d_r(C^\perp) + 1$ para algum $\Delta \geq 1$. Então existe uma matriz geradora G para C (equivalentemente uma matriz de checagem de paridade para $C^\perp$) tal que, sem perda de generalidade, as últimas $d_r(C^\perp) - 1$ posições das $t + \Delta$ linhas são todas nulas. Seja $I = \{n - d_r(C^\perp) + 2, \ldots, n\}$. Então os últimos $|I|$ vetores colunas de G geram um espaço vetorial de dimensão $\leq k - t - \Delta = d_r(C^\perp) - r - \Delta$. Note que $|I| = n - (n - d_r(C^\perp + 2)) + 1 = d_r(C^\perp) - 1$. Façamos $s := |I| - (d_r(C^\perp) - r - \Delta) = d_r(C^\perp) - 1 - (d_r(C^\perp) - r - \Delta) = r + \Delta - 1$. Então $s \geq r$. Pelo Teorema 2.1.7 $d_r(C^\perp) \leq d_s(C^\perp)$. Como $|I| - \dim(< H_i;\ i \in I >) \geq d_r(C^\perp) - 1 - (d_r(C^\perp) - r - \Delta) = r + \Delta - 1 = s$, temos $d_s(C^\perp) \leq |I| = d_r(C^\perp) - 1 < d_r(C^\perp)$, o que é absurdo. Portanto

$$d_{t+\Delta}(C) \neq n - d_r(C^\perp) + 1.$$

Agora, basta juntar as peças. Dado $r \in \{1, \ldots, n-k\}$, já provamos que $d_t(C) \leq n - d_r(C^\perp) < n + 1 - d_r(C^\perp)$. Pelo Teorema 2.1.7, $d_1(C) < d_2(C) < \cdots < d_t(C) < n + 1 - d_r(C^\perp)$.

Logo $n+1-d_r(C^\perp) \notin \{d_1(C), d_2(C), \ldots, d_t(C)\}$. Mas, como já mostramos também, $n+1-d_r(C^\perp) \neq d_{t+\Delta}(C)$ para todo $\Delta \geq 1$. Segue então que $n+1-d_r(C^\perp) \notin \{d_t(C);\ 1 \leq t \leq k\}$. □

Observe que o teorema 2.1.11 poderia ser também enunciado da seguinte maneira: Sejam C um código $[n,k]$ e $C^\perp$ seu código dual. Então $\{d_r(C);\ 1 \leq r \leq k\} \cup \{n+1-d_r(C^\perp);\ 1 \leq r \leq n-k\} = \{1, 2, \ldots, n\}$.

Observação 2.1.12 *Como $d_1(C^\perp) < d_2(C^\perp) < \ldots < d_{n-k}(C^\perp)$, então $n+1-d_{n-k}(C^\perp) < n+1-d_{n-k-1}(C^\perp) < \ldots < n+1-d_2(C^\perp) < n+1-d_1(C^\perp)$. Logo pelo teorema 2.1.11, se conhecermos $n+1-d_{n-k}(C^\perp)$ determinamos $d_i(C)$ para todo $i = 1, 2, \ldots, (n-d_{n-k}(C^\perp))$, a saber $d_i(C) = i$.*

2.2 Códigos de Goppa e distâncias generalizadas de Hamming

Nesta seção apresentaremos os códigos de Goppa. Iremos determinar alguns limitantes para as distâncias generalizadas de Hamming de tais códigos.

Definição 2.2.1 *Sejam $F/\mathbb{F}_q$ um corpo de funções algébricas de gênero g, $P_1, \ldots, P_n$ lugares de $F/\mathbb{F}_q$ dois a dois distintos e de grau 1, $D = P_1 + \cdots + P_n$ e G um divisor de $F/\mathbb{F}_q$ tal que supp $G \cap$ supp $D = \emptyset$. Então o código geométrico de Goppa denotado por $C_{\mathcal{L}}(D,G)$ associado aos divisores D e G é definido por*

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

Definição 2.2.2 *Sejam G e $D = P_1 + \cdots + P_n$ divisores tais que P_i são lugares de grau um, dois a dois distintos, com $i = 1, \ldots, n$; e supp $D \cap$ supp $G = \emptyset$. Então, definimos o código $C_\Omega(D,G) \subseteq \mathbb{F}_q^n$ por*

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

Teorema 2.2.3 *$C_{\mathcal{L}}(D,G)$ é um código $[n,k,d]$ com parâmetros*

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

Demonstração
Considere a aplicação $ev_D : \mathcal{L}(G) \longrightarrow C_{\mathcal{L}}(D,G)$ definida por

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

É claro que ev_D é $\mathbb{F}_q$-linear e sobrejetiva. Note ainda que

$$\ker(ev_D) = \{x \in \mathcal{L}(G);\ (x(P_1), \ldots, x(P_n)) = 0\} =$$

$$\{x \in \mathcal{L}(G);\ x(P_i) = 0, \text{ para } i = 1, \ldots, n\} = \{x \in \mathcal{L}(G);\ x \in P_i, \text{ para } i = 1, \ldots, n\} =$$

$$\{x \in \mathcal{L}(G);\ v_{P_i}(x) > 0 \text{ para } i = 1, \ldots, n\} = \{x \in F;\ v_{P_i}(x) > 0, \text{ para } i = 1, \ldots, n \text{ e } x \in \mathcal{L}(G)\} =$$

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

Pelo teorema do núcleo e imagem

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

Portanto $k = \dim G - \dim (G - D)$.
A afirmação $d \geq n - \deg G$ a ser mostrada considera a distância mínima d e, portanto, não faz sentido considerar $C_{\mathcal{L}}(D, G) = 0$. Suponhamos então $C_{\mathcal{L}}(D, G) \neq 0$.
Seja $x = (x(P_1), \ldots, x(P_n))) \in \mathcal{L}(G)$ com $w(ev_D(x)) = d$. Então

$$d = w((x(P_1), \ldots, x(P_n))) = |\{i;\ x(P_i) \neq 0\}| = n - |\{i;\ x(P_i) = 0\}| =$$

$$n - |\{i;\ v_{P_i}(x) > 0\}| = n - \text{ número de lugares no suporte de } D \text{ que são zeros de } x.$$

Ou seja, existem exatamente $n - d$ lugares $P_{i_1}, \ldots, P_{i_{n-d}}$ no suporte de D que são zeros de x, logo

$$0 \neq x \in \mathcal{L}(G - (P_{i_1}, \ldots, P_{i_{n-d}})).$$

Daí $\dim \mathcal{L}(G - (P_{i_1}, \ldots, P_{i_{n-d}})) \neq 0$. Pelo corolário 1.1.35, item (b),

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

Logo $d \geq n - \deg G$. □

Corolário 2.2.4 *Suponha no teorema anterior que o grau de G seja estritamente menor que n. Então a aplicação $ev_D : \mathcal{L}(G) \longrightarrow C_{\mathcal{L}}(D, G)$, definida na demonstração do teorema 2.2.3 é injetora e, mais ainda*

(i) $C_{\mathcal{L}}(D, G)$ é um código $[n, k, d]$ com

$$d \geq n - \deg G \text{ e } k = \dim (G) \geq \deg G + 1 - g$$

Portanto,

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

(ii) Se, supusermos ainda, $2g - 2 < \deg G < n$, então

$$k = \deg G + 1 - g.$$

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

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

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

Demonstração
Se $\deg G < n$, então $\deg(G - D) = \deg G - n < 0$. Logo, pelo corolário 1.1.35, item (b), $\mathcal{L}(G - D) = \{0\}$. Como, na demonstração do teorema 2.2.3, vimos que $\ker(ev_D) = \mathcal{L}(G - D)$, temos ev_D é injetora.

Pelo teorema 2.2.3, $C_{\mathcal{L}}(D, G)$ é um código $[n, k, d]$ com parâmetros $d \geq n - \deg G$ e $k = \dim(G) - \dim(G - D) = \dim(G)$. Pelo Teorema de Riemann-Roch, $\dim G \leq \deg G + 1 - g$. Logo $k = \dim G \leq \deg G + 1 - g$, o que prova o item (i).

Suponha agora $2g - 2 < \deg G < n$. Pela observação 1.2.25 temos que G é um divisor não especial e, logo, $\dim G = \deg G + 1 - g$. Segue que

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

O que prova o item (ii).

O item (iii) é óbvio. □

Definição 2.2.5 *O inteiro* $d^* := n - \deg G$ *é chamado de distância designada do código* $C_{\mathcal{L}}(D, G)$.

Proposição 2.2.6 *Suponhamos que* $\dim G > 0$ *e* $d^* = n - \deg G > 0$. *Então* $d^* = d$ *se, e somente se, existe um divisor* D' *com* $0 \leq D' \leq D$, $\deg D' = \deg G$ *e* $\dim (G - D') > 0$.

Demonstração
Assumindo que $d = d^* = n - \deg G > 0$, então existe um elemento $0 \neq x \in \mathcal{L}(G)$ tal que a palavra $(x(P_1), \ldots, x(P_n)) \in C_{\mathcal{L}}(D, G)$ tem precisamente $n - d = n - d^* = \deg G$ componentes zeros, a saber $x(P_{i_j})$, com $j = 1, \ldots, \deg G$. Defina

$$D' := \sum\nolimits_{j=1}^{\deg G} P_{i_j}.$$

Então $0 \leq D' \leq D$, $\deg D' = \deg G$ e $\dim (G - D') > 0$ (pois $0 \neq x \in \mathcal{L}(G - D')$).

Reciprocamente, suponha que exista um divisor D' satisfazendo as propriedades acima. Como $\dim (G - D') > 0$, então existe $0 \neq y \in \mathcal{L}(G - D')$. Como $\deg D' = \deg G$ e $0 \leq D' \leq D$, temos que $d \leq w((y(P_1), \ldots, y(P_n))) = n - \deg G = d^*$. Pelo teorema 2.2.3, $d \geq n - \deg G = d^*$, logo temos que $d^* = d$. □

Lema 2.2.7 *Sejam* P *um lugar de grau um e* ω *uma diferencial de Weil com* $v_P(\omega) \geq -1$. *Então*

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

Demonstração
Como estamos considerando $v_P(\omega)$, está implícito que $\omega \neq 0$. Pela proposição 1.2.31,

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

que nos garante

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

Suponha que $\omega_P(1) = 0$ e seja $x \in F$ com $v_P(x) \geq 0$. Como deg $P = 1$, podemos escrever $x = a + y$ com $a \in \mathbb{F}_q$ e $v_P(y) \geq 1$. Então, como $v_P(\omega) \geq -1$ e $v_P(y) \geq 1$, temos que $\omega_P(y) = 0$. Logo

$$\omega_P(x) = \omega_P(a) + \omega_P(y) = a\omega_P(1) + 0 = 0.$$

Reciprocamente, suponhamos $v_P(\omega) \geq 0$. Então existe $0 \leq r \in \mathbb{Z}$, tal que $\omega_P(x) = 0$ para todo $x \in F$ com $v_P(x) \geq -r$. Como $v_P(1) = 0 \geq -r$, temos que $\omega_P(1) = 0$. □

Teorema 2.2.8 $C_\Omega(D, G)$ *é um código* $[n, k', d']$ *com parâmetros*

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

Demonstração
Seja $P \in \mathbb{P}_F$ um lugar de grau um e ω uma diferencial de Weil com $v_P(\omega) \geq -1$. Pelo lema 2.2.7,

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

Considere a aplicação $\varrho_D : \Omega_F(G - D) \longrightarrow C_\Omega(D, G)$ tal que $\varrho_D(\omega) = (\omega_{P_1}(1), \ldots, \omega_{P_n}(1))$. Temos que ϱ_D é sobrejetiva. Note que

$$\varrho_D(\omega) = 0 \Leftrightarrow \omega_{P_i}(1) = 0, \forall i = 1, \ldots, n \Leftrightarrow v_{P_i}(\omega) \geq 0, \forall i = 1, \ldots, n \Leftrightarrow \omega \in \Omega_F(G).$$

Logo $\ker \varrho_D = \Omega_F(G)$. Pelo teorema do núcleo e imagem

$$\dim \Omega(G-D) = \dim \ker \varrho_D + \dim C_\Omega(D,G),$$

ou seja,

$$k' = \dim \Omega_F(G-D) - \dim \Omega_G = i(G-D) - i(G).$$

Seja $\varrho_D(\omega) \in C_\Omega(D,G)$ uma palavra de peso $m > 0$. Então $\omega_{P_i}(1) = 0$ para certos índices $i = i_1, \ldots, i_{n-m}$, logo

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

Como $\Omega_F(A) \neq 0$ implica que $\deg A \leq 2g-2$ (de fato, pelo teorema 1.2.12, $\dim(W-A) \neq 0$ com W divisor canônico; assim, pelo teorema 1.2.13, $\dim A \neq \deg A + g - 1$ e, por fim, pelo teorema 1.2.15, $\deg A < 2g-1$, ou ainda, $\deg A \leq 2g-2$), obtemos

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

Assim, $m \geq \deg G - (2g-2)$. Como m foi tomado arbitrário, então a distância mínima d' de $C_\Omega(D,G)$ satisfaz a desigualdade $d' \geq \deg G - (2g-2)$. □

Corolário 2.2.9 *No teorema anterior, se adicionarmos a hipótese de que* $\deg G > 2g-2$, *teremos*

$$k' = i(G-D) \geq n + g - 1 - \deg G.$$

Mais ainda, se $2g - 2 < \deg G < n$, *então*

$$k' = n + g - 1 - \deg G.$$

Demonstração
Suponha que $\deg G > 2g-2$, então, pelo teorema 1.2.15, $i(G) = 0$. Assim, pelo teorema 2.2.8 e pelo teorema de Riemann-Roch temos

$$k' = i(G-D) = \dim(G-D) - \deg(G-D) - 1 + g = \dim(G-D) + n + g - 1 - \deg G \geq n + g - 1 - \deg G.$$

Suponha ainda que $2g - 2 < \deg G < n$. Como $\deg(G-D) = \deg G - n < 0$, pelo corolário 1.1.35, item (b), teremos que $\dim(G-D) = 0$ e, daí,

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

□

Teorema 2.2.10 *Dados os códigos* $C_\Omega(D,G)$ *e* $C_\mathcal{L}(D,G)$, *então*

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

Demonstração
Ver [7], Teorema II.2.8. □

Lema 2.2.11 *Existe uma diferencial de Weil* η *tal que*

$$v_P(\eta) = -1 \text{ e } \eta_{P_i}(1) = 1, \text{ para } i = 1, \ldots, n.$$

Demonstração
Ver [7], Lema II.2.9. □

Proposição 2.2.12 *Seja η uma diferencial de Weil tal que $v_{P_i}(\eta) = -1$ e $\eta_{P_i}(1) = 1$ para $i = 1, \ldots, n$. Então*

$$C_{\mathcal{L}}(D,G)^{\perp} = C_{\Omega}(D,G) = C_{\mathcal{L}}(D,H), \text{ com } H := D - G + (\eta).$$

Demonstração
Ver [7], Lema II.2.10. □

Corolário 2.2.13 *Se $\deg G > 2g - 2$, o código $C_{\mathcal{L}}(D,G)$ satisfaz*

$$d_r(C_{\mathcal{L}}(D,G)) = n - k + r, \forall r, g + 1 \leq r \leq k,$$

onde k é a dimensão de $C_{\mathcal{L}}(D,G)$.

Demonstração
Como $C_{\mathcal{L}}(D,G)^{\perp} = C_{\mathcal{L}}(D,H)$ com $H := D - G + (\eta)$ onde (η) é uma diferencial de F/K com $v_P(\eta) = -1$ e $\eta_P(1) = 1$ para todo $P \in supp(D)$(ver proposição 2.2.12), pelo teorema 2.2.3 e pelo corolário 1.2.14, teremos

$$d_1(C_{\mathcal{L}}(D,G)^{\perp}) = d_1(C_{\mathcal{L}}(D,H)) \geq n - \deg H = \deg G - 2g + 2.$$

Pelo teorema 2.1.11 temos

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

para todo i com $0 \leq i \leq \deg G - 2g$. Por hipótese $\deg G > 2g - 2$, assim $k = \dim G - \dim (G - D) \leq \dim G = \deg G + 1 - g$ (ver teoremas 1.2.15 e 2.2.3). Daí $k - (\deg G - 2g) \leq g + 1$. □

Observação 2.2.14 *Se $0 \leq \deg G \leq 2g - 2$, teremos*

$$k \leq \dim G \leq 1 + \frac{1}{2} \deg G \leq g.$$

De fato, a primeira desigualdade é conseqüência imediata do teorema 2.2.3 e a segunda desigualdade vem do teorema 1.2.28.

Definição 2.2.15 *Seja C um código $[n,k]$. Dizemos que C tem l-ésimo posto MDS se sua hierarquia de pesos satisfaz*

$$d_r(C) = n - k + r, \forall r, l \leq r \leq k.$$

Lema 2.2.16 *Códigos MDS têm primeiro posto MDS.*

Demonstração
Seja C um código $[n,k,d]$ MDS, então

$$d_1(C) = d = n + 1 - k.$$

Pelos corolários 2.1.8 e 2.1.9

$$n + 1 - k + t = d_1(C) + t \leq d_{1+t}(C) \leq n - k + 1 + t, \forall t = 0, \ldots, k - 1.$$

Logo $d_{1+t}(C) = n - k + (t + 1)$ para todo $t = 0, \ldots, k - 1$. □

Do corolário 2.2.13 tem que se $C_{\mathcal{L}}(D,G)$ é um código de Goppa com $\deg G > 2g - 2$, então $C_{\mathcal{L}}(D,G)$ tem $(g + 1)$-ésimo posto MDS.

Definição 2.2.17 *Sejam F/K um corpo de funções algébricas com corpo constante K e $\mathcal{D}_F$ o conjunto de todos os divisores de F/K. Dado um inteiro $r \geq 1$, definimos a r-ésima gonalidade por*

$$\gamma_r := \min\{\deg A;\ A \in \mathcal{D}_F \ e\ \dim A \geq r\}.$$

A seqüência $(\gamma_r)_{r\geq 1}$ é chamada de seqüência de gonalidades de F/K.

Observação 2.2.18 *O inteiro γ_2 é a gonalidade usual, isto é, $\gamma_2 = \min\{[F : K(u)];\ u \in F\}$.*

Esta observação sobre γ_2 pode ser encontrada em [5].

Lema 2.2.19 *Com a notação da definição* 2.2.17*, temos que $\gamma_1 = 0$.*

Demonstração
Pelo corolário 1.1.35, item (b), dado um divisor $A \in \mathcal{D}_F$, se $\dim A \geq 1$, então $\deg A \geq 0$. Pelo lema 1.1.30, item (iii), o divisor 0 tem dimensão igual a um e grau zero, logo $\gamma_1 = 0$. □

Lema 2.2.20 *Seja p_r a r-ésima ordem de pólo de um lugar racional Q (ver definição* 1.2.21*). Então $\gamma_r \leq p_r$, para todo $r \geq 1$.*

Demonstração
Sabemos que $\mathcal{L}(0) = \mathcal{L}(p_1Q) \subsetneq \mathcal{L}(p_2Q) \subsetneq \ldots \subsetneq \mathcal{L}((p_r-1)Q) \subsetneq \mathcal{L}(p_rQ)$. Assim $\dim \mathcal{L}(p_rQ) \geq r$ e $\deg p_rQ = p_r$. Logo $\gamma_r \leq p_r$. □

Proposição 2.2.21 *Seja F/K um corpo de funções algébricas de gênero g. Suponha que F/K tem um lugar de grau um. Então:*

(a) $0 = \gamma_1 < \gamma_2 < \cdots < \gamma_r < \gamma_{r+1} < \cdots$, *para todo* $r \geq 1$.

(b) $\gamma_r = r + g - 1$ *para todo* r *com* $r > g$.

(c) $\gamma_g = 2g - 2$ *e* $\gamma_r \geq 2(r-1)$ *para todo* r *com* $1 \leq r \leq g$.

Demonstração

(a) Seja A um divisor tal que $\deg A = \gamma_r$ e $\dim A \geq r$. Basta provarmos que existe um divisor A' com $\deg A' < \gamma_r$ e $\dim A' \geq r - 1$. Seja $A' := A - P$, onde $\deg P = 1$. Temos que $\dim A \leq \dim A' + \deg P = \dim A' + 1$. De fato, considere a aplicação

$$\varphi = \begin{cases} \mathcal{L}(A' + P) \longrightarrow F_P = K, \\ h \longmapsto ht^{v_P(A')+1}(P) \end{cases}$$

onde t é primo para P. É claro que φ é uma aplicação K-linear.

Mostremos que φ está bem definida:

$$v_P(ht^{v_P(A')+1}) = v_P(h) + v_P(A') + 1 \geq -v_P(A') - 1 + v_P(A') + 1 = 0.$$

Logo $ht^{v_P(A')+1}$ está em $\mathcal{O}_P$ e tem sentido tomar a classe $ht^{v_P(A')+1}(P)$ que é um elemento de K.

Temos que

$$\varphi(h) = 0 \Leftrightarrow v_P(ht^{v_P(A')+1}) = v_P(h) + v_P(A') + 1 > 0 \Leftrightarrow v_P(h) \geq -v_P(A'),$$

ou seja, $\ker \varphi = \mathcal{L}(A)$. Pelo teorema do núcleo e imagem,

$$\dim (A' + P) - \dim A' = \dim Im\ \varphi \leq \deg P = 1.$$

Logo, $\dim A' \geq \dim A - 1 \geq r - 1$.

(b) Seja A um divisor de F/K com $\deg A = r + g - 1 > 2g - 1$. Pelo teorema 1.2.15, temos que $\dim A = \deg A + 1 - g = r$, logo temos que $\gamma_r \leq r + g - 1$. Agora considere um divisor B de grau menor do que $r + g - 1$. Então existe um divisor B' tal que $B \leq B'$ e $\deg B' = r + g - 2 > 2g - 2$. Então $\dim B \leq \dim B'$ e $\dim B' = \deg B' + 1 - g = r - 1$, logo $\gamma_r \geq r + g - 1$.

(c) Considere um divisor canônico W de F/K. Então $\deg W = 2g - 2$ e $\dim W = g$, logo temos que $\gamma_g \leq 2g - 2$, pela definição de γ_g. Temos por (a) que $0 \leq \gamma_r \leq 2g - 2$ para todo r com $1 \leq r \leq g$. Seja A um divisor tal que $\deg A = \gamma_r$ e $\dim A \geq r$. Pelo teorema de Clifford temos

$$\dim A \leq 1 + (1/2)\deg A = 1 + \gamma_r/2.$$

Logo $r \leq 1 + \gamma_r/2$, isto é $\gamma_r \geq 2(r-1)$, onde $1 \leq r \leq g$. Para $r = g$, $\gamma_g \geq 2g - 2$. Segue que $\gamma_g = 2g - 2$.

□

Teorema 2.2.22 *Seja $C_{\mathcal{L}}(D, G)$ um código de Goppa, então*

$$d_r(C_{\mathcal{L}}(D, G)) \geq n - \deg G + \gamma_r, \forall 1 \leq r \leq k,$$

onde k é a dimensão de $C_{\mathcal{L}}(D, G)$.

Demonstração
Para simplificar a notação notaremos $d_r := d_r(C_{\mathcal{L}}(D, G))$. Sejam $D = \sum_{i=1}^{n} P_i$, onde $P_1, \ldots, P_n$ são lugares racionais de $F/\mathbb{F}_q$ e V_r um subcódigo de $C_{\mathcal{L}}(D, G)$ com suporte de tamanho $|\chi(V_r)| = d_r$ e com dimensão r. Seja ainda $\varphi : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n$ definida da forma $\varphi(f) = (f(P_1), \ldots, f(P_n))$. Podemos assumir que V_r é gerado por r palavras-código $\varphi(f_1), \ldots, \varphi(f_r)$, onde $f_1, \ldots, f_r \in \mathcal{L}(G)$ são linearmente independentes sobre $\mathbb{F}_q$ (a independência linear de $f_1, \ldots, f_r$ vem do fato de $\{\varphi(f_1), \ldots, \varphi(f_r)\}$ ser linearmente independente e de φ ser linear). Então, dizer que $|\chi(V_r)| = d_r$, é equivalente a dizer que todas as palavras-código da base $\{\varphi(f_1), \ldots, \varphi(f_r)\}$ de V_r compartilham exatamente $n - d_r$ posições distintas onde, nessas posições, elas são nulas, sem perda de generalidade, suponhamos que sejam as primeiras $n - d_r$ entradas. Esta afirmação pode ser reescrita em termos de divisores da seguinte forma: se $1 \leq i \leq r$, então

$$(f_i) = A + B_i - G,$$

onde $0 \leq A \leq D$, $\deg A = n - d_r$ e $B_i \geq 0$, para $i = 1, \ldots, r$.

De fato, para todo i com $1 \leq i \leq r$, $\varphi(f_i)$ se anula nas $(n - d_r)$-ésimas primeiras coordenadas, ou seja, se $1 \leq i \leq r$ e $1 \leq j \leq n - d_r$, então $v_{P_j}(f_i) = 1 + b^i_{P_j}$, com $b^i_{P_j} \geq 0$. Como $f_i \in \mathcal{L}(G)$, $1 \leq i \leq r$, temos que $v_P(f_i) = -v_P(G) + b^i_P$, com $P \geq 0$, $\forall P \in \mathbb{P}_F \setminus \{P_1, \ldots, P_{n-d_r}\}$. Defina

$$B_i := \sum_{P \in \mathbb{P}_F} b^i_P P$$

e

$$A := \sum_{P \in \{P_1, \ldots, P_{n-d_r}\}} P.$$

Note que o conjunto $\{f_1/f_1, f_2/f_1, \ldots, f_r/f_1\}$ é l.i. e $f_1/f_1, f_2/f_1, \ldots, f_r/f_1 \in \mathcal{L}(B_1)$, uma vez que $v_P(f_i/f_1) = v_P(f_i) - v_P(f_1) = v_P(B_i) - v_P(B_1) \geq -v_P(B_1)$. Logo $\deg B_1 \geq \gamma_r$, pela definição de γ_r. O fato de $\deg B_1 = \deg G - \deg A$ completa a demonstração. □

Note que, para o caso da distância mínima, como $\gamma_1 = 0$, temos que

$$d = d_1(C_{\mathcal{L}}(D, G)) \geq n - \deg G,$$

o que está de acordo com o teorema 2.2.3.

Observação 2.2.23 *O teorema* 2.2.22 *pode ser usado para dar uma nova prova do corolário* 2.2.13*, com a hipótese adicional de que* $\deg G < n$*. De fato, se* $2g-2 < \deg G < n = \deg D$*, então,* $k = \dim G - \dim(G-D) = \dim G = \deg G + 1 - g$ *e*

$$d_r(C_{\mathcal{L}}(D,G)) \geq n - \deg G + \gamma_r$$

$$= n - (\deg G + 1 - g) + r, \ (\textit{proposição } 2.2.21, \ \textit{item } (b))$$

$$= n - k + r$$

para todo r *com* $g+1 \geq r \geq k$*. Usando a cota de Singleton Generalizada (ver Corolário* 2.1.9*), temos que* $d_r(C_{\mathcal{L}}(D,G)) \leq n-k+r$*. Logo, se* $2g-2 < \deg G < n$*, temos*

$$d_r(C_{\mathcal{L}}(D,G)) = n-k+r$$

para todo r *com* $g+1 \leq r \leq k$*.*

2.3 Códigos Hermitianos e distâncias generalizadas de Hamming

Essa seção é baseada, em parte, na referência [9].

Seja $K = GF(q^2)$ onde q é potência de algum número primo p e $F = K(x,y)$ o corpo de funções definido por

$$F = K(x,y), \text{ com } y^q + y = x^s \text{ e } s|q+1.$$

Se $s = q+1$, então F/K é chamado de corpo de funções Hermitiano sobre K. Se $s < q+1$, então F/K é isomorfo a um subcorpo do corpo de funções Hermitiano e , então, podemos nos referir a F/K como um subcorpo de um corpo de funções Hermitiano. Em ambos os casos ($s = q+1$ e $s < q+1$), o gênero do corpo de funções F/K é dado por

$$g = \frac{(q-1)(s-1)}{2} \text{ (ver [7] proposição VI.4.1, } (e))$$

e podemos mostrar que o divisor da diferencial dx é dado por

$$(dx) = (2g-2)Q_\infty \text{ (ver [7] proposição VI.4.1, } (f)),$$

onde Q_∞ é o pólo comum de x e y.

Examinemos agora os lugares de grau um do corpo F/K. O lugar Q_∞ é um deles. Seja $\alpha \in K$. O polinômio $p(T) = T^q + T - \alpha^s$ tem raiz em K se, e somente se, $\alpha^s \in GF(q)$. Se α é tal que $\alpha^s \in GF(q)$, então existem exatamente q raízes distintas de $p(T)$ em K. Seja U^* o subgrupo de ordem $(q-1)s$ do grupo multiplicativo K^* e seja $U = U^* \cup \{0\}$. Então, para $\alpha \in K$, $\alpha^s \in GF(q)$ se, e somente se, $\alpha \in U$. Logo o número de lugares de grau um em F/K é

$$N = q|U| + 1 = q(1 + (q-1)s) + 1.$$

Como $N = 1 + q^2 + 2gq = 1 + q^2 + q(q-1)(s-1)$, F/K satisfaz a cota de Hasse-Weil e, logo, é um corpo de função maximal (ver [7] exemplo VI.4.2 e proposição VI.4.1, (i)).

Nós definimos $P_{\alpha,\beta}$ como sendo o zero comum de $x-\alpha$ e $y-\beta$ onde $\alpha \in U$ e $\beta \in K$ são tais que $\beta^q + \beta = \alpha^s$. De [7] vem que para todo $\alpha, \beta \in K$, os divisores $x-\alpha$ e $y-\beta$ são:

$$(x-\alpha) = \begin{cases} \sum_{\beta^q+\beta=\alpha^s}^{\beta \in K} P_{\alpha,\beta} - qQ_\infty, \text{ se } \alpha \in U, \\ R_\alpha - qQ\infty, \text{ se } \alpha \in K \setminus U, \end{cases}$$

onde R_α é um divisor de grau q em F/K, dependendo de α, cujo suporte não contém quaisquer lugares de grau um e

$$(y-\beta) = \begin{cases} \sum_{\alpha^s=\beta^q+\beta}^{\alpha\in K} P_{\alpha,\beta} - sQ_\infty, \text{ se } \beta^q+\beta \neq 0, \\ sP_{0,\beta} - sQ_\infty, \text{ se } \beta^q+\beta = 0, \end{cases}$$

Segue também de [7] proposição VI.4.1, (i).
Para cada inteiro $m \geq 0$, considere o conjunto

$$\mathcal{L}(mQ_\infty) = \{f \in F;\ f = 0 \text{ ou } (f) \geq -mQ_\infty\}.$$

Denotaremos por B_m ao conjunto

$$B_m := \{x^i y^j;\ i \geq 0,\ 0 \leq j \leq q-1 \text{ e } iq+js \leq m\}.$$

O conjunto B_m assim definido é uma base para $\mathcal{L}(mQ_\infty)$ (ver [7] proposição VI.4.1, (h)).
Defina t através de $s.t := q+1$. Daqui para frente, assumiremos que

$$G := mQ_\infty \text{ e } D := \sum_{\alpha\in U} \sum_{\substack{\beta\in K, \\ \beta^q+\beta=\alpha^s}} P_{\alpha,\beta}.$$

Para simplificar a notação, considere

$$C_m := C_{\mathcal{L}}(D, mQ_\infty).$$

Seja $d_r(C_m)$ o r-ésimo peso generalizado de Hamming do código C_m.

Proposição 2.3.1 *(a) O código C_m é um código linear de comprimento $n = q((q-1)s+1)$;*

(b) Se $m_1 \leq m_2$, então $C_{m_1} \subseteq C_{m_2}$;

(c) Se $m_1 \leq m_2$, então $d_r(C_{m_1}) \geq d_r(C_{m_2})$.

Demonstração

(a) Todos os lugares $P_{\alpha,\beta}$ possuem grau um. Então basta contar os lugares do suporte de D. Note que $|U| = (q-1)s+1$ e, para cada $\alpha \in U$, o polinômio $\beta^q+\beta = \alpha^s$ possui q raízes distintas. Portando $n = \deg D = q((q-1)s+1)$.

(b) Se $m_1 \leq m_2$, temos $m_1Q_\infty \leq m_2Q_\infty$. Pelo lema 1.1.31, temos que $\mathcal{L}(m_1Q_\infty) \subseteq \mathcal{L}(m_2Q_\infty)$. Assim, dado $h \in C_{m_1}$, então $h = (f(P_1), \ldots, f(P_n))$, onde $f \in \mathcal{L}(m_1Q_\infty)$, logo $h = (f(P_1), \ldots, f(P_n))$, com $f \in \mathcal{L}(m_2Q_\infty)$, pois $\mathcal{L}(m_1Q_\infty) \subseteq \mathcal{L}(m_2Q_\infty)$. Assim $C_{m_1} \subseteq C_{m_2}$.

(c) Seja D subcódigo de C_{m_2} com $\dim D = r$. Como $C_{m_1} \subseteq C_{m_2}$, então, também, D é subcódigo de C_{m_2} com $\dim D = r$. Assim $\{|\chi(D)|; D \text{ é subcódigo de } C_{m_1} \text{ com } \dim D = r\}$ é subconjunto de $\{|\chi(D)|; D \text{ é subcódigo de } C_{m_2} \text{ com } \dim D = r\}$. Portanto, $d_r(C_{m_1}) \geq d_r(C_{m_2})$.

□

Observação 2.3.2 *Considere a função u definida por $u := \prod_{\alpha\in U}(x-\alpha)$. Então $(u) = D - nQ_\infty$ e*

$$u = x.\prod_{\alpha\in U^*}(x-\alpha) = x(x^{(q-1)s}-1) = x^{1+(q-1)s} - x.$$

Lema 2.3.3 *Seja $\omega := dx/u$. Então temos*

$$(\omega) = (dx) - (u) = (n + 2g - 2)Q_\infty - D.$$

Demonstração
Temos que $(dx) = (2g - 2)Q_\infty$ (Ver [7], Proposição VI.4.1) e pela observação 1.3.28, temos

$$(\omega) = ((\frac{1}{u})dx) = (dx) + (\frac{1}{u}) = (dx) - (u) = (2g - 2)Q_\infty - D + nQ_\infty = (n + 2g - 2)Q_\infty - D.$$

□

Corolário 2.3.4 *Seja $\omega := dx/u$. Então $v_P(\omega) = -1$ para todo lugar $P \in supp\ (D)$, onde $v_P(.)$ é a valorização discreta de F/K em P.*

O corolário 2.3.4 segue direto do lema acima.

Definição 2.3.5 *Para todo código linear C de comprimento n sobre K e para toda n-upla $\underline{a} := (a_1, \ldots, a_n)$, onde $0 \neq a_i \in K$ para todo i, definimos*

$$\underline{a}.C := \{(a_1c_1, \ldots, a_nc_n); (c_1, \ldots, c_n) \in C\}.$$

Proposição 2.3.6 *Para todo inteiro $m \geq 0$, os códigos C_m e $\underline{a}.C_{n+2g-2-m}$ são duais um do outro, onde $\underline{a} := (res_{P_1}\ \omega, \ldots, res_{P_n}\ \omega)$ e $res_P\ \omega$ é o resíduo de ω em P.*

Demonstração
Ver [8], Teorema 2.5. □

Lema 2.3.7 *(a) A diferencial $\eta := du/u$ satisfaz $v_P(\eta) = -1$ e $res_P\ \eta = 1$ para todo $P \in supp(D)$. Se $s \equiv 1\ mod\ p$, então $du = -dx$ e $(\eta) = (n + 2g - 2)Q_\infty - D$. Logo, C_m e $C_{n+2g-2-m}$ são duais um do outro neste caso.*

(b) A condição $s \equiv 1\ mod\ P$ vale para $p = 2$, pois s e q são relativamente primos. Esta condição vale para corpos Hermitianos, pois $s = q + 1$.

A demonstração da letra (a) pode ser encontrada em [2] e a demonstração da letra (b) pode ser encontrada em [6].

Proposição 2.3.8 *Um inteiro $l \geq 0$ é uma de lacuna de Q_∞ se não existir função $f \in F$ tal que $f \in \mathcal{L}(lQ_\infty) \setminus \mathcal{L}((l-1)Q_\infty)$. Caso contrário, l é uma ordem de pólo de Q_∞.*

Demonstração
Basta mostrar que tal afirmação é equivalente à definição 1.2.21. De fato

$$f \in \mathcal{L}(nQ_\infty) \setminus \mathcal{L}((n-1)Q_\infty) \Leftrightarrow$$

$$(f) \geq -nQ_\infty \text{ e } (f) \notin \mathcal{L}((n-1)Q_\infty) \Leftrightarrow$$

$$v_P(f) \geq 0, \forall P \in \mathbb{P}_F \setminus \{Q_\infty\} \text{ e } v_{Q_\infty}(f) = -n \Leftrightarrow$$

$$(f)_\infty = nQ_\infty.$$

□

Proposição 2.3.9 *Seja S o conjunto de todas as lacunas de Q_∞. Temos que*

$$S = S_1 \cup S_2,$$

onde

$$S_1 = \{iq + js + l;\ 0 \leq i \leq s-2, 0 \leq j \leq t-2, i+1 \leq l \leq s-1\}$$

e

$$S_2 = \{iq + (t-1)s + l;\ 0 \leq i \leq s-3, i+1 \leq l \leq s-2\}.$$

Demonstração
No que se segue, dados $a, b \in \mathbb{Z}$ usamos a notação $[a, b]$ para indicar o conjunto $\{n \in \mathbb{Z} \mid a \leq n \leq b\}$.

Seja $\mathbf{H} = \{iq+js \mid 0 \leq i, 0 \leq j \leq q-1\}$ o semigrupo das ordens de pólo em Q_∞. Queremos determinar o conjunto $\mathbb{N}_0 \setminus \mathbf{H}$. Quando $s = 1$ o corpo de funções F é racional, de modo que $\mathbb{N}_0 \setminus \mathbf{H} = \emptyset$. Vamos assumir então que $s \geq 2$.

Do teorema de Riemann-Roch temos que $\{n \in \mathbb{N} \mid n \geq 2g\} \subset \mathbf{H}$. Sabemos que $2g = (q-1)(s-1) = (s-1)q-(s-1) = (s-2)q+(q+1-s)$ e de $(s-2)q+(q-1)s > (s-2)q+(q+1-s)$ (e mais ainda, $(s-1+i')q+j' > (s-2)q+(q+1-s)$ sempre que $s', j' \geq 0$) vem que

$$\mathbf{H} = \{iq + js \mid 0 \leq i \leq s-2, 0 \leq j \leq q-1\} \cup \{n \in \mathbb{N} \mid n \geq 2g\}.$$

Observe que $q - 1 = q + 1 - 2 = st - 2 = (s-1)t + t - 2$, logo, para $i \in [0, s-2]$ vale

$$\{iq + js \mid 0 \leq j \leq q-1\} = \left(\bigcup_{k=0}^{s-2} \{iq + (kt+\ell)s \mid \ell \in [0, t-1]\}\right) \cup \{iq + ((s-1)t+\ell)s \mid \ell \in [0, t-2]\}.$$

Usando que $(kt+\ell)s = k(q+1) + \ell s = kq + k + \ell s$ para todo $k \in [0, s-1]$ temos, para $i \in [0, s-2]$, que

$$\left(\bigcup_{k=0}^{s-2} \{iq + (kt+\ell)s \mid \ell \in [0, t-1]\}\right) \cup \{iq + ((s-1)t+\ell)s \mid \ell \in [0, t-2]\} =$$
$$\left(\bigcup_{k=0}^{s-2} \{(i+k)q + k + \ell s \mid \ell \in [0, t-1]\}\right) \cup \{(i+s-1)q + s - 1 + \ell s \mid \ell \in [0, t-2]\}.$$

Observe que $k + (t-1)s = k + q + 1 - s < q$ para todo $k \in [0, s-2]$ e da mesma forma $s - 1 + (t-2)s = s - 2 + q + 1 - 2s = q - 1 - s < q$, ou seja, os elementos nos conjuntos do lado direito da última igualdade acima estão escritos na forma $uq+r$, com $r \in [0, q-1]$. Lembrando que $2g = (s-2)q+(q+1-s)$ e que $\{n \in \mathbb{N} \mid n \geq 2g\} \subset \mathbf{H}$, nos interessa determinar o conjunto $\{uq + r \in \mathbf{H} \mid \text{ com } r \in [0, q-1] \text{ e } uq + r < (s-2)q + (q+1-s)\}$. De $(s-1)q + s - 1 > (s-2)q + (q+1-s)$ temos que $\{(i+s-1)q + s - 1 + \ell s \mid \ell \in [0, t-2]\} \subset \{n \in \mathbb{N} \mid n \geq 2g\}$; assim, do que já fizemos, vem que

$$\mathbf{H} = \left(\bigcup_{i=0}^{s-2} \{iq + js \mid 0 \leq j \leq q-1\}\right) \cup \{n \in \mathbb{N} \mid n \geq 2g\} =$$
$$\left(\bigcup_{i=0}^{s-2} \bigcup_{k=0}^{s-2} \{(i+k)q + k + \ell s \mid \ell \in [0, t-1]\}\right) \cup \{n \in \mathbb{N} \mid n \geq 2g\}$$

Chamando $u := i + k$ podemos escrever esse conjunto da seguinte forma

$$\left(\bigcup_{u=0}^{s-2}\bigcup_{k=0}^{u}\bigcup_{\ell=0}^{t-1} uq + k + \ell s\right) \cup \{n \in \mathbb{N} \mid n \geq 2g\}.$$

Agora é fácil verificar que

$$\mathbb{N}_0 \setminus \mathbf{H} = \left(\bigcup_{u=0}^{s-2}\bigcup_{\ell=0}^{t-2}[uq + \ell s + u + 1, uq + \ell s + s - 1]\right) \cup \left(\bigcup_{u=0}^{s-3}[uq + (t-1)s + u + 1, uq + (t-1)s + s - 2]\right).$$

□

Proposição 2.3.10 *(a) Se $t = 1$ (i.e., $s = q + 1$), então F/K é o corpo de funções Hermitiano e*

$$S = \{iq + l;\ 0 \leq i \leq q - 2, i + 1 \leq l \leq q - 1\}.$$

Em particular, o comprimento n do código C_m é $n = q^3$.

(b) Se $t = q+1$ (i.e., $s = 1$), então F/K é um corpo de funções racionais, pois $F = K(x, y) = K(y)$. Neste caso, Q_∞ não tem lacunas e $n = q^2$.

(c) No caso Hermitiano as ordens de pólo menores que $2g$ são $\bigcup_{i=0}^{q-1}\{iq + j; j = 0, \ldots, i\}$.

Demonstração

(a) Note que para $t = 1$, S_1 é vazio. Logo, substituindo $t = 1$ e $s = q + 1$ em S_2, temos a expressão de S.

(b) Se $t = q + 1$, então $s = 1$ e, como temos $x = y + y^q$, segue que $K(x, y) = K(Y)$. Daí $S_1 = S_2 = \emptyset$. Portanto $S = \emptyset$.

(c) No caso Hermitiano, por (a), temos

$$S = \{iq + l; 0 \leq i \leq q - 2 \text{ e } i + 1 \leq l \leq q - 1\}.$$

Se $i = 0$, então $iq + l = l \leq q - 1 < q < q + 1$.

Se $i \geq 1$, então $l \geq 2$ e $iq + l = q + l \geq q + 2 > q + 1 > q$.

Portanto q e $q + 1$ não podem ser lacunas, logo são ordens de pólo de Q_∞. Pela observação 1.2.22, o conjunto de ordens de pólo de Q_∞ forma um sub-semigrupo e, pelo teorema 1.2.23, $p_1 = 0$ é a menor ordem de pólo de Q_∞ e a todas as lacunas são menores ou iguais a $2g - 1 = 2[(q-1)(s-1)/2] - 1 = q^2 - q - 1$. Com estas informações, podemos obter ordens de pólo apenas somando as que já possuímos, a saber 0, q, $q + 1$ e n, tal que $n \geq 2g$. Logo o semigrupo é composto pelos inteiros

0

$q, q + 1$

$2q, 2q+1, 2q+2$

$3q, 3q+1, 3q+2, 3q+3$

$4q, 4q+1, 4q+2, 4q+3, 4q+4$

$\vdots$

$(q-2)q, (q-2)q+1, \ldots, 2g-2 = q^2-q-2 = (q-2)q+(q-2)$

$(q-1)q = 2g > 2g-1, (q-1)q+1, \ldots, (q-1)q+(q-1), (q-1)q, (q-1)q+1, (q-1)q+2, \ldots$

Observe que ao passarmos da i-ésima linha para a $(i+1)$-ésima, saltamos $iq-(i-1)q-(i-1)-1 = q-i$ inteiros. Logo da primeira linha até a $(q-1)$-ésima, saltamos

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

Pelo teorema das lacunas de Weiertrass não há mais lacunas a partir da q-ésima linha.

□

Proposição 2.3.11 *Sejam p_r a r-ésima ordem de pólo de Q_∞ e $\{\gamma_r; r \geq 1\}$ a seqüência de gonalidade do corpo de funções F/K definido por $y^q + y = x^s$, onde s divide $q+1$. Então:*

(a) $\gamma_1 = p_1 = 0$;

(b) $\gamma_2 = p_2 = \begin{cases} q \text{ se } s = q+1 \\ s \text{ se } s < q+1. \end{cases}$

(c) $\gamma_3 = p_3 = q+1$, *se* $s = q+1$.

Demonstração

(a) Segue direto do Teorema das Lacunas de Weiertrass e da proposição 2.2.21.

(b) Seja N o número de lugares de grau um de F/K. Seja $u \in F/K$ tal que $\gamma_2 = [F : K(u)]$. Seja ainda $P \in \mathbb{P}_{K(u)}$ um lugar de grau um, $P'_1, \ldots, P'_r$ todos os lugares de $\mathbb{P}_F$ tais que $P'_i|P$, $e_i := e(P'_i)$ e $f_i := f(P'_i|P) = [F_{P'_i} : F_P]$. Pelo teorema 1.4.7

$$\sum_{i=1}^{r} e_i f_i = \gamma_2.$$

Se $[F_{P'_i} : K] = 1$, então $[F_{P'_i} : F_P] = 1$, pois $K \subseteq F_P \subseteq F_{P'_i}$. Se $P'_{i_1}, \ldots, P'_{i_l}$ são lugares de grau um em $\mathbb{P}_F$, temos $l \leq \sum_{j=1}^{l} e_{i_j} = \sum_{j=1}^{l} e_{i_j} f_{i_j} \leq \sum_{i=1}^{r} e_i f_i = \gamma_2$. Logo, P tem no máximo γ_2 extensões de grau um em F/K. Note que se $Q \in \mathbb{P}_{K(u)}$ é um lugar tal que $\deg Q \geq 2$ e $Q' \in \mathbb{P}_F$ é tal que $Q'|Q$, então $[F_{Q'} : K] = [F_{Q'} : F_Q].[F_Q : K] \geq 2$. Assim nenhum outro lugar em $K(u)/K$ tem extensões de grau um em F/K. Logo $N \leq (q^2+1)\gamma_2$.

Consideremos primeiramente o caso Hermitiano ($s = q+1$). Se $\gamma_2 < q$, então temos que $N < q^3+1$, o que é absurdo. Logo $\gamma_2 \geq q$. Como $\gamma_2 = \min\{[F : K(u)];\ u \in F\}$ e $[F : K(x)] = q$ (ver [7], proposição VI.4,1 (a)), temos $\gamma_2 \leq q$. Logo $\gamma_2 = q$.

Suponhamos agora $s < q+1$. Se $s = 1$, então F/K é o corpo de funções racionais, tal caso é de simples verificação. Podemos supor que $s > 1$. Suponhamos que $\gamma_2 < s$. De $N \leq (q^2+1)\gamma_2$ temos

$$q + q(q-1)s < s(q^2+1) \Leftrightarrow q + q(q-1)s + 1 \leq s(q^2+1) \Leftrightarrow$$

$$q + 1 \leq qs + s,$$

o que é absurdo. Logo $\gamma_2 \geq s$. Como $\gamma_2 \leq [K(x,y) : K(y)] \leq \deg(T^s - (y^q + y)) = s$, onde $T^s - (y^q + y) \in K(y)[T]$, então $\gamma_2 = s$.

(c) Se $s = q+1$, então $\gamma_3 > \gamma_2 = q$ pela proposição 2.2.21 e $\gamma_3 \leq p_3 = q+1$ pela observação 2.2.20. Logo $\gamma_3 = p_3 = q+1$.

□

A dimensão do código C_m é facilmente determinada pela seqüência de lacunas dada pelo conjunto S. Seja

$$I(m) := \{l \leq m; l = iq + js, i \geq 0 \text{ e } 0 \leq j \leq q-1\}.$$

Dado um inteiro m, este pode ser expresso de maneira única na forma

$$m = iq + js + l,$$

com $i \geq 0, 0 \leq j \leq t-2$ e $0 \leq l \leq s-1$, ou

$$m = iq + (t-1)s + l,$$

com $i \geq 0$ e $0 \leq l \leq s-2$.

De fato, seja m um inteiro não negativo, afirmamos que existem únicos inteiros a, u e v tais que podemos escrever m da seguinte *forma especial*: ou $m = aq + us + v$, com $a \geq 0$, $0 \leq u \leq t-2$ e $0 \leq v \leq s-1$ ou $m = aq + (t-1)s + v$, com $a \geq 0$ e $0 \leq v \leq s-2$. De fato, fazendo a divisão euclidiana de m por q encontramos inteiros a e b tais que $m = aq + b$, com $a \geq 0$ e $0 \leq b \leq q-1$. Fazendo a divisão euclidiana de b por s encontramos inteiros u e v tais que $m = aq + us + v$, com $0 \leq u$ e $0 \leq v \leq s-1$. No entanto, como $us + v \leq q-1$ e $ts = q+1$ temos que ter $0 \leq u \leq t-1$. Mais ainda, se $u = t-1$ então $v \leq s-2$ pois $(t-1)s + s - 2 = q + 1 - 2 = q - 1$.

É fácil verificar que se $m_i = a_i q + u_i s + v_i$ é uma expressão de m_i na forma especial, com $i \in \{1,2\}$, então $m_1 > m_2$ se $a_1 > a_2$, ou se $a_1 = a_2$ e $u_1 > u_2$ ou se $a_1 = a_2$, $u_1 = u_2$ e $v_1 > v_2$ (de fato, por exemplo, se $a_1 > a_2$ então chamando $b_i = u_i s + v_i$, com $i \in \{1,2\}$ temos $m_1 - m_2 = (a_1 - a_2)q + b_1 - b_2 > 0$ pois $|b_1 - b_2| \leq q-1$).

Seja m um inteiro não negativo, que escrevemos como $m = aq + us + v$, com $a \geq 0$, $0 \leq u \leq t-2$ e $0 \leq v \leq s-1$ ou $m = aq + (t-1)s + v$, com $a \geq 0$ e $0 \leq v \leq s-2$. Vamos usar as considerações dos parágrafos acima para contar os elementos do conjunto $I(m) := \{c \leq m \mid c = iq + js,\ i \geq 0, 0 \leq j \leq q-1\}$. A idéia é escrever elementos c na forma especial, impor a condição $c \leq m$ e obter $|I(m)|$ através de uma contagem dos possíveis coeficientes de q, s e 1 na expressão de c.

Sabemos que $I(m) = \dim \mathcal{L}(mQ_\infty)$, ou seja, $I(m)$ é o número de ordens de pólo em Q_∞ que são menores ou iguais a m, logo, do teorema de Riemann-Roch temos que se $m > 2g-2$ então $\dim \mathcal{L}(mQ_\infty) = m+1-g$. Assim, resta tratar o caso $m \leq 2g-2$. De $g = (q-1)(s-1)/2$ temos $2g-2 = (s-1)q-(s-1)-2 = (s-2)q+q-s-1 = (s-2)q+st-1-s-1 = (s-2)q+(t-1)s-2$, logo se escrevermos $2g-2$ na forma especial o coeficiente de q será $s-2$ e o coeficiente de s será no máximo $t-2$ (pois o coeficiente de 1 tem que ser não negativo). Assim, como $m = aq + us + v \leq 2g-2$, temos que ter $0 \leq a \leq s-2$. Seja $c = iq + js$, com $i \geq 0$ e $0 \leq j \leq q-1$. Seja $j = kt + \ell$, com $0 \leq \ell \leq t-1$ a divisão euclidiana de j por t, temos então

que $c = (i+k)q + \ell s + k$. De $q - 1 = st - 2$ e $j \leq q - 1$ vem que $0 \leq k \leq s - 1$; mais ainda, $k \leq s - 2$ caso $\ell = t - 1$ (pois $(s-1)t + t - 1 = q$). Como $c \leq m$ temos que $0 \leq i + k \leq a$. Dividimos a contagem das possibilidades para $c \leq m$ em três casos.

1) Quando $i + k =: a' \in \{0, \ldots, a-1\}$ temos que k pode assumir qualquer valor no conjunto $\{0, \ldots, a'\}$ (pois $a' < a \leq s - 2$) e ℓ pode assumir qualquer valor no conjunto $\{0, \ldots, t-1\}$. Assim, temos um total de $\sum_{a'=0}^{a} a't = a(a+1)t/2$ valores possíveis para c.

2) Quando $i + k = a$ e $\ell \in \{0, \ldots, u-1\}$ para cada valor de ℓ o inteiro k pode assumir qualquer valor no conjunto $\{0, \ldots, a\}$ (pois $a \leq s - 2$), logo temos $(a+1)u$ valores possíveis para c.

3) Quando $i + k = a$ e $\ell = u$ temos que ter $k \in \{0, \ldots, v\}$ e de $k = a - i$ temos que ter $k \in \{0, \ldots, a\}$ logo as possibilidades para c são em número de $\min\{a, v\} + 1$.

Daí vem que $|I(m)| = a(a+1)t/2 + (a+1)u + \min\{a, v\} + 1$, onde $m = aq + us + v$ está escrito na forma especial.

Proposição 2.3.12 *Assuma que* $0 \leq m \leq n + 2g - 2 = q^2 - s - 1$. *Então a dimensão de* C_m *é dada por*

$$\dim C_m = \begin{cases} |I(m)| \text{ se } 0 \leq m \leq 2g - 1 = qs - q - s, \\ n - |I(m^\perp)| \text{ se } n \leq m \leq n + 2g - 2 \end{cases}$$

onde $m^\perp := n + 2g - 2 - m = q^2 s - s - 1 - m$. *Para* $2g - 2 < m < n$ *temos*

$$\dim C_m = m + 1 - g$$

Demonstração
Para $0 \leq m < n$, nós temos que $\dim C_m = \dim \mathcal{L}(mQ_\infty) = |I(m)|$. Para $n \leq m \leq n + 2g - 2$, nós temos pela proposição 2.3.6 que

$$\dim C_m = n - \dim C_m^\perp = n - \dim aC_{n+2g-2-m}$$

$$= n - \dim C_{n+2g-2-m} = n - |I(m^\perp)|,$$

onde $m^\perp = n + 2g - 2 - m \leq 2g - 2 < n$. □

Dado um inteiro $m \geq 0$, seja $\tilde{m}$ a maior ordem de pólo de Q_∞ com $\tilde{m} \leq m$. Temos que $\mathcal{L}(mQ_\infty) = \mathcal{L}(\tilde{m}Q_\infty)$. De fato, como $\tilde{m} \leq m$, então $\mathcal{L}(\tilde{m}Q_\infty) \subseteq \mathcal{L}(mQ_\infty)$. Se $m = \tilde{m}$ acabou. Suponhamos que $\tilde{m} < m$. Então os números $\tilde{m} + 1, \tilde{m} + 2, \ldots, m$ não são ordens de pólo, ou seja, $|I(\tilde{m})| = |I(\tilde{m} + 1)| = \cdots = |I(m)|$. Mas, $|I(\tilde{m} + i)|$ é também o número de elementos de $B_{\tilde{m}+i}$, para $0 \leq i \leq m - \tilde{m}$. Logo $\dim \mathcal{L}(mQ_\infty) = \dim \mathcal{L}(\tilde{m}Q_\infty)$, ou seja, $\mathcal{L}(mQ_\infty) = \mathcal{L}(\tilde{m}Q_\infty)$. Então, sem perda de generalidade, podemos sempre supor que m é uma ordem de pólo de Q_∞.

Lema 2.3.13 *Sejam* $\alpha_1, \ldots, \alpha_s \in U$ *raízes da equação* $x^s = 1$. *Então*

$$\prod_{v=1}^{s}(x - \alpha_v) = \lambda \prod_{\mu=1}^{q}(y - \beta_\mu),$$

onde α_v*'s são elementos dois a dois distintos e* $\beta_\mu^q + \beta_\mu = 1$ *para todo* μ *com* $1 \leq \mu \leq q$ *e* $\lambda \in K$.

Demonstração
O divisor de $\prod_{v=1}^{s}(x-\alpha_v)$ é igual ao divisor de $\prod_{\mu=1}^{q}(y-\beta_\mu)$. Logo o divisor de $\prod_{v=1}^{s}(x-\alpha_v)/\prod_{\mu=1}^{q}(y-\beta_\mu)$ é o divisor nulo. Dessa forma $\prod_{v=1}^{s}(x-\alpha_v)/\prod_{\mu=1}^{q}(y-\beta_\mu) \in K$, isto é,

$$\prod_{v=1}^{s}(x-\alpha_v) = \lambda \prod_{\mu=1}^{q}(y-\beta_\mu).$$

□

Lema 2.3.14 (Caso Hermitiano) *Seja $s = q+1$. Assuma que $2q^2-q-2 \leq m < n = q^3$ e que $n-m$ é uma ordem de pólo de Q_∞. Então existe $f \in \mathcal{L}(mQ_\infty)$ tal que f tem m zeros no suporte de D e é da forma*

$$f = h\prod_{\mu=1}^{q-2}(y-\beta_\mu),$$

onde $\beta_\mu^q + \beta_\mu = 1$, para todo μ com $1 \leq \mu \leq q-2$, e $h \in \mathcal{L}(m^{'}Q_\infty)$ com $m^{'} = m-(q-2)(q+1)$.

Demonstração
Da proposição 2.3.10, como m é ordem de pólo, podemos escrever $m = iq + j(q+1)$ com $i \geq 0$ e $0 \leq j \leq q-1$. Seja δ um elemento primitivo de $GF(q)$. Dividiremos nossa demonstração em três casos:

Caso (a) $2q^2-q-2 \leq m < q^3-q^2$: Então $i \leq q^2-q-1$ e nós temos dois casos. Se $j = q-2$ ou $j = q-1$, então definimos

$$f := \prod_{v=1}^{i}(x-\alpha_v).\prod_{\mu=1}^{j}(y-\beta_\mu),$$

onde $\beta_\mu^q + \beta_\mu = 1$ para todo μ, com $1 \leq \mu \leq j$, e α_v's são elementos dois a dois distintos em K com $\alpha_v^{q+1} \neq 1$.

Se $0 \leq j \leq q-3$, então $iq \geq 2q^2-q-2-j(q+1) \geq q^2+q+1$, logo temos que $i \geq q+1$. Seja $A := \{\alpha \in K; \alpha^{q+1} \neq \delta^{q-2}\}$. Neste caso escolha $\alpha_v \in A$ tal que α_v's são elementos dois a dois distintos para todo v, com $1 \leq v \leq i$ e, mais ainda, $\alpha_v^{q+1} = 1$ para todo v, com $1 \leq v \leq q+1$. Seja

$$f := \prod_{v=1}^{i}(x-\alpha_v).\prod_{\mu=1}^{j}(y-\beta_\mu^{'})$$

onde os elementos $\beta_\mu^{'} \in K$ são dois a dois distintos e $\beta_\mu^{'\,q} + \beta_\mu^{'} = \delta^{q-2}$ para todo μ, com $1 \leq \mu \leq j$. Como

$$\prod_{v=1}^{q+1}(x-\alpha_v) = \lambda\prod_{\mu=1}^{q}(y-\beta_\mu),$$

onde $\lambda \in K$ e β_v's são elementos dois a dois distintos e $\beta_\mu^q + \beta\mu = 1$ para todo μ, com $1 \leq \mu \leq q$, nós obtemos o resultado desejado para esse caso.

Caso (b) $q^3 - q^2 \leq m < q^3$ e $m \equiv 0 \; mod \; q$: Nós temos que $m = iq$ com $q^2 - q \leq i < q^2$. Seja

$$f := \prod_{v=1}^{i}(x - \alpha_v),$$

onde α_v's são elementos dois a dois distintos em K para todo v, com $1 \leq v \leq i$ e, mais ainda, $\alpha_v^{q+1} = 1$ para todo v, com $1 \leq v \leq q+1$. Nós podemos converter f da mesma maneira que foi feito no caso (a).

Caso (c) $q^3 - q^2 \leq m < q^3$ e $m \not\equiv 0 \; mod \; q$: Como $n - m$ é ordem de pólo de Q_∞ por hipótese, então m pode ser escrito unicamente da forma $m = q^3 - q^2 + aq + b$ onde $0 \leq a < b \leq q - 1$. Vamos mostrar tal afirmação. Como $q^3 - q^2 \leq m < q^3$, então $m = q^3 - q^2 + c$ com $0 \leq c \leq q^2 - 1$. Sabemos que $n - m \neq 0$ e de $n - m$ ser ordem de pólo temos que $n - m \geq q$. Logo $q^2 - c \geq q$ e, daí $0 \leq c \leq q(q-1)$. Fazendo a divisão euclidiana de c por q, temos que $c = r_1 q + r_2$, com $0 \leq r_2 \leq q - 1$ e $r_1 \leq q - 1$, pois $c \leq q(q-1)$. Como $q^2 - c = q^2 - r_1 q - r_2 = q(q - r_1) - r_2 = q(q - (r_1 + 1)) + (q - r_2)$ é ordem de pólo, temos que $q - r_2 \leq q - (r_1 + 1)$, portanto $r_1 < r_2$. Logo $m = (q^2 - q - b + a)q + b(q+1)$ e, assim, $i := q^2 - q - b + a \leq q^2 - q - 1$. Podemos, então, encontrar f do mesmo jeito que foi feito na segunda parte do caso (a).

□

Teorema 2.3.15 (Caso Hermitiano) *Seja $s = q + 1$ e seja p_r a r-ésima ordem de pólo de Q_∞. Assuma que $2q^2 - q - 2 \leq m < n = q^3$ e que $n - m$ é uma ordem de pólo de Q_∞. Então, para todo r com $1 \leq r \leq g$, temos*

$$d_r(C_m) \leq n - m + p_r.$$

Demonstração
Seja $f \in \mathcal{L}(mQ_\infty)$ uma função com precisamente m zeros distintos no suporte de D e da forma

$$f = h \prod_{\mu=1}^{q-2}(y - \beta_\mu)$$

onde $\beta_\mu^q + \beta\mu = 1$ para todos μ, com $1 \leq \mu \leq q-2$ e $h \in \mathcal{L}(m'Q_\infty)$, com $m' = m - (q-2)(q+1)$, como descrito no lema 2.3.14. Escolha α_v's com $\alpha_v^{q+1} = 1$ para todo v, com $1 \leq v \leq q-2$. Agora, sejam

$$z_1 := (y - \beta_1)(y - \beta_2)(y - \beta_3) \cdots (y - \beta_{q-2}),$$
$$z_2 := (x - \alpha_1)(y - \beta_2)(y - \beta_3) \cdots (y - \beta_{q-2}),$$
$$z_3 := (y - \beta_2)(y - \beta_3) \cdots (y - \beta_{q-2}),$$
$$z_4 := (x - \alpha_1)(x - \alpha_2)(y - \beta_3) \cdots (y - \beta_{q-2}),$$
$$z_5 := (x - \alpha_2)(y - \beta_3) \cdots (y - \beta_{q-2}),$$
$$z_6 := (y - \beta_3) \cdots (y - \beta_{q-2}),$$
$$\vdots$$
$$z_{g-2} := (x - \alpha_{q-3})(x - \alpha_{q-2}),$$
$$z_{g-1} := (x - \alpha_{q-2}),$$
$$z_g := 1$$

e defina $f_r := hz_r$ para r com $1 \leq r \leq g$. É fácil verificar que $f_r \in \mathcal{L}(mQ_\infty)$ para todo r com $1 \leq r \leq g$ e $f_1, \ldots, f_g$ são linearmente independentes sobre K. Seja V_r o subcódigo r-dimensional de C_m gerado por $f_1, \ldots, f_r$. Temos que $|\chi(V_r)| = n - m + p_r$. De fato, podemos encontrar um termo geral para os elementos z_r, a saber

$$z_{(1+\cdots+i)+j} = (x - \alpha_j).\cdots.(x - \alpha_i)(y - \beta_{i+1}).\cdots.(y - \beta_{q-2}),$$

se $1 \leq i \leq q-2$ e $j \in \{1, \ldots, i\}$,

$$z_{(1+\cdots+i)} = (y - \beta_i).\cdots.(y - \beta_{q-2})$$

se $1 \leq i \leq q-2$ e

$$z_g = 1.$$

Podemos também escrever as ordens de pólo de uma maneira geral, análoga a feita acima, a saber

$$p_{1+(1+\cdots+i)+j} = iq + j$$

onde $j \leq i$, daí

$$p_{(1+\cdots+i)} = p_{1+(1+\cdots+(i-1))+(i-1)} = (i-1)q + (i-1)$$

para todo $i \geq 0$. Tendo em vista estas considerações, se $r = 1 + 2 + \cdots + i$ temos

$$|V_{(1+2+\cdots+i)}| = n - |\{\text{zeros de } f_r\}| = n - |\{\text{zeros de } h\}| - |\{\text{zeros de } z_r\}| =$$

$$n - [m + (q-2)(q+1)] - [(q-1-i)(q+1)] = n - m + q(i-1) + (i-1) =$$

$$n - m + p_{(1+\cdots+i)} = n - m + p_r.$$

Dados $i \in \{1, \ldots, q-2\}$, $j \in \{1, \ldots, i\}$ e $r = (1 + 2 + \cdots + i) + j$ temos ainda

$$|V_r| = |V_{r+i+1-j}| - |\{\text{zeros comuns de } \prod_{u=j}^{i}(x - \alpha_u) \text{ e } (y - \beta_i)\}| =$$

$$n - m + iq + i - [i - j + 1] = n - m + iq + j - 1 = n - m + p_{1+(1+\cdots+i)+j-1} = n - m + p_r.$$

Logo temos $d_r(C_m) \leq n - m + p_r$. □

Teorema 2.3.16 (Caso Hermitiano) *Seja $s = q+1$. Assuma que $2q^2 - q - 2 \leq m < q^3 = n$ e que $n - m$ é uma ordem de pólo de Q_∞. Então temos que*

(i) $d_1(C_m) = n - m$,

(ii) $d_2(C_m) = n - m + q$,

(iii) $d_3(C_m) = n + m + q + 1$,

(iv) $d_{g-i}(C_m) = n - m + 2g - 2 - i$, *para todo i com $0 \leq i \leq q-2$.*

Demonstração
Como $\gamma_1 = 0 = p_1$, $\gamma_2 = q = p_2$ e $\gamma_3 = q+1 = p_3$ pela proposição 2.3.11, (i), (ii) e (iii) seguem dos teoremas 2.2.22 e 2.3.15. Seja $m^\perp := n + 2g - 2 - m$. Então temos que $q^2 - q - 2 < m^\perp \leq q^3 - q^2$. Logo, existe uma função $f \in \mathcal{L}(m^\perp Q_\infty)$ tal que f tem $m^\perp$ zeros distintos no suporte de D e f é da forma $f = h(x - \alpha)$ com $h \in \mathcal{L}((m^\perp)Q_\infty)$ (para ver isso procedemos de maneira análoga à demonstração do lema 2.3.14). Assim $d_1(C_m^\perp) = n - m^\perp = m - 2g + 2$. O subcódigo bidimensional V_2 de $C_{m^\perp}$ gerado por f e h tem $|\chi(V_2)| = n - m^\perp + q = m - 2g + 2 + q$ e, logo, temos que $d_2(C_m^\perp) = n - m^\perp + q = m - 2g + 2 + q$ pelo teorema 2.2.22 e pela proposição 2.3.11. O item (iv) segue do teorema 2.1.11 e da observação 2.1.12. □

Teorema 2.3.17 (Caso não-Hermitiano) *Seja $s < q + 1$. Assuma que $0 \leq m < q((q-1)s + 1) = n$ e que, ambos, m e $n - m$ são ordens de pólo de Q_∞. Então temos*

(i) $d_1(C_m) = n - m$

(ii) $d_2(C_m) = n - m + s$, *se* $m \not\equiv 0 \ mod\ q$ *ou* $m \geq qs$.

Demonstração

Caso (a1) Suponhamos que $m = n - (s-1)q = q((q-2)s + 2)$. Sejam $\alpha_1, \ldots, \alpha_i \in U$ elementos dois a dois distintos onde $i := (q-2)s + 2$. Então a função

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

tem exatamente $iq = m$ zeros distintos no suporte de D. Logo $d_1(C_m) \leq n - m$. Pelo teorema 2.2.22 $d_1(C_m) \geq n - \deg G + \gamma_1 = n - m$. Assim $d_1(C_m) = m - n$.

Caso (a2) Suponhamos que $m < n - (s-1)q = q((q-2)s + 2)$. Como m é uma ordem de pólo de Q_∞, podemos escrever $m = iq + js$ com $i \geq 0$ e $0 \leq j \leq q - 1$. Logo $i \leq (q-2)s + 1 = (q-1)s + 1 - s$. Seja $A := \{\alpha \in U; \alpha^s \neq 1\}$. Então $|A| = (q-1)s + 1 - s \geq i$, pois todas as s raízes da unidade estão em U e $|U| = (q-1)s + 1$. Escolha $\alpha_1, \ldots, \alpha_i \in A$ elementos dois a dois distintos. O elemento

$$z_1 := \prod_{v=1}^{i} (x - \alpha_v)$$

tem iq zeros distintos no suporte de D. Escolha agora $\beta_1, \ldots, \beta j \in K$ dois a dois distintos tais que $\beta_\mu^q + \beta_\mu = 1$ para $1 \leq \mu \leq j$ e seja

$$z_2 := \sum_{\mu=1}^{j} (y - \beta_\mu).$$

Note que essa escolha é possível pois $j \leq q - 1$. Então $f = z_1 z_2 \in \mathcal{L}(mQ_\infty)$ tem exatamente m zeros no suporte de D. Analogamente ao que foi feito em $(a1)$, temos $d_1(C_m) = m - n$.

Caso (a3) Por fim, suponhamos agora $n - (s-1)q = q((q-2)s + 2) < m < n$. Temos que $0 < n - m < (s-1)q < q((q-2)s + 2)$. Como, por hipótese, $n - m$ é uma ordem de pólo de Q_∞ existe um elemento $z \in \mathcal{L}((n-m)Q_\infty)$ com divisor $(z) = E - (n-m)Q_\infty$ onde $0 \leq E \leq D$ e $\deg E = n - m$. Para ver isso, basta escrever $n - m = iq + js$ com

$i \geq 0$ e $0 \leq j \leq q-1$. Teremos $i \leq (q-2)s+1$ e podemos encontrar z_1 e z_2 como no caso (a_2). Faça $z = z_1 z_2$. O elemento $u := x^{(q-1)s+1} - x \in F$ tem seu divisor principal da forma $(u) = D - nQ_\infty$, logo fazendo $f = u/z$ temos

$$(f) = (u) - (z) = (D - E) - mQ_\infty.$$

Assim a palavra do código correspondente a $f \in \mathcal{L}(mQ_\infty)$ tem m zeros distintos no suporte de D, o que demonstra o item (a) do teorema.

(b) Escreva $m = iq + js$ com $i \geq 0$ e $0 \leq j \leq q-1$. Se q não divide m, então o elemento f definido no caso (a) pode ser escrito como $f = h(y - \beta)$ para algum β com $\beta^q + \beta \neq 0$. Considere o subcódigo bidimensional V_2 de C_m gerado por f e h. Temos que $|\chi(V_2)| = n - m + s$. Analogamente, se $m > qs$, então podemos também encontrar V_2. Logo, $d_2(C_m) \leq n - m + s$ em ambos os casos. Pelo teorema 2.2.22 e pela proposição 2.3.11, temos que $d_2 \geq n - m + \gamma_2 = n - m + s$.

□

Exemplo 2.3.18 (Corpos de funções hiperelípticas) *Assuma que char $K > 2$ e $s = 2$ (corpo de funções hiperelípticas). Seja p_r a r-ésima ordem de pólo de Q_∞. Assuma que $4g = 2q - 2 \leq m < n = q(2(q-1)+1) = 2q^2 - q$ e que $n - m$ é uma ordem de pólo de Q_∞. Então, temos que $\gamma_r = 2(r-1) = p_r$ e $d_r(C_m) = n - m + \gamma_r = n - m + p_r$, $\forall r$, com $1 \leq r \leq g = (q-1)/2$.*

Demonstração
Temos que o conjunto das lacunas S é dado por

$$S = \{2j + 1; 0 \leq j \leq (q-3)/2\},$$

ou seja, todas as ordens de pólo até $q-1$ são pares. Logo $p_r = 2(r-1)$, para todo r, com $1 \leq r \leq g$.

Pela observação 2.2.20, $\gamma_r \leq p_r$, para todo $r \geq 1$ e, pela proposição 2.2.21, $\gamma_r \geq 2(r-1) = p_r$, para todo r, com $0 \leq r \leq g$. Assim $\gamma_r = p_r$, onde $1 \leq r \leq g$.

Se $2q - 2 \leq m < n$ e $n - m$ é ordem de pólo de Q_∞, então existe um elemento $f \in \mathcal{L}(mQ_\infty)$ definido na demonstração do teorema 2.3.17 tal que f pode ser expresso como $f = h \prod_{\mu=1}^{(q-1)/2} (y - \beta_\mu)$, onde β'_μ são dois a dois distintos como na prova do lema 2.3.14. Seja $f_r = h \prod_{\mu=r}^{(q-1)/2} (y - \beta_\mu)$ onde $1 \leq r \leq g$. É fácil verificar que $f_1, \ldots, f_g$ são linearmente independentes sobre K. O subcódigo V_r de C_m gerado por $f_1, \ldots, f_r$ tem $|\chi(V_r)| = n - m + p_r$, como feito na prova do teorema 2.3.15, logo temos que $d_r(C_m) \leq n - m + p_r = n - m + \gamma_r$ para r com $1 \leq r \leq g$. A igualdade segue do teorema 2.2.22. □

Outros resultados sobre distâncias generalizadas de códigos Hermitianos podem ser encontrados por exemplo, em [1], onde os autores completam o trabalho [9] calculando todas as distâncias generalizadas em códigos de Hamming suportados em um ponto. Também em [4] encontramos resultados sobre distâncias generalizadas que levam em consideração a chamada "abundância" do código, que é a dimensão de $\mathcal{L}(G - D)$.

Referências Bibliográficas

[1] BARBERO, A. I.; MUNUERA, C. *The weight hierarchy of Hermitian codes* SIAM J. Discrete Math. 13, No. 1, pp. 79 - 104, 2000.

[2] GARCIA, A. *On Goppa Codes and Artin-Schreier Extensions* Comm. in Algebra 20, pp. 3683 - 3689, 1992.

[3] GURUSWAMI, V. *List decoding from erasures: bounds and code constructions*, Lect. Notes Comput. Sci. 2245, pp. 195 - 206, 2001.

[4] MUNUERA, C. *On the generalized Hamming weights of geometric Goppa codes* IEEE Trans. Inf. Theory 40, No.6, pp. 2092 - 2099, 1994.

[5] PELLIKAAN, R. *On the gonality of curves, abundant codes and decoding* H. Stichtenoth and M. A. Tsfasman, eds., Lectures Notes in Mathematics, vol. 1518, Coding Theory and Algebraic Geometry, Springer-Verlag, pp. 132 - 144, 1992.

[6] STICHTENOTH, H. *A Note on Hermitian Codes over* $GF(q^2)$ IEEE Trans. Inform. Theory., vol. IT-34, pp. 1348, Sept. 1988.

[7] STICHTENOTH, H. *Algebric Function Fields.* Berlim Heidelberg New York: Springer-Velarg. 1993.

[8] STICHTENOTH, H. *Self-dual Goppa Codes* J. Pure and Appl. Math., vol. 55, pp. 199-211, 1988.

[9] STICHTENOTH, H.,KUMAR, P.V. E YANG,K. *On the Weight Hierarchy of Geometric Goppa Codes.* IEEE Trans. Inform. Theory., vol. 40, pp. 913-920, 1994.

[10] WEI, K. V. *Generalized Hamming Weights for Linear Codes* IEEE Trans. Inform. Theory., vol. IT-33, pp. 605-609, 1987.