Wagner Dias Alves de Souza

Semigrupo de Weierstrass e Códigos AG Bipontuais

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2017

Wagner Dias Alves de Souza

Semigrupo de Weierstrass e Códigos AG Bipontuais

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: Álgebra.

Orientador: Prof. Dr. Guilherme Chaud Tizziotti.

UBERLÂNDIA - MG
2017

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

S729s 2017

Souza, Wagner Dias Alves de, 1990-
Semigrupo de Weierstrass e códigos AG bipontuais / Wagner Dias Alves de Souza. - 2017.
45 f. : il.

Orientador: Guilherme Chaud Tizziotti.
Dissertação (mestrado) - Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Inclui bibliografia.

1. Matemática - Teses. 2. Geometria algébrica - Teses. 3. Códigos de Goppa - Teses. I. Tizziotti, Guilherme Chaud. II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III. Título.

CDU: 51

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: Wagner Dias Alves de Souza

NÚMERO DE MATRÍCULA: 11512MAT011.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Álgebra.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Semigrupo de Weierstrass e Códigos AG Bipontuais.

ORIENTADOR: Prof. Dr. Guilherme Chaud Tizziotti.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 06 de Março de 2017, às 9h, pela seguinte Banca Examinadora:

NOME	ASSINATURA
Prof. Dr. Guilherme Chaud Tizziotti UFU - Universidade Federal de Uberlândia (orientador)	
Prof. Dr. Alonso Sepúlveda Castellanos UFU - Universidade Federal de Uberlândia	
Prof. Dr. Juan Elmer Villanueva Zevallos UFMT - Universidade Federal de Mato Grosso	

Uberlândia-MG, 06 de Março de 2017.

Dedicatória

Dedico este trabalho ao meus pais Amauri Alves de Souza e Marlenice Dias Pereira de Souza ao qual sempre contei com apoio incondicional. A minha querida companheira Gizele Damaceno Silva, que está ao meu lado em todos os momentos, e sempre tem uma palavra de incentivo para eu continuar enfrentendo os problemas da vida de cabeça erguida.

Agradecimentos

Agradeço ao meu orientador Guilherme Chaud Tizziotti que compartilhou seu conhecimento para o desenvolvimento deste trabalho.
Agradeço aos meus pais por me darem o dom da vida e serem para mim, exemplo de pessoas de bem.
Aos meu familiares por todo afeto a mim dado, em especial aos meus padrinhos João Donizeth (in memorian) e Darlice Helena.
Aos meus colegas do mestrado: Alexandre, Guilherme, José Lucas, Magna e Suelen pelo companheirismo durante essa dura jornada de nossas vidas.
Ao professor Alonso Sepúlveda Castellanos, uma pessoa fundamental no meu desenvolvimento acadêmico e moral.
A FAPEMIG pelo apoio financeiro.

Resumo

Neste trabalho, estudamos conceitos de geometria algébrica relacionados à teoria de códigos de Goppa algébricos geométricos (códigos AG). Vimos como o cálculo do semigrupo de Weierstrass pode ser aplicado na obtenção dos parâmetros de certos códigos AG. Em particular, calculamos o semigrupo de Weierstrass em dois pontos da curva $\mathcal{X}_{q^{2r}}$ dada pela equação afim $y^q + y = x^{q^r+1}$ sobre $\mathbb{F}_{q^{2r}}$, onde r é um inteiro positivo ímpar e q é uma potência de um número primo, e construímos um código AG bipontual sobre $\mathcal{X}_{q^{2r}}$, cujos parâmetros relativos são melhores que códigos AG pontuais comparáveis também construídos sobre esta curva. A principal referência deste trabalho foi [8].

Palavras-chave: códigos AG, semigrupo de Weierstrass

de Souza W. D. A. *Semigrupo de Weierstrass e Códigos Bipontuais.* 2017. - . Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Abstract

In this work we study basics concepts of the algebraic geometry related to Algebraic Geometric Goppa codes theory (AG codes). We have seen how the calculation of the Weierstrass semigroup can be applied in obtaining the parameters of certain AG codes. In particular, we calculated the Weierstrass semigroup at two points on the curve $\mathcal{X}_{q^{2r}}$ defined by afim equation $y^q + y = x^{q^r+1}$ over $\mathbb{F}_{q^{2r}}$, where r is a positive odd integer and q is a prime power, and construct a two-point AG code over $\mathcal{X}_{q^{2r}}$ whose relative parameters are better than comparable one-point AG code. The main reference of this work was [8].

Keywords: AG Codes, Weierstrass semigroup

LISTA DE SÍMBOLOS

$\mathbb{N}$	$\{1, 2, 3, \ldots\}$
$\mathbb{R}$	Conjunto dos números reais
$\mathbb{C}$	Conjunto dos números complexos
$\mathbb{K}$	Corpo
$\mathcal{X}$	Curva projetiva, não singular e absolutamente irredutível
$\mathbb{K}(\mathcal{X})$	Corpo de funções da curva $\mathcal{X}$
$C_\Omega(D, G)$	Código algébrico geométrico de Goppa associado aos divisores D e G
$\mathbb{F}_q$	Corpo finito com q elementos
$\Omega(G - D)$	Espaço das diferenciais ω sobre $\mathcal{X}$ tal que $div(\omega) = (G - D) \succeq 0$
$div(f)$	Divisor da função $f \in k(\mathcal{X})$
$div_\infty(f)$	Divisor de pólos da função $f \in k(\mathcal{X})$
$H(P)$	Semigrupo de Weierstrass de $\mathcal{X}$ em P
$G(P)$	Conjunto de lacunas de Weiestrass de P
$H(P_1, P_2)$	Semigrupo de Weierstrass de $\mathcal{X}$ em P_1 e P_2
$G(P_1, P_2)$	Conjunto de lacunas de Weiestrass do par (P_1, P_2)
$\mathcal{L}(G)$	Espaço das funções $f \in k(\mathcal{X})$ tal que $div(f) + G \succeq 0$ unido com o zero
$\Gamma(P, Q)$	Gerador miminal de $H(P, Q)$
$\omega(x)$	Peso da palavra x

SUMÁRIO

INTRODUÇÃO

A teoria dos códigos corretores de erros é um campo de pesquisa muito ativo na atualidade em diversas áreas do conhecimento: matemática, computação, engenharia, estatística, entre outros.

Na transmissão de mensagens, na vida real, às vezes ocorrem problemas, como por exemplo interferências eletromagnéticas ou erros humanos (por exemplo, erros de digitação) que fazem com que a mensagem recebida seja diferente daquela que foi enviada. O objetivo da teoria é desenvolver métodos que permitam detectar e corrigir estes erros que ocorrem no processo de transmissão da mensagem.

Nesta dissertação, vamos estudar uma classe de códigos corretores de erros, os chamados códigos de Goppa algébricos geométricos, ou simplesmente códigos AG, que foram introduzidos no início da década de 1980 por V. D. Goppa. Tais códigos são construídos a partir de curvas sobre corpos finitos e seus parâmetros (comprimento, distância mínima e dimensão) podem ser obtidos ou estipulados a partir de resultados e conceitos da geometria algébrica. A introdução da geometria algébrica para construir bons códigos foi um dos maiores desenvolvimentos da teoria de códigos corretores de erros. A partir desse momento, muitos estudos emergiram e a teoria de semigrupo de Weierstrass é uma parte importante disso. Primeiramente, ela começou a ser usada para códigos pontuais, onde existe uma forte conexão entre os parâmetros de códigos pontuais com o semigrupo de Weierstrass em um ponto da curva em que o código foi construído, veja [13]. Mais tarde, resultados foram estendidos para códigos bipontuais e m-pontuais, $m \geq 3$. Em [5], G. Matthews mostra, para curvas arbitrárias, que o semigrupo de Weierstrass em dois pontos pode ser explorado na construção de códigos com distância mínima maior do que a cota de Goppa. Porém, na construção do semigrupo de Weierstrass em dois e em mais pontos é uma dificuldade, e de certa forma limita o estudo de códigos AG bipontuais e m-pontuais. Nesse sentido, códigos construídos a partir de curvas específicas têm sido estudados. O objetivo deste trabalho é estudar o semigrupo de Weierstrass em dois pontos da curva $\mathcal{X}_{q^{2r}}$, dada pela equação afim $y^q + y = x^{q^r+1}$ sobre $\mathbb{F}_{q^{2r}}$, onde r é um inteiro positivo ímpar e q é uma potência de um número primo, e veremos como tal semigrupo pode ser importante no tratamento de códigos AG bipontuais sobre esta curva. A referência para este estudo é [1], [8], [9] e [10].

O primeiro capítulo será dividido em três partes. Na primeira parte, falaremos um pouco de códigos corretores de erros aprofundando um pouco mais na teoria de códigos lineares. Na segunda parte, apresentaremos resultados e conceitos básicos da geometria algébrica que servirão de base para a terceira parte, onde estudaremos os códigos de Goppa algébricos geométricos.

No capítulo 2, dividido em quatro partes, estudaremos semigrupos de Weierstrass e códigos bipontuais sobre a curva $\mathcal{X}_{q^{2r}}$.

CAPÍTULO 1

As principais referências deste capítulo são [1], [10] e [12].

Seja A um conjunto finito qualquer e, para um inteiro $n \geq 1$, seja $A^n = \{(a_1, \cdots, a_n) : a_i \in A, i = 1, \cdots, n\}$.

Para quaisquer $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ em A^n, definimos a *distância de Hamming* entre u e v por

$$d(u, v) = |\{i : u_i \neq v_i, 1 \leqslant i \leqslant n\}|,$$

em que, para um conjunto M qualquer, $|M|$ denota a cardinalidade de M. Observamos que a distância de Hamming é uma métrica. De fato, sejam $u, v, w \in A^n$ quaisquer.

i) É claro que $d(u, v) \geq 0$. Agora, $d(u, v) = 0$ se, e somente se, u e v coincidem em todas as suas coordenadas, ou seja, se, e somente se, $u = v$.

ii) O número de coordenadas em que u difere de v é igual ao número de coordenadas que v difere de u. Logo, $d(u, v) = d(v, u)$.

iii) $d(u, v)$ é igual ao menor número de coordenadas diferentes entre u e v. Por sua vez, $d(v, w)$ é igual ao menor número de coordenadas diferentes entre v e w, a qual será no máximo $d(u, v) + d(v, w)$. Logo, $d(u, v) + d(v, w) \geq d(u, w)$.

Um *código* C é um subconjunto não vazio de A^n. O conjunto A é chamado *alfabeto* e os elementos de código C são chamados *palavras-código* ou simplismente *palavras.*

O número n é o *comprimento* do código $C \subset A^n$ e a *distância minima* de C é o inteiro nãonegativo

$$d = min\{d(u, v) : u, v \in C \text{ e } u \neq v\}.$$

Como veremos a seguir, estes dois parâmetros, n e d, são muito importantes no estudo da teoria de códigos.

Basicamente a teoria de códigos é aplicada na seguinte situação. Suponha que um emissor queira transmitir uma mensagem m, para um certo receptor, através de um canal (linha telefônica, internet ou um CD, por exemplo). Durante este processo de transmissão, m pode sofrer alterações e chegar modificada em seu destino. Estas alterações

são chamadas de *erros*. Aprofundando um pouco mais neste processo, temos o seguinte: o emissor codifica a mensagem m, utilizando um código C, e a envia através de um canal, e o receptor decodifica a mensagem que chega até ele com a finalidade de obter a mensagem m. A seguir, veremos que a capacidade de correção de erros neste processo de transmissão está diretamente ligado à distância mínima.

Para $a \in A^n$ e $t > 0$, os conjuntos $D(a,t) = \{u \in A^n : d(u,a) \leqslant t\}$ e $S(a,t) = \{u \in A^n : d(u,a) = t\}$ são chamados, respectivamente, *disco* e *esfera de Hamming* de centro a e raio t.

Para um número real x, denotamos o maior inteiro menor do que ou igual a x por $[x]$.

Lema 1.0.1 *Seja C um código com distância mínima d e seja $\overline{d} = \left[\frac{d-1}{2}\right]$. Se a e a' são duas palavras distintas de C, então $D(a,\overline{d}) \cap D(a',\overline{d}) = \emptyset$.*

Demonstração. *Suponha que um elemento u pertença a $D(a,\overline{d}) \cap D(a',\overline{d})$, então $d(u,a) \leqslant \overline{d}$ e $d(u,a') \leqslant \overline{d}$. A desigualdade triangular juntamente com a simetria da métrica de Hamming nos dá:*

$$d(a,a') \leqslant d(a,u) + d(u,a') \leqslant \left[\frac{d-1}{2}\right] + \left[\frac{d-1}{2}\right] = 2\overline{d} \leqslant d-1,$$

um absurdo, uma vez que C tem distância mínima d por hipótese. ■

Teorema 1.0.2 *Seja C um código e d sua distância mínima. Então, C pode detectar no máximo $d-1$ e pode corrigir no máximo $\overline{d} = \left[\frac{d-1}{2}\right]$ erros.*

Demonstração. Suponhamos que uma palavra $u \in C$ seja transmitida com t erros, $t \leqslant \overline{d}$, sendo recebida a palavra r. Segue, que $d(u,r) \leqslant t \leqslant \overline{d}$. Pelo lema anterior,

$$r \in D(u,\overline{d}) \Rightarrow r \notin D(a,\overline{d}), \text{ para quaisquer } a \in C \text{ e } a \neq u \Rightarrow d(a,r) > \overline{d}.$$

Logo, a palavra u é única a partir de r. Por outro lado, dada uma palavra do código, podemos introduzir no máximo $d-1$ erros de modo a não conseguirmos uma outra palavra do código. Logo é possivel detectarmos o erro e o resultado segue. ■

Observe que o teorema anterior nos diz que quanto maior for a distância mínima de um código, maior sua capacidade de detecção e correção de erros. Se o receptor recebe uma palavra r, acontece uma das seguintes situações:

i) $r \in D(a,\overline{d})$, para algum $a \in C$

ii) $r \notin D(a,\overline{d})$, para todo $a \in C$.

No primeiro caso, pelo teorema anterior, r é único e neste caso decodifica-se r por a. No segundo caso, não é possível decodificar r com precisão.

1.1 Códigos Lineares

A partir de agora, o alfabeto A será um corpo finito com q elementos, denotado por $\mathbb{F}_q$. Para cada inteiro positivo n, $\mathbb{F}_q^n$ é um $\mathbb{F}_q$-espaço vetorial de dimensão n.

Definição 1.1.1 Seja $C \subseteq \mathbb{F}_q^n$. Dizemos que C é um *código linear* se for um subespaço vetorial de $\mathbb{F}_q^n$.

A seguir, veremos como esta estrutura de espaço vetorial é importante no tratamento de códigos corretores de erros.

Sejam $C \subseteq \mathbb{F}_q^n$ um código linear e k a dimensão de C como $\mathbb{F}_q$-espaço vetorial. O comprimento n, a distância mínima d e a dimensão k formam um conjunto de parâmetros para C. Um código com tais parâmetros é chamado de $[n,k,d]-$código ou código $[n,k,d]$. Seja $B = \{v_1, \cdots, v_k\}$ uma base de C. Assim, se $v \in C$, então existem únicos $\lambda_1, \cdots, \lambda_k \in \mathbb{F}_q$ tais que

$$v = \lambda_1 v_1 + \cdots + \lambda_k v_k.$$

Observe que $|C| = q^k$, ou seja, o número de palavras em C é q^k. Assim, quanto maior for a dimensão k, maior será o número de palavras de C. Além disso, já sabemos que quanto maior for a distância mínima d, maior será a capacidade de detectar e corrigir erros. Assim, quanto maiores forem d e k melhor. Porém, temos a seguinte relação entre estes parâmetros: $d + k \leqslant n + 1$.

Esta relação é chamada *cota de Singleton* e sua veracidade será mostrada mais adiante.

Outro parâmetro que envolve a distância entre palavras é o peso de um código. Para cada $v \in \mathbb{F}_q^n$, definimos o *peso* de v como sendo

$$w(v) = |\{i : v_i \neq 0, 1 \leqslant i \leqslant n\}|.$$

Note que $w(v) = |\{i : v_i \neq 0, 1 \leqslant i \leqslant n\}| = d(v, 0)$

Definição 1.1.2 *Definimos o peso de um código linear C como sendo o inteiro*

$$w(C) := min\{w(v) : v \in C - \{0\}\}.$$

Proposição 1.1.3 *Se $C \subseteq \mathbb{F}_q^n$ é um código linear com distância mínima d, então:*

i) $d(u, v) = w(u - v)$, *para todo* $u, v \in \mathbb{F}_q^n$;

ii) $d = w(C)$.

Demonstração.

i) Dados $u, v \in \mathbb{F}_q^n$, temos:

$$w(u - v) = |\{i : u_i - v_i \neq 0, 1 \leqslant i \leqslant n\}| = |\{i : u_i \neq v_i, 1 \leqslant i \leqslant n\}| = d(u, v)$$

ii) Para todos $u, v \in C$ com $u \neq v$, segue que $z = u - v \in C - \{0\}$. Logo;

$$d = min\{i : u_i \neq v_i, 1 \leqslant i \leqslant n\} = min\{i : u_i - v_i \neq 0, 1 \leqslant i \leqslant n\} = min\{i : z_i \neq 0, 1 \leqslant i \leqslant n\} = min\{w(z) : z \in C - \{0\}\} = w(C)$$

■

A seguir, veremos um método de codificação para códigos lineares. Para cada $i = 1, \cdots, k$, tomemos $v_i = (v_{i1}, \cdots, v_{in}) \in B$ e consideremos a seguinte matriz:

$$G = \begin{bmatrix} v_1 \\ \vdots \\ v_k \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{bmatrix}.$$

Chamaremos tal matriz de *matriz geradora* do código C à base B.

- **Sistemática de codificação para códigos lineares:** Considere a transformação linear dada por:

$$T : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$$

$$x \longmapsto x \cdot G$$

Logo, se $x = (x_1, \cdots, x_k) \in \mathbb{F}_q^k$, então $T(x) = x \cdot G = x_1 v_1 + \cdots + x_k v_k \in C$.

A partir de T, podemos associar, de maneira única, cada elemento de $\mathbb{F}_q^k$ a um elemento de C, ou seja, podemos codificar qualquer elemento $x \in \mathbb{F}_q^k$.

Note que G não é determinada de forma única, uma vez que a base de C não é única. Além disso, se G e G' são duas matrizes que geram o mesmo código, então uma é obtida da outra através de permutação de linhas, multiplicação de uma linha por um escalar não nulo e adição de um múltiplo escalar de uma linha à outra, ou seja, sequência de operações nas quais também uma base é obtida a partir da outra.

Para construir um código linear a partir de uma matriz geradora G é necessário que suas linhas sejam linearmente independentes e que o código seja definido como uma imagem da tranformação linear T, definida anteriormente. Logo, se $u \in C = Im(T)$, então existe $v \in \mathbb{F}_q^k$ tal que

$$v \cdot G = u.$$

Entretanto, resolver um sistema como esse pode ser um pouco complicado, dependendo da forma da matriz G. Contudo, podemos escrever G de tal forma que tal sistema seja mais fácil de ser resolvido.

Definição 1.1.4 *Seja $C \subseteq \mathbb{F}_q^k$ um código linear com matriz geradora G. Dizemos que G está na forma padrão se*

$$G = [Id_k | A]_{k \times n},$$

onde Id_k é a matriz identidade de ordem k e A é uma matriz de ordem $k \times (n-k)$.

Toda matriz G, geradora de um código C pode ser posta na forma padrão, basta efetuar sequências de operações como permutar colunas e/ou multiplicar uma coluna por um escalar não nulo. Todavia, efetuando tais sequências de operações em G, estaremos fazendo o mesmo em todas as palavras de C. Logo efetuar sequências de operações em G, matriz geradora de C, é obter uma matriz G', na forma padrão, que será a geradora de um código C', equivalênte a C.

Seja G a matriz geradora de um código C na forma

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ \vdots & \vdots & & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}$$

Colocando G na forma padrão. Note que as linhas são linearmente independentes. Sem perda de generalidade, suponhamos que $g_{11} \neq 0$. Multiplicando a primeira linha pelo inverso de g_{11} teremos o primeiro elemento da matriz igual a 1. Somando à i-ésima linha, para todo $i = 1, \cdots, k$, a primeira linha multiplicada respectivamente por $-1(g_{i1})$ obtemos a matriz

$$\begin{bmatrix} 1 & b_{12} & \cdots & b_{1n} \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{k2} & \cdots & b_{kn} \end{bmatrix}$$

Na segunda linha da matriz anterior, existe um elemento não nulo que pode ser colocado na segunda linha e segunda coluna. Multiplicando a segunda linha pelo inverso deste elemento, obtemos uma matriz da forma:

$$\begin{bmatrix} 1 & c_{12} & c_{13} & \cdots & c_{1n} \\ 0 & 1 & c_{23} & \cdots & c_{2n} \\ 0 & c_{32} & c_{33} & \cdots & c_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & c_{k2} & c_{k3} & \cdots & c_{kn} \end{bmatrix}$$

Prosseguindo com esse processo, obteremos:

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & a_{1(k+1)} & \cdots & a_{1n} \\ 0 & 1 & \cdots & 0 & a_{2(k+1)} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & a_{k(k+1)} & \cdots & a_{kn} \end{bmatrix}$$

que é a matriz na forma padrão $G' = [Id_k | A_{k\times(n-k)}]$.

Definição 1.1.5 *Dizemos que $F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_p^m$ é uma isometria se F preserva distância de Hamming, isto é, dados $u, v \in \mathbb{F}_q^n$, temos $d(F(u), F(v)) = d(u, v)$.*

Assim, dizemos que dois códigos C e C', ambos contidos em $\mathbb{F}_q^n$, são equivalêntes se existe uma isometria F de $\mathbb{F}_q^n$ tal que $F(C) = C'$. Desta definição, segue que códigos equivalêntes possuem os mesmos parâmetros.

Teorema 1.1.6 *Todo código C possui um código equivalênte C' gerado por uma matriz na forma padrão.*

Demonstração. A demonstração segue da observação feita acima.
■

Definição 1.1.7 *Seja $C \in \mathbb{F}_q^n$ um código linear. Definimos o código dual de C por*

$$C^{\perp} = \{v \in \mathbb{F}_q^n; \langle u, v\rangle = 0, \forall\ u \in C\},$$

onde $\langle u, v\rangle$ é o produto interno usual entre u e v.

Proposição 1.1.8 *Seja $C \in \mathbb{F}_q^n$ um código linear com matriz geradora G. Então,*

1) $C^{\perp}$ é um subespaço vetorial de $\mathbb{F}_q^n$;

2) $x \in C^{\perp} \Leftrightarrow G \cdot x^t = 0$.

Demonstração.

1) Como para todo $u \in C$, temos que $\langle u, 0\rangle = 0$, concluimos que $0 \in C^{\perp}$.
Sejam agora, $v, w \in C^{\perp}$. Para todo $u \in C$ temos que

$$\langle u, v + w\rangle = \langle u, v\rangle + \langle u, w\rangle = 0;$$

Portanto $v + w \in C^{\perp}$.
Tome $\lambda \in \mathbb{F}$ e $v \in C^{\perp}$. Para todo $u \in C$ temos

$$\langle u, \lambda \cdot v\rangle = \lambda\langle u, v\rangle = \lambda \cdot 0 = 0.$$

Logo, $\lambda \cdot v \in C^{\perp}$.
Portanto $C^{\perp}$ é subespaço vetorial de $\mathbb{F}_q^n$.

2) Sabemos que $x \in C^{\perp}$ se, e somente se x é ortogonal a todos os elementos de C, em particular a todos os elementos da base de C. Como as linhas de G são base de C, segue que $G \cdot x^t = 0$.

■

Observação 1.1.9 *$C^{\perp} \subseteq \mathbb{F}_q^n$ também é um código linear.*

Proposição 1.1.10 *Seja $C \subseteq \mathbb{F}_q^n$ um código linear de dimensão k com matriz geradora $G = [Id_k|A]_{k\times n}$ na forma padrão. Então,*

1) $dimC^{\perp} = n - k$

2) $H = [-A^t|Id_{n-k}]$ é a matriz geradora de $C^{\perp}$.

Demonstração.

1) Do item 2 do lema anterior, um vetor $x = (x_1, \cdots, x_n) \in C^{\perp}$ se, e somente se,

$$G \cdot x^t = 0 \Leftrightarrow (Id_k|A) \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = 0 \Leftrightarrow \left[\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} + A \cdot \begin{bmatrix} x_{k+1} \\ \vdots \\ x_n \end{bmatrix} \right] = 0 \Leftrightarrow \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} = -A \cdot \begin{bmatrix} x_{k+1} \\ \vdots \\ x_n \end{bmatrix}.$$

Observamos que $\begin{bmatrix} x_{k+1} \\ \vdots \\ x_n \end{bmatrix}$ há $n-k$ entradas e cada uma delas possui q possibilidades de escolha, uma vez que estão em $\mathbb{F}_q^n$. Logo, $C^{\perp}$ possui q^{n-k} elementos, o que quer dizer que $dimC^{\perp} = n - k$.

2) Observe que as linhas de H são linearmente independentes por Id_{n-k}. Além disso, as linhas de H são ortogonais às linhas de G, pois calculando o produto interno entre os elementos de i-ésima linha de H pelos elementos da j-ésima coluna de G, temos

$$\langle(-a_{1j}, \cdots, -a_{ij}, \cdots, -a_{kj}, 0, \cdots, 0, 1, 0, \cdots, 0), (0, \cdots, 0, 1, 0, \cdots, 0, a_{i(k+1)}, \cdots, a_{ij}, \cdots, a_{in})\rangle$$

$$= -a_{ij} + a_{ij} = 0,$$

para $i = 1, \cdots, k$ e $j = k+1, \cdots, n$.

Logo, as linhas de H geram um espaço contido em $C^{\perp}$ de dimensão $n-k$, que é a dimensão de $C^{\perp}$. Portanto, a matriz $H = [-A|Id_{n-k}]$ gera o código dual $C^{\perp}$.

■

Proposição 1.1.11 *Seja $C \subseteq \mathbb{F}_q^n$ um código linear de dimensão k e matriz geradora G. Uma matriz H de ordem $(n-k) \times n$ com entradas em $\mathbb{F}_q^n$ e linhas linearmentes independentes é geradora de $C^{\perp}$ se, e somente, $G \cdot H^t = 0$.*

Demonstração. Note que as linhas de H geram um espaço vetorial contido $\mathbb{F}_q^n$, de dimensão $n-k$, igual a dimensão de $C^{\perp}$. Por outro lado, se $h_1, \cdots, h_{n-k}$ e $g_1, \cdots, g_k$ são respectivamente, as representações das linhas de H e G, temos:

$$(G \cdot H^t)_{i,j} \ = \ \langle g_i, h_j \rangle, \ i = 1, \cdots, k \text{ e } j = 1, \cdots, n-k.$$

Logo,

$$G \cdot H^t = 0 \Leftrightarrow \langle g_i, h_j \rangle = \ 0, \ i = 1, \cdots, k \text{ e } j = 1, \cdots, n-k.$$

Assim, todos os vetores do subespaço gerado pelas linhas de H, pertencem a $C^{\perp}$.

Reciprocamente, o subespaço gerado pelas linhas de H tem dimensão igual a de $C^{\perp}$. Portanto,

$$G \cdot H^t = 0 \Leftrightarrow C^{\perp} \text{ é gerado pelas linhas de } H.$$

■

Corolário 1.1.12 *Seja $C \subseteq \mathbb{F}_q^n$ um código linear. Então, $(C^{\perp})^{\perp} = C$.*

Demonstração. Sejam G e H matrizes geradoras de C e $C^{\perp}$, respectivamente. Da proposição anterior sabemos que

$$G \cdot H = 0 \Leftrightarrow (G \cdot H^t)^t = 0 \Leftrightarrow H \cdot G^t = 0.$$

Isto é G^t é a matriz geradora de $(C^{\perp})^{\perp}$. ■

Proposição 1.1.13 *Sejam $C \subseteq \mathbb{F}_q^n$ um código linear e H a matriz geradora de $C^{\perp}$. Então,*

$$v \in C \Leftrightarrow H \cdot v^t = 0.$$

Demonstração. Pelo corolário anterior e pelo item 2 da Proposição 1.1.10, obtemos:

$$v \in C \Leftrightarrow v \in (C^{\perp})^{\perp} \Leftrightarrow H \cdot v^t = 0.$$

■

A matriz H, geradora de $C^{\perp}$, é chamada de matriz de checagem ou matriz teste de paridade de C.

Para cada $v \in \mathbb{F}_q^n$, o vetor $s = H \cdot v^t$ é chamado de síndrome de v.

Proposição 1.1.14 *Seja $C \subseteq \mathbb{F}_q^n$ um código linear e H sua matriz de checagem. Então, quaisquer $s-1$ colunas de H são linearmente independentes se e somente se $\omega(C) \geq s$.*

Demonstração. Suponhamos que qualquer conjunto contendo quaisquer $s-1$ colunas de H seja linearmente independente. Seja $0 \neq c = (c_1, \cdots, c_n) \in C$ e $h_1, \cdots, h_n$ as colunas de H. Por hipótese, H é a matriz e checagem de C, então

$$0 = H \cdot c^t = \sum_{i=1}^{n} h_i \cdot c_i$$

Como $\omega(C)$ é o número de componentes não nulas de c, suponha que $\omega(c) \leq s-1$, então a equação anterior seria uma combinação linear de r colunas de H, com $1 \leq r \leq s-1$, o que é uma contradição. Logo, $\omega(c) \geq s$.

Reciprocamente, suponhamos que $\omega(C) \geq s$ e que H tenha $s-1$ colunas linearmente dependentes, que podemos supor sem perda de generalidade que sejam $h_{i_1}, \cdots, h_{i_{s-1}}$. Então existiriam $c_{i_1}, \cdots, c_{i_n} \in \mathbb{F}_q$ não todos nulos tais que

$$\sum_{j=1}^{s-1} c_{i_j} \cdot h_{i_j} = 0.$$

O que quer dizer que $c = (0, \cdots, 0, c_{i_1}, \cdots, c_{i_{s-1}}, 0, \cdots, 0) \in C$ e logo, $\omega(C) \leq s-1 < s$, o que é um absurdo. Logo H tem $s-1$ colunas linearmente independentes. ■

Teorema 1.1.15 *Seja $C \subseteq \mathbb{F}_q^n$ um código linear e H sua matriz de checagem. Então $\omega(C) = s$ se, e somente se, qualquer conjunto contendo quaisquer $s-1$ colunas de H é linearmente independentes e existe um conjunto contendo quaisquer s colunas de H linearmente dependentes.*

Demonstração. Por hipótese, $\omega(C) = s$. Assim, da proposição anterior, segue que quaisquer $s-1$ colunas de H são linearmente independentes. Alem disso, existem s colunas de H linearmente independentes, do contrário, teríamos que ter $\omega(C) \geq s+1$, o que seria uma contradição.

Reciprocamente, da proposição anterior temos que $\omega(C) \geq s$. Suponhamos então que $\omega(C) > s$, e assim seguiria também da proposição anterior que qualquer conjunto contendo quaisquer s colunas de H seria linearmente independente, o que contradiz a hipótese. Portanto $\omega(C) = s$. ■

Corolário 1.1.16 ***(Cota de Singleton)*** *Se (n, k, d) são os parâmetros de um código linear C, então vale*

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

Demonstração. Seja H a matriz de checagem de C. Note que H tem posto $n-k$ e $d-1$ colunas linearmente independentes. Logo, H tem no máximo $n-k$ colunas linearmente independentes, isto é, $d-1 \leq n-k$, como queriamos. ■

1.2 Um pouco de Geometria Algébrica

A partir de agora, k será um corpo algebricamente fechado, mais especificamente, o fecho algébrico do corpo $\mathbb{F}_q$, isto é, $k = \overline{\mathbb{F}_q}$. Denotaremos o *espaço afim* de dimensão n, com coordenadas $x_1, \cdots, x_n$, por $\mathbb{A}^n$, e o *espaço projetivo* de dimensão $n+1$, com coordenadas

$x_0, x_1, \cdots, x_n$ será denotado por $\mathbb{P}^n$. Em um primeiro momento, discutiremos sobre o espaço afim, para em seguida estudarmos o espaço projetivo.

No espaço $\mathbb{A}^n$, introduzimos a topologia de Zariski. Os conjuntos fechados são os conjuntos de zeros de ideais I de $k[x_1, \cdots, x_n]$, ou seja,

$$V(I) := \{(x_1, \cdots, x_n) \in \mathbb{A}^n; f(x_1, \cdots, x_n) = 0, \forall f \in I\}$$

Definição 1.2.1 *Seja I_p um ideal primo de $k[x_1, \cdots, x_n]$. O conjunto $\mathcal{X}$ de zeros do ideal I_p é chamado de variedade afim.*

Como exemplo, podemos tomar em $\mathbb{A}^3$ a esfera unitária $x^2 + y^2 + z^2 = 1$. Então, a variedade afim $\mathcal{X}$ será o conjunto formado pelos zeros do ideal $I = \langle x^2 + y^2 + z^2 - 1 \rangle$.

Definição 1.2.2 *Seja I_p um ideal primo de $k[x_1, \cdots, x_n]$. O anel $k[\mathcal{X}] := k[x_1, \cdots, x_n]/I_p$ é chamado de anel de coordenadas da varidedade afim $\mathcal{X}$.*

Como I_p é um ideal primo, segue que $k[\mathcal{X}]$ é um domínio.

Definição 1.2.3 *O corpo quociente de $k[\mathcal{X}]$, denotado por $k(\mathcal{X})$, é chamado de corpo de funções da variedade $\mathcal{X}$. A dimensão da variedade $\mathcal{X}$ é o grau de trancendência de $k(\mathcal{X})$ sobre k. Se tal dimensão for igual a 1, então dizemos que $\mathcal{X}$ é uma curva algébrica.*

Definimos a relação $\sim$ em $\mathbb{A}^{n+1} - \{0\}$:

$$(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n) \Leftrightarrow \exists\ \lambda \in \mathbb{F}_q^*, \text{ tal que } (x_0, \cdots, x_n) = \lambda(y_0, \cdots, y_n).$$

Vejamos que esta relação é de equivalência. De fato, sejam $(x_0, \cdots, x_n), (y_0, \cdots, y_n)$ e $(z_0, \cdots, z_n) \in \mathbb{A}^{n+1}$:

i) Para $\lambda = 1$, temos que $(x_0, \cdots, x_n) = 1 \cdot (x_0, \cdots, x_n)$. Logo, $(x_0, \cdots, x_n) \sim (x_0, \cdots, x_n)$.

ii) Se $(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n)$, então existe $\lambda \in \mathbb{F}_q^*$ tal que $(x_0, \cdots, x_n) = \lambda(y_0, \cdots, y_n)$. Como $\mathbb{F}_q$ é um corpo e $\lambda \neq 0$, temos $\lambda^{-1} \in \mathbb{F}_q^*$, e assim teremos $(y_0, \cdots, y_n) = \lambda^{-1}(x_0, \cdots, x_n)$. Logo, $(y_0, \cdots, y_n) \sim (x_0, \cdots, x_n)$.

iii) Se $(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n)$ e $(y_0, \cdots, y_n) \sim (z_0, \cdots, z_n)$ existem λ e μ em $\mathbb{F}_q$ tais que $(x_0, \cdots, x_n) = \lambda(y_0, \cdots, y_n)$ e $(y_0, \cdots, y_n) = \mu(z_0, \cdots, z_n)$. Portanto, $(x_0, \cdots, x_n) = \lambda \cdot \mu(z_0, \cdots, z_n)$, e assim $(x_0, \cdots, x_n) \sim (z_0, \cdots, z_n)$.

Definição 1.2.4 *Definimos o espaço projetivo n-dimensional sobre $\mathbb{F}_q$ como sendo*

$$\mathbb{P}^n := (\mathbb{A}^{n+1} - \{0\})/\sim.$$

Denotaremos um ponto P de $\mathbb{P}^n$ por

$$P = (x_0 : \cdots : x_n) = \{(y_0, \cdots, y_n); (y_0, \cdots, y_n) \sim (x_0, \cdots, x_n)\},$$

e diremos que $(x_0 : \cdots : x_n)$ são as coordenadas projetivas de P.

Geometricamente, podemos pensar nos pontos de $\mathbb{P}^n$ como o conjunto das retas que passam pela origem em $\mathbb{A}^{n+1}$.

Exemplo 1.2.5 *Considere as aplicações*

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \Leftrightarrow \exists\ \lambda \in \mathbb{F}_q^*, \text{ tal que } (x_1, y_1, z_1) = \lambda(x_2, y_2, z_2)$$

$$\begin{array}{c} \mathbb{A}^2 \longrightarrow \{\pi : z = 1\} \subseteq \mathbb{A}^3 \\ (x, y) \longmapsto (x, y, 1) \end{array}$$

e

$$\pi \longrightarrow \{ \text{ retas } r \subseteq \mathbb{A}^3 \text{ que passam pela origem e tais que } r \nsubseteq \pi.$$

É facil ver que estas são bijeções. Assim, dada uma reta $s \in \pi$, o espaço (plano) projetivo $\mathbb{P}^2$ será o conjunto dos pontos das retas r, que passam pela origem de $\mathbb{A}^3$ e intersectam s, isto é, $\mathbb{P}^2 = (\mathbb{A}^3 - \{(0,0,0)\})/\sim$.

A proxima proposição nos mostra como relacionar os espaços afim e projetivo.

Proposição 1.2.6 *Seja $U = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n; x_0 \neq 0\}$ e considere a aplicação*

$$\varphi : \mathbb{A}^n \longrightarrow \mathbb{P}^{n+1}$$

$$(a_1, \cdots, a_n) \longmapsto (1 : a_1 : \cdots : a_n)$$

Então, φ é injetora e $Im(\varphi) = U$.

Demonstração.

Note que $\varphi(a_1, \cdots, a_n) = (1 : a_1 : \cdots : a_n) \in U$. Logo, podemos escrever

$$\varphi : \mathbb{A}^n \longrightarrow U$$

Definimos

$$\psi : U \longrightarrow \mathbb{A}^n$$

$$(a_0 : a_1 : \cdots : a_n) \longmapsto \left(\frac{a_1}{a_0}, \cdots, \frac{a_n}{a_0}\right)$$

Note que ψ está bem definida. De fato, se dados $(a_0 : \cdots : a_n) = (b_0 : \cdots : b_n)$ em U, existe $\lambda \in \mathbb{F}_q^*$, tal que $(b_0, \cdots, b_n) = \lambda(a_0, \cdots, a_n)$, ou seja, $b_i = \lambda a_i$ para $i = 0, \cdots, n$. Logo,

$$\left(\frac{b_1}{b_0}, \cdots, \frac{b_n}{b_0}\right) = \left(\frac{\lambda a_1}{\lambda a_0}, \cdots, \frac{\lambda a_n}{\lambda a_0}\right) = \left(\frac{a_1}{a_0}, \cdots, \frac{a_n}{a_0}\right)$$

Observe também que :

$$(\psi \circ \varphi)(a_0, \cdots, a_n) = \psi(\varphi(a_0, \cdots, a_n)) = \psi(1 : a_1 : \cdots : a_n) = \left(\frac{a_1}{1}, \cdots, \frac{a_n}{1}\right) = (a_0, \cdots, a_n)$$

e

$$(\varphi \circ \psi)(a_0 : \cdots : a_n) = \varphi(\psi(a_0 : \cdots : a_n)) = \varphi\left(\frac{a_1}{a_0}, \cdots, \frac{a_n}{a_0}\right) = \left(1 : \frac{a_1}{a_0}, \cdots, \frac{a_n}{a_0}\right) = (a_0 : a_1 : \cdots : a_n).$$

Portanto, $\psi \circ \varphi = Id_{\mathbb{A}^n}$ e $\varphi \circ \psi = Id_U$. Mostrando que φ é injetora e $Im(\varphi) = U$. ■

Com isso, temos $U \cap \{P \in \mathbb{P}^n; P = (0 : x_1 : \cdots : x_n)\}$, e pela proposição anterior podemos identificar U com $\mathbb{A}^n$.

E notando que:

$$\mathbb{P}^{n-1} \longrightarrow \{P \in \mathbb{P}^n; P = (0 : x_1 : \cdots : x_n)\}$$

$$(x_1 : \cdots : x_n) \longmapsto (0 : x_1 : \cdots : x_n)$$

é claramente uma bijeção, e podemos identificar $\{P \in \mathbb{P}^n; P = (0 : x_1 : \cdots : x_n)\}$ com $\mathbb{P}^{n-1}$. Logo, temos

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$$

Logo, para o caso, $n = 1$, obtemos $\mathbb{P}^1 = \mathbb{A}^1 \cup \mathbb{P}^0$. Podemos então identificar $\mathbb{P}^0$ com o conjunto $\{(0 : y); y \in \mathbb{F}_q\} = \{(0 : y)\}$. Então, $\mathbb{P}^0$ tem um único ponto que chamaremos de ponto no infinito e denotaremos por P_∞. Definimos então a reta projetiva por $\mathbb{P}^1 = \mathbb{A}^1 \cup \{P_\infty\}$.

A seguir, estudaremos o comportamento de variedades no espaço projetivo. Embora devemos nos restringir alguns conceitos para conseguir nosso objetivo. Vejamos o porquê no próximo exemplo.

Exemplo 1.2.7 *Considere o polinômio* $f = 2y - z^3 \in \mathbb{R}[x, y, z]$.
Queremos determinar os elementos do conjunto $V(f) = \{(x_0, x_1, x_2) \in \mathbb{P}^2; f(x_0, x_1, x_2) = 0\}$ *contido em* $\mathbb{P}^2$.

Note que $P = (1 : 32 : 4) \in V(f)$, *pois* $f(P) = 0$, *mas* $P' = 2P = (2 : 64 : 8) \notin V(f)$, *pois* $f(P') = -384$.

Isso se deve ao fato dos termos do polinômio f *não ser homogêneo.*

Para não nos depararmos com tal situação, iremos trabalhar apenas com polinômios homogêneos. De forma análoga ao que foi estudado no caso afim, trabalharemos com polinômios homogêneos de um ideal primo I_p de $k[x_0, x_1, \cdots, x_n]$.

Definição 1.2.8 *Seja* I_p *um ideal primo de* $k[x_0, x_1, \cdots, x_n]$. *Uma variedade projetiva* $\mathcal{X}$ *é o conjunto de zeros em* $\mathbb{P}^n$ *de polinômios homogêneos de* I_p.

Para simplificar as notações, denotaremos pelo mesmo símbolo $\mathcal{X}$ tanto na variedade afim quanto na projetiva e mensionaremos sempre quais delas especificamente estaremos trabalhando.

Além disso, podemos tornar um polinômio homogêneo pela inclusão e exclusão de variáveis. Em nosso trabalho, usaremos apenas com a inclusão de variáveis, como na definição a seguir.

Definição 1.2.9 *Seja $f(x_1, \cdots, x_n) \in k[x_1, \cdots, x_n]$ um polinômio de grau m. definimos a homogenização de f com respeito a x_{n+1} por*

$$f_h = x_{n+1}^m \cdot f\left(\frac{x_1}{x_{n+1}}, \cdots, \frac{x_n}{x_{n+1}}\right).$$

Exemplo 1.2.10 *Considere $f(x, y) = x^5 + 3x^2y^2 - 7y^3$ em $\mathbb{F}_q[x, y]$.*

Observe que $gr(f) = 5$, entretanto, não é um polinômio homogêneo. Assim, homogenizando f com respeito a z, temos

$$f_h(x, y, z) = x^5 + 3x^2y^2z - 7y^3z^2.$$

Já vimos que no espaço projetivo $\mathbb{P}^n$, precisamos trabalhar com coordenadas homogêneas. Isto significa que necessáriamente, temos que estudar funções racionais tais que tanto o numerador e o denominador sejam polinômios homogêneo e de mesmo grau.

Se considerarmos agora o subanel $R(\mathcal{X})$ de $k(x_0, x_1, \cdots, x_n)$ que consiste das funções racionais $\frac{f}{g}$, em que f e g são polinômios homogêneos de mesmo grau e $g \notin I_p$, onde I_p é um ideal primo. Veremos que $R(\mathcal{X})$ tem um único ideal maximal $M(\mathcal{X}) \subsetneqq R(\mathcal{X})$, consistindo das funções racionais $\frac{f}{g}$ com $f \in I_p$ e o corpo de funções $k(\mathcal{X})$ é por definição o quociente $R(\mathcal{X})/M(\mathcal{X})$.

De fato, observe que $R(\mathcal{X}) = \left\{\frac{f}{g} \in k(\mathcal{X}); g \notin I_p\right\}$. Seja $M(\mathcal{X}) = \left\{\frac{f}{g} \in R(\mathcal{X}); f \in I_p\right\}$. Mostremos que $M(\mathcal{X})$ é um ideal.

Sejam $\frac{f_1}{g_1}$ e $\frac{f_2}{g_2} \in M(\mathcal{X})$. Logo $\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1g_2 + g_1f_2}{g_1g_2} \in M(\mathcal{X})$, pois f_1g_2, $g_1f_2 \in I_p$ e, como I_p é um ideal primo, $g_1g_2 \notin I_p$.

Sejam $\frac{f}{g} \in M(\mathcal{X})$ e $h = \frac{f_1}{g_1} \in R(\mathcal{X})$, com $g_1 \notin I_p$. Assim $\frac{f}{g} \cdot h = \frac{ff_1}{gg_1} \in M(\mathcal{X})$, pois I_p é um ideal primo e portanto $gg_1 \notin I_p$.

Logo $M(\mathcal{X})$ é um ideal. Vejamos que $M(\mathcal{X})$ é um ideal maximal.

Suponha que exista um ideal J de $R(\mathcal{X})$ tal que $M(\mathcal{X}) \subsetneqq J \subseteq R(\mathcal{X})$. Logo existe $\frac{f}{g} \in J$ tal que $\frac{f}{g} \notin M(\mathcal{X})$. Logo, $f \notin J$ e $\frac{g}{f} \in R(\mathcal{X})$. Temos então:

$$\frac{f}{g}\cdot\frac{g}{f}\in J\Rightarrow 1\in J\Rightarrow J=R(\mathcal{X}).$$

Vejamos que $M(\mathcal{X})$ é único. Suponha que exista $M'(\mathcal{X})$ maximal, tal que $M'(\mathcal{X})\subsetneqq R(\mathcal{X})$.

Dado $h\in M'(\mathcal{X})$, como $M'(\mathcal{X})\subseteq R(\mathcal{X})$, temos que $h=\dfrac{f}{g}$, onde $g\notin I_p$. Se $f\in I_p$, então $h\in M(\mathcal{X})$. Se $f\notin I_p$ então $\dfrac{g}{f}\in R(\mathcal{X})$, daí como $M'(\mathcal{X})$ é um ideal, $\dfrac{f}{g}\cdot\dfrac{g}{f}\in M'(\mathcal{X})$, ou seja, $1\in M'(\mathcal{X})$, contradição. Logo, $M'(\mathcal{X})\subseteq M(\mathcal{X})$, e como ambos são maximais, temos $M'(\mathcal{X})=M(\mathcal{X})$.

Definição 1.2.11 *Sejam $\mathcal{X}$ uma variedade projetiva, P um ponto em $\mathcal{X}$, U_p uma vizinhança de P e, f e g polinômios homogêneos de mesmo grau, com $g(p)\neq 0$. O quociente $\varphi:=\dfrac{f}{g}$ definido em U_p, é chamado regular no ponto P, se $\varphi(P)=0$.*

As funções que são regulares em todo ponto de U_p formam um anel que será denotado por $k(U_p)$.

Na Proposição 1.2.6, foi mostrado como podemos relacionar os espaços afim e projetivo. Nosso interesse agora é estender uma variedade afim para uma variedade projetiva de forma análoga. Considere então um polinômio f em $k[x_1,\cdots,x_n]$. Seja f^* um polinômio homogêneo associado à f definido da seguinte forma

$$f^*(x_1,\cdots,x_n,x_{n+1}):=x_{n+1}^m\cdot f\left(\frac{x_1}{x_{n+1}},\cdots,\frac{x_n}{x_{n+1}}\right),$$

onde $m=gr(f)$.

Seja $\mathcal{X}$ uma variedade afim em $\mathbb{A}^n$ definida pelo ideal primo I. Seja I^* o ideal primo gerado pelo conjunto $\{f^*; f\in I\}$. Então I^* define uma variedade projetiva $\mathcal{X}^*$ em $\mathbb{P}^n$.

Definimos $\mathcal{X}^*_{x_0}:=\{(x_0:\cdots:x_n)\in\mathcal{X}^*; x_0\neq 0\}$. Então, a aplicação

$$h:\mathcal{X}\longrightarrow\mathcal{X}^*_{x_0},$$

$$(x_1,\cdots,x_n)\longmapsto(1:x_1:\cdots:x_n)$$

é um isomorfismo.

Os pontos $(x_0:\cdots:x_n)\in\mathcal{X}^*$ com $x_0=0$ são chamados de pontos no infinito da variedade afim $\mathcal{X}$. Além disso, os corpos de funções $k(\mathcal{X})$ e $k^*(\mathcal{X})$ são isomorfos por $\dfrac{f}{g}\longmapsto\dfrac{f^*x_0^m}{g^*}$, onde $m=gr(g)-gr(f)$.

Antes de ilustrarmos tais conceitos, vale observar que $\mathcal{X}^*_{x_0}$ pode ser definido para qualquer coordenada.

Exemplo 1.2.12 *Considere $\mathbb{P}^3$ com coordenadas projetivas $(x : y : z)$ a variedade projetiva $\mathcal{X}$ dada por $xz - y^2 = 0$.*

Observe que o polinômio que define $\mathcal{X}$ é homogêneo. Entretanto, o mesmo pode ter sido homogeneizado com respeito a x ou a z. Assim, quando $z = 0$, o polinômio $xz - y^2$ é zero se, e somente se $y = 0$. Então, se $x \neq 0$, o ponto $P = (1 : 0 : 0)$ é um ponto no infinito de $\mathcal{X}$. Quando $x = 0$, o polinômio $xz - y^2$ também se anula quando y é zero. Logo, se $z \neq 0$, o ponto $Q = (0 : 0 : 1)$ também é ponto no infinito de $\mathcal{X}$.

Agora observe que a função racional $\varphi = \dfrac{2xz + z^2}{y^2 + z^2}$ não é regular em Q, pois $\varphi(Q) = 1 \neq 0$. Substituindo y^2 por xz em φ temos $\varphi' = \dfrac{2x + z}{x + z}$ não é regular em P, pois $\varphi'(P) = 2 \neq 0$.
Por outro lado, a função $\psi = \dfrac{x^3 + y^3}{z^3}$ se anula em Q, e pode ser escrito como $\psi = \dfrac{y^3}{z^3} \cdot \dfrac{y^3 + z^3}{z^3} = \dfrac{(y^2)^3 + y^3 z^3}{z^6}$ e tomando $y^2 = xz$ obtemos $\dfrac{x^3 z^3 + y^3 z^3}{z^6} = \dfrac{x^3 + y^3}{z^3}$.

Entretanto, $\dfrac{y^3}{z^3}$ é zero em Q mas $\dfrac{y^3 + z^3}{z^3}$ não é regular em Q.

O objetivo do exemplo acima é mostrar que o produto de dois polinômios regulares não necessariamente é um polinômio regular.

Se $k = \mathbb{C}$, para pontos na vizinhança de P, há na topologia usual, uma correspondência biunívoca com $\dfrac{y}{z}$, o que não é verdadeiro para $\dfrac{x}{z}$. Este é um exemplo onde trabalhamos com o chamado parâmetro local, que será definido mais adiante.

De maneira particular, considerando apenas curvas em $\mathbb{A}^2$, temos a seguinte definição:

Definição 1.2.13 *Considere uma curva em $\mathbb{A}^2$ definida por $f(x, y) = 0$. Seja $P = (a, b)$ um ponto desta curva. Se pelo menos uma das derivadas parciais f_x ou f_y não se anula em P, então dizemos que P é um ponto nãosingular da curva. Uma curva em que todos os pontos são não singulares é chamado de suave ou nãosingular.*

Para construção de códigos, que veremos mais adiante, estaremos interessados em pontos que têm suas coordenadas no alfabeto $\mathbb{F}_q$. Tais pontos recebem um nome especifico.

Definição 1.2.14 *Se k é o fecho algébrico de $\mathbb{F}_q$ e $\mathcal{X}$ é uma curva sobre k, então os pontos de $\mathcal{X}$ cujas coordenadas estão em $\mathbb{F}_q$ são chamados de pontos racionais.*

O conceito que veremos a seguir, pode ser entendido como um mecanismo de contagem de pólos e zeros de uma função f em uma curva $\mathcal{X}$, além da informação de onde eles se encontram e quais são suas multiplicidades. Consideremos $\mathcal{X}$ uma curva algébrica suave projetiva sobre k.

Definição 1.2.15 *Um divisor é uma soma formal* $D = \sum_{P \in \mathcal{X}} n_P P$ *em que* $n_P \in \mathbb{Z}$ *e é igual a zero a menos de um número finito de pontos de* P.

O conjunto dos divisores de $\mathcal{X}$ denotado por $Div(\mathcal{X})$, é um grupo aditivo com a soma formal em $\mathcal{X}$.

Definição 1.2.16 *Um divisor* D *é chamado divisor efetivo, e denotamos por* $D \succcurlyeq 0$ *se todos os coeficientes* n_p *são nãonegativos.*

Definição 1.2.17 *Definimos o grau de um divisor* $D = \sum_{P \in \mathcal{X}} n_P P$ *por* $\sum n_P$ *e definimos o suporte do divisor como sendo* $supp(D) = \{P; n_P \neq 0\}$.

Definição 1.2.18 *Se* f *é uma função racional, não identicamente nula em* $\mathcal{X}$*, definimos o divisor de* f *por*

$$(f) := \sum_{P \in \mathcal{X}} v_P P.$$

onde v_P *é a valorização de* f *em relação a* P.

Em certo sentido, o divisor de f é um dispositivo que nos diz quais são seus zeros e pólos com suas respectivas multiplicidades. Como f é uma função racional, em que numerador e denominador têm o mesmo grau, e como k é algebricamente fechado, segue que f possui o mesmo número de zeros e pólos. Assim, o grau de um divisor de uma função racional é sempre zero.

Chamaremos o divisor (f) de uma função racional de divisor principal. Os divisores $(f)_0 := \sum_{v_P(f)>0} v_P(f)P$ e $(f)_\infty := \sum_{v_P(f)<0} v_P(f)P$ são chamados respectivamente divisor de zeros e divisor de pólos de f.

Dizemos que dois divisores D e D' são linearmentes equivalentes, e denotamos por $D \equiv D'$, se $D - D'$ é um divisor principal. Pode-se mostrar que esta relação é de equivalência.

Definição 1.2.19 *Seja* D *um divisor em uma curva* $\mathcal{X}$*. Definimos o espaço vetorial* $\mathcal{L}(D)$ *sobre* $\mathbb{F}_q$ *por*

$$\mathcal{L}(D) = \{f \in \mathbb{F}(\mathcal{X})^*; (f) + D \succcurlyeq 0\} \cup \{0\}.$$

Observe que, se $D = \sum_{i=1}^{r} n_i \cdot P_i - \sum_{j=i}^{s} m_j \cdot Q_j$, $\forall n_i,\ m_j > 0$, então $\mathcal{L}(D)$ é composto por 0 mais as funções que tem zeros de multiplicidade no mínimo m_j, em Q_j $(1 \leq j \leq s)$ e que não tem pólos, exceto possivelmente, nos pontos P_i com ordem máxima n_i, $(1 \leq i \leq r)$.

Mostraremos adiante que este espaço tem dimensão finita. Antes, note que se $D \equiv D'$ e g é uma função racional tal que $(g) = D' - D$, então a aplicação $f \longmapsto f \cdot g$ e o fato de que $(f \cdot g) = (f) + (g)$ nos diz que $\mathcal{L}(D)$ e $\mathcal{L}(D')$ são isomorfos.

Teorema 1.2.20 *Considere o espaço $\mathcal{L}(D)$. Então:*

1) $\mathcal{L}(D) = 0 \Leftrightarrow gr(D) < 0$.

2) $l(D) := dim_k \mathcal{L}(D) \geq 1 + gr(D)$.

Demonstração.

1) Como $gr(D) < 0$, então para qualquer função $f \in k(\mathcal{X})^*$ temos que $gr((f)+D) < 0$, o que quer dizer que $f \notin \mathcal{L}(D)$, o que implica que $\mathcal{L}(D) = \{0\}$.

2) Suponha que $f \in \mathcal{L}(D)$ com $f \neq 0$. Logo, $D^{'} = D + (f)$ é um divisor efetivo, e pelo que foi observardo anteriormente, $\mathcal{L}(D^{'})$ tem a mesma dimensão de $\mathcal{L}(D)$.

   Assim, podemos assumir, que D é efetivo e pode ser expresso como $D = \sum_{i=1}^{r} n_i \cdot P_i$, $(n_i \geq 0,\ 1 \leq i \leq)$. Agora, no ponto P_i, podemos fazer uma correspondência entre f e um elemento do espaço vetorial $(t_i^{-n_i} O_{P_i})/O_{P_i}$ de dimensão n_i, em que t_i é um parâmetro local em P_i. Com isso, obtemos uma aplicação de f na soma direta desses espaços vetorias (no caso de $f = 0$, levamos 0 no espaço nulo). Esta aplicação é linear e se f está no núcleo desta aplicação significa que f não possui nenhum pólo em qualquer um dos pontos P_i, ou seja, f é constante. Daí segue que $dim_k = \mathcal{L}(D) \leq 1 + \sum_{i=1}^{r} n_i = 1 + gr(D)$.

■

Considere $\mathcal{X}$ em $\mathbb{A}^2$ uma curva suave afim, definida por $f(X,Y) = 0$, $P = (a,b)$ um ponto de $\mathcal{X}$, T_P a tangente em P, definida por $d_P f = f_x(X-a) + f_y(Y-b) = 0$ e $\Phi[\mathcal{X}]$ o conjunto de todos os mapeamentos que associam cada ponto $P \in \mathcal{X}$ a um elemento de T_P^*, isto é, o conjunto de todas as funções lineares da forma:

$$\phi : \mathcal{X} \longrightarrow k[\mathcal{X}]$$

$$P \longmapsto d_P\phi \in T_P^*$$

Definição 1.2.21 *Um elemento ϕ de $\Phi[\mathcal{X}]$ é chamado de forma diferencial regular em $\mathcal{X}$ se todo ponto $P \in \mathcal{X}$ tem uma vizinhança U_P tal que nesta vizinhança, ϕ pode ser representado por*

$$\phi = \sum_{i=1}^{n} f_i \cdot dg_i,$$

onde f_i e g_i são funções regulares em U_P.

Para o nosso caso, as formas diferencias em $\mathcal{X}$ formam um $k[\mathcal{X}]-$módulo, denotado por $\Omega[\mathcal{X}]$. Tal módulo é gerado por elementos df com $f \in k[\mathcal{X}]$ munido das relações:

i) $d(f+g) = df + dg$;

ii) $d(f \cdot g) = g \cdot df + f \cdot dg$;

iii) $d(a) = 0,\ \forall\ a \in \mathbb{F}_q$.

Entretanto, para as formas diferencias racionais, temos a relação:

iv) $d\dfrac{f}{g} = \dfrac{g \cdot df - f \cdot dg}{g^2}$.

Vamos agora, extender a definição de forma diferencial racional para curvas projetivas suaves $\mathcal{X}$. Para isso, considere o par (U, ω), onde $\emptyset \neq U \subseteq \mathcal{X}$ e $\omega = g \cdot df$ em U. Dados os pares (U, ω) e (V, η), dizemos que elas são equivalêntes se $\omega = \eta$ em $U \cap V$.

Definição 1.2.22 *Definimos a forma diferencial racional para uma curva projetiva suave $\mathcal{X}$ como sendo a classe de equivalência para a relação acima.*

Para simplificar a notação, chamaremos as formas diferencias racionais em $\mathcal{X}$ apenas por diferenciais e denotaremos o espaço dos diferencias em $\mathcal{X}$ por $\Omega(\mathcal{X})$.

Definição 1.2.23 *Definimos o divisor (ω) do diferencial ω em uma curva projetiva suave $\mathcal{X}$ por*

$$(\omega) := \sum_{P \in \mathcal{X}} v_P(f_P)P,$$

onde $\omega = f_P dt_P$ é a representação local de ω e v_P é a valorização em O_P.

Se ω é um diferencial, o divisor $W = (\omega)$ é chamado de divisor canônico. Se ω' é outro diferencial nãonulo, então $\omega' = f\omega$ para alguma função racional f. Assim, $(\omega') = W' = W$ e, portanto, divisores canônicos formam uma classe de equivalência, que também é denotada por W.

Daqui para frente, denotaremos, para um divisor D, $l(D) := dim_k \mathcal{L}(D)$.

Definição 1.2.24 *Seja $\mathcal{X}$ uma curva projetiva suave sobre $\mathbb{F}_q$. Definimos o gênero g de $\mathcal{X}$ por $g = max\{grau D - l(D) + 1; D$ é um divisor de $\mathcal{X}\}$.*

Definição 1.2.25 *Seja D um divisor em uma curva algébrica projetiva não singular $\mathcal{X}$. Definimos o conjunto*

$$\Omega(D) := \{\omega \in \Omega(\mathcal{X}); (\omega) - D\}$$

e denotamos $\delta(D) = dim_k \Omega(D)$ o chamado índice de especialidade do divisor D.

O próximo resultado, é muito importante não só na geometria algébrica, mas também para o estudo de códigos sobre curvas algébricas, que veremos na próxima seção. A demonstração deste resultado se encontra em [10].

Teorema 1.2.26 ***(Riemann-Roch)*** *Seja D um divisor em uma curva algébrica suave projetiva $\mathcal{X}$ de gênero g. Então, para qualquer divisor canônico W, temos*

$$l(D) - l(W - D) = gr(D) - g + 1.$$

Demonstração. Ver Teorema 1.5.15 em [10]. ■

Corolário 1.2.27 *Para um divisor canônico W, temos $gr(W) = 2g - 2$.*

Demonstração. Note que todas as funções regulares em uma curva projetiva $\mathcal{X}$ são constantes. Em particular, para $W = 0$, temos $\mathcal{L}(0) = \mathbb{F}_q$, isto é, $l(0) = dim_{\mathbb{F}_q}\mathcal{L}(W) = 1$. Fazendo, $D = W$ no Teorema de Riemann-Roch e pela definição de gênero, segue que $l(W) - l(0) = gr(W) - g + 1$. Como $l(0) = 1$, temos que

$$\begin{gathered} l(W) = gr(W) - g + 2 \Longrightarrow \\ g = gr(W) - g + 2 \Longrightarrow \\ gr(W) = 2g - 2. \end{gathered}$$

■

Corolário 1.2.28 *Seja D um divisor em uma curva algébrica suave projetiva $\mathcal{X}$ de gênero g tal que $gr(D) > 2g - 2$. Então*

$$l(D) = gr(D) - g + 1.$$

Demonstração. Devemos provar que $l(W - D) = 0$ no Teorema de Riemann-Roch. Do corolário anterior, temos que $gr(W - D) < 0$. Do item 1) do Teorema 1.2.20, temos que $\mathcal{L}(W - D) = 0$, ou seja $l(W - D) = dim_{\mathbb{F}_q}\mathcal{L}(W - D)$, como queriamos. ■

1.3 Códigos Sobre uma Curva Algébrica $\mathcal{X}$

Seja $\mathcal{X}$ uma curva nãosingular, projetiva, geometricamente irredutível, curva algébrica de gênero $g \geq 1$ sobre o corpo finito $\mathbb{F}_q$ com q elementos, $\mathbb{F}_q(\mathcal{X})$ o corpo das funções racionais em $\mathcal{X}$ e $\mathbb{F}_q(\mathcal{X})^*$. Dado um divisor G em $\mathcal{X}$, considere o espaço vetorial

$$\mathcal{L}(G) = \{f \in \mathbb{F}(\mathcal{X})^*; (f) + G \succcurlyeq 0\} \cup \{0\}$$

e

$$\Omega(G) = \{forma\ racional\ diferencial\ \omega; (\omega) \succcurlyeq G\} \cup \{0\}.$$

Para distintos pontos racionais $P_1, \cdots, P_n$ em $\mathcal{X}$ com $P_i \in supp(G)$ para todo i, considere as aplicações:

$$ev_{\mathcal{L}} : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n;\ f \longmapsto (f(P_1), \cdots, f(P_n))$$

$$ev_{\Omega} : \Omega(G) \longrightarrow \mathbb{F}_q^n;\ \omega \longmapsto (res_{P_1}(\omega), \cdots, res_{P_n}(\omega))$$

Sejam $D = \sum_{i=1}^{n} P_i$ e $G = \sum_{i=1}^{l} a_i Q_i$ divisores em $\mathcal{X}$ tais que $supp(G) \cap supp(D) = \emptyset$. Definimos os códigos de Goppa algébricos geométricos $C_\ell(D,G)$ e $C_\Omega(D,G)$, respectivamente, por

$$C_{\mathcal{L}}(D,G) := ev_{\mathcal{L}}(\mathcal{L}(G)) \text{ e } C_\Omega(D,G) := ev_\Omega(\Omega(G-D)).$$

Tais códigos também são chamados de códigos AG.

A condição de que G tenha suporte disjunto de D não é necessária e pode ser trocada pela codificação da aplicação $ev_{\mathcal{L}}$ e ev_Ω, localmente nas coordenadas de $P \in supp(G) \cap supp(D)$, ver referência [11].

Teorema 1.3.1 $C_\Omega(D,G) = C_{\mathcal{L}}(D,G)^\perp$.

Demonstração. Ver Teorema 2.2.8 em [10]. ■

Se $G = aQ$ para algum ponto racional $Q \in \mathcal{X}$ e D é uma somatória de todos os outros pontos racionais em $\mathcal{X}$, então os códigos $C_{\mathcal{L}}(D,G)$ e $C_\Omega(D,G)$ são chamados de pontuais.

Analogamente se $G = a_1Q_1 + a_2Q_2 + \cdots + a_mQ_m$, para m distintos pontos racionais, então $C_{\mathcal{L}}(D,G)$ e $C_\Omega(D,G)$ é chamado de m-pontual código AG. Se $m = 2$, diremos que o código é bipontual. Para mais detalhes sobre a teoria de códigos AG veja [10], [12] e [13].

Teorema 1.3.2 *Seja $C_{\mathcal{L}}(D,G)$ um código de Goppa algébrico geométrico. Então:*

1) $dim C_L(D,G) = k = dim\mathcal{L}(G) - dim\mathcal{L}(G-D)$;

2) $C_L(D,G)$ tem distância mínima $d \geq n - gr(G)$.

Demonstração.

1) Sabemos que a aplicação $ev_{\mathcal{L}}$ é sobrejetiva sobre sua imagem. Observe que $ker(ev_{\mathcal{L}}) = \{f \in \mathcal{L}(G); v_{P_i}(f) > 0, i = 1, \cdots, n\} = \mathcal{L}(G-D)$. Então, $\mathcal{L}(G)/\mathcal{L}(G-D) \simeq C(D,G)$ e portanto $k = dim\mathcal{L}(G) - dim\mathcal{L}(G-D)$.

2) A afirmação relativa a distância mínima só faz sentido se $C(D,G) \neq 0$, então assumiremos assim. Seja $f \in \mathcal{L}(G)$ diferente de zero com $\omega(\alpha(f)) = d$. Então, existem $n-d$ pontos $P_{i_1}, \cdots, P_{i_{n-d}}$ no suporte de D tais que $f(P_{i_j}) = 0$, para $j = 1, \cdots, n-d$. Então,

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

Como $gr(G - (P_{i_1} + \cdots + P_{i_{n-d}})) \geq 0$, segue que $d \geq n - gr(G)$, como queriamos.

■

Corolário 1.3.3 *Suponha que $gr(G) < n$. Então:*

1) α *é injetiva e* $C(D,G)$ *é* $[n,k,d]$ *código em que*

$$d \geq n - gr(G) \text{ e } k = dim\mathcal{L}(G) \geq gr(G) + 1 - g,$$

donde segue que $k + d \geq n + 1 - g$.

2) Se $2g - 2 < gr(G) < n$, *então* $k = gr(G) + 1 - g$.

3) Se $\{f_1, \cdots, f_k\}$ *é uma base de* $\mathcal{L}(G)$, *então*

$$M = \begin{bmatrix} f_1(P_1) & \cdots & f_1(P_n) \\ \vdots & \vdots & \vdots \\ f_k(P_1) & \cdots & f_k(P_n) \end{bmatrix}$$

é uma matriz geradora do código $C(D,G)$.

Demonstração.

1) Como $gr(G - D) < 0$, segue que $dim\mathcal{L}(G - D) = 0$ e como este conjunto é o núcleo da aplicação α, temos então que α é injetiva.

2) Como $gr(G) < 2g - 2$, segue que $dim\mathcal{L}(G - D) = 0$, e pelo Teorema de Riemann-Roch temos que $k = gr(G) + 1 - g$.

■

Pelos resultados acima, é interessante construir códigos sobre curvas com muitos pontos racionais. Aí entram as chamadas curvas maximais. Dizemos que uma curva $\mathcal{X}$ sobre $\mathbb{F}_q$ de gênero g é maximal se o número de pontos racionais de $\mathcal{X}$ atinge a cota de Hasse-Weil, ou seja, se o número de pontos racionais é igual a $q + 1 + 2g\sqrt{q}$.

CAPÍTULO 2

SEMIGRUPO DE WEIERSTRASS E CÓDIGOS SOBRE A CURVA $Y^Q + Y = X^{Q^R+1}$

A principal referência deste capítulo foi [8].

2.1 A curva $y^q + y = x^{q^r+1}$

Considere a curva $\mathcal{X}$ definida sobre $\mathbb{F}_{q^{2r}}$ pela equação afim

$$y^q + y = x^{q^r+1},$$

em que q é potência de um número primo e r é um inteiro ímpar. Vamos denotar tal curva por $\mathcal{X}_{q^{2r}}$. Observamos que quando $r = 1$, a curva $\mathcal{X}_{q^2}$ é a curva Hermitiana, que é uma curva muito importante no estudo de códigos AG e semigrupos de Weierstrass.

A curva $\mathcal{X}_{q^{2r}}$ tem gênero $g = q^r(q-1)/2$, possui um único ponto no infinito $P = (0 : 1 : 0)$, além de outros q^{2r+1} pontos racionais. Com esta quantidade de pontos, esta curva atinge a cota de Hasse-Weil e, portanto, é uma curva maximal. Estas informações podem ser verificadas na seção VI.4.1 do livro do Stichtenoth([10]).

2.2 Semigrupos de Weierstrass

Seja $\mathcal{X}$ uma curva nãosingular, projetiva, irredutivel, curva algebrica de gênero $g \geqslant 1$ sobre o corpo finito $\mathbb{F}_q$ e $\mathbb{F}_q(\mathcal{X})$ o corpo das funções racionais em $\mathcal{X}$. Seja P um ponto racional de $\mathcal{X}$ e $\mathbb{N}_0$ o conjunto dos números inteiros não negativos. O conjunto

$$H(P) := \{n \in \mathbb{N}_0; \exists\, f \in \mathbb{F}_q(\mathcal{X}) \; com \; (f)_\infty = nP\}$$

onde $(f)_\infty$ denota o divisor de pólos de f, é um semigrupo numérico, chamado o semigrupo de Weierstrass de $\mathcal{X}$ em P. O conjunto $G(P) = \mathbb{N}_0 \setminus H(P)$ é chamada de conjunto

de lacunas de Weierstrass de P e sua cardinalidade é g, como veremos a seguir.

Lema 2.2.1 *Seja P um ponto racional. Então, para qualquer $n \geq 2g$, existe uma função $f \in \mathbb{F}(\mathcal{X})$ com divisor de pólos da forma $(f)_\infty = nP$.*

Demonstração. Pelo Corolário 1.2.28, sabemos que $dim((n-1)P) = (n-1)grau(P) + 1 - g$ e $dim(nP) = n \cdot grau(P) + 1 - g$, assim $\mathcal{L}((n-1)P) \subsetneqq \mathcal{L}(nP)$. Qualquer elemento $f \in \mathcal{L}(nP) \setminus \mathcal{L}((n-1)P)$ tem divisor de pólos nP.

■

Teorema 2.2.2 *Sejam $\mathcal{X}$ uma curva de gênero g e P um ponto racional. Então existem exatamente g lacunas $i_1 < \cdots < i_g$ de P. Temos ainda que:*

$$i_1 = 1 \ e \ i_g \leqslant 2g - 1.$$

Demonstração. Qualquer número de lacunas de P é menor ou igual a $2g-1$ pelo Lema anterior, e claramente 0 é um polo. Temos a seguir uma caracterização do número de lacunas:

$$i \text{ é um lacuna de } P \Leftrightarrow \mathcal{L}((i-1)P) = \mathcal{L}(iP).$$

Considere a sequência de espaços vetorias:

$$K = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \cdots \subseteq \mathcal{L}((2g-1)P) \tag{2.1}$$

onde $dim\mathcal{L}(0) = 1$ e $dim\mathcal{L}((2g-1)P) = g$ pelo corolário 1.2.28. Observe que

$$dim\mathcal{L}(iP) \leqslant dim\mathcal{L}((i-1)P) + 1$$

para qualquer i, por um resultado em [10]. Então temos em 2.1 exatamente $g-1$ números $1 \leqslant i \leqslant 2g-1$ com $\mathcal{L}((i-1)P) \subsetneqq \mathcal{L}(iP)$. Os remanescentes g números são lacunas de P.

Finalmente, devemos mostrar que 1 é um gap. Suponha que não, então 1 é um polo de P. Como o números de polos formam um semigrupo aditivo, qualquer $n \in \mathbb{N}$ é um polo, e assim não há lacunas, e isso é uma contradição, pois $g > 0$.

■

No caso de dois pontos racionais distintos P_1 e P_2 em $\mathcal{X}$ temos o conjunto

$$H(P_1, P_2) := \{(n_1, n_2) \in \mathbb{N}_0^2; \exists \ f \in \mathbb{F}_q(\mathcal{X}) \ com \ (f)_\infty = n_1P_1 + n_2P_2\}$$

isto é, o semigrupo de Weierstrass de $\mathcal{X}$ em P_1 e P_2. Analogamente, o conjunto $G(P_1, P_2) = \mathbb{N}_0^2 \setminus H(P_1, P_2)$ é chamada de lacuna de Weierstrass do par (P_1, P_2). Ao contrário do caso pontual, a cardinalidade de $G(P_1, P_2)$ depende da escolha dos pontos P_1 e P_2, ver referência [3].

Agora introduziremos conceitos que serão importantes para este trabalho. Sejam P_1 e P_2 pontos racionais em $\mathcal{X}$. Definimos

$$\beta_\alpha := min\{\beta \in \mathbb{N}_0; (\alpha, \beta) \in H(P_1, P_2)\}.$$

onde $\alpha \in \mathbb{N}_0$.

Lema 2.2.3 *Para $\alpha \in G(P_1)$, tem se $(\gamma, \beta_\alpha) \notin H(P_1, P_2)$, para todo $\gamma < \alpha$. Ou seja, $\alpha = min\{\gamma; (\gamma, \beta_\alpha) \in H(P_1, P_2)\}$.*

Demonstração. Ver referência [2].
■

Com este resultado conseguimos

Proposição 2.2.4 *Seja β_α como no lema anterior. Então $\{\beta_\alpha; \alpha \in G(P_1)\} = G(P_2)$.*

Demonstração. O Lema anterior implica que $\beta_\alpha \notin H(P_2)$. De fato, suponha que $\beta_\alpha \in H(P_2)$. Como $(\alpha, \beta_\alpha) \in H(P_1, P_2)$, existe $f \in k(\mathcal{X})$ tal que $(f)_\infty = \alpha P_1 + \beta_\alpha P_2$. Se $\beta_\alpha \in H(P_2)$ temos que existe h tal que $(h)_\infty = \beta_\alpha P_2$, logo $\left(\frac{f}{h}\right)_\infty = \alpha P_1$ o que implica que $\alpha \in H(P_1)$, o que gera uma contradição com o lema anterior.

Temos também que $\beta_\alpha \neq \beta_\gamma$ se $\alpha \neq \gamma$. Assim, o conjunto $\beta_\alpha; \alpha \in G(P_1)$ está contido em $G(P_2)$ e sua cardinalidade é exatamente g. Portanto, devemos ter $\{\beta_\alpha; \alpha \in G(P_1)\} = G(P_2)$, como queriamos.
■

Assim, se $\alpha_1 < \alpha_2 < \cdots < \alpha_g$ e $\beta_1 < \beta_2 < \cdots < \beta_g$ são uma sequência de lacunas de Weierstrass em P_1 e P_2, respectivamente, então a relação acima implica que existe uma correspondência biunívoca entre $G(P_1)$ e $G(P_2)$. Portanto, existe uma permutação σ do conjunto $\{1, 2, \cdots, g\}$ tal que $\beta_{\alpha_i} = \beta_{\sigma(i)}$. Esta permutação é denotada por $\sigma(P_1, P_2)$.

Consideremos o conjunto

$$\Gamma(P_1, P_2) := \{(\alpha_i, \beta_{\alpha_i}); i = 1, 2, \cdots, g\} = \{(\alpha_i, \beta_{\sigma(i)}); i = 1, 2, \cdots, g\}.$$

Lema 2.2.5 *Seja Γ' um subconjunto de $(G(P_1) \times G(P_2)) \cap H(P_1, P_2)$. Se existe uma permutação τ de $i = \{1, 2, \cdots, g\}$ tal que $\Gamma' = \{(\alpha_i, \beta_{\tau(i)}); i = 1, 2, \cdots, g\}$, então $\Gamma' = \Gamma(P_1, P_2)$.*

Demonstração.
Da definição de $\sigma = \sigma(P, Q)$, temos que $\ell'_{\tau(i)} \leq \ell'_{\sigma(i)}$, para cada $i = 1, \ldots, g$. Logo, $\tau = \sigma$ e o resultado segue. ■

Dado $\Gamma(P_1, P_2)$, podemos computar $H(P_1, P_2)$ como segue. Dado $x = (\alpha_1, \beta_1), y = (\alpha_2, \beta_2) \in \mathbb{N}_0^2$ o menor limite superior de x e y, denotado por $lub(x, y)$, e é definido como

$$lub(x, y) := (max\{\alpha_1, \alpha_2\}, max\{\beta_1, \beta_2\}).$$

O resultado a seguir nos diz como podemos obter $H(P_1, P_2)$.

Lema 2.2.6 *Sejam P_1 e P_2 dois pontos racionais distintos. Então*

$$H(P_1, P_2) = \{lub(x, y); (x, y) \in \Gamma(P_1, P_2) \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2))\}.$$

Demonstração. Ver referência [3].
■

Pela igualdade dada no lema anterior, o conjunto $\Gamma(P_1, P_2)$ é chamado de *gerador minimal* do semigrupo $H(P_1, P_2)$.

Em [7], foi introduzido o conceito de curva castelo. Sejam $\sharp\mathcal{X}(\mathbb{F}_q)$ o número de pontos racionais de $\mathcal{X}$ e $H(P) = \{m_1 = 0 < m_2 < \ldots\}$. Se $H(P)$ é simétrico e $\sharp\mathcal{X}(\mathbb{F}_q) = m_2 q + 1$, então a curva $\mathcal{X}$ é chamada *curva Castelo.*

2.3 O Semigrupo de Weierstrass $H(P_0, P_\infty)$ para $\mathcal{X}_{q^{2r}}$

Seja $P_{a,b}$ a raiz comum de $x - a$ e $y - b$, onde $a, b \in \mathbb{F}_{q^{2r}}$. O divisor de $x - a$ e $y - b$ são dados, respectivamente, por

$$(x - a) = P_{a,b_1} + \cdots + P_{a,b_q} - qP_\infty, \tag{2.2}$$

onde $b_1, \cdots, b_q$ são as soluções em $\mathbb{F}_{q^{2r}}$ para a equação $y^q + y = a^{q^{r+1}}$, e

$$(y - b) = P_{a_1,b} + \cdots + P_{a_{q^{r+1}},b} - (q^r + 1)P_\infty, \tag{2.3}$$

onde $a_1, \cdots, a_{q^r+1}$ são soluções em $\mathbb{F}_{q^{2r}}$ para a equação $x^{q^r+1} = b^q + b$. Em particular, se $b^q + b = 0$, então $a_i = 0$ para todo i.

Assim $\langle q, q^r + 1\rangle \subseteq H(P_\infty)$. Como $g = \dfrac{q^r(q-1)}{2}$, segue que $H(P_\infty) = \langle q, q^r + 1\rangle$ é um semigrupo simétrico.

Assim, podemos concluir que $\mathcal{X}_{q^{2r}}$ é uma curva Castelo.

Seja $P_0 = P_{0,0}$. Na próxima proposição, computamos o semigrupo de Weierstrass $H(P_0)$.

Proposição 2.3.1 *O semigrupo de Weierstrass de $\mathcal{X}_{q^{2r}}$ em P_0 é*

$$H(P_0) = \langle q^r + 1 - q^{r-1}, q^r + 1 - (q^{r-1} - 1), \cdots, q^r, q^r + 1\rangle. \tag{2.4}$$

Demonstração. De (2.3) , $\left(\frac{x^{q^{r-1}-i}}{y}\right)_\infty = (q^r - q^{r-1} + i + 1)P_0$ para todo $0 \leqslant i \leqslant q^{r-1}$. Assim, $q^r - q^{r-1} + 1, q^r - q^{r-1} + 2, \cdots, q^r, q^r + 1 \in H(P_0)$, e então é sufuciente provar que o semigrupo $H = \langle q^r - q^{r-1} + 1, q^r - q^{r-1} + 2, \cdots, q^r, q^r + 1\rangle$ tem $g = \frac{q^r(q-1)}{2}$ lacunas. Mas o número de lacunas de H é $(q^r - q^{r-1}) + (q^r - 2q^{r-1} + (q^r - 3q^{r-1}) + \cdots + (q^r - (q-1)q^{r-1})) = q^r(q-1) - q^{r-1}(1 + 2 + \cdots + q - 1) = g$.
■

O próximo teorema completa o semigrupo de Weierstrass $H(P_0, P_\infty)$ para $\mathcal{X}_{q^{2r}}$.

Teorema 2.3.2 *Com notações como no Lema 2.2.6, tomando $P_1 = P_\infty$ e $P_2 = P_0$ temos que*

$$\Gamma(P_\infty, P_0) = \left\{ \gamma_{ij} : \begin{array}{l} 0 \leq j - 1 \leq -2 \text{ para } 1 \leq i \leq j \leq q - 1; \\ 0 \leq j - 1 \leq q - (s+1) \\ \text{para } (s-1)(q^{r-1} - 1) + q \leq j \leq s(q^{r-1} - 1) + q - 1 \\ \text{e } 1 \leq s \leq q - 1 \end{array} \right\},$$

onde $\gamma_{ij} := ((q - j + i - 1)(q^r + 1) - iq, (j - i)(q^r + 1) + i)$ e $(i, j) \in \mathbb{N}_0^2$.

Demonstração. Pelas condições de i e j segue que $(j_1 - i_1)((q^r + 1) + i_1) \neq (j_2 - i_2)((q^r + 1) + i_2)$ se $(i_1, j_1) \neq (i_2, j_2)$.

Entretanto, temos que o números de pares (i, j) é igual a $(1 + 2 + \cdots + (q-1)) + (q^{r-1} - 1)(1 + 2 + \cdots + (q-1)) = \frac{q^r(q-1)}{2} = g$.

Agora, vejamos que os números $(q - j + i - 1)(q^r + 1) - iq$ são lacunas em P_∞. Suponha que exista um par (i, j) tal que $(q - j + i - 1)(q^r + 1) - iq \in \langle q, q^r + 1\rangle$. Então, existe inteiros não negativos a e b tais que $aq + b(q^r + 1) = (q - j + i - 1)(q^r + 1) - iq$. Então, $(q - (j - i) - 1 - b)(q^r + 1) = (a + i)q$ é positivo e q divide $(q - (j - i) - 1 - b)$, o que é uma contradição.

De (2.4), se $(j-i)(q^r+1)+i \in H(P_0)$, então existem inteiros não negativos, $a_1, a_2, \cdots, a_{q^{r-1}+1}$ tal que $(j-i)(q^r+1)+i = a_1(q^r+1-q^{r-1}) + a_2(q^r+1-(q^{r-1}-1)) + \cdots + a_{q^{r-1}+1}(q^r+1)$, ou equivalentemente,

$$(j-i)(q^r+1) = (a_1 + a_2 + \cdots + a_{q^{r-1}+1})(q^r+1) - (a_1 q^{r-1} + a_2(q^{r-1}-1) + \cdots + a_{q^{r-1}} + i).$$

Pelas condições de $j-i$ acima, esta equação não é verdadeira. Portanto, $(j-i)(q^r+1)+i \in G(P_0)$.

Como $\left(\frac{x^{q^r+1-i}}{y^{j-i+1}}\right)_\infty = ((q-j+i-1)(q^r+1)-iq)P_\infty + ((j-i)(q^r+1)+i)P_0$, concluimos que $((q-j+i-1)(q^r+1)-iq, (j-i)(q^r+1)+i) \in (G(P_\infty) \times G(P_0)) \cap H(P_\infty, P_0)$ e o resultado

segue pelo Lema 2.2.5 e o fato de pares $((q-j+i-1)(q^r+1)-iq),(j-i)(q^r+1)+i)$ ser igual ao de g. ■

2.4 Comparando Códigos Pontuais e Bipontuais

O próximo resultado relaciona a lacuna de Weierstrass de um par de pontos com a distância mínima de um código bipontual correspondente.

Teorema 2.4.1 *Suponha que* $(a_1,a_2)\in G(P_1,P_2)$ *com* $a_1\geqslant 1$ *e* $dim(L(a_1P_1+a_2P_2))=dim(L((a_1-1)P_1+a_2P_2))$. *Suponha* $(b_1,b_2-t-1)\in G(P_1,P_2)$ *para todo* t, $0\leqslant t\leqslant min\{b_2-1,2g-1-(a_1+a_2)\}$. *Seja o conjunto* $G=(a_1+b_1-1)P_1+(a_2+b_2-1)P_2$, *e seja* $D=Q_1+\cdots+Q_n$, *onde* Q_i *são pontos racionais distintos, cada um não pertencente ao suporte de* G. *Se a dimensão de* $C_\omega=(D,G)$ *é positivo, então a distância mínima desse código é pelo menos* $grau(G)-2g+3$.

Demonstração. Tome $w=grau(G)-2g+2$. Se existe uma palavra código de peso w, então existe um diferencial $\eta\in\Omega(G-D)$ com exatamente w pólos simples $Q_1,\cdots,Q_w$. Temos então $(\eta)\geq G-(Q_1,\cdots,Q_w)$. Assim $2g-2=grau(\eta)\geq grau(G)-w=2g-2$. Segue então que

$$(\eta)=G-(Q_1+\cdots+Q_w).$$

Como $\ell(\alpha_1P_1+\alpha_2P_2)=\ell((\alpha_1-1)P_1+\alpha_2P_2)$, pelo Teorema de Riemann-Roch existe uma função racional

$$h\in\mathcal{L}(K-((\alpha_1-1)P_1+\alpha_2P_2))\backslash\mathcal{L}(K-(\alpha_1P_1+\alpha_2P_2))$$

Para qualquer divisor canônico K em $\mathcal{X}$. Assim, $(h)=((\alpha_1-1)P_1+\alpha_2P_2)-K+E$, onde E é um divisor efetivo de grau $2g-1-(\alpha_1+\alpha_2)$, onde P_1 não contido em seu suporte. Escreva $E=E'+tP_2$, onde E' é um divisor efetivo, na qual seu suporte não contém P_2 (então $0\leq t\leq grau(E)=2g-1-(\alpha_1+\alpha_2)$). Então podemos expressar o divisor de h como

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

Agora

$$G-(Q_1+\cdots+Q_w)=(\eta)\backsim K\backsim(\alpha_1-1)P_1+(\alpha_2+t)P_2+E'$$

Segue então que existe uma função racional f com divisor

$$(f)=-\gamma P_1-(\gamma_2-t-1)P_2+(Q_1+\cdots+Q_w)+E'.$$

Se $t\leqslant\gamma_2-1$, então f tem divisor de polos $(f)_\infty=\gamma_1P_1+(\gamma_2-t-1)P_2$, contradizendo o fato de $(\gamma_1,\gamma_2-t-1)\in G(P_1,P_2)$. Por outro lado, f tem divisor de pólos $(f)_\infty=\gamma P_1$, o que é uma contradição, pois γ_1 é uma lacuna em P_1.
■

Corolário 2.4.2 *Seja m um inteiro positivo com $q^{2r} - q^r + q^{r-1} < m < q^{2r}$. Dado um código pontual $C(D, mqP_\infty)$ em $\mathcal{X}_{q^{2r}}$, onde $D = \sum_{j=0}^{q^{2r+1}-1} P_j$ é a soma de todos os pontos racionais de $\mathcal{X}_{q^{2r}}$ com $P_j \neq P_\infty$, existe um código bipontual $C_\Omega(\overline{D}, G)$ com $supp(G) = \{P_\infty, P_0\}$ em $\mathcal{X}_{q^{2r}}$ tendo parâmetros relativos melhores do que $C(D, mqP_\infty)$ onde $\overline{D} = D - P_0$.*

Demonstração. Seja α um gerador de $\mathbb{F}_{q^{2r}}^*$ e seja m um inteiro positivo com $q^{2r} - q^r + q^{r-1} < m < q^{2r}$. Como $\mathcal{X}_{q^{2r}}$ é uma curva castelo, pela proposição 3.6 em [5] segue que a distância mínima de $C(D, mqP_\infty)$ é $d = q^{2r+1} - mq$. Por outro lado, a dimensão desse código é $k = mq - g + 1$.

Consideremos agora o código bipontual $C = C_\Omega(\overline{D}, (q^{2r+1} + 2g - mq - 4)P_\infty + P_0)$, onde $\overline{D} = D - P_0$. O código C tem comprimento $n = q^{2r+1} - 1$ e dimensão $k = mq - g + 1$. De fato, como $grau(G) < grau(D)$ temos que $dim(C) = dim(L(W - G + D)) = mq - g + 1$, onde W é um divisor canônico.

Pelo Teorema 2.4.1, $(2g - 1, 1) \in \Gamma(P_\infty, P_0)$. Então, $(\alpha, 1) \in G(P_\infty, P_0)$, para todo $1 \leq \alpha \leq 2g - 2$. Usando as notações do Teorema 2.4.1, tomando $a_1 = 2g - 2$, $b_1 = q^{2r+1-mq-1}$ e $a_2 = b_2 = 1$ temos que $t = 0$ e como não existe inteiros a e b tais que $q^{2r+1} - mq - 1 = aq + b(q^r + 1)$ então $(q^{2r+1} - mq - 1, 0) \in G(P_\infty, P_0)$. Assim, pelo Teorema 2.4.1, segue que a distância mínima de C é $q^{2r+1} - mq$. ■

O próximo resultado nos mostra como o conhecimento do semigrupo de Weierstrass $H(P_\infty, P_0)$ da curva $\mathcal{X}_{q^{2r}}$ pode ser usado para melhorar os parâmetros dos códigos correspondentes.

Teorema 2.4.3 *Sejam $G = (a_1 + b_1 - 1)P_\infty + (a_2 + b_2 - 1)P_0$ e $D = \sum_{i=1}^{n} P_i$ a soma de todos os outros pontos racionais em $\mathcal{X}_{q^{2r}}$. Considere o caso bipontual $C_\Omega = C_\Omega(D, G)$ com parâmetros $[n, k_\Omega, d_\Omega]$ e suponha que:*

i) $a_1 \geq 1$, $(a_1, a_2) \in G(P_\infty, P_0)$ e $dim(L(a_1P_\infty + a_2P_0)) = dim(L((a_1 - 1)P_\infty + a_2P_0))$;

ii) $(b_1, b_2 - c - 1)$, $(b_1 + 1, b_2 - c - 1)$, $(b_1 + q^r + 1, b_2 - c - 1)$, $(b_1, b_2 - c) \in G(P_\infty, P_0)$ para todo c, $0 \leq c \leq min\{b_2 - 1, 2g - 1 - (a_1 + a_2)\}$.

Sob essas condições, se $k_\Omega > 0$ então $d_\Omega \geq grau(G) - 2g + 4$.

Demonstração. Pelo Teorema 2.4.1, d_Ω é pelo menos $grau(G) - 2g + 3$. Suponha que $d_\Omega = grau(G) - 2g + 3$.

Se existe $c \in C_\Omega$ com $w(c) = d_\Omega$, então existe um diferencial $\omega \in \Omega(G - D)$ com exatamente d_Ω polos simples no conjunto $\{P_1, \cdots, P_n\}$. Sejam $P_{\omega_1}, \cdots, P_{\omega_{d_\Omega}}$ tais pontos. O grau $grau(\omega) = 2g - 2 = grau(G) - d_\Omega + 1$ então $div(\omega) = G - (P_{\omega_1} + \cdots + P_{\omega_{d_\Omega}}) + P$,

onde $P \in supp(D) \setminus \{P_{\omega_1}, \cdots, P_{\omega_{d_\Omega}}\}$.

Utilizando o Teorema de Riemann-Roch na hipótese (i), para um divisor canônico W, temos

$$dim(L(W - a_1P_\infty + a_2P_0)) = dim(L(W - (a_1 - 1)P_\infty + a_2P_0)) - 1$$

Então, $L(W - a_1P_\infty + a_2P_0) \neq L(W - (a_1 - 1)P_\infty + a_2P_0)$. Assim, existe uma função racional tal que $div(f) = (a_1 - 1)P_\infty + (a_2 + c)P_0 - W + E$, onde E é um divisor efetivo com $P_0,\ P_\infty \notin supp(E)$, e $0 \leqslant c \leqslant 2g - 1 - (a_1 + a_2)$.

Então, $div(\omega) \sim W \sim (a_1 - 1)P_\infty + (a_2 + c)P_0 + E$ e existe uma função racional g tal que $div(g) = -b_1P_\infty - (b_2 - c - 1)P_0 - P + (P_{\omega_1} + \cdots + P_{\omega_{d_\Omega}}) + E$. Mas isso é impossível porque se $c \leqslant b_2 - 1$ e $P \in supp(E)$, então $div_\infty(g) = b_1P_\infty + (b_2 - c - 1)P_0$, contradizendo o fato de que $(b_1, b_2 - c - 1) \in G(P_\infty, P_0)$.

Se $P = P_\infty$ então $div_\infty(g) = (b_1 + 1)P_\infty + (b_2 - c - 1)P_0$, contradizendo o fato de que $(b_1 + 1, b_2 - c - 1) \in G(P_\infty, P_0)$. O mesmo ocorre se $P = P_\infty$. Finalmente, se $P = P_{a,b}$ para algum $P_{a,b} \neq \{P_{\omega_1}, \cdots, P_{\omega_{d_\Omega}}\}$, como $div(y - b) = P_{a,b} + \sum_\alpha P_{\alpha,b} - (q^r + 1)P_\infty$, temos que $div_\infty(g(y - b)) = (b_1 + q^r + 1)P_\infty + (b_2 - c - 1)P_0$, contradizendo o fato $(b_1 + q^r + 1, b_2 - c - 1) \in G(P_\infty, P_0)$.

Portanto, $d_\Omega \geq grau(G) - 2g + 4$.

■

Observação 2.4.4 *Por [4] existe um automorfismo σ de $\mathcal{X}_{q^{2r}}$ tal que $\sigma(P_0) = P_{0,b}$, onde $b \in \mathbb{F}_{q^{2r}}$ corre sobre as raízes de $y^{q-1} + 1 = 0$. Assim os resultados das seções anteriores também são válidos para qualquer par $(P_\infty, P_{0,b})$.*

Exemplo 2.4.5 *Tomando $q = 2$ e $r = 5$, obtemos a curva $y^2 + y = x^{33}$ cujo gênero é $g = \dfrac{2^5(2-1)}{2} = 16$ sobre $\mathbb{F}_{2^{2\cdot 5}} = \mathbb{F}_{1024}$ os semigrupos de Weierstrass e seus respectivos conjunto de gaps são dados por*

i) $H(P_\infty) = \langle 2, 2^5+1\rangle = \langle 2, 33\rangle$ *e* $G(P_\infty) = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$.

ii) $H(P_0) = \langle 2^5+1, -2^4, 2^5+1-(2^4-1), 2^5+1-(2^4-2), \cdots, 2^5, 2^5+1\rangle = \langle 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33\rangle$ *e* $G(P_0) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$

Pelo Teorema 2.3.2, temos $\Gamma(P_\infty, P_0) = \{(31, 1), (29, 2), (27, 3), (25, 4), (23, 5), (21, 6), (19, 7), (17, 8), (15, 9), (13, 10), (11, 11), (9, 12), (7, 13), (5, 14), (3, 15), (1, 16)\}$ *e pelo Lema 2.2.6*

$$H(P_\infty, P_0) = \{lub(x,y); x, y \in \Gamma(P_\infty, P_0) \cup (H(P_\infty) \times \{0\}) \cup (\{0\}) \times H(P_0)\}.$$

Para estes valores de q e r não foi possível encontrar valores para a_1, a_2, b_1 e b_2 que satisfizessem o Teorema 2.4.3.

Exemplo 2.4.6 *Tome $q = 3$ e $r = 3$ e consideremos a curva $y^3 + y = x^{28}$ de gênero $g = 27$ sobre $\mathcal{X}_{729}$. O semigrupo de Weierstrass são como segue:*

- $H(P_\infty) = \langle 3, 28\rangle$ *,assim* $G(P_\infty) = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53\}$;

- $H(P_0) = \langle 19, 20, 21, 22, 23, 24, 25, 26, 27, 28\rangle$ *,assim* $G(P_0) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 29, 30, 31, 32, 33, 34, 35, 36, 37\}$

Assim pelo 2.3.2, obtemos $\Gamma(P_\infty, P_0) = \{(53, 1), (25, 29), (50, 2), (22, 30), (47, 3), (19, 31), (44, 4), (16, 32), (41, 5), (13, 33), (38, 6), (10, 34), (35, 7), (7, 35), (32, 8), (4, 36), (29, 9), (1, 37), (26, 10), (23, 11), (20, 12), (17, 13), (14, 14), (11, 15), (8, 16), (5, 17), (2, 18)\}$ *e pelo lema 2.2.6 obtemos*

$$H(P_\infty, P_0) = \{lub(x,y); x, y \in \Gamma(P_\infty, P_0) \cup (H(P_\infty) \times \{0\}) \cup (\{0\}) \times H(P_0)\}.$$

Considere o código pontual $C(D, 2171P_\infty)$. Os parâmetros de $C(D, 2171P_\infty)$ são: $n = q^{2r+1} = 2187, k = 2171 - g + 1 = 2145$ e $d = q^{2r+1} - 2171 = 16$, assim $C(D, 2171P_\infty)$ é um código$-[2187, 2145, 16]$.
Considere agora o código bipontual $C_\Omega(D, 76P_\infty + P_0)$, onde $76 = q^{2r+1} + 2g - 2171 - 4$. Seu comprimento é $n = q^{2r+1} - 1 = 2186$ e sua dimensão é $k_\Omega = 2145$. Tomando $a_1 = 52$, $b_1 = 25$, e $a_2 = b_2 = 1$ no Teorema 2.4.3, temos que $d_\Omega \geq 27$.

Exemplo 2.4.7 *Considerando $q = 3$ e $r = 5$ teremos a curva $y^3 + y = x^{244}$ de gênero $g = \dfrac{3^5(3-1)}{2} = 243$ sobre o corpo $\mathbb{F}_{32768}$. O semigrupo de Weierstrass e o conjunto dos gaps estão determinados assim:*

1) $H(P_\infty) = \langle 3, 244\rangle$ *e* $G(P_\infty) = \{1, 2, 4, 5, 7, 8, \cdots, 241, 242, 245, 248, \cdots, 482, 485\}$

2) $H(P_0) = \langle 163, 164, \cdots, 243, 244\rangle$ *e* $G(P_0) = \{1, 2, 3, \cdots, 161, 162, 245, 246, \cdots, 322, 323, 324, 325\}$

Do Teorema 2.3.2, tiramos as seguintes condições: $0 \leqslant j - i \leqslant 1$ para $1 \leqslant i \leqslant j \leqslant 2$. $0 \leqslant j - i \leqslant 3 - (s + 1)$ para $80(s - 1) + 3 \leqslant j \leqslant 80s + 2$, com $1 \leqslant s \leqslant 2$. Então, para $s = 1$ temos $3 \leqslant j \leqslant 82$ e $0 \leqslant j - i \leqslant 1$, e para $s = 2$, temos $83 \leqslant j \leqslant 162$ e $i = j$.

Assim, $\Gamma(P_\infty, P_0) = \{(485, 1), (241, 245), (482, 2), (238, 246), (479, 3), (235, 247), (476, 4), (232, 248), (473, 5), (229, 249), (470, 6), (226, 250), (467, 7), (223, 251), (464, 8), (220, 252),$

$(461,9),(217,253),(458,10),(214,254),(455,11),(211,255),(452,12),(208,256),(449,13),$
$(205,257),(446,14),(202,258),\cdots\}$

O Lema 2.2.6 nos dá a caracterização do semigrupo $H(P_\infty,P_0)$*:*

$$H(P_\infty,P_0)=\{lub(x,y);x,y\in\Gamma(P_\infty,P_0)\cup(\langle 3,244\rangle)\times\{0\})\cup(\{0\})\times\langle 163,164,\cdots,244\rangle\}.$$

Seja o código pontual $C(D,177000P_\infty)$ *cujos parâmetros são:* $n=3^{2\cdot 5+1}=3^{11}=177147$*,* $k=177000-243+1=176758$ *e* $d=3^{11}-177000=147$*. Logo,* $C(D,177000P_\infty)$ *é um* $[177147,176758,147]$*-código.*

Tomando o código bipontual $C_\Omega(D,629P_\infty+P_0)$*, onde* $629=3^{11}+2\cdot 243-177000-4$*. Seu comprimento é* $n=3^{11}-1=177146$ *e sua dimensão é* $k_\Omega=176758$*. Tomando* $a_1=482$*,* $b_1=238$*,* $a_2=b_2=1$ *no Teorema 2.4.3, obtemos* $d_\Omega\geq 148$*.*

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Hefez, A. e Villela, M., *Códigos Corretores de Erros, IMPA, Rio de Janeiro 2008.*

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

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

[4] Kondo S., Katagiri T., Ogihara T. , *Automorphism group of one-point codes from the curves* $y^q + y = x^{q^r+1}$*, IEEE Trans. Inform. Theory, 47, (2001), 2573-2579.*

[5] Matthews G. L. , *Weierstrass pairs and minimum distance of Goppa codes. J. Designs. Codes and Cryptography, 22 (2001), 107-121.*

[6] Matthews G. L. , - *Codes from the suzuki function field, IEEE Transactions on Information Theory, 50(12) (2004), 3298-3302 .*

[7] Munuera C., Sepúlveda A. and Torres F.- *Castle Curves and Codes. Advances in Mathematichs of communications, 3 (2009), 399-408.*

[8] Sepúlveda A. and Tizziotti G.- *Weierstrass Semigroup and Codes Over the Curve* $y^q + y = x^{q^r+1}$*. Advances in Mathematichs of communications, vol 8 , 67-72 (2014).*

[9] Silva, T. R. - *Bases de Gröbner e a Geometria Algébrica na Teoria de Códigos Corretores de Erros . 2015. 48p Dissertação de Mestrado. UFU, Uberlândia-MG.*

[10] Stichtenoth H. , *Algebraic Function Fields and Codes, Springer, Berlim, 1993.*

[11] Tsfasman M., Vladut S. and Nogin D. *Algebraic Geometric Codes: Basic Notions, American Mathematical Society, Providence, 2007.*

[12] van Lint J. H. *Introduction to Coding Theory, Springer, New York, 1982.*

[13] van Lint J. H., Hoholdt T. and Pellikann R. *Algebraic Geometric Codes, Elsevier, Handbook of Coding Theory, Amsterdam, 1998.*