Universidade Estadual de Campinas
Faculdade de Engenharia Elétrica e de Computação
Departamento de Telemática

Forma Combinada da Conjunto de Sinais e Códigos de Goppa Através da Geometria Algébrica

Jéfferson Luiz Rocha Bastos

Tese de Doutorado

Orientador: **Prof. Dr. Reginaldo Palazzo Jr.**

Banca Examinadora:
Prof. Dr. Reginaldo Palazzo Jr. - FEEC/UNICAMP
Prof. Dr. Eduardo Brandani da Silva - UEM
Prof. Dr. Fernando E. Torres Orihuela - IMECC/UNICAMP
Prof. Dr. Givaldo Oliveira dos Santos - CEFET/ALAGOAS
Prof. Dr. Renato da Rocha Lopes - FEEC/UNICAMP
Prof. Dr. Trajano Pires da Nóbrega Neto - IBILCE/UNESP

Tese apresentada na Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas, como parte dos requisitos exigidos para a obtenção do título de Doutor em Engenharia Elétrica.

13 de Setembro de 2007
Campinas - SP

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA - BAE - UNICAMP

Bastos, Jéfferson Luiz Rocha
B321 Forma combinada de conjunto de sinais e códigos de Goppa através da geometria algébrica. / Jéfferson Luiz Rocha Bastos. – Campinas, SP: [s.n.], 2007.

Orientador: Reginaldo Palazzo Junior.
Tese (doutorado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Riemann, Superfícies de. 2. Curvas algébricas. 3. Geometria algébrica. I. Palazzo Junior, Reginaldo Palazzo. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título

Título em Inglês:	Combined form of signal set and Goppa code using algebraic geometry
Palavras-chave em Inglês:	Riemann surface, Algebraic curves, Goppa codes, Modulation
Área de concentração:	Engenharia de Computação
Titulação:	Doutor em Engenharia Elétrica
Banca Examinadora:	Eduardo Brandani da Silva, Fernando E. Torres Orihuela, Givaldo Oliveira dos Santos, Renato da Rocha Lopes, Trajano Pires da Nóbrega Neto
Data da defesa:	13/09/2007
Programa de Pós-Graduação:	Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE DOUTORADO

Candidato: Jéfferson Luiz Rocha Bastos

Data da Defesa: 13 de setembro de 2007

Título da Tese: "Forma Combinada de Conjunto de Sinais e Códigos de Goppa através da Geometria Algébrica"

Prof. Dr. Reginaldo Palazzo Júnior (Presidente): _____

Prof. Dr. Givaldo Oliveira dos Santos: _____

Prof. Dr. Eduardo Brandani da Silva: _____

Prof. Dr. Trajano Pires da Nóbrega Neto: _____

Prof. Dr. Fernando Eduardo Torres Orihuela: _____

Prof. Dr. Renato da Rocha Lopes: _____

Resumo

Tendo como base trabalhos recentes que associam o desempenho de sistemas de comunicação digital ao gênero de uma superfície compacta de Riemann, este trabalho tem como objetivo propor uma integração entre modulação e codificação de canal, tendo como base o gênero da superfície. Para atingir tais objetivos, nossa proposta é a seguinte: fixado um gênero g ($g = 0, 1, 2, 3$), encontrar curvas com este gênero e fazer uma análise dos parâmetros dos códigos associados a esta curva, a fim de se obter uma modulação e um sub-código desta modulação para ser utilizado na codificação de canal.

Palavras-chave: superfície de Riemann, curvas algébricas, códigos de Goppa, modulação.

Abstract

Based on recent research showing that the performance of bandwidth efficent communication systems also depends on the genus of a compact Riemann surface in which the communication channel is embedded, this study aims at proposing a combined form of modulation and coding technique when only the genus of a surface is given to the communication system designer. To achieve this goal, the following procedure is proposed. Knowing that the channel is embedded in a surface of genus g, find algebraic curves with the given genus which will give rise to the modulation system, an $(n, n, 1)$ type of code, and from this find the best (n, k, d) subcode, to be employed in the aforementioned combined form.

Keywords: Riemann surface, algebraic curves, Goppa codes, modulation.

Agradecimentos

Ao meu orientador, Professor Reginaldo Palazzo Jr., sou grato pela orientação, pelas discussões e pelo incentivo dado neste período.

Aos membros da banca examinadora: Prof. Dr. Eduardo Brandani da Silva, Prof. Dr. Fernando Torres, Prof. Dr. Givaldo Oliveira dos Santos, Prof. Dr. Renato da Rocha Lopes e Prof. Dr. Trajano Pires da Nóbrega Neto.

Ao Departamento de Matemática do IBILCE/UNESP pelo apoio irrestrito durante este período.

À minha família pela torcida constante.

Aos meus amigos, que sempre tinham uma palavra de carinho e que me ajudaram a me distrair nos momentos mais difíceis.

À minha esposa, que foi a pessoa que mais sofreu durante o período, pois teve que aguentar meu mau humor, minhas crises e ainda assim sempre me incentivou e me ajudou a superar problemas. Agradeço pelo carinho, pelas cobranças e acima de tudo pelo amor que me dedicou nas horas mais complicadas.

Sumário

Lista de Tabelas

Lista de Símbolos

$k[X,Y]$	-	Anel dos polinômios em duas indeterminadas sobre o corpo k
$k[X,Y,Z]$	-	Anel dos polinômios em três indeterminadas sobre o corpo k
$F_*(X,Y)$	-	Desomogeneização do polinômio $F(X,Y,Z)$
$f^*(X,Y,Z)$	-	Homogeneização do polinômio $f(X,Y)$
$\mathbb{P}^2(k)$	-	Plano projetivo sobre o corpo k
$\mathcal{X},\ \mathcal{C}$	-	Curvas planas projetivas
$\mathcal{X}_F$	-	Curva plana projetiva definida pelo polinômio F
$g(\mathcal{X})$	-	Gênero da curva $\mathcal{X}$
$F_X,\ F_Y,\ F_Z$	-	Derivadas parciais do polinômio F em relação às variáveis $X,\ Y,\ Z$
$I(P,F,G)$	-	Multiplicidade de intersecção das curvas $\mathcal{X}_F$ e $\mathcal{X}_G$ no ponto P
$\mathcal{X}(K)$	-	Conjunto dos K-pontos racionais da curva $\mathcal{X}$
$\sigma_{p,n}$	-	Automorfismo de Frobenius
D	-	Divisor
$deg(D)$	-	Grau do divisor D
$Supp(D)$	-	Suporte do divisor D
$\mathbb{F}_q(\mathcal{X})$	-	Corpo das funções racionais da curva $\mathcal{X}$
$div(f)$	-	Divisor da função racional f
$\mathcal{L}(D)$	-	Espaço vetorial das funções racionais associadas ao divisor D
$\mathcal{C}(\mathcal{X},\mathcal{P},D)$	-	Código algébrico-geométrico associado à $\mathcal{X}$, ao conjunto $\mathcal{P}$ e ao divisor D
$>_{lex}$	-	Ordem lexicográfica
$>_{grlex}$	-	Ordem lexicográfica graduada
$>_{grevlex}$	-	Ordem lexicográfica graduada reversa
$LC(f)$	-	Coeficiente líder do polinômio f
$LM(f)$	-	Monômio líder do polinômio f
$LT(f)$	-	Termo líder do polinômio f
$P_*(X)$	-	Desomogeneização do polinômio $P(X,Y)$
$p^*(X,Y)$	-	Homogeneização do polinômio $p(X)$
$\mathbb{P}_K$	-	Reta projetiva associada ao corpo K
$K(\mathbb{P}_K)$	-	Corpo das funções racionais associadas a $\mathbb{P}_K$
υ_{P_1}	-	Função valoração associada ao elemento $P_1 \in \mathbb{P}_K$
$gr(D)$	-	Grau do divisor D
$\varphi(P)$	-	Valor da função φ no elemento P
$C(D,E)$	-	Código de Goppa associado aos divisores $D,\ E$
$\mathcal{X} \cap X$	-	Conjunto dos pontos da curva $\mathcal{X}$ com $X = 0$
$\mathcal{X} \cap Y$	-	Conjunto dos pontos da curva $\mathcal{X}$ com $Y = 0$
$\mathcal{X} \cap Z$	-	Conjunto dos pontos da curva $\mathcal{X}$ com $Z = 0$

Capítulo 1

Introdução

Na busca por projetar sistemas de comunicações mais confiáveis e menos complexos, espaços métricos provenientes de espaços vetoriais foram associados a cada um dos blocos do diagrama de blocos de um sistema de comunicação tradicional (veja figura I).

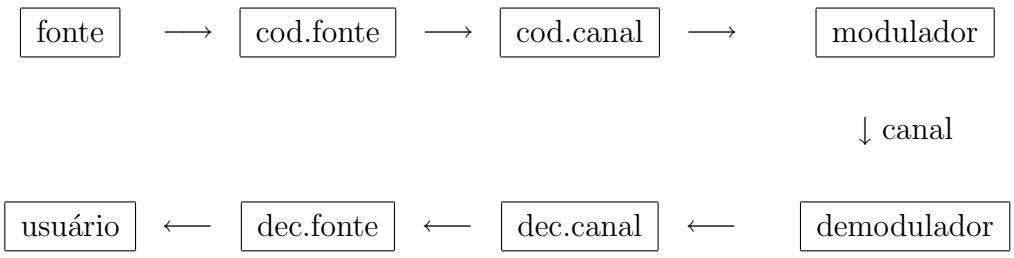

Figura I-Modelo tradicional de um sistema de comunicação digital

Posteriormente, novas associações foram feitas, como por exemplo a utilização de espaços topológicos [1]. Desta forma, novos conceitos matemáticos passaram a ter importância no estudo de sistemas de comunicação. Baseados na informação de que sistemas de comunicações utilizando o canal discreto sem memória $C_{2,8}[8,2]$ (quantização de 3 bits) apresentam melhor desempenho do que sistemas de comunicações utilizando o canal discreto sem memória $C_{2,2}[2,2]$ (quantização de 1 bit), trabalhos recentes (ver [1], [2]) mostraram que quanto maior o gênero da superfície no qual o canal pode ser mergulhado, melhor o desempenho do sistema. Uma das motivações dos trabalhos citados anteriormente foi perceber que o canal $C_{2,8}[8,2]$, que é um dos canais mais utilizados em sistemas de comunicações, pode ser mergulhado em superfícies com gênero $g = 0, 1, 2, 3$, enquanto que o canal $C_{2,2}[2,2]$ só pode ser mergulhado em uma superfície com gênero $g = 0$. A partir de então, um novo conceito passa a ser de interesse no estudo de sistemas de comunicações: o gênero de uma superfície.

Os códigos de Goppa, ou códigos algébrico-geométricos, formam uma classe de códigos com

um bom desempenho e estão associados a curvas algébricas. Um dos conceitos fundamentais no estudo de curvas é o conceito de gênero da curva. Curvas algébricas e superfícies de Riemann estão relacionadas através do gênero (da curva ou da superfície). Em [3] é mostrado que:

- os pólos e os zeros de funções racionais de curvas com gênero $g = 0$ estão distribuídas na superfície de uma esfera (superfície de Riemann de gênero 0), assim como os códigos de Slepian;
- os pólos e os zeros de funções racionais de curvas com gênero $g = 1$ estão distribuídas na superfície de um toro (superfície de Riemann de gênero 1), assim como os códigos reticulados.

Da associação entre gênero de curvas e gênero de superfícies nos quais os canais podem ser mergulhados, surgiu a motivação do trabalho aqui apresentado. Nosso objetivo é propor um sistema de comunicação digital baseado em um único parâmetro: o gênero da superfície. Para isso, a proposta é fazer uma combinação entre modulação e codificação de canal, isto é, fixado o gênero da superfície na qual o canal será mergulhado, buscar códigos que estejam associados a uma curva de mesmo gênero, que sirvam de moduladores, e subcódigos destes códigos, que possam servir para a codificação de canal. Dividimos esta tarefa nas seguintes etapas:

- Fixado um gênero g ($g = 0, 1, 2, 3$), procurar curvas com este gênero e fazer uma análise dos parâmetros dos códigos de Goppa associados a estas curvas;
- Verficar se, para um dado gênero, é possível conseguir uma curva que forneça um código de Goppa que sirva como uma modulação e também subcódigos deste código que possam ser usados na codificação de canal;
- Verificar se os subcódigos buscados para a codificação de canal podem formar uma partição do modulador, a fim de construir códigos multiníveis.

O trabalho está organizado da seguinte maneira:

No capítulo A, são apresentados os conceitos e resultados fundamentais da teoria de curvas algébricas que serão necessários para a compreensão do que será desenvolvido nos capítulos seguintes. Neste capítulo também é apresentada uma parte da teoria de bases de Groebner, utilizada na determinação de bases para os espaços vetoriais associados a curvas e divisores. Não são apresentadas demonstrações dos resultados. Para os interessados nestas demonstrações, recomendamos a leitura de [4], [5], [6] e [7].

No capítulo 2, desenvolvemos a teoria de códigos de Goppa racionais, que são códigos associados a curvas de gênero 0. Estes códigos são tratados de uma forma diferente da forma

como serão tratados os códigos provenientes de curvas com gênero $g = 1, 2, 3$ e assim, uma descrição simples desta forma é feita na primeira seção. Ao final do capítulo é apresentado um algoritmo para a obtenção de subcódigos com máxima distância de separação (MDS) de um código racional com parâmetros $(n, n, 1)$.

No capítulo 3, tratamos dos códigos provenientes de curvas com gênero 1. Inicialmente, apresentamos dois exemplos de códigos sobre $\mathbb{F}_4$, um deles associado à curva Hermitiana e outro associado à curva de Hurwitz generalizada. Estes exemplos servem para termos idéia das dificuldades que podem surgir, visto que no primeiro podemos trabalhar com divisores com um único ponto base e no segundo precisamos de divisores com dois pontos base. Para finalizar o capítulo, apresentamos um resultado onde são derivados os parâmetros de todos os códigos provenientes de curvas maximais de gênero 1 com divisores da forma $D = rP_\infty$.

No capítulo 4, apresentamos dois exemplos de códigos: um originário de uma curva de gênero 2 e outro de uma curva de gênero 3. Neste capítulo não foi possível apresentar uma generalização, pois não se conhecem muitas curvas maximais com gênero 2 e 3. No final do capítulo, veremos que os códigos de Goppa podem ser utilizados na construção de códigos multiníveis, que é uma maneira de se fazer concatenação de códigos, visando a obtenção de códigos com comprimentos grandes a partir de códigos menores.

No capítulo 5, apresentamos as conclusões e fornecemos algumas propostas de trabalhos futuros.

Capítulo 2

Códigos de Goppa Racionais

Neste capítulo, iremos analisar os códigos de Goppa racionais, códigos estes provenientes de curvas com gênero $g = 0$. Estes códigos são sempre códigos com máxima distância de separação, isto é, códigos MDS, mas seus subcódigos podem não apresentar esta propriedade. Assim sendo, apresentaremos também um processo para construção de subcódigos MDS de códigos racionais. Veremos também que é possível utilizar códigos racionais para a construção de códigos multiníveis. Neste capítulo, usaremos uma abordagem diferente da que será utilizada nos demais capítulos, já que aqui não precisaremos da equação da curva para a construção dos códigos. Entretanto, será necessário o conhecimento e o entendimento de alguns conceitos de geometria algébrica tais como polinômios homogêneos, funções racionais, divisores e espaços vetoriais associados a divisores.

Este capítulo está organizado da seguinte forma. As Seções 2.1 e 2.2 contêm os conceitos necessários para o entendimento da abordagem utilizada neste capítulo. Na Seção 2.3 serão apresentados alguns exemplos de códigos racionais, dentre eles os códigos de Reed-Solomon. Por meio desses exemplos, veremos que os subcódigos de códigos racionais podem não ser MDS. Na Seção 2.4, apresentaremos um processo para a construção de subcódigos MDS de códigos racionais.

2.1 Conceitos Preliminares

Sejam k um corpo e $k[X, Y]$ o anel de polinômios em duas indeterminadas sobre k. Nesta seção, veremos alguns conceitos e resultados sobre polinômios em duas variáveis que nos serão úteis para a definição dos códigos de Goppa racionais.

Um **polinômio homogêneo** de grau r, ou uma **forma** de grau r, é o polinômio nulo ou um polinômio em que todos os monômios possuem grau r. Todo polinômio homogêneo de grau

r pode ser escrito na forma

$$P(X,Y) = a_0X^r + a_1X^{r-1}Y + ... + a_{r-1}XY^{r-1} + a_rY^r = \sum_{j=0}^{r} a_jX^{r-j}Y^j,\ a_j \in k.$$

Neste caso, vamos considerar o polinômio nulo como polinômio homogêneo de qualquer grau. Uma forma é dita **regular** se não for divisível por Y.

Mais adiante precisaremos de formas que sejam irredutíveis. A proposição a seguir nos fornece uma condição para saber se uma forma é ou não irredutível.

Proposição 2.1.1 ([4]) *Seja $P \in k[X,Y]$, P não constante e uma forma regular. Então P é irredutível em $k[X,Y]$ se, e somente se, $P_* = P(X,1)$ é irredutível em $k[X]$.*

Observação 2.1.1 *Seja $p(X) \in k[X]$ um polinômio de grau r. O polinômio*

$$P(X,Y) = p^*(X,Y) = Y^r p(\frac{X}{Y}),$$

*é um polinômio homogêneo de grau r. Este processo de obtenção de polinômios homogêneos é chamado de **homogeneização**.*

Uma forma de grau r P é **mônica** se P_* é um polinômio mônico, isto é, se

$$P_*(X) = P(X,1) = X^r + a_1X^{r-1} + ... + a_r.$$

O teorema a seguir nos mostra que toda forma em duas variáveis pode ser fatorada como produto de formas mônicas regulares, além do polinômio Y. Esta decomposição será importante para o entendimento dos elementos do corpo das funções racionais e de divisores associados a estes elementos.

Teorema 2.1.1 ([4]) *Seja $P \in k[X,Y]$, $P \notin k$ uma forma. Existem um único elemento $a \in k^* = k - \{0\}$, um único número natural r, formas mônicas regulares e irredutíveis $P_1, ..., P_s \in k[X,Y]$ duas-a-duas distintas e inteiros positivos $n_1, ..., n_s$ tais que os pares (P_i, n_i) são univocamente determinados, a menos de ordem, satisfazendo*

$$P = aY^r P_1^{n_1} ... P_s^{n_s}.$$

2.2 Funções Racionais, Divisores e Códigos de Goppa

Nesta seção, apresentaremos alguns conceitos de geometria algébrica que são necessários para a definição e entendimento dos códigos racionais.

A **reta projetiva** associada ao corpo k é o conjunto

$$\mathbb{P}_k = \{P \in k[X,Y];\ P \text{ forma mônica irredutível }\}.$$

Da Proposição 2.1.1, temos que $\mathbb{P}_k$ é formado pelo polinômio (variável) Y e por todas as formas regulares $P \in k[X,Y],\ P \notin k$, tais que P_* é mônico e irredutível.

Definimos o **corpo das funções racionais** de $\mathbb{P}_k$ como sendo

$$K(\mathbb{P}_k) = \left\{ \frac{F}{G};\ F, G \text{ formas de mesmo grau},\ G \neq 0 \right\}.$$

Observação 2.2.1 *Seja $\varphi \neq 0$ em $K(\mathbb{P}_k)$. Sabemos então que existem formas F, G de mesmo grau tais que*

$$\varphi = \frac{F}{G}.$$

Usando o Teorema 2.1.1 e considerando que $Y \in \mathbb{P}_k$, podemos escrever

$$F = a_1 \prod_{P \in \mathbb{P}_k} P^{r_P},\ G = a_2 \prod_{P \in \mathbb{P}_k} P^{s_P},$$

com r_P, s_P não nulos somente para um número finito de elementos $P \in \mathbb{P}_k$. Dessa forma,

$$\varphi = \frac{a_1 \prod_{P \in \mathbb{P}_k} P^{r_P}}{a_2 \prod_{P \in \mathbb{P}_k} P^{s_P}} = \frac{a_1}{a_2} \prod_{P \in \mathbb{P}_k} P^{r_P - s_P} = a \prod_{P \in \mathbb{P}_k} P^{n_P},$$

com $n_P \neq 0$ somente para um número finito de elementos $P \in \mathbb{P}_k$.

Tendo como base a observação anterior, dado um elemento qualquer $P_1 \in \mathbb{P}_k$, podemos definir uma **função valoração** em $K(\mathbb{P}_k) \setminus \{0\}$ da seguinte forma:

$$\begin{array}{rcl} v_{P_1} : K(\mathbb{P}_k) \setminus \{0\} & \longrightarrow & \mathbb{Z} \\ \varphi = P_1^{n_1}(a \prod\limits_{P \neq P_1} P^{n_P}) & \longmapsto & v_{P_1}(\varphi) = n_1. \end{array} \tag{2.1}$$

Esta função será utilizada posteriormente na definição de grau de divisores.

Um **divisor** em $\mathbb{P}_k$ é uma soma formal de um número finito de elementos de $\mathbb{P}_k$ com coeficientes inteiros. Assim, todo divisor é uma expressão da forma

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

onde n_P são inteiros diferentes de 0 somente para um número finito de $P's$. Esses inteiros são chamados **peso** de D em P e é denotado por $\upsilon_P(D)$. Assim, podemos escrever

$$D = \sum_{P \in \mathbb{P}_k} \upsilon_P(D)P.$$

Dados dois divisores $D = \sum_{P \in \mathbb{P}_k} n_P P$ e $D' = \sum_{P \in \mathbb{P}_k} m_P P$, dizemos que D é **maior ou igual** a D', denotado por $D \geq D'$, se $n_P \geq m_P$. Um divisor $D \geq 0$ (0 é o divisor nulo) é chamado **divisor positivo**.

Um divisor é **primo** se for da forma $D = 1P = P$. Dado um divisor qualquer $D = \sum_{P \in \mathbb{P}_k} \upsilon_P(D)P$, o **suporte** do divisor é o conjunto formado pelos elementos $P \in \mathbb{P}_k$ que aparecem na expressão do divisor D com coeficientes não nulos. Assim,

$$Supp(D) = \{P \in \mathbb{P}_k |\ \upsilon_P(D) \neq 0\}.$$

Definimos também o **grau** de um divisor D como sendo

$$gr(D) = \sum_{P \in \mathbb{P}_k} \upsilon_P(D) gr(P),$$

onde $gr(P)$ é o grau de P como um polinômio.

Dada uma função racional $\varphi \in K(\mathbb{P}_k) \setminus \{0\}$, o **divisor associado** a esta função racional é

$$div(\varphi) = \sum_{P \in \mathbb{P}_k} \upsilon_P(\varphi)P.$$

onde $\upsilon_P(\varphi)$ é a função valoração definida em (2.1). Não definimos $div(0)$.

Seja D um divisor em $\mathbb{P}_K$. O **espaço vetorial associado** a D é o conjunto

$$\mathcal{L}(D) = \{\varphi \in K(\mathbb{P}_k) | div(\varphi) + D \geq 0\} \cup \{0\}.$$

$\mathcal{L}(D)$ é um sub-espaço vetorial de $K(\mathbb{P}_k)$ e vale $\mathcal{L}(0) = k$.

Um divisor D é **principal** se existe $\varphi \in K(\mathbb{P}_k) \setminus \{0\}$ tal que $div(\varphi) = D$. Dados dois divisores D e D', dizemos que eles são **linearmente equivalentes**, denotado por $D \equiv D'$, se $D - D'$ é um divisor principal. O teorema a seguir caracteriza divisores principais e divisores linearmente equivalentes. Além disso, este teorema fornece informações sobre os espaços vetoriais definidos anteriormente.

Teorema 2.2.1 ([4]) *Sejam D, D' divisores em $\mathbb{P}_k$. Então:*

i) D *é principal* $\Longleftrightarrow gr(D) = 0$*;*

ii) $D \equiv D' \Longleftrightarrow gr(D) = gr(D')$*;*

iii) $\mathcal{L}(D) \neq \{0\}$ *se, e somente se, existir um divisor* D' *linearmente equivalente a* D *tal que* $D' \geq 0$*;*

iv) Se $D \equiv D'$*, então os espaços* $\mathcal{L}(D)$ *e* $\mathcal{L}(D')$ *são isomorfos. Assim, se* D *é um divisor de grau* r*, então* $\mathcal{L}(D)$ *é isomorfo a* $\mathcal{L}(rY)$*.*

Tendo como base as informações do Teorema 2.2.1, podemos caracterizar os espaços vetoriais $\mathcal{L}(D)$ por meio da seguinte proposição:

Proposição 2.2.1 ([4]) *Seja* $D = \sum v_P(D)P$ *um divisor com* $gr(D) = r > 0$*. Então*

$$\mathcal{L}(D) = \left\{ \prod_{P \in \mathbb{P}_k} P^{-v_P(D)} \left(\sum_{i+j=r} a_{ij} X^i Y^j \right) ;\ a_{ij} \in K \right\}.$$

Além disso, temos que $dim_k \mathcal{L}(D) = gr(D) + 1 = r + 1$*.*

Seja $\varphi \in K(\mathbb{P}_k)$ não nulo e $P \in \mathbb{P}_k$ um polinômio de grau um tal que $v_P(\varphi) \geq 0$. O **valor** de φ em P é definido como

$$\varphi(P) = \begin{cases} \varphi(a, 1), \text{ se } P = X - aY; \\ \\ \varphi(1, 0), \text{ se } P = Y. \end{cases} \tag{2.2}$$

Seja $k = \mathbb{F}_q$ o corpo finito com q elementos. Seja s um inteiro tal que $1 \leq s \leq q$ e sejam $a_1, ..., a_s \in \mathbb{F}_q$ distintos dois-a-dois. Consideremos os elementos $P_1 = X - a_1 Y, ..., P_s = X - a_s Y, P_{s+1} = Y$ em $\mathbb{P}_k$ e o divisor $D = P_1 + ... + P_s + \delta P_{s+1}$ onde $\delta = 0$ ou $\delta = 1$. Seja n o grau do divisor D ($n = s$ ou $n = s + 1$). Consideremos também um divisor E, com $gr(E) > 0$, e tal que $Supp(D) \cap Supp(E) = \emptyset$.

O **código de Goppa** $C(D, E)$ associado aos divisores D e E é o conjunto imagem da aplicação linear

$$\begin{array}{rccc} Av_D : \mathcal{L}(E) & \longrightarrow & k^n \\ \varphi & \longmapsto & (\varphi(P_1), ..., \varphi(P_n)) \end{array} \tag{2.3}$$

Os parâmetros desses códigos são dados no teorema a seguir.

Teorema 2.2.2 ([4]) *O código de Goppa* $C(D, E)$ *é um* $(n, k, d)-$*código linear, onde* $n = s$ *(caso* $\delta = 0$*) ou* $n = s + 1$ *(caso* $\delta = 1$*),* $k = dim\mathcal{L}(E) - dim\mathcal{L}(E - D)$ *e* $d \geq n - gr(E)$*. Além disso, se* $0 < gr(E) < n$ *então* $k = dim\mathcal{L}(E) = gr(E) + 1$ *e* $d = n - k + 1$*.*

Corolário 2.2.2.1 *Se $0 < gr(E) < n$, então os códigos de Goppa $C(D, E)$ são códigos MDS.*

2.3 Exemplos de Códigos Racionais

Tendo como base as informações das seções 2.1 e 2.2, faremos nesta seção a construção de alguns códigos racionais. O corpo considerado para a construção dos exemplos será $\mathbb{F}_4$ (corpo com 4 elementos). Nos quatro primeiros exemplos vamos construir códigos com comprimento máximo ($n = 5$) e, para isso, consideraremos o divisor D da forma

$$D = P_1 + P_2 + P_3 + P_4 + P_5,$$

onde

$$P_1 = Y,\ P_2 = X,\ P_3 = X + Y,\ P_4 = X + \alpha Y,\ P_5 = X + \alpha^2 Y.$$

De acordo com o Teorema 2.2.2, se considerarmos um divisor E, com $0 < gr(E) < 5$, e tal que $Supp(D) \cap Supp(E) = \emptyset$, então os códigos resultantes têm parâmetros $n = 5, k = gr(E) + 1$ e $d = 5 - gr(E)$. Uma das maneiras de se obter divisores E nas condições desejadas é a seguinte:

- Encontrar um polinômio $p(X) \in \mathbb{F}_4[X]$ que seja mônico, irredutível e tal que $1 \leq deg(p(X)) \leq 4$;
- Considerar o divisor E como a homogeneização de $p(X)$, isto é, $E = P(X, Y) = p^*(X, Y)$.

Nestes exemplos veremos que os códigos gerados são sempre MDS porém, ao escolhermos subcódigos de forma aleatória, estes podem não ter esta propriedade.

No último exemplo, consideraremos o divisor

$$D = P_1 + P_2 + P_3 + P_4,$$

onde

$$P_1 = X,\ P_2 = X + Y,\ P_3 = X + \alpha Y,\ P_4 = X + \alpha^2 Y,$$

e consideraremos $E = rY$ com $1 \leq r \leq 3$. Neste caso, os parâmetros dos códigos associados são $n = 4,\ k = r + 1,\ d = 4 - r$. Os códigos assim obtidos são os códigos Reed-Solomon.

Exemplo 2.3.1 *Neste exemplo, vamos gerar um código com parâmetros $(5, 5, 1)$. Para isso, seguindo as observações anteriores, precisamos de um divisor E de grau 4. O polinômio $g(X) = X^4 + X + 1$ é mônico irredutível em $\mathbb{F}_4[X]$ e sua homogeneização $G(X, Y) = X^4 + XY^3 + Y^4$*

é um elemento em $\mathbb{P}_K$. *Considerando* $E = G(X, Y)$, *de acordo com a Proposição 2.2.1, temos que o conjunto*

$$\mathcal{B} = \left\{ G_1 = \frac{X^4}{G}, G_2 = \frac{X^3Y}{G}, G_3 = \frac{X^2Y^2}{G}, G_4 = \frac{XY^3}{G}, G_5 = \frac{Y^4}{G} \right\}$$

é uma base do espaço $\mathcal{L}(E)$. *Por definição, o código* $C(D, E)$ *tem matriz geradora dada por*

$$M = [G_i(P_j)],\ i = 1, ..., 5,\ j = 1, ..., 5.$$

Sendo $G(X, Y) = X^4 + XY^3 + Y^4$ *e usando (2.2), temos que*

- $G(P_1) = G(1, 0) = 1$;
- $G(P_2) = G(0, 1) = 1$;
- $G(P_3) = G(1, 1) = 1$;
- $G(P_4) = G(\alpha, 1) = 1$;
- $G(P_5) = G(\alpha^2, 1) = 1$.

Portanto, temos

- $G_1(P_1) = 1,\ G_1(P_2) = 0,\ G_1(P_3) = 1,\ G_1(P_4) = \alpha,\ G_1(P_5) = \alpha^2$;
- $G_2(P_1) = 0,\ G_2(P_2) = 0,\ G_2(P_3) = 1,\ G_2(P_4) = 1,\ G_2(P_5) = 1$;
- $G_3(P_1) = 0,\ G_3(P_2) = 0,\ G_3(P_3) = 1,\ G_3(P_4) = \alpha^2,\ G_3(P_5) = \alpha$;
- $G_4(P_1) = 0,\ G_4(P_2) = 0,\ G_4(P_3) = 1,\ G_4(P_4) = \alpha,\ G_4(P_5) = \alpha^2$;
- $G_5(P_1) = 0,\ G_5(P_2) = 1,\ G_5(P_3) = 1,\ G_5(P_4) = 1,\ G_5(P_5) = 1$.

Desta forma

$$M = \begin{bmatrix} 1 & 0 & 1 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & \alpha^2 & \alpha \\ 0 & 0 & 1 & \alpha & \alpha^2 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Vejamos agora alguns subcódigos que podem ser obtidos a partir do código racional encontrado.

- *Subcódigos de dimensão* 4.

  Temos 5 *subespaços de* $\mathcal{L}(E)$ *de dimensão* 4 *gerados pelos conjuntos*

  $$\mathcal{B}_1 = \{G_1, G_2, G_3, G_5\}, \quad \mathcal{B}_2 = \{G_1, G_2, G_4, G_5\}, \quad \mathcal{B}_3 = \{G_1, G_3, G_4, G_5\}$$
  $$\mathcal{B}_4 = \{G_1, G_2, G_3, G_4\}, \quad \mathcal{B}_5 = \{G_2, G_3, G_4, G_5\}.$$

  Todos estes geradores nos fornecem $(5, 4, 1)-$ *códigos. Para isto basta observar que as matrizes geradoras dos códigos obtidos de* $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_5$ *possuem a segunda e a quinta linha de* M*, cuja soma é um vetor de peso* 1*. Os códigos obtidos de* $\mathcal{B}_3, \mathcal{B}_4$ *possuem a primeira e a quarta linha de* M *que, somadas, nos fornecem um vetor de peso* 1*.*

- *Subcódigos de dimensão* 3*.*

  Podemos obter um subcódigo com parâmetros $(5, 3, 1)$*, tomando como gerador o conjunto* $\mathcal{B}_1 = \{G_1, G_2, G_5\}$*; um subcódigo com parâmetros* $(5, 3, 2)$*, tomando como gerador o conjunto* $\mathcal{B}_2 = \{G_1, G_2, G_3\}$ *e também um subcódigo com parâmetros* $(5, 3, 3)$*, tomando como gerador o conjunto* $\mathcal{B}_3 = \{G_1, G_3, G_5\}$*.*

- *Subcódigos de dimensão* 2

  Podemos obter um subcódigo com parâmetros $(5, 2, 4)$*, tomando como gerador o conjunto* $\mathcal{B}_1 = \{G_1, G_5\}$ *e também um subcódigo com parâmetros* $(5, 2, 1)$*, tomando como gerador o conjunto* $\mathcal{B}_2 = \{G_1, G_4\}$*.*

Exemplo 2.3.2 *Neste exemplo, vamos construir um código racional com parâmetros* $(5, 4, 2)$*. Como* $k = 4$*, precisamos de um divisor com grau* 3*. Logo, precisamos de um polinômio irredutível de grau* 3*. O polinômio* $p(X) = X^3 + X + 1$ *é mônico e irredutível. Vamos considerar o divisor* $E = P(X, Y) = p^*(X, Y) = X^3 + XY^2 + Y^3$*. Neste caso, teremos como base do espaço* $\mathcal{L}(E)$ *o conjunto*

$$\mathcal{B} = \left\{ G_1 = \frac{X^3}{P},\ G_2 = \frac{X^2Y}{P},\ G_3 = \frac{XY^2}{P},\ G_4 = \frac{Y^3}{P} \right\}.$$

A matriz geradora do código é dada por

$$M = [G_i(P_j)],\ i = 1, ..., 4,\ j = 1, ..., 4.$$

Seguindo o mesmo procedimento do Exemplo 2.3.1, a matriz geradora é dada por

$$M = \begin{bmatrix} 1 & 0 & 1 & \alpha^2 & \alpha \\ 0 & 0 & 1 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha^2 & \alpha \end{bmatrix}.$$

Todos os subcódigos de dimensão 3 *apresentam parâmetros* $(5, 3, 2)$*. Dentre os subcódigos de dimensão 2 temos um com parâmetros* $(5, 2, 2)$*, quando consideramos o subespaço gerado pelo conjunto* $\mathcal{B}_1 = \left\{ \frac{X^3}{P}, \frac{Y^3}{P} \right\}$*, e também um subcódigo com parâmetros* $(5, 2, 3)$*, tendo como gerador o conjunto* $\mathcal{B}_2 = \left\{ \frac{X^3}{P}, \frac{X^2Y}{P} \right\}$.

Exemplo 2.3.3 *Neste exemplo, construiremos um código racional com parâmetros* $(5, 4, 2)$*. Para isso, utilizaremos o polinômio* $p(X) = X^3 + \alpha X^2 + 1$ *que é mônico e irredutível. Considerando-se o divisor primo* $E = P(X, Y) = X^3 + \alpha X^2 Y + Y^3$*, teremos como base do espaço* $\mathcal{L}(E)$ *o conjunto*

$$\mathcal{B} = \left\{ \frac{X^3}{P}, \frac{X^2Y}{P}, \frac{XY^2}{P}, \frac{Y^3}{P} \right\}.$$

A matriz geradora do código é dada por

$$M = \begin{bmatrix} 1 & 0 & \alpha^2 & 1 & \alpha \\ 0 & 0 & \alpha^2 & \alpha^2 & \alpha^2 \\ 0 & 0 & \alpha^2 & \alpha & 1 \\ 0 & 1 & \alpha^2 & 1 & \alpha \end{bmatrix}.$$

Assim como no Exemplo 2.3.2, todos os subcódigos de dimensão 3 *possuem parâmetros* $(5, 3, 2)$*. Dentre os subcódigos de dimensão 2, temos um com parâmetros* $(5, 2, 2)$*, quando consideramos o subespaço gerado pelo conjunto* $\mathcal{B}_1 = \left\{ \frac{X^3}{P}, \frac{Y^3}{P} \right\}$ *e um com parâmetros* $(5, 2, 3)$*, tendo como gerador o conjunto* $\mathcal{B}_2 = \left\{ \frac{X^3}{P}, \frac{X^2Y}{P} \right\}$.

Exemplo 2.3.4 *Neste exemplo, vamos construir um código racional com parâmetros* $(5, 3, 3)$*. Para isso, usaremos o polinômio* $p(X) = X^2 + X + \alpha$ *que é mônico e irredutível. Considerando-se o divisor primo* $E = P(X, Y) = X^2 + XY + \alpha Y^2$*, teremos como base do espaço* $\mathcal{L}(E)$ *o conjunto*

$$\mathcal{B} = \left\{ \frac{X^2}{P}, \frac{XY}{P}, \frac{Y^2}{P} \right\}.$$

A matriz geradora do código é dada por

$$M = \begin{bmatrix} 1 & 0 & \alpha^2 & 1 & \alpha^2 \\ 0 & 0 & \alpha^2 & \alpha^2 & 1 \\ 0 & \alpha^2 & \alpha^2 & \alpha & \alpha \end{bmatrix}.$$

Neste exemplo, conseguimos um subcódigo com parâmetros $(5, 2, 4)$*, tomando como gerador o conjunto* $\mathcal{B}_1 = \{\frac{X^2}{P}, \frac{Y^2}{P}\}$*, e também um subcódigo com parâmetros* $(5, 2, 3)$*, considerando o subespaço gerado pelo conjunto* $\mathcal{B}_2 = \{\frac{X^2}{P}, \frac{XY}{P}\}$*.*

Podemos também construir um código com prâmetros $(5, 5, 1)$*. Para isso, vamos considerar o divisor primo* $E_1 = 2P(X, Y)$*. Neste caso, o espaço* $\mathcal{L}(E_1)$ *é gerado pelo conjunto*

$$\mathcal{B}_1 = \left\{ \frac{X^4}{P^2}, \frac{X^3Y}{P^2}, \frac{X^2Y^2}{P^2}, \frac{XY^3}{P^2}, \frac{Y^4}{P^2} \right\},$$

e a matriz geradora é dada por

$$M_1 = \begin{bmatrix} 1 & 0 & \alpha & 1 & \alpha \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 \\ 0 & 0 & \alpha & \alpha & 1 \\ 0 & 0 & \alpha & 1 & \alpha \\ 0 & \alpha & \alpha & \alpha^2 & \alpha^2 \end{bmatrix}.$$

Como no Exemplo 2.3.1, todos os subcódigos de dimensão 4 *têm parâmetros* $(5, 4, 1)$*. Dentre os subcódigos de dimensão 3, temos um subcódigo com parâmetros* $(5, 3, 3)$*, gerado pelo conjunto* $\mathcal{B}_2 = \left\{ \frac{X^4}{P^2}, \frac{X^2Y^2}{P^2}, \frac{Y^4}{P^2} \right\}$*, um subcódigo com parâmetros* $(5, 3, 2)$*, gerado pelo conjunto* $\mathcal{B}_3 = \left\{ \frac{X^2Y^2}{P^2}, \frac{XY^3}{P^2}, \frac{Y^4}{P^2} \right\}$ *e um subcódigo com parâmetros* $(5, 3, 1)$*, gerado pelo conjunto* $\mathcal{B}_4 = \left\{ \frac{X^4}{P^2}, \frac{X^2Y^2}{P^2}, \frac{XY^3}{P^2} \right\}$*.*

Exemplo 2.3.5 *Neste exemplo, os divisores serão da forma* $E = rY$*, com* $1 \leq r \leq 3$*. Considerando-se* $r = 3$*, o espaço* $\mathcal{L}(E = 3Y)$ *é gerado pelo conjunto*

$$\mathcal{B} = \left\{ \frac{X^3}{Y^3}, \frac{X^2}{Y^2}, \frac{X}{Y}, 1 \right\}.$$

A matriz geradora correspondente é dada por

$$G = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

Esta matriz dá origem a um código racional com parâmetros $(4, 4, 1)$.

Considerando-se $r = 2$*, o espaço* $\mathcal{L}(2Y)$ *é gerado pelo conjunto*

$$\mathcal{B}_1 = \left\{ \frac{X^2}{Y^2}, \frac{X}{Y}, 1 \right\}.$$

A matriz geradora correspondente é dada por

$$G_1 = \begin{bmatrix} 0 & 1 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

Esta matriz dá origem a um código racional com parâmetros $(4, 3, 2)$*. Note que este código é um subcódigo do código anterior.*

Considerando-se $r = 1$*, o espaço* $\mathcal{L}(Y)$ *é gerado pelo conjunto*

$$\mathcal{B}_2 = \left\{ \frac{X}{Y}, 1 \right\}.$$

A matriz geradora correspondente é dada por

$$G_2 = \begin{bmatrix} 0 & 1 & \alpha & \alpha^2 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

Esta matriz dá origem a um código racional com parâmetros $(4, 2, 3)$*. Note que este código é um subcódigo dos códigos obtidos anteriormente.*

Observação 2.3.1 *No Exemplo 2.3.5, notamos que sempre que tivermos códigos Reed-Solomon, é possível através da matriz geradora (modulação) obter subcódigos que sejam sempre MDS. Dos Exemplos 2.3.1, 2.3.2, 2.3.3 e 2.3.4, notamos que os subcódigos obtidos através da matriz geradora podem não ser subcódigos MDS. Na próxima seção iremos propor um procedimento de construção de subcódigos racionais de Goppa que são sempre MDS.*

2.4 Processo de Construção de Subcódigos Racionais MDS

Sem perda de generalidade, iremos considerar o corpo $\mathbb{F}_{p^m}$, com p primo, e para simplificar as notações usaremos

$$\alpha_1 = 0,\ \alpha_2 = 1,\ \alpha_3 = \ \alpha, ...,\ \alpha_{p^m} = \alpha^{p^m-2}$$

e também

$$P_1 = (1,0), P_2 = (\alpha_1, 1), P_3 = (\alpha_2, 1), ..., P_{p^m+1} = (\alpha_{p^m}, 1).$$

Vamos considerar $D = P_1 + ... + P_{p^m+1}$ e supor que exista um polinômio irredutível $g(X)$ de modo que o divisor $E(X,Y) = rG(X,Y)$, onde $G(X,Y) = g^*(X,Y)$, tenha grau p^m. Neste caso, o espaço $\mathcal{L}(E)$ é gerado pelo conjunto

$$\left\{ \frac{X^{p^m}}{G(X,Y)^r},\ \frac{X^{p^m-1}Y}{G(X,Y)^r}, ...,\ \frac{XY^{p^m-1}}{G(X,Y)^r},\ \frac{Y^{p^m}}{G(X,Y)^r} \right\},$$

dando origem a um $(p^m+1, p^m+1, 1)-$código racional.

Seja $2 \leq k \leq p^m$. Para a construção de subcódigos MDS de dimensão k do código $(p^m + 1, p^m + 1, 1)$, os seguintes polinômios serão utilizados na obtenção dos geradores.

- $f_1(X) = c_1 \prod_{i=1}^{k-1} (X + \alpha_i)$
- $f_t(X) = c_t \prod_{\substack{i=1 \\ i \neq t-1}}^{k-1} (X + \alpha_i),\ t = 2, ..., k.$

A constante c_1 é um elemento de $\mathbb{F}_{p^m}$ escolhido de modo que

$$f_1(X) = X + h(X),\ deg(h(X)) \geq 2.$$

Os polinômios $f_t(X)$ são os polinômios de interpolação, [4], dos elementos $\alpha_1, ..., \alpha_{k-1}$. Assim, temos que

$$f_t(\alpha_{t-1}) = 1,\ f_t(\alpha_i) = 0,\ i = 1, ..., k-1,\ i \neq t-1.$$

Os geradores do subcódigo serão obtidos, por meio dos polinômios anteriores, da seguinte forma:

- $F_1(X,Y) = \dfrac{G(P_1)^r (X^{p^m} + Y^{p^m} h(\frac{X}{Y}))}{G(X,Y)^r}$

- $F_t(X,Y) = \dfrac{G(P_t)^r Y^{p^m} f_t(\frac{X}{Y})}{G(X,Y)^r},\ t = 2, ..., k.$

Os polinômios $F_t(X,Y),\ t = 2, ..., k$ são obtidos fazendo-se a homogeneização dos polinômios $f_t(X)$. Assim, temos que

$$F_t(a,1) = \frac{G(P_t)^r f_t(a)}{G(a,1)^r} = \beta_t f_t(a), \forall\ a \in \mathbb{F}_{p^m}.$$

O polinômio $F_1(X,Y)$ não é a homogeneização de $f_1(X)$, porém, como $a^{p^m} = a$, satisfaz a seguinte condição:

$$F_1(a,1) = \frac{G(P_1)^r (a^{p^m} + h(a))}{G(a,1)^r} = \frac{G(P_1)^r f_1(a)}{G(a,1)^r} = \beta_1 f_1(a), \forall\ a \in \mathbb{F}_{p^m}.$$

É interessante observar que, da forma como foram construídos estes polinômios, valem as seguintes igualdades:

$$F_i(P_j) = \delta_{ij},\ i = 1, ..., k,\ j = 1, ..., k.$$

Portanto, os polinômios $F_1(X,Y), F_2(X,Y), ..., F_k(X,Y)$ são linearmente independentes. Assim, eles geram um subespaço de dimensão k, isto é, geram um subcódigo de dimensão k, com matriz geradora na forma

$$M = [Id_k | M_1],$$

onde

$$M_1 = \begin{bmatrix} F_1(P_{k+1}) & F_1(P_{k+2}) & ... & F_1(P_{p^m+1}) \\ F_2(P_{k+1}) & F_2(P_{k+2}) & ... & F_2(P_{p^m+1}) \\ \vdots & \vdots & ... & \vdots \\ F_k(P_{k+1}) & F_k(P_{k+2}) & ... & F_k(P_{p^m+1}) \end{bmatrix}.$$

Para uma melhor compreensão do que foi feito até agora, vamos usar o processo para obter subcódigos MDS de um código racional com parâmetros $(9, 9, 1)$ sobre o corpo $\mathbb{F}_8$, obtido pelo quociente de $\mathbb{F}_2[X]$ pelo polinômio irredutível $X^3 + X^2 + 1$. Dessa forma,

$$\mathbb{F}_8 \cong \frac{\mathbb{F}_2[X]}{\langle X^3 + X^2 + 1 \rangle} = \{a_0 1 + a_1 x + a_2 x^2,\ a_0, a_1, a_2 \in \mathbb{F}_2\}.$$

Os elementos de $\mathbb{F}_8$ são mostrados na Tabela 2.1.

Elemento	1	α	α^2
1	1	0	0
α	0	1	0
α^2	0	0	1
α^3	1	0	1
α^4	1	1	1
α^5	1	1	0
α^6	0	1	1

Tab. 2.1: Elementos de $\mathbb{F}_8$.

De acordo com a notação vista no início da seção, resulta os seguintes pontos

$$\begin{array}{lll} P_1 = (1,0) & P_2 = (0,1) & P_3 = (1,1) \\ P_4 = (\alpha,1) & P_5 = (\alpha^2,1) & P_6 = (\alpha^3,1) \\ P_7 = (\alpha^4,1) & P_8 = (\alpha^5,1) & P_9 = (\alpha^6,1). \end{array}$$

O polinômio $g(X) = X^2 + X + 1$ é irredutível em $\mathbb{F}_8[X]$. Assim, considerando

$$E(X,Y) = 4G(X,Y) = 4(X^2 + XY + Y^2),$$

temos que $\mathcal{L}(E)$ é um espaço vetorial de dimensão 9 com conjunto gerador

$$\left\{ \frac{X^{8-i}Y^i}{G(X,Y)^4},\ i = 0, ..., 8. \right\}.$$

Como exemplo, vamos construir um subcódigo com parâmetros $(9, 5, 5)$. Para isso selecionamos os pontos

$$P_1 = (1,0), P_2 = (0,1), P_3 = (1,1), P_4 = (\alpha,1), P_5 = (\alpha^2,1)$$

e os seguintes polinômios

- $f_1(X) = \alpha^4[X(X+1)(X+\alpha)(X+\alpha^2)] = \alpha^4X^4 + \alpha X^3 + \alpha^2X^2 + X$;
- $f_2(X) = \alpha^4[(X+1)(X+\alpha)(X+\alpha^2)] = \alpha^4X^3 + \alpha X^2 + \alpha^2X + 1$;
- $f_3(X) = \alpha^6[X(X+\alpha)(X+\alpha^2)] = \alpha^6X^3 + \alpha^5X^2 + \alpha^2X$;
- $f_4(X) = \alpha^2[X(X+1)(X+\alpha^2)] = \alpha^2X^3 + \alpha^5X^2 + \alpha^4X$;

- $f_5(X) = \alpha^3[X(X+1)(X+\alpha)] = \alpha^3X^3 + \alpha X^2 + \alpha^4 X$

Estes polinômios dão origem aos seguintes geradores do subespaço de $\mathcal{L}(E)$:

- $F_1(X,Y) = \frac{G(1,0)^4(\alpha^4X^4Y^4+\alpha X^3Y^5+\alpha^2X^2Y^6+X^8)}{G(X,Y)^4}$;
- $F_2(X,Y) = \dfrac{G(0,1)^4(\alpha^4X^3Y^5 + \alpha X^2Y^6 + \alpha^2XY^7 + Y^8)}{G(X,Y)^4}$;
- $F_3(X,Y) = \dfrac{G(1,1)^4(\alpha^6X^3Y^5 + \alpha^5X^2Y^6 + \alpha^2XY^7)}{G(X,Y)^4}$;
- $F_4(X,Y) = \dfrac{G(\alpha,1)^4(\alpha^2X^3Y^5 + \alpha^5X^2Y^6 + \alpha^4XY^7)}{G(X,Y)^4}$;
- $F_5(X,Y) = \dfrac{G(\alpha^2,1)^4(\alpha^3X^3Y^5 + \alpha X^2Y^6 + \alpha^4XY^7)}{G(X,Y)^4}$.

A matriz geradora do código é da forma $M = [Id_5|M_1]$ com

$$M_1 = \begin{bmatrix} F_1(\alpha^3,1) & F_1(\alpha^4,1) & F_1(\alpha^5,1) & F_1(\alpha^6,1) \\ F_2(\alpha^3,1) & F_2(\alpha^4,1) & F_2(\alpha^5,1) & F_2(\alpha^6,1) \\ F_3(\alpha^3,1) & F_3(\alpha^4,1) & F_3(\alpha^5,1) & F_3(\alpha^6,1) \\ F_4(\alpha^3,1) & F_4(\alpha^4,1) & F_4(\alpha^5,1) & F_4(\alpha^6,1) \\ F_5(\alpha^3,1) & F_5(\alpha^4,1) & F_5(\alpha^5,1) & F_5(\alpha^6,1) \end{bmatrix}.$$

Voltando ao processo de construção, vamos mostrar que estes subcódigos são MDS, isto é, que a distância mínima é da forma $d = n - k + 1 = p^m - k + 2$. Para isso, vamos mostrar que quaisquer $n - k = p^m - k + 1$ colunas da matriz verificação de paridade são linearmente independentes. Sabemos que a matriz verificação de paridade é da forma

$$H = [-M_1^t|Id_{p^m+1-k}].$$

Denotaremos suas k primeiras colunas por

$v_1 = -(F_1(P_{k+1}), F_1(P_{k+2}), ..., F_1(P_{p^m+1})) = -(\beta_1 f_1(\alpha_k), ..., \beta_1 f_1(\alpha_{p^m}))$

$v_2 = -(F_2(P_{k+1}), F_2(P_{k+2}), ..., F_2(P_{p^m+1})) = -(\beta_2 f_2(\alpha_k), ..., \beta_2 f_2(\alpha_{p^m}))$

$\vdots$

$v_k = -(F_k(P_{k+1}), F_k(P_{k+2}), ..., F_k(P_{p^m+1})) = -(\beta_k f_k(\alpha_k), ..., \beta_k f_k(\alpha_{p^m}))$

Vamos considerar $\{v_{i_j},\ j = 1, ..., r\}$ um conjunto formado por r colunas da matriz $-M_1^t$ e $\{c_{i_t},\ t = 1, ..., n-k-r\}$ um conjunto formado por $n-k-r$ colunas da matriz Id_{p^m+1-k}. Uma combinação linear nula desses vetores é da forma

$$\sum_{j=1}^{r} a_{i_j} v_{i_j} + \sum_{t=1}^{n-k-r} b_{i_t} c_{i_t} = 0,$$

portanto, podemos escrever

$$\sum_{t=1}^{n-k-r} b_{i_t} c_{i_t} = -\sum_{j=1}^{r} a_{i_j} v_{i_j}. \tag{2.4}$$

Sabemos que uma combinação linear de $n-k-r$ vetores de Id_{p^m+1-k} tem, pelo menos, r entradas nulas e que

$$-\sum_{j=1}^{r} a_{i_j} v_{i_j} = (\sum_{j=1}^{r} a_{i_j} F_{i_j}(P_{k+1}), ..., \sum_{j=1}^{r} a_{i_j} F_{i_j}(P_{p^m+1})) = (\sum_{j=1}^{r} a'_{i_j} f_{i_j}(\alpha_k), ..., \sum_{j=1}^{r} a'_{i_j} f_{i_j}(\alpha_{p^m})),$$

com $a'_{i_j} = \beta_{i_j} a_{i_j}$.

Se $v_1 \in \{v_{i_j}, j = 1, ..., r\}$ então o polinômio $\sum a_{i_j} f_{i_j}$ tem grau menor ou igual a $k-1$ e tem $k-r$ zeros entre os elementos $\alpha_1, ..., \alpha_{k-1}$. Assim,

$$\sum_{j=1}^{r} a'_{i_j} f_{i_j}(X) = g(X)h(X), \tag{2.5}$$

onde $g(\alpha_i) \neq 0,\ i = k, ..., p^m$ e $gr(h(X)) \leq (k-1) - (k-r) = r-1$.

Se $v_1 \notin \{v_{i_j}, j = 1, ..., r\}$ então o polinômio $\sum a_{i_j} f_{i_j}$ tem grau $k-2$ e tem $k-1-r$ zeros entre os elementos $\alpha_1, ..., \alpha_{k-1}$. Assim,

$$\sum_{j=1}^{r} a_{i_j} f_{i_j}(X) = g(X)h(X), \tag{2.6}$$

onde $g(\alpha_i) \neq 0,\ i = k, ..., p^m$ e $gr(h(X)) = (k-2) - (k-1-r) = r-1$.

Portanto, se tomarmos uma combinação linear nula de r colunas de $-M_1^t$ e $n-k-r$ colunas de Id_{p^m+1-k}, chegaríamos a (2.4) e, pelo que foi observado em (2.5) e (2.6), temos que o polinômio $h(X)$ possui r zeros entre os elementos $\alpha_k, ..., \alpha_{p^m}$. Como $gr(h(X)) \leq r-1$ então $h(X)$ é o polinômio nulo, ou seja,

$$\sum_{j=1}^{r} a'_{i_j} f_{i_j}(X) = 0.$$

Como os polinômios $f_{i_1},\ f_{i_2},...,\ f_{i_r}$ são linearmente independentes, concluímos que $a_{i_j} = 0$. Voltando a (2.4), temos que $b_{i_t} = 0$, isto é, os vetores escolhidos são linearmente independentes.

Para finalizar, vamos considerar o caso em que $p^m + 1 - k < k$ e mostrar que quaisquer $n - k$ vetores entre $v_1, ..., v_k$ formam um conjunto linearmente independente. Sabemos que se

$$\sum_{j=1}^{n-k} a_{i_j} v_{i_j} = 0,$$

então o polinômio $\sum_{j=1}^{n-k} a'_{i_j} f_{i_j}(X)$ tem como raízes os elementos $\alpha_k, ..., \alpha_{p^m}$. Da mesma forma como fizemos anteriormente, temos que:

- se $f_1 \in \{f_{i_j}, j = 1, ..., n-k\}$ então os polinômios f_{i_j} têm $k - (n-k)$ zeros em comum entre os elementos $\alpha_1, ..., \alpha_{k-1}$ e a combinação linear deles tem grau $k-1$. Colocando-se os fatores comuns em evidência, temos que

$$\sum_{j=1}^{r} a'_{i_j} f_{i_j}(X) = g(X)h(X),$$

  onde $g(\alpha_i) \neq 0,\ i = k, ..., p^m$ e $gr(h(X)) = (k-1) - (k - (n-k)) = n - k - 1$.

- se $f_1 \notin \{f_{i_j}, j = 1, ..., r\}$ então os polinômios f_{i_j} têm $k - 1 - (n-k)$ zeros em comum entre os elementos $\alpha_1, ..., \alpha_{k-1}$ e a combinação linear deles tem grau $k-2$. Colocando-se os fatores comuns em evidência, temos que

$$\sum_{j=1}^{r} a_{i_j} f_{i_j}(X) = g(X)h(X),$$

  onde $g(\alpha_i) \neq 0,\ i = k, ..., p^m$ e $gr(h(X)) = (k-2) - (k-1-(n-k)) = n - k - 1$.

Assim, em cada um dos casos acima, o polinômio $h(X)$ tem grau $n - k - 1$ e $n - k$ raízes, isto é, $h(X)$ é o polinômio nulo. Seguindo raciocínio análogo ao que foi feito no caso anterior, concluímos que $a_{i_j} = 0$.

Finalizaremos nosso exemplo mostrando que o código obtido pelos geradores escolhidos é um $(9, 5, 5)-$código.

1. **Passo 1:** $\{F_1, F_2, F_3, F_4, F_5\}$ é um conjunto linearmente independente. De fato, tomando-se uma combinação linear

$$a_1F_1(X,Y) + a_2F_2(X,Y) + a_3F_3(X,Y) + a_4F_4(X,Y) + a_5F_5(X,Y) = 0,$$

basta verificar que:

- $F_1(1,0) = 1, F_2(1,0) = F_3(1,0) = F_4(1,0) = F_5(1,0) = 0$ e assim $a_1 = 0$;
- $F_2(0,1) = 1, F_3(0,1) = F_4(0,1) = F_5(0,1) = 0$ e assim $a_2 = 0$;
- $F_3(1,1) = 1, F_4(1,1) = F_5(1,1) = 0$ e assim $a_3 = 0$;
- $F_4(\alpha,1) = 1, F_5(\alpha,1) = 0$ e assim $a_4 = 0$;
- $F_5(\alpha^2,1) = 1$ e, assim $a_5 = 0$.

2. **Passo 2:** A matriz geradora desse código é dada por

$$M = [Id_5|M_1]\,,$$

onde

$$M_1 = \begin{bmatrix} F_1(\alpha^3,1) & F_1(\alpha^4,1) & F_1(\alpha^5,1) & F_1(\alpha^6,1) \\ F_2(\alpha^3,1) & F_2(\alpha^4,1) & F_2(\alpha^5,1) & F_2(\alpha^6,1) \\ F_3(\alpha^3,1) & F_3(\alpha^4,1) & F_3(\alpha^5,1) & F_3(\alpha^6,1) \\ F_4(\alpha^3,1) & F_4(\alpha^4,1) & F_4(\alpha^5,1) & F_4(\alpha^6,1) \\ F_5(\alpha^3,1) & F_5(\alpha^4,1) & F_5(\alpha^5,1) & F_5(\alpha^6,1) \end{bmatrix}.$$

3. **Passo 3:** Vamos mostrar que $d = 5$. Para isso, mostraremos que quaisquer 4 colunas da matriz verificação de paridade são linearmente independentes. As seguintes informações serão úteis:

$$v_1 = (F_1(\alpha^3,1), F_1(\alpha^4,1), F_1(\alpha^5,1), F_1(\alpha^6,1)) = (f_1(\alpha^3), f_1(\alpha^4), f_1(\alpha^5), f_1(\alpha^6))$$

$$v_2 = (F_2(\alpha^3,1), F_2(\alpha^4,1), F_2(\alpha^5,1), F_2(\alpha^6,1)) = (f_2(\alpha^3), f_2(\alpha^4), f_2(\alpha^5), f_2(\alpha^6))$$

$$v_3 = (F_3(\alpha^3,1), F_3(\alpha^4,1), F_3(\alpha^5,1), F_3(\alpha^6,1)) = (f_3(\alpha^3), f_3(\alpha^4), f_3(\alpha^5), f_3(\alpha^6))$$

$$v_4 = (F_4(\alpha^3,1), F_4(\alpha^4,1), F_4(\alpha^5,1), F_4(\alpha^6,1)) = (f_4(\alpha^3), f_4(\alpha^4), f_4(\alpha^5), f_4(\alpha^6))$$

$$v_5 = (F_5(\alpha^3,1), F_5(\alpha^4,1), F_5(\alpha^5,1), F_5(\alpha^6,1)) = (f_5(\alpha^3), f_5(\alpha^4), f_5(\alpha^5), f_5(\alpha^6))$$

Para conjuntos formados de 4 colunas da matriz verificação de paridade, temos as seguintes possibilidades:

- $\{v_2, v_3, v_4, v_5\}$

Tomando-se a combinação linear $\sum_{i=2}^{5} a_i v_i$ temos que cada coordenada é da forma

$$\sum_{i=2}^{5} a_i F_i(\alpha^j, 1) = \sum_{i=2}^{5} a_i f_i(\alpha^j),\ j \in \{3,4,5,6\}.$$

Assim, se $\sum_{i=2}^{5} a_i v_i = 0$, então o polinômio $\sum_{i=2}^{5} a_i F_i(X,1) = \sum_{i=2}^{5} a_i f_i(X)$ tem 4 raízes e, como é um polinômio de grau 3, só pode ser o polinômio nulo, isto é

$$\sum_{i=2}^{5} a_i F_i(X,1) = 0,\ \forall\ X.$$

Observando o que foi feito no **Passo 1**, concluímos que $a_i = 0,\ i = 2,3,4,5$. Logo, o conjunto é linearmente independente.

- $\{v_1, v_i, v_j, v_k\},\ i,j,k \in \{2,3,4,5\}$
  Tomando-se uma combinação linear nula desses vetores teremos, como anteriormente, que o polinômio

  $$a_1F_1(X,1)+a_iF_i(X,1)+a_jF_j(X,1)+a_kF_k(X,1) = a_1f_1(X)+a_if_i(X)+a_jf_j(X)+a_kf_k(X),$$

  tem os elementos $\{\alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ como raízes. Porém, o polinômio acima pode ser escrito da seguinte forma

  $$(X + c\alpha^s)P(X),\ c \in \{0,1\},\ s \in \{0,1,2\},$$

  onde $P(X)$ tem grau no máximo 3 e, portanto, é o polinômio nulo. Assim, temos que

  $$a_1F_1(X,1) + a_iF_i(X,1) + a_jF_j(X,1) + a_kF_k(X,1) = 0,\ \forall X$$

  e, tendo como base o procedimento anterior, temos que $a_1 = 0, a_i = 0, a_j = 0, a_k = 0$, isto é, o conjunto é linearmente independente.
- $\{v_i, v_j, v_k, c_s\},\ i,j,k \in \{2,3,4,5\},\ c_s$ uma coluna da matriz Id_4.
  Se este conjunto fosse linearmente dependente teríamos uma combinação linear

  $$a_iv_i + a_jv_j + a_kv_k = c_s,$$

  isto é, o polinômio

  $$Q(X) = a_iF_i(X,1) + a_jF_j(X,1) + a_kF_k(X,1) = a_if_i(X) + a_jf_j(X) + a_kf_k(X),$$

possui 3 raízes no conjunto $\{\alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. Porém,

$$Q(X) = (X + c\alpha^s)P(X),\ c \in \{0,1\},\ s \in \{0,1,2\},$$

com $P(X)$ um polinômio de grau no máximo 2 . Assim, tendo como base o procedimento anterior, o conjunto é linearmente independente.

- $\{v_1, v_j, v_k, c_s\},\ j,k \in \{2,3,4,5\},\ c_s$ coluna da matriz Id_4.
  Da mesma forma, se o conjunto acima for linearmente dependente teremos uma combinação linear da forma

  $$a_1v_1 + a_jv_j + a_kv_k = c_s,$$

  isto é, o polinômio

  $$Q(X) = a_1F_1(X,1) + a_jF_j(X,1) + a_kF_k(X,1) = a_1f_1(X) + a_jf_j(X) + a_kf_k(X),$$

  possui 3 raízes no conjunto $\{\alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. Porém,

  $$Q(X) = (X + c\alpha^s)(X + \alpha^t)P(X),\ c \in \{0,1\},\ t,s \in \{0,1,2\},\ s \neq t,$$

  com $P(X)$ polinômio de grau no máximo 2 . Assim, o conjunto é linearmente independente.

Seguindo raciocínio análogo podemos mostrar que se tomarmos dois vetores pertencentes ao conjunto $\{v_1, v_2, v_3, v_4, v_5\}$ e dois vetores de Id_4, este novo conjunto é um conjunto linearmente independente, o mesmo valendo para um vetor entre os $v_i's$ e três vetores de Id_4. Portanto, o código resultante é um $(9,5,5)-$código .

Para finalizar, se desejarmos construir um $(p^m+1, 1, p^m+1)-$subcódigo tomamos como gerador o elemento

$$F(X,Y) = \frac{X^{p^m}}{G(X,Y)^r} + \frac{X^{p^m-1}Y}{G(X,Y)^r} + ... + \frac{XY^{p^m-1}}{G(X,Y)^r} + \frac{Y^{p^m}}{G(X,Y)^r} = \frac{X^{p^m} + X^{p^m-1}Y + ... + Y^{p^m}}{G(X,Y)^r}$$

pois temos que:

- $F(1,0) = \dfrac{1}{G(1,0)^r}$;
- $F(0,1) = \dfrac{1}{G(0,1)^r}$;

- $F(1,1) = \dfrac{1}{G(1,1)^r}$;
- $F(a,1) = \dfrac{1+a}{G(a,1)^r}, \forall\ a \in \mathbb{F}_{p^m},\ a \neq 0,1.$

2.5 Conclusões

Neste capítulo, vimos como construir códigos de Goppa racionais. Vimos também que estes códigos são sempre códigos com máxima distância de separação (MDS). Entretanto, ao escolhermos subcódigos a partir da matriz geradora do código racional, vimos que estes podem não ser MDS. Apresentamos então, um processo de construção de subcódigos MDS de códigos racionais com parâmetros $(n, n, 1)$.

Capítulo 3

Códigos Associados a Curvas Elípticas

Neste capítulo, vamos considerar códigos de Goppa associados a curvas de gênero $g = 1$. Os conceitos básicos para o entendimento do que será desenvolvido pode ser visto no Capítulo 2 e, para leituras complementares, sugerimos ao leitor as seguintes referências [8], [7]. De acordo com o Teorema A.2.4 os códigos associados possuem parâmetros $(n,\ k = gr(D),\ n - k \leq d \leq n - k + 1)$. Nas duas primeiras seções, como exemplos, calcularemos os parâmetros dos códigos associados às curvas Hermitiana e de Hurwitz. Para isto, calcularemos os pontos racionais destas curvas e, baseados na Observação A.2.1, encontraremos bases para os espaços $\mathcal{L}(D)$ e buscaremos palavras-código com o peso desejado. Baseados nestes dois exemplos, na última seção apresentaremos um resultado que nos dará informações sobre os parâmetros dos códigos associados à curvas maximais de gênero $g = 1$.

Este capítulo está organizado da seguinte forma. Na Seção 3.1, analisaremos os códigos, sobre o corpo $\mathbb{F}_4$, associados à curva Hermitiana. Esta curva é maximal possuindo 9 pontos racionais. Veremos que, se considerarmos divisores da forma $D = rP_\infty$, isto é, divisores com um ponto base, os parâmetros dos códigos associados são, em sua maioria, da forma $(n, k, d) = (8, r, 8 - r)$. Na Seção 3.2, analisaremos os códigos associados à curva maximal de gênero 1, chamada curva de Hurwitz generalizada. Porém, nesta análise, usaremos divisores tendo dois pontos base, isto é, divisores da forma $D = rP_1 + sP_2$ (P_1 e P_2 pontos no infinito), e veremos que, assim como no caso da Hermitiana, os parâmetros dos códigos associados são, quase sempre, da forma $(7, k = r + s, d = 7 - r - s)$. Na Seção 3.3 apresentaremos um resultado contendo informações sobre os parâmetros de códigos associados a curvas maximais de gênero $g = 1$.

3.1 Curva Hermitiana

Uma curva plana projetiva definida pela equação

$$\mathcal{C} : Y^q Z + Y Z^q = X^{q+1},$$

sobre o corpo $\mathbb{F}_{q^2}$ (q potência de primo) é chamada **curva Hermitiana**. Sabemos que estas curvas são não singulares, de gênero $g(\mathcal{C}) = \frac{q(q-1)}{2}$ e a quantidade de pontos racionais é dada por $\mathcal{C}(\mathbb{F}_{q^2}) = q^3 + 1$, [5] e [9].

Como estamos trabalhando com curvas de gênero 1 ($\frac{q(q-1)}{2} = 1 \Rightarrow q = 2$), vamos considerar a curva Hermitiana $\mathcal{C}$, sobre o corpo $\mathbb{F}_4$ ($\mathbb{F}_{q^2}$), definida pela equação

$$ZY^2 + Z^2Y = X^3. \tag{3.1}$$

A quantidade de pontos racionais ($\mathcal{C}(\mathbb{F}_{2^2}) = 2^3 + 1 = 9$) atinge a cota máxima para curvas de gênero 1. Logo, $\mathcal{C}$ é maximal. Vamos considerar

$$\mathbb{F}_4 = \frac{\mathbb{F}_2[t]}{\langle t^2 + t + 1 \rangle} = \{0, 1, \alpha, \alpha^2\},$$

onde $\alpha = \overline{t}$ e, portanto, satisfaz $\alpha^2 = \alpha + 1$.

A Tabela 3.1 ilustra os pontos racionais desta curva.

$P_\infty = (0:1:0)$	$P_1 = (0:0:1)$	$P_2 = (0:1:1)$
$P_3 = (1:\alpha:1)$	$P_4 = (1:\alpha^2:1)$	$P_5 = (\alpha:\alpha:1)$
$P_6 = (\alpha^2:\alpha^2:1)$	$P_7 = (\alpha^2:\alpha:1)$	$P_8 = (\alpha:\alpha^2:1)$

Tab. 3.1: Pontos $\mathbb{F}_4$-racionais da curva Hermitiana.

De acordo com o Teorema A.2.4, considerando $\mathcal{P} = \{P_1, ..., P_8\}$ e $D = rP_\infty$, temos que se $0 < gr(D) < 8$, o código resultante terá parâmetros $(n, k, d) = (8, gr(D), d)$, com $8 - gr(D) \leq d \leq 8 - gr(D) + 1$. Como $D = rP_\infty$, então

$$\mathcal{L}(D) = \{\varphi \in \mathbb{F}_q(\mathcal{C}) |\ div(\varphi) + rP_\infty \geq 0\}.$$

Para calcularmos a matriz geradora dos códigos de Goppa, precisamos conhecer alguma base do espaço $\mathcal{L}(D)$. Para encontrarmos uma base desse espaço, será interessante o conhecimento dos seguintes conjuntos:

- $\mathcal{C} \cap X = \{P \in \mathcal{C} |\ X = 0\} = \{P_\infty, P_1, P_2\}$;

- $\mathcal{C} \cap Y = \{P \in \mathcal{C} |\ Y = 0\} = \{P_1\}$;

- $\mathcal{C} \cap Z = \{P \in \mathcal{C} |\ Z = 0\} = \{P_\infty\}$.

Por meio desses conjuntos, podemos calcular os divisores de intersecção. Neste caso,

$$\begin{aligned} div(\mathcal{C} \cap X) &= P_\infty + P_1 + P_2; \\ div(\mathcal{C} \cap Y) &= 3P_1; \\ div(\mathcal{C} \cap Z) &= 3P_\infty. \end{aligned}$$

Desta forma,

$$div\left(\frac{X^i Y^j}{Z^{i+j}}\right) = (3j+i)P_1 + iP_2 - (2i+3j)P_\infty.$$

Portanto,

$$\frac{X^i Y^j}{Z^{i+j}} \in \mathcal{L}(rP_\infty) \iff 2i + 3j \leq r. \tag{3.2}$$

Tendo como base estas informações, o objetivo é determinar as bases dos espaços $\mathcal{L}(D)$ com elementos da forma $\dfrac{X^i Y^j}{Z^{i+j}}$. A seguir, analisaremos caso-a-caso a determinação dos códigos de Goppa com divisores da forma $D = rP_\infty$, com $1 \leq r \leq 7$.

- Caso 1: $D = 7P_\infty$

  O objetivo é determinar uma base para o espaço vetorial

  $$\mathcal{L}(7P_\infty) = \{\varphi \in \mathbb{F}_4(\mathcal{C});\ div(\varphi) + 7P_\infty \geq 0\}.$$

  De (3.2) temos

  $$\frac{X^i Y^j}{Z^{i+j}} \in \mathcal{L}(7P_\infty) \iff 2i + 3j \leq 7.$$

  Variando-se i e j, conseguimos o seguinte subconjunto de $\mathcal{L}(7P_\infty)$

  $$A = \left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY}{Z^2}, \frac{X^3}{Z^3}, \frac{X^2 Y}{Z^3}\right\}.$$

  Dos elementos encontrados, precisamos saber quais são linearmente independentes.

  Em (3.1), fazendo-se a divisão por Z^3 temos

$$\frac{Y^2}{Z^2} + \frac{Y}{Z} + \frac{X^3}{Z^3} = 0$$

isto é, os elementos

$$\frac{Y^2}{Z^2}, \frac{Y}{Z}, \frac{X^3}{Z^3}$$

são linearmente dependentes. Podemos, então, retirar o elemento $\frac{X^3}{Z^3}$ do conjunto A.

Lema 3.1.1 *O conjunto* $\mathcal{B}_1 = \left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}\right\}$ *é linearmente independente.*

Demonstração:

Suponhamos que existam $a_1, a_2, ..., a_7$, elementos em $\mathbb{F}_4$, tais que

$$a_1.1 + a_2\frac{X}{Z} + a_3\frac{Y}{Z} + a_4\frac{X^2}{Z^2} + a_5\frac{Y^2}{Z^2} + a_6\frac{XY}{Z^2} + a_7\frac{X^2Y}{Z^3} = 0.$$

Baseados na relação de equivalência do corpo de funções (A.2), temos

$$a_1Z^3 + a_2XZ^2 + a_3YZ^2 + a_4ZX^2 + a_5ZY^2 + a_6ZXY + a_7X^2Y \in \langle F \rangle,$$

isto é, o polinômio

$$G(X, Y, Z) = a_1Z^3 + a_2XZ^2 + a_3YZ^2 + a_4ZX^2 + a_5ZY^2 + a_6ZXY + a_7X^2Y$$

é divisível por $F(X, Y, Z) = Y^2Z + YZ^2 + X^3$, que é o polinômio que define a curva $\mathcal{C}$. Usando a ordem monomial $X > Y > Z$, temos que nenhum dos monômios de G é divisível por X^3 (termo líder do polinômio $F(X, Y, Z)$). Assim, a única possibilidade para a divisão é $a_i = 0$ para $i = 1, 2, ..., 7$. Portanto, os elementos do conjunto

$$\mathcal{B}_1 = \left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}\right\},$$

são linearmente independentes. ■

Como o espaço $\mathcal{L}(7P_\infty)$ tem dimensão 7, temos que o conjunto $\mathcal{B}_1$ é uma base. De acordo com (A.4), a matriz geradora do código é da forma

$$M_1 = [G_i(P_j)],\ i = 1, ..., 7,\ j = 1, ..., 8,$$

com $\{G_i\}$ uma base de $\mathcal{L}(7P_\infty)$. Neste caso, considerando-se

$$G_1 = 1,\ G_2 = \frac{X}{Z},\ G_3 = \frac{Y}{Z},\ G_4 = \frac{X^2}{Z^2},\ G_5 = \frac{Y^2}{Z^2},\ G_6 = \frac{XY}{Z^2},\ G_7 = \frac{X^2Y}{Z^3},$$

temos

$$M_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 & \alpha & 1 & 1 \\ 0 & 0 & \alpha & \alpha^2 & 1 & 1 & \alpha^2 & \alpha \end{bmatrix}.$$

Escrevendo a matriz M_1 na forma padrão, isto é, $M_1 = [Id_7|M_1']$, temos

$$M_1' = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}^t,$$

e a matriz verificação de paridade é da forma

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Assim, obtemos um código de Goppa C_1 com parâmetros $(n, k, d) = (8, 7, 2)$.

- $D = 6P_\infty$

  O objetivo é determinar uma base para o espaço vetorial

$$\mathcal{L}(6P_\infty) = \{\varphi \in \mathbb{F}_4(\mathcal{C});\ div(\varphi) + 6P_\infty \geq 0\}.$$

  O conjunto dos elementos da forma $\dfrac{X^iY^j}{Z^{i+j}}$ pertencentes ao espaço $\mathcal{L}(6P_\infty)$, é dado por

$$\mathcal{B}_2 = \left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY}{Z^2}\right\}.$$

  Como $\mathcal{B}_2 \subseteq \mathcal{B}_1$ (base de $\mathcal{L}(7P_\infty)$) , temos que $\mathcal{B}_2$ é linearmente independente e, portanto,

uma base do espaço. A matriz geradora do código é

$$M_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 & \alpha & 1 & 1 \end{bmatrix}.$$

Escrevendo a matriz M_2 na forma padrão, isto é, $M_2 = [Id_6|M_2']$, temos

$$M_2' = \begin{bmatrix} \alpha & \alpha & \alpha^2 & \alpha^2 & 0 & 1 \\ \alpha^2 & \alpha^2 & \alpha & \alpha & 1 & 0 \end{bmatrix}^t,$$

com a matriz verificação de paridade dada por

$$H_2 = \begin{bmatrix} \alpha & \alpha & \alpha^2 & \alpha^2 & 0 & 1 & 1 & 0 \\ \alpha^2 & \alpha^2 & \alpha & \alpha & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Assim, obtemos um código de Goppa C_2 com parâmetros $(n, k, d) = (8, 6, 2)$.

- $D = 5P_\infty$

  O objetivo é determinar uma base para o espaço vetorial

$$\mathcal{L}(5P_\infty) = \{\varphi \in \mathbb{F}_4(\mathcal{C});\ div(\varphi) + 5P_\infty \geq 0\}.$$

  O conjunto dos elementos da forma $\dfrac{X^iY^j}{Z^{i+j}}$ pertencentes ao espaço $\mathcal{L}(5P_\infty)$, é dado por

$$\mathcal{B}_3 = \left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}, \frac{XY}{Z^2}\right\}.$$

  Como $\mathcal{B}_3 \subseteq \mathcal{B}_2$ (base de $\mathcal{L}(6P_\infty)$), temos que $\mathcal{B}_3$ é linearmente independente e, portanto, uma base do espaço. A matriz geradora do código é

$$M_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha & \alpha & \alpha^2 \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 & \alpha & 1 & 1 \end{bmatrix}.$$

Escrevendo a matriz M_3 na forma padrão, isto é, $M_3 = [Id_5|M_3']$, temos

$$M_3' = \begin{bmatrix} 1 & \alpha^2 & \alpha^2 \\ 0 & \alpha & \alpha^2 \\ \alpha & 1 & \alpha \\ \alpha^2 & 0 & \alpha \\ 1 & 1 & 1 \end{bmatrix},$$

com a matriz verificação de paridade dada por

$$H_3 = \begin{bmatrix} 1 & 0 & \alpha & \alpha^2 & 1 & 1 & 0 & 0 \\ \alpha^2 & \alpha & 1 & 0 & 1 & 0 & 1 & 0 \\ \alpha^2 & \alpha^2 & \alpha & \alpha & 1 & 0 & 0 & 1 \end{bmatrix}$$

Assim, obtemos um código de Goppa C_3 com parâmetros $(n, k, d) = (8, 5, 3)$.

- $D = 4P_\infty$

  O objetivo é determinar uma base para o espaço vetorial

$$\mathcal{L}(4P_\infty) = \{\varphi \in \mathbb{F}_4(\mathcal{C});\ div(\varphi) + 4P_\infty \geq 0\}.$$

O conjunto dos elementos da forma $\dfrac{X^iY^j}{Z^{i+j}}$ pertencentes ao espaço $\mathcal{L}(4P_\infty)$, é dado por

$$\mathcal{B}_4 = \left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}\right\}.$$

Como $\mathcal{B}_4 \subseteq \mathcal{B}_3$ (base de $\mathcal{L}(5P_\infty)$), temos que $\mathcal{B}_4$ é linearmente independente e, portanto, uma base do espaço. A matriz geradora do código é

$$M_4 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha & \alpha & \alpha^2 \end{bmatrix}.$$

Escrevendo a matriz M_4 na forma padrão, isto é, $M_4 = [Id_4|M_4']$, temos

$$M_4' = \begin{bmatrix} 1 & \alpha & \alpha^2 & 1 \\ 1 & \alpha^2 & \alpha & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix},$$

com a matriz verificação de paridade dada por

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ \alpha & \alpha^2 & 1 & 1 & 0 & 1 & 0 & 0 \\ \alpha^2 & \alpha & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Assim, obtemos um códigos de Goppa C_4 com parâmetros $(n, k, d) = (8, 4, 4)$.

- $D = 3P_\infty$
  O objetivo é determinar uma base para o espaço vetorial

$$\mathcal{L}(3P_\infty) = \{\varphi \in \mathbb{F}_4(\mathcal{C});\ div(\varphi) + 3P_\infty \geq 0\}.$$

  O conjunto dos elementos da forma $\dfrac{X^i Y^j}{Z^{i+j}}$ pertencentes ao espaço $\mathcal{L}(3P_\infty)$, é dado por

$$\mathcal{B}_5 = \left\{1, \frac{X}{Z}, \frac{Y}{Z}\right\}.$$

  Como $\mathcal{B}_5 \subseteq \mathcal{B}_4$ (base de $\mathcal{L}(4P_\infty)$), temos que $\mathcal{B}_5$ é linearmente independente e, portanto, uma base do espaço. A matriz geradora do código é

$$M_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \end{bmatrix}.$$

  Escrevendo a matriz M_5 na forma padrão, isto é, $M_5 = [Id_3 | M_5']$, temos

$$M_5' = \begin{bmatrix} 1 & \alpha & 0 & 1 & \alpha^2 \\ 1 & 1 & \alpha & \alpha^2 & 0 \\ 1 & \alpha & \alpha^2 & \alpha^2 & \alpha \end{bmatrix},$$

  com a matriz verificação de paridade dada por

$$H_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ \alpha & 1 & \alpha & 0 & 1 & 0 & 0 & 0 \\ 0 & \alpha & \alpha^2 & 0 & 0 & 1 & 0 & 0 \\ 1 & \alpha^2 & \alpha^2 & 0 & 0 & 0 & 1 & 0 \\ \alpha^2 & 0 & \alpha & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Assim, obtemos um código de Goppa C_5 com parâmetros $(n, k, d) = (8, 3, 5)$.

- $D = 2P_\infty$
  O objetivo é determinar uma base para o espaço vetorial

$$\mathcal{L}(2P_\infty) = \{\varphi \in \mathbb{F}_4(\mathcal{C});\ div(\varphi) + 2P_\infty \geq 0\}.$$

  O conjunto dos elementos da forma $\dfrac{X^i Y^j}{Z^{i+j}}$ pertencentes ao espaço $\mathcal{L}(2P_\infty)$, é dado por

$$\mathcal{B}_6 = \left\{1, \frac{X}{Z}\right\}.$$

  Como $\mathcal{B}_6 \subseteq \mathcal{B}_5$ (base de $\mathcal{L}(3P_\infty)$), temos que $\mathcal{B}_6$ é linearmente independente e, portanto, uma base do espaço. A matriz geradora do código é

$$M_6 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha^2 & \alpha^2 & \alpha \end{bmatrix}.$$

  Escrevendo a matriz M_6 na forma padrão, isto é, $M_6 = [Id_2 | M_6']$, temos

$$M_6' = \begin{bmatrix} 1 & 0 & \alpha^2 & \alpha & \alpha & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & \alpha^2 & \alpha \end{bmatrix},$$

  com a matriz verificação de paridade dada por

$$H_6 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ \alpha^2 & \alpha & 0 & 0 & 1 & 0 & 0 & 0 \\ \alpha & \alpha^2 & 0 & 0 & 0 & 1 & 0 & 0 \\ \alpha & \alpha^2 & 0 & 0 & 0 & 0 & 1 & 0 \\ \alpha^2 & \alpha & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

  Assim, obtemos um código de Goppa C_6 com parâmetros $(n, k, d) = (8, 2, 6)$.

- $D = P_\infty$
  Neste caso, obtemos um código de Goppa C_7, com parâmetros $(n, k, d) = (8, 1, 8)$ e a matriz geradora correspondente é dada por

$$M_7 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Observação 3.1.1 *Note que, a inclusão dos espaços vetoriais*

$$\mathcal{L}(P_\infty) \subseteq \mathcal{L}(2P_\infty) \subseteq ... \subseteq \mathcal{L}(7P_\infty),$$

resulta na seguinte relação entre os códigos associados

$$C_1 \supseteq C_2 \supseteq ... \supseteq C_7.$$

3.2 Curva de Hurwitz

Em [10] é mostrado que o modelo não singular da curva

$$X^nY + Y^nZ + Z^nX = 0,$$

é maximal em $\mathbb{F}_{q^2}$ se, e somente se, $q+1 \equiv 0 \ mod(n^2-n+1)$. Esta família de curvas é conhecida como **curvas de Hurwitz**. Considerando-se $q=2,\ n=2$, vemos que a condição anterior é satisfeita. Assim, o modelo não singular da curva $\mathcal{C}$ definida por

$$X^2Y + Y^2Z + Z^2X = 0,$$

é maximal em $\mathbb{F}_4$. Porém, como

$$\frac{\partial F}{\partial X} = Z^2,\ \frac{\partial F}{\partial Y} = X^2,\ \frac{\partial F}{\partial Z} = Y^2,$$

então a curva $\mathcal{C}$ é não singular. Além disso, o gênero desta curva é $g(\mathcal{C}) = 1$ e, assim como a curva Hermitiana da Seção 4.1, temos $\mathcal{C}(\mathbb{F}_4) = 9$. Os pontos racionais da curva $\mathcal{C}$ são apresentados na Tabela 3.2.

$P_1 = (0:1:0)$	$P_2 = (1:0:0)$	$P_3 = (0:0:1)$
$P_4 = (1:\alpha:1)$	$P_5 = (1:\alpha^2:1)$	$P_6 = (\alpha:1:1)$
$P_7 = (\alpha^2:1:1)$	$P_8 = (\alpha:\alpha:1)$	$P_9 = (\alpha^2:\alpha^2:1)$

Tab. 3.2: Pontos $\mathbb{F}_4$-racionais da curva de Hurwitz.

Além disso, temos que

$$\begin{aligned}\mathcal{C} \cap X &= \{P \in \mathcal{C} |\ X = 0\} = \{P_1, P_3\},\\ \mathcal{C} \cap Y &= \{P \in \mathcal{C} |\ Y = 0\} = \{P_2, P_3\},\\ \mathcal{C} \cap Z &= \{P \in \mathcal{C} |\ Z = 0\} = \{P_1, P_2\},\end{aligned}$$

e os divisores de intersecção são dados por:

$$\begin{aligned}div(\mathcal{C} \cap X) &= 2P_3 + P_1;\\ div(\mathcal{C} \cap Y) &= 2P_2 + P_3;\\ div(\mathcal{C} \cap Z) &= 2P_1 + P_2.\end{aligned}$$

Portanto,

$$div\left(\frac{X^iY^j}{Z^{i+j}}\right) = (2i+j)P_3 + (j-i)P_2 - (2j+i)P_1.$$

Tendo como base as informações anteriores, e considerando divisores da forma $D = rP_1 + sP_2$ temos

$$\frac{X^iY^j}{Z^{i+j}} \in \mathcal{L}(D) \Longleftrightarrow 2j + i \leq r \text{ e } i \leq j + s. \tag{3.3}$$

De acordo com o Teorema A.2.4 , considerando $\mathcal{P} = \{P_3, ..., P_9\}$ e se $0 < gr(D) = r + s < 7$, o código de Goppa terá parâmetros $(n, k, d) = (7, gr(D), d)$, com $7 - gr(D) \leq d \leq 7 - gr(D) + 1$.

A seguir, analisaremos caso-a-caso a determinação dos códigos de Goppa quando o grau do divisor varia entre 1 e 6.

1. ***gr(D)=r+s=6***

   Neste caso, a dimensão do espaço é 6 e, portanto, devemos ter 6 elementos linearmente independentes da forma $\frac{X^iY^j}{Z^{i+j}}$. Variando-se os valores de r e s em (3.3), resulta na Tabela 3.3.

   Nas três primeiras linhas da Tabela 3.3 não foi possível encontrar seis elementos que sejam linearmente independentes restando, então, as seguintes possibilidades:

   - $\boldsymbol{2j+i \leq 3,\ i \leq j+3}$

     Neste caso, os elementos

$$G_1 = 1,\ G_2 = \frac{X}{Z},\ G_3 = \frac{Y}{Z},\ G_4 = \frac{XY}{Z^2},\ G_5 = \frac{X^2}{Z^2},\ G_6 = \frac{X^3}{Z^3},$$

r	s	condição
0	6	$2j+i \leq 0,\ i \leq j+6$
1	5	$2j+i \leq 1,\ i \leq j+5$
2	4	$2j+i \leq 2,\ i \leq j+4$
3	3	$2j+i \leq 3,\ i \leq j+3$
4	2	$2j+i \leq 4,\ i \leq j+2$
5	1	$2j+i \leq 5,\ i \leq j+1$
6	0	$2j+i \leq 6,\ i \leq j+0$

Tab. 3.3: Condições para $r+s=6$.

pertencem ao espaço $\mathcal{L}(3P_1+3P_2)$ e são linearmente independentes. De fato, se existirem elementos $a_i \in \mathbb{F}_4,\ i=1,2,..,6$ tais que

$$a_1.1 + a_2\frac{X}{Z} + a_3\frac{Y}{Z} + a_4\frac{XY}{Z^2} + a_5\frac{X^2}{Z^2} + a_6\frac{X^3}{Z^3} = 0,$$

então

$$a_1Z^3 + a_2XZ^2 + a_3YZ^2 + a_4XYZ + a_5X^2Z + a_6X^3 \in \langle X^2Y + Y^2Z + Z^2X\rangle.$$

Tomando-se a ordem monomial $Y > X > Z$ temos que nenhum dos monômios da combinação linear é divisível por Y^2Z (termo líder do polinômio gerador da curva). Portanto, $a_i = 0$, $1 \leq i \leq 6$. Sendo

$$M = [G_i(P_j)],\ i=1,...,6,\ j=3,...,9$$

a matriz geradora do código, então

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & 1 & 1 & \alpha^2 & \alpha & \alpha^2 & \alpha \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

dando origem a um código de Goppa com parâmetros $(n,k,d) = (7,6,1)$.

- $\boldsymbol{2j+i \leq 4,\ i \leq j+2}$

Neste caso, uma base para o espaço $\mathcal{L}(4P_1 + 2P_2)$ é dada pelo conjunto

$$\left\{G_1 = 1, G_2 = \frac{X}{Z}, G_3 = \frac{Y}{Z}, G_4 = \frac{XY}{Z^2}, G_5 = \frac{X^2}{Z^2}, G_6 = \frac{Y^2}{Z^2}\right\}.$$

Calculando a matriz geradora $M = [G_i(P_j)]$ temos

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & 1 & 1 & \alpha^2 & \alpha & \alpha^2 & \alpha \\ 0 & \alpha^2 & \alpha & 1 & 1 & \alpha^2 & \alpha \end{bmatrix}.$$

Escrevendo M na forma padrão, isto é, $M = [Id_6|M']$, temos

$$M' = \begin{bmatrix} \alpha & 1 & \alpha^2 & 1 & \alpha^2 & \alpha^2 \end{bmatrix}^t.$$

Dessa forma, a matriz verificação de paridade do código é dada por

$$H = \begin{bmatrix} \alpha & 1 & \alpha^2 & 1 & \alpha^2 & \alpha^2 & 1 \end{bmatrix},$$

e o código de Goppa associado é um código com parâmetros $(n, k, d) = (7, 6, 2)$.

- $\boldsymbol{2j+i \leq 5,\ i \leq j+1}$

  Neste caso, uma base para o espaço $\mathcal{L}(5P_1 + P_2)$ é dada pelo conjunto

$$\left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY^2}{Z^3}\right\}.$$

  Calculando a matriz geradora temos

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & \alpha^2 & \alpha & 1 & 1 & \alpha^2 & \alpha \\ 0 & \alpha^2 & \alpha & \alpha & \alpha^2 & 1 & 1 \end{bmatrix}.$$

Escrevendo M na forma padrão, isto é, $M = [Id_6|M']$, temos

$$M' = \begin{bmatrix} \alpha & 1 & \alpha^2 & 1 & \alpha^2 & \alpha^2 \end{bmatrix}^t.$$

Assim, o código de Goppa associado tem parâmetros $(7, 6, 2)$.

- $\boldsymbol{2j+i \leq 6,\ i \leq j+0}$

  Neste caso, uma base para o espaço $\mathcal{L}(6P_1)$ é dada pelo conjunto

$$\left\{1, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY^2}{Z^3}, \frac{Y^3}{Z^3}\right\}.$$

  Calculando a matriz geradora temos

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & \alpha^2 & \alpha & 1 & 1 & \alpha^2 & \alpha \\ 0 & \alpha^2 & \alpha & \alpha & \alpha^2 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

  O código de Goppa associado neste caso tem parâmetros $(n, k, d) = (7, 6, 1)$.

2. $\boldsymbol{gr(D)=r+s=5}$

   Assim como no caso anterior, variando-se os valores de r e s, resulta na Tabela 3.4.

r	s	condição
0	5	$2j + i \leq 0,\ i \leq j + 5$
1	4	$2j + i \leq 1,\ i \leq j + 4$
2	3	$2j + i \leq 2,\ i \leq j + 3$
3	2	$2j + i \leq 3,\ i \leq j + 2$
4	1	$2j + i \leq 4,\ i \leq j + 1$
5	0	$2j + i \leq 5,\ i \leq j + 0$

Tab. 3.4: Condições para $r + s = 5$.

Nas três primeiras linhas da Tabela 3.4 não foi possível encontrar bases da forma $\frac{X^iY^j}{Z^{i+j}}$. Desta forma, consideraremos os seguintes casos:

- $\boldsymbol{2j+i \leq 3,\ i \leq j+2}$

  Neste caso, uma base para o espaço $\mathcal{L}(3P_1 + 2P_2)$ é o conjunto

  $$\left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2}{Z^2}\right\},$$

  e a matriz geradora do código é dada por

  $$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & 1 & 1 & \alpha^2 & \alpha & \alpha^2 & \alpha \end{bmatrix}.$$

  O polinômio $P(X, Y, Z) = (X + Y)(X + Z) = X^2 + XZ + YX + YZ$ se anula nos pontos P_3, P_4, P_5, P_8, P_9. Dessa forma, o elemento

  $$\frac{X^2}{Z^2} + \frac{X}{Z} + \frac{YX}{Z^2} + \frac{Y}{Z}$$

  gera uma palavra-código com peso 2. Logo, o código associado tem parâmetros $(7, 5, 2)$.

- $\boldsymbol{2j+i \leq 4,\ i \leq j+1}$

  Neste caso, uma base para o espaço $\mathcal{L}(4P_1 + P_2)$ é o conjunto

  $$\left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{Y^2}{Z^2}\right\},$$

  e a matriz geradora do código é dada por

  $$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & \alpha^2 & \alpha & 1 & 1 & \alpha^2 & \alpha \end{bmatrix}.$$

  O polinômio $P(X, Y, Z) = (Y + X)(Y + Z) = Y^2 + YZ + XY + XZ$ se anula nos

pontos P_3, P_4, P_5, P_8, P_9. Dessa forma, o elemento

$$\frac{Y^2}{Z^2} + \frac{Y}{Z} + \frac{XY}{Z^2} + \frac{X}{Z}$$

gera uma palavra-código com peso 2. Logo, o código associado tem parâmetros $(7, 5, 2)$.

- $\boldsymbol{2j+i \leq 5,\ i \leq j+0}$

  Neste caso, uma base para o espaço $\mathcal{L}(5P_1)$ é o conjunto

$$\left\{1, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY^2}{Z^3}\right\},$$

  e a matriz geradora associada é dada por

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & \alpha^2 & \alpha & 1 & 1 & \alpha^2 & \alpha \\ 0 & \alpha^2 & \alpha & \alpha & \alpha^2 & 1 & 1 \end{bmatrix}.$$

  Somando-se as 4 últimas linhas da matriz, obtemos uma palavra-código com peso 2. Dessa forma, o código associado tem parâmetros $(7, 5, 2)$.

3. $\boldsymbol{gr(D)=r+s=4}$

Assim como nos casos anteriores, a Tabela 3.5 ilustra as condições a serem satisfeitas.

r	s	condição
0	4	$2j + i \leq 0,\ i \leq j + 4$
1	3	$2j + i \leq 1,\ i \leq j + 3$
2	2	$2j + i \leq 2,\ i \leq j + 2$
3	1	$2j + i \leq 3,\ i \leq j + 1$
4	0	$2j + i \leq 4,\ i \leq j + 0$

Tab. 3.5: Condições para $r + s = 4$.

Nas duas primeiras linhas da Tabela 3.5 não foi possível encontrar bases da forma $\frac{X^iY^j}{Z^{i+j}}$. Assim, iremos considerar as três últimas linhas da tabela mencionada.

- $\boldsymbol{2j+i \leq 2,\ i \leq j+2}$

  Neste caso, uma base para o espaço $\mathcal{L}(2P_1 + 2P_2)$ é o conjunto

  $$\left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}\right\},$$

  e a matriz geradora é dada por

  $$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \\ 0 & 1 & 1 & \alpha^2 & \alpha & \alpha^2 & \alpha \end{bmatrix}.$$

  O polinômio $P(X, Y, Z) = X^2 + XZ + Z^2$ se anula nos pontos P_6, P_7, P_8, P_9. Logo, o elemento

  $$\frac{X^2}{Z^2} + \frac{XZ}{Z^2} + 1,$$

  gera uma palavra-código com peso 3. Temos, então, um código com parâmetros $(7, 4, 3)$.

- $\boldsymbol{2j+i \leq 3,\ i \leq j+1}$

  Neste caso, uma base para o espaço $\mathcal{L}(3P_1 + P_2)$ é o conjunto

  $$\left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{XY}{Z^2}\right\}.$$

  Dessa forma, a matriz geradora associada é dada por

  $$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha \end{bmatrix}.$$

  O polinômio $P(X, Y, Z) = (X + Z)(Y + Z) = XY + XZ + YZ + Z^2$ se anula nos pontos P_4, P_5, P_6, P_7. Logo, o elemento

  $$\frac{XY}{Z^2} + \frac{X}{Z} + \frac{Y}{Z} + 1,$$

  gera uma palavra-código com peso 3. Dessa forma, o código associado tem parâmetros $(7, 4, 3)$.

- $\boldsymbol{2j+i \leq 4,\ i \leq j+0}$
  Neste caso, uma base para o espaço $\mathcal{L}(4P_1)$ é o conjunto

$$\left\{1, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{Y^2}{Z^2}\right\},$$

  e matriz geradora é dada por

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & \alpha^2 & \alpha & 1 & 1 & \alpha^2 & \alpha \end{bmatrix}.$$

  O elemento

$$\frac{Y^2}{Z^2} + \frac{Y}{Z} + 1,$$

  se anula nos pontos P_4, P_5, P_8, P_9, gerando, assim, uma palavra-código com peso 3. Dessa forma, o código associado tem parâmetros $(7, 4, 3)$.

4. $\boldsymbol{gr(D)=r+s=3}$
   A variação de r e s dá origem à Tabela 3.6.

r	s	condição
0	3	$2j + i \leq 0,\ i \leq j + 3$
1	2	$2j + i \leq 1,\ i \leq j + 2$
2	1	$2j + i \leq 2,\ i \leq j + 1$
3	0	$2j + i \leq 3,\ i \leq j + 0$

Tab. 3.6: Condições para $r + s = 3$.

Assim como nos casos anteriores, nas duas primeiras linhas da Tabela 3.6 não foi possível encontrar 3 elementos linearmente indepedentes. Desse modo, só nos resta considerar as duas últimas linhas.

- $\boldsymbol{2j+i \leq 2,\ i \leq j+1}$
  Neste caso, uma base para o espaço $\mathcal{L}(2P_1 + P_2)$ é o conjunto

$$\left\{1, \frac{X}{Z}, \frac{Y}{Z}\right\},$$

e a matriz geradora é dada por

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \end{bmatrix}.$$

O elemento

$$\frac{X}{Z} + \frac{Y}{Z},$$

se anula nos pontos P_3, P_8, P_9, gerando uma palavra-código com peso 4. Portanto, o código associado tem parâmetros $(7, 3, 4)$.

- $\boldsymbol{2j+i \leq 3,\ i \leq j+0}$

  Neste caso, uma base para o espaço $\mathcal{L}(3P_1)$ é o conjunto

$$\left\{1, \frac{Y}{Z}, \frac{XY}{Z^2}\right\},$$

  e a matriz geradora é dada por

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha \end{bmatrix}.$$

  O polinômio $P(X, Y, Z) = Y(X + Z) = XY + YZ$ se anula nos pontos P_3, P_4, P_5. Dessa forma, o elemento

$$\frac{XY}{Z^2} + \frac{Y}{Z},$$

  nos fornece uma palavra-código com peso 4. Desta forma, o código associado tem parâmetros $(7, 3, 4)$.

5. $\boldsymbol{gr(D)=r+s=2}$

   Neste caso, os códigos associados terão parâmetros $n = 7,\ k = deg(D) = 2,\ 5 \leq d \leq 6$. A variação de r e s dá origem à Tabela 3.7.

   Assim como nos casos anteriores, na primeira linha da Tabela 3.7 não foi possível encontrar dois elementos linearmente indepedentes. Desse modo, só nos resta considerar as duas últimas linhas.

   - $\boldsymbol{2j+i \leq 1,\ i \leq j+1}$

r	s	condição
0	2	$2j+i \leq 0,\ i \leq j+2$
1	1	$2j+i \leq 1,\ i \leq j+1$
2	0	$2j+i \leq 2,\ i \leq j+0$

Tab. 3.7: Condições para $r+s=2$.

Neste caso, uma base para o espaço $\mathcal{L}(P_1+P_2)$ é o conjunto

$$\left\{1, \frac{X}{Z}\right\},$$

e a matriz geradora dada por

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 \end{bmatrix}.$$

O elemento

$$\frac{X}{Z}+1,$$

se anula nos pontos P_4, P_5 gerando, então, uma palavra-código com peso 5. Desta forma, o código associado tem parâmetros $(7,2,5)$.

- $\boldsymbol{2j+i \leq 2,\ i \leq j+0}$

  Neste caso, uma base para o espaço $\mathcal{L}(2P_1)$ é o conjunto

$$\left\{1, \frac{Y}{Z}\right\},$$

  e a matriz geradora é dada por

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & \alpha^2 \end{bmatrix}.$$

  O elemento

$$\frac{Y}{Z}+1,$$

  se anula nos pontos P_6, P_7 gerando, então, uma palavra-código com peso 5. Desta forma, o código associado tem parâmetros $(7,2,5)$.

Observação 3.2.1 *Da mesma forma que no caso de divisores com um único ponto base, se*

$r_1 \leq r_2$ então existe a inclusão dos espaços vetoriais

$$\mathcal{L}(r_1P_1 + sP_2) \subseteq \mathcal{L}(r_2P_1 + sP_2),$$

e o código associado ao espaço $\mathcal{L}(r_1P_1 + sP_2)$ é um subcódigo do código associado ao espaço $\mathcal{L}(r_2P_1 + sP_2)$.

3.3 Curvas Elípticas

Nesta seção serão obtidos os parâmetros de todos os códigos associados às curvas elípticas maximais, isto é, curvas de gênero $g = 1$ e que sejam maximais. Isto será feito por meio da seguinte proposição.

Proposição 3.3.1 *: Seja $\mathcal{X}$ uma curva elíptica maximal sobre o corpo finito $K = \mathbb{F}_{p^{2t}}$, seja $P_\infty = (0 : 1 : 0)$ o ponto no infinito de $\mathbb{P}^2(K)$, $D = rP_\infty$ um divisor sobre $\mathcal{X}$ e $\mathcal{P} = \{$pontos racionais$\}\backslash\{P_\infty\}$. Então vale:*

- *$car(K) = 2$*
  O código $\mathcal{C}(\mathcal{X}, \mathcal{P}, D)$ possui parâmetros $n = 2^{2t} + 2^{t+1}$, $k = r$, $d = n - r$ se r for um número par. Se r for ímpar então $d = n - r$ ou $d = n - r + 1$, o que não altera a quantidade de erros corrigidos pelo código.

- *$car(K) = p \neq 2$*
  O código $\mathcal{C}(\mathcal{X}, \mathcal{P}, D)$ possui parâmetros $n = p^{2t} + 2p^t$, $k = r$, $d = n - r$.

Demonstração:

- *$car(K) = 2$*

De acordo com [8] a curva $\mathcal{X}$ pode ser escrita como

$$ZY^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2ZX^2 + a_4XZ^2 + a_6Z^3. \tag{3.4}$$

Como, por hipótese, a curva é maximal, então deverá conter $1 + 2^{2t} + 2^{t+1}$ pontos racionais. Substituindo $Z = 0$ em (3.4) temos $X^3 = 0$. Assim, $P_\infty = (0 : 1 : 0) \in \mathcal{X}$ e $div(\mathcal{X} \cap Z) = 3P_\infty$.

Os restantes $2^{2t} + 2^{t+1}$ pontos racionais possuem coordenada $Z = 1$. Dado $\alpha \in \mathbb{F}_{2^{2t}}$, substituindo $X = \alpha$ em (3.4) obtemos

$$Y^2 + (a_1\alpha + a_3)Y = \alpha^3 + a_2\alpha^2 + a_4\alpha + a_6. \tag{3.5}$$

Se $a_1 \neq 0$, tomando-se $\alpha = \frac{a_3}{a_1}$ a equação (3.5) transforma-se em

$$Y^2 = \alpha^3 + a_2\alpha^2 + a_4\alpha + a_6,$$

possuindo solução única. Mais ainda, dado $\beta \neq \alpha$ a equação

$$Y^2 + (a_1\beta + a_3)Y = \beta^3 + a_2\beta^2 + a_4\beta + a_6$$

possui duas ou nenhuma solução. Assim, caso $a_1 \neq 0$ conseguiremos um número ímpar de pontos racionais com coordenada $Z = 1$. Como precisamos de $2^{2t} + 2^{t+1}$ pontos concluímos que, se a curva é maximal, devemos ter $a_1 = 0$. Além disso, existem $\frac{2^{2t}+2^{t+1}}{2} = 2^{2t-1} + 2^t$ elementos em $\mathbb{F}_{2^{2t}}$ para os quais a equação

$$Y^2 + a_3Y = \alpha^3 + a_2\alpha^2 + a_4\alpha + a_6, \tag{3.6}$$

possui duas soluções. Sejam $\alpha_i,\ i = 1, 2, ..., 2^{2t-1} + 2^t$, os elementos em $\mathbb{F}_{2^{2t}}$ para os quais a equação (3.6) possui 2 soluções. Desta forma, os pontos racionais são $(\alpha_i : \beta_1^i : 1),\ (\alpha_i : \beta_2^i : 1),\ i = 1, ..., 2^{2t-1} + 2^t$.

Os outros divisores de intersecção são dados por

$$div(\mathcal{X} \cap X) = P_\infty + Q_1 + Q_2;$$
$$div(\mathcal{X} \cap Y) = R_1 + R_2 + R_3,\ R_i \neq P_\infty.$$

Desta forma, temos

$$div\left(\frac{X^iY^j}{Z^{i+j}}\right) = i(P_\infty + Q_1 + Q_2) + j(R_1 + R_2 + R_3) - 3(i+j)P_\infty =$$
$$= i(Q_1 + Q_2) + j(R_1 + R_2 + R_3) - (2i + 3j)P_\infty.$$

Como os divisores são da forma $D = rP_\infty$, segue que

$$\frac{X^iY^j}{Z^{i+j}} \in \mathcal{L}(D) \Leftrightarrow 2i + 3j \leq r.$$

- $0 < r = 2u < 2^{2t} + 2^{t+1}$
  Neste caso, temos
  $$1, \frac{X}{Z}, ..., \frac{X^u}{Z^u} \in \mathcal{L}(D).$$

O elemento

$$\frac{X^u}{Z^u} + S_1(\alpha_1, ..., \alpha_u)\frac{X^{u-1}}{Z^{u-1}} + S_2(\alpha_1, ..., \alpha_u)\frac{X^{u-2}}{Z^{u-2}} + ... + S_u(\alpha_1, ..., \alpha_u),$$

onde os S_i's são os polinômios simétricos elementares, se anula em $2u = r$ pontos racionais, isto é, temos uma palavra-código com peso $n - r$. Portanto, $d = n - r$.

- $0 < r = 2u + 1 < 2^{2t} + 2^{t+1}$

  Neste caso, sabemos que $d = n - r$ ou $d = n - r + 1$. Porém, temos também que $\left[\frac{n-r-1}{2}\right] = \left[\frac{2^{2t}+2^{t+1}-2u-2}{2}\right] = 2^{2t-1} + 2^t - u - 1$;

  $\left[\frac{n-r+1-1}{2}\right] = \left[\frac{2^{2t}+2^{t+1}-2u-1}{2}\right] = 2^{2t-1} + 2^t - u - 1.$

  Portanto, sendo $d = n-r$ ou $d = n-r+1$, não teremos alteração na quantidade de erros corrigidos pelo código.

- $car(K) = p \neq 2$

Neste caso, usando a forma canônica de Legendre [8], a curva tem equação da forma

$$Y^2 = X(X-1)(X-\lambda),\ \lambda \in K,\ \lambda \neq 0, 1.$$

Os divisores de intersecção são dados por

$$\begin{aligned} &div(\mathcal{X} \cap Z) = 3P_\infty; \\ &div(\mathcal{X} \cap X) = P_\infty + 2(0:0:1) = P_\infty + 2P_1; \\ &div(\mathcal{X} \cap Y) = Q_1 + Q_2 + Q_3,\ Q_i \neq P_\infty. \end{aligned}$$

Desta forma,

$$\begin{aligned} div\left(\frac{X^iY^j}{Z^{i+j}}\right) = i(P_\infty + 2P_1) + j(Q_1 + Q_2 + Q_3) - 3(i+j)P_\infty = \\ = 2iP_1) + j(Q_1 + Q_2 + Q_3) - (2i + 3j)P_\infty. \end{aligned}$$

Portanto,

$$\frac{X^iY^j}{Z^{i+j}} \in \mathcal{L}(D) \Leftrightarrow 2i + 3j \leq r.$$

Como a curva é maximal ela deve possuir $1+p^{2t}+2p^t$ pontos racionais. O ponto $P_\infty = (0:1:0)$ é, novamente, o único ponto no infinito e, pela equação da curva, podemos encontrar também os pontos $P_1 = (0:0:1),\ P_2 = (1:0:1),\ P_3 = (\lambda:0:1)$. Os demais $p^{2t} + 2p^t - 3$ pontos

racionais são da forma $(\alpha_i : \beta_1^i : 1),\ (\alpha_i : \beta_2^i : 1),$ com $i = 1, ..., \frac{p^{2t}+2p^t-3}{2}$.

- $r = p^{2t} + 2p^t - 1$(par)
  Neste caso, temos que $d = 1$ ou $d = 2$ e este código denotará a modulação ou o rótulo dos pontos da constelação de sinais.

- $0 < r = 2u < p^{2t} + 2p^t - 3$
  Neste caso, temos
  $$1, \frac{X}{Z}, ..., \frac{X^u}{Z^u} \in \mathcal{L}(D),$$
  e o elemento
  $$\frac{X^u}{Z^u} + S_1(\alpha_1, ..., \alpha_u)\frac{X^{u-1}}{Z^{u-1}} + S_2(\alpha_1, ..., \alpha_u)\frac{X^{u-2}}{Z^{u-2}} + ... + S_u(\alpha_1, ..., \alpha_u)$$
  se anula em $2u = r$ pontos racionais, gerando uma palavra-código com peso $n - r$. Portanto, $d = n - r$.

- $r = 3$
  Neste caso, $\frac{Y}{Z} \in \mathcal{L}(3P_\infty)$ e este se anula em $P_1,\ P_2$ e P_3, gerando uma palavra-código com peso $n - 3$.

- $3 < r = 2u + 1 < p^{2t} + 2^p t$
  Seja $r - 3 = 2v$. Temos que
  $$1, \frac{XY}{Z^2}, ..., \frac{X^vY}{Z^{v+1}} \in \mathcal{L}(D).$$
  O elemento
  $$\frac{X^vY}{Z^{v+1}} + S_1(\alpha_1, ..., \alpha_v)\frac{X^{v-1}Y}{Z^v} + S_2(\alpha_1, ..., \alpha_v)\frac{X^{v-2}Y}{Z^{v-1}} + ... + S_v(\alpha_1, ..., \alpha_v)\frac{Y}{Z},$$
  se anula em $2v + 3 = r$ pontos racionais, gerando uma palavra-código com peso $n - r$.

Além de encontrarmos os parâmetros dos códigos associados aos espaços $\mathcal{L}(rP_\infty)$, podemos também encontrar geradores para estes espaços. Para isso, vamos considerar os seguintes casos:

- $r = 3q$
  Os elementos
  $$1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}, ..., \frac{Y^{q-1}}{Z^{q-1}}, \frac{XY^{q-1}}{Z^q}, \frac{Y^q}{Z^q}$$
  estão em $\mathcal{L}(D)$ e são todos linearmente independentes. Como temos $3(q-2)+6 = 3q$ elementos, eles formam uma base do espaço.

- $r = 3q + 1$
  Os elementos

$$1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}, ..., \frac{Y^{q-1}}{Z^{q-1}}, \frac{XY^{q-1}}{Z^q}, \frac{X^2Y^{q-1}}{Z^{q+1}}, \frac{Y^q}{Z^q}$$

  estão em $\mathcal{L}(D)$ e são todos linearmente independentes. Como temos $3(q-1)+4 = 3q+1$ elementos, eles formam uma base do espaço.

- $r = 3q + 2$
  Os elementos

$$1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}, ..., \frac{Y^{q-1}}{Z^{q-1}}, \frac{XY^{q-1}}{Z^q}, \frac{X^2Y^{q-1}}{Z^{q+1}}, \frac{Y^q}{Z^q}, \frac{XY^q}{Z^{q+1}}$$

  estão em $\mathcal{L}(D)$ e são todos linearmente independentes. Como temos $3(q-1)+5 = 3q+2$ elementos, eles formam uma base do espaço.

Podemos observar que se $r_1 < r_2$ então $\mathcal{L}(r_1P_\infty)$ é um subespaço de $\mathcal{L}(r_2P_\infty)$ e o código $\mathcal{C}(\mathcal{X}, \mathcal{P}, r_1P_\infty)$ é um subcódigo de $\mathcal{C}(\mathcal{X}, \mathcal{P}, r_2P_\infty)$. ■

3.4 Conclusões

Neste capítulo, por meio de dois exemplos, apresentamos a construção de códigos de Goppa associados a curvas elípticas (gênero $g = 1$) maximais. Vimos também que, em sua maioria, os códigos possuem parâmetros $(n, k, d = n - k)$.

Capítulo 4

Curvas com Gêneros $g = 2$ e $g = 3$

Neste capítulo, vamos analisar os parâmetros dos códigos de Goppa provenientes de curvas com gêneros $g = 2$ e $g = 3$, usando as idéias apresentadas na Observação A.2.1. No caso $g = 2$, uma das dificuldades encontradas foi que curvas com este gênero são sempre curvas singulares e o processo de dessingularização não é um processo simples de ser tratado. No caso $g = 3$, a dificuldade encontrada foi a obtenção de curvas maximais com este gênero. Mostraremos também que os códigos de Goppa podem ser utilizados para fazer concatenações de códigos.

Este capítulo está organizado da seguinte forma. Na Seção 4.1, analisaremos os parâmetros dos códigos associados a uma curva de gênero 2, maximal sobre $\mathbb{F}_{16}$ encontrada em [11]. Na Seção 4.2, analisaremos os parâmetros dos códigos associados à quártica de Klein, que é a curva conhecida, de gênero 3, com o maior número de pontos. Na Seção 4.3, veremos o conceito de concatenação generalizada ou equivalentemente, codificação multinível, apresentada em [12], e como os códigos algébrico-geométricos podem ser usados para fazer este tipo de concatenação.

4.1 Curva com Gênero 2

Em [11] é mostrado que a curva dada pela equação

$$\mathcal{C} : Y^2Z^3 + YZ^4 + X^5 = 0,$$

é singular no ponto $P_\infty = (0 : 1 : 0)$, tem gênero $g = 2$ e é maximal sobre $\mathbb{F}_{16}$. Os pontos racionais desta curva são mostrados na Tabela 4.1.

$P_1 = (0 : 0 : 1)$	$P_2 = (0 : 1 : 1)$	$P_3 = (1 : \alpha^5 : 1)$	$P_4 = (1 : \alpha^{10} : 1)$
$P_5 = (\alpha : \alpha : 1)$	$P_6 = (\alpha^2 : \alpha^2 : 1)$	$P_7 = (\alpha^4 : \alpha^4 : 1)$	$P_8 = (\alpha^8 : \alpha^8 : 1)$
$P_9 = (\alpha : \alpha^4 : 1)$	$P_{10} = (\alpha^2 : \alpha^8 : 1)$	$P_{11} = (\alpha^4 : \alpha : 1)$	$P_{12} = (\alpha^8 : \alpha^2 : 1)$
$P_{13} = (\alpha^3 : \alpha^5 : 1)$	$P_{14} = (\alpha^6 : \alpha^{10} : 1)$	$P_{15} = (\alpha^{12} : \alpha^5 : 1)$	$P_{16} = (\alpha^9 : \alpha^{10} : 1)$
$P_{17} = (\alpha^3 : \alpha^{10} : 1)$	$P_{18} = (\alpha^6 : \alpha^5 : 1)$	$P_{19} = (\alpha^{12} : \alpha^{10} : 1)$	$P_{20} = (\alpha^9 : \alpha^5 : 1)$
$P_{21} = (\alpha^5 : \alpha^2 : 1)$	$P_{22} = (\alpha^{10} : \alpha^4 : 1)$	$P_{23} = (\alpha^5 : \alpha^8 : 1)$	$P_{24} = (\alpha^{10} : \alpha : 1)$
$P_{25} = (\alpha^7 : \alpha : 1)$	$P_{26} = (\alpha^{14} : \alpha^2 : 1)$	$P_{27} = (\alpha^{13} : \alpha^4 : 1)$	$P_{28} = (\alpha^{11} : \alpha^8 : 1)$
$P_{29} = (\alpha^7 : \alpha^4 : 1)$	$P_{30} = (\alpha^{14} : \alpha^8 : 1)$	$P_{31} = (\alpha^{13} : \alpha : 1)$	$P_{32} = (\alpha^{11} : \alpha^2 : 1)$

Tab. 4.1: Pontos racionais da curva $\mathcal{C}$ ($g = 2$).

Os divisores de intersecção são dados por:

$$\begin{aligned} div(\mathcal{C} \cap X) &= P_1 + 3P_\infty + P_2; \\ div(\mathcal{C} \cap Y) &= 5P_1; \\ div(\mathcal{C} \cap Z) &= 5P_\infty. \end{aligned}$$

Desta forma,

$$div\left(\frac{X^i Y^j}{Z^{i+j}}\right) = (i + 5j)P_1 + iP_2 - (2i + 5j)P_\infty.$$

Considerando divisores da forma $D = rP_\infty$, temos

$$\frac{X^i Y^j}{Z^{i+j}} \in \mathcal{L}(D) \quad \Longleftrightarrow \quad 2i + 5j \leq r \tag{4.1}$$

Pelo Teorema A.2.4, se $2 = 2g-2 < gr(D) < 32$, então os parâmetros dos códigos associados são $n = 32,\ k = gr(D) + 1 - g = gr(D) - 1,\ d \geq n - gr(D)$. Vamos calcular os parâmetros dos códigos com taxa $\frac{k}{n} \leq \frac{1}{2}$. Com isso, temos

$$\frac{k}{n} \leq \frac{1}{2} \quad \Rightarrow \quad \frac{gr(D) - 1}{32} \leq \frac{1}{2} \quad \Rightarrow \quad gr(D) - 1 \leq 16 \quad \Rightarrow \quad gr(D) \leq 17.$$

Vamos então calcular os parâmetros dos códigos associados a divisores da forma $D = rP_\infty$, com $3 \leq r \leq 17$.

- $D = 3P_\infty$.
  Os parâmetros do código neste caso são: $n = 32,\ k = 2,\ d \geq 29$. Tendo como base a condição (4.1), um conjunto gerador para o espaço $\mathcal{L}(3P_\infty)$ é dado por

$$\left\{1, \frac{X}{Z}\right\}.$$

Lema 4.1.1 *Não existe palavra com peso* 29 *neste código.*

Demonstração: De fato, se existir uma palavra de peso 29, então existe um elemento da forma

$$u_1 + u_2\frac{X}{Z},\ u_2 \neq 0$$

que se anula em 3 pontos racionais $P_i = (a_i : b_i : 1),\ P_j = (a_j : b_j : 1),$ e $P_k = (a_k : b_k : 1)$. Assim,

$$\left(u_1 + u_2\tfrac{X}{Z}\right)(P_i) = 0 \Rightarrow u_1 + u_2 a_i = 0 \Rightarrow a_i = u_1 u_2^{-1}$$

$$\left(u_1 + u_2\tfrac{X}{Z}\right)(P_j) = 0 \Rightarrow u_1 + u_2 a_j = 0 \Rightarrow a_j = u_1 u_2^{-1}$$

$$\left(u_1 + u_2\tfrac{X}{Z}\right)(P_k) = 0 \Rightarrow u_1 + u_2 a_k = 0 \Rightarrow a_k = u_1 u_2^{-1},$$

isto é, à existência de uma palavra-código com peso 29 é equivalente a existência de 3 pontos racionais com as primeiras coordenadas iguais (absurdo, ver Tabela 4.1). Logo, $d \geq 30$. O elemento $\dfrac{X}{Z}$ se anula nos pontos P_1, P_2, gerando uma palavra-código com peso 30. Portanto, $d = 30$. ■

- $D = 4P_\infty$

  Os parâmetros do código neste caso são: $n = 32,\ k = 3,\ d \geq 28$. Uma base para o espaço $\mathcal{L}(4P_\infty)$ é dada pelo conjunto

  $$\left\{1, \frac{X}{Z}, \frac{X^2}{Z^2}\right\}.$$

  Seja

  $$f = \frac{X}{Z} + \frac{X^2}{Z^2} = \frac{XZ + X^2}{Z^2} \in \mathcal{L}(4P_\infty).$$

  Avaliando esta função racional nos pontos da curva temos
  $f(P_1) = f((0 : 0 : 1)) = 0;$
  $f(P_2) = f((0 : 1 : 1)) = 0;$
  $f(P_3) = f((1 : \alpha^5 : 1)) = 0;$
  $f(P_4) = f((1 : \alpha^{10} : 1)) = 0.$

  Como todos os pontos racionais, diferentes de P_∞, são da forma $P_i = (\alpha_i : \beta_i : 1)$, então

  $$f(P_i) = 0 \Leftrightarrow \alpha_i + \alpha_i^2 = 0 \Leftrightarrow \alpha_i(\alpha_i + 1) = 0 \Leftrightarrow \alpha_i = 0, 1.$$

  Desta forma, a palavra-código $v = (f(P_1), f(P_2), ..., f(P_{32}))$ tem peso 28 e, portanto, $d = 28$.

Observação 4.1.1 *A idéia utilizada anteriormente, de encontrar funções racionais que se anulem em um certo número de pontos racionais e nos forneçam palavras-códigos com os pesos desejados, será utilizada nos demais casos que seguem.*

- $D = 5P_\infty$

  Os parâmetros do código neste caso são: $n = 32,\ k = 4,\ 27 \leq d$. Uma base para o espaço $\mathcal{L}(5P_\infty)$ é dada pelo conjunto

  $$\left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}\right\}.$$

  O elemento

  $$\frac{X}{Z} + \frac{Y}{Z} = \frac{X+Y}{Z},$$

  se anula nos pontos $P_1,\ P_5,\ P_6,\ P_7$ e P_8. Assim, conseguimos uma palavra-código com peso 27, ou seja, $d = 27$.

- $D = 6P_\infty$

  Os parâmetros do código neste caso são: $n = 32,\ k = 5,\ 26 \leq d$. Uma base para o espaço $\mathcal{L}(6P_\infty)$ é dada pelo conjunto

  $$\left\{1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{X^3}{Z^3},\ \frac{Y}{Z}\right\}.$$

  O elemento

  $$\frac{X^3}{Z^3} + 1,$$

  se anula nos pontos $P_3, P_4, P_{21}, P_{22}, P_{23}$ e P_{24}. Assim, conseguimos uma palavra-código com peso 26 ou seja, $d = 26$.

- $D = 7P_\infty$

  Os parâmetros do código são $n = 32,\ k = 6,\ 25 \leq d$. Uma base para o espaço $\mathcal{L}(7P_\infty)$ é dada pelo conjunto

  $$\left\{1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{X^3}{Z^3},\ \frac{Y}{Z},\ \frac{XY}{Z^2}\right\}.$$

  O polinômio

  $$P(X, Y, Z) = X(Y + \alpha^5 Z) = XY + \alpha^5 XZ,$$

  se anula nos pontos da curva onde $X = 0$ ou $Y = \alpha^5$. Assim sendo, o elemento

  $$\frac{XY}{Z^2} + \alpha^5 \frac{X}{Z},$$

se anula nos pontos $P_1, P_2, P_3, P_{13}, P_{15}, P_{18}, P_{20}$, gerando uma palavra-código com peso 25. Logo, $d = 25$.

- $D = 8P_\infty$
  Os parâmetros do código são $n = 32,\ k = 7,\ 24 \leq d$. Uma base para o espaço $\mathcal{L}(8P_\infty)$ é dada pelo conjunto
  $$\left\{1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{X^3}{Z^3}, \frac{X^4}{Z^4}, \frac{Y}{Z}, \frac{XY}{Z^2}\right\}.$$
  O polinômio
  $$P(X, Y, Z) = (X^2 + XZ + Z^2)(X^2 + XZ) = X^4 + XZ^3,$$
  se anula nos pontos da curva onde $X = 0,\ 1,\ \alpha^5,\ \alpha^{10}$. Assim sendo, temos que
  $$\frac{X^4}{Z^4} + \frac{X}{Z},$$
  gera uma palavra-código com peso 24. Portanto, $d = 24$.

- $D = 9P_\infty$
  Os parâmetros do código são $n = 32,\ k = 8,\ 23 \leq d$. Uma base para o espaço $\mathcal{L}(9P_\infty)$ é dada pelo conjunto
  $$\left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}, \frac{XY}{Z^2}, \frac{X^3}{Z^3}, \frac{X^2Y}{Z^3}, \frac{X^4}{Z^4}\right\}.$$
  O polinômio
  $$P(X, Y, Z) = (X^2 + XZ)(Y + \alpha Z) = X^2Y + \alpha X^2Z + XYZ + \alpha XZ^2,$$
  se anula nos pontos da curva onde $X = 0, 1$ ou $Y = \alpha$. Assim, o elemento
  $$\frac{X^2Y}{Z^3} + \alpha\frac{X^2}{Z^2} + \frac{XY}{Z} + \alpha\frac{X}{Z},$$
  se anula nos pontos $P_i,\ i \in \{1, 2, 3, 4, 5, 11, 24, 25, 31\}$, gerando uma palavra-código com peso 23. Portanto, $d = 23$.

- $D = 10P_\infty$
  Neste caso, os parâmetros do código são: $n = 32,\ k = 9,\ 22 \leq d$. Uma base para o espaço

$\mathcal{L}(10P_\infty)$ é dada pelo conjunto

$$\left\{1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{X^3}{Z^3}, \frac{X^4}{Z^4}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}, \frac{Y^2}{Z^2}\right\}.$$

O polinômio

$$P(X, Y, Z) = (Y + \alpha^5 Z)(Y + \alpha^{10} Z) = Y^2 + YZ + Z^2,$$

se anula nos pontos da curva onde $Y = \alpha^5,\ \alpha^{10}$. Assim sendo, o elemento

$$\frac{Y^2}{Z^2} + \frac{Y}{Z} + 1,$$

gera uma palavra-código com peso 22. Portanto, $d = 22$.

- $D = 11P_\infty$
  Os parâmetros do código são: $n = 32,\ k = 10,\ 21 \leq d \leq 23$. Uma base para o espaço $\mathcal{L}(11P_\infty)$ é o conjunto

$$\left\{1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{X^3}{Z^3}, \frac{X^4}{Z^4}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}, \frac{X^3Y}{Z^4}, \frac{Y^2}{Z^2}\right\}.$$

  O polinômio

$$P(X, Y, Z) = X(X + \alpha^5 Z)(X + \alpha^{10} Z)(Y + \alpha^5 Z) = (X^3 + X^2Z + XZ^2)(Y + \alpha^5 Z),$$

  se anula nos pontos da curva onde $X = 0,\ \alpha^5,\ \alpha^{10}$ ou $Y = \alpha^5$. Assim, o elemento

$$\frac{X^3Y}{Z^4} + \alpha^5\frac{X^3}{Z^3} + \frac{X^2Y}{Z^3} + \alpha^5\frac{X^2}{Z^2} + \frac{XY}{Z^2} + \alpha^5\frac{X}{Z},$$

  gera uma palavra-código com peso 21. Portanto, $d = 21$.

- $D = 12P_\infty$
  Neste caso, os parâmetros do código são: $n = 32,\ k = 11,\ 20 \leq d \leq 22$. Uma base para o espaço $\mathcal{L}(12P_\infty)$ é dada pelo conjunto

$$\left\{1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{X^3}{Z^3}, \frac{X^4}{Z^4}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}, \frac{X^3Y}{Z^4}, \frac{Y^2}{Z^2}, \frac{XY^2}{Z^3}\right\}.$$

  O polinômio

$$P(X, Y, Z) = (Y^2 + YZ + Z^2)X = XY^2 + XYZ + XZ^2,$$

se anula nos pontos da curva onde $X = 0$ ou $Y = \alpha^5,\ \alpha^{10}$. Assim sendo, o elemento

$$\frac{XY^2}{Z^3} + \frac{XY}{Z^2} + \frac{X}{Z},$$

gera uma palavra-código com peso 20. Logo, $d = 20$.

- $D = 13P_\infty$

  Neste caso, teremos um código com parâmetros $n = 32,\ k = 12,\ 19 \leq d$. Uma base para o espaço $\mathcal{L}(13P_\infty)$ é dada pelo conjunto

  $$\left\{1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{X^3}{Z^3}, \frac{X^4}{Z^4}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}, \frac{X^3Y}{Z^4}, \frac{X^4Y}{Z^5}, \frac{Y^2}{Z^2}, \frac{XY^2}{Z^3}\right\}.$$

  O polinômio

  $$P(X,Y,Z) = (X^4+XZ^3+Z^4)(Y+\alpha^5 Z) = X^4Y+\alpha^5X^4Z+XYZ^3+\alpha^5XZ^4+YZ^4+\alpha^5Z^5,$$

  se anula nos pontos da curva onde $X = \alpha,\ \alpha^2,\ \alpha^4,\ \alpha^8$ ou $Y = \alpha^5$. Assim sendo, o elemento

  $$\frac{X^4Y}{Z^5} + \alpha^5\frac{X^4}{Z^4} + \frac{XY}{Z^2} + \alpha^5\frac{X}{Z} + \frac{Y}{Z} + \alpha^5,$$

  gera uma palavra-código com peso 19. Portanto, $d = 19$.

- $D = 14P_\infty$

  Neste caso, teremos um código com parâmetros $n = 32,\ k = 13,\ 18 \leq d$. Uma base para o espaço $\mathcal{L}(14P_\infty)$ é o conjunto

  $$\left\{1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{X^3}{Z^3}, \frac{X^4}{Z^4}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}, \frac{X^3Y}{Z^4}, \frac{X^4Y}{Z^5}, \frac{Y^2}{Z^2}, \frac{XY^2}{Z^3}, \frac{X^2Y^2}{Z^4}\right\}.$$

  O polinômio

  $$P(X,Y,Z) = (X^2 + XZ + Z^2)(Y^2 + YZ + Z^2),$$

  se anula nos pontos da curva onde $X = \alpha^5,\ \alpha^{10}$ ou $Y = \alpha^5,\ \alpha^{10}$. Assim sendo, o elemento

  $$\frac{X^2Y^2}{Z^4} + \frac{X^2Y}{Z^3} + \frac{X^2}{Z^2} + \frac{XY^2}{Z^3} + \frac{XY}{Z^2} + \frac{X}{Z} + \frac{Y^2}{Z^2} + \frac{Y}{Z} + 1,$$

  gera uma palavra-código com peso 18. Portanto, $d = 18$.

- $D = 15P_\infty$

  Os parâmetros do código são: $n = 32,\ k = 14,\ 17 \leq d$. Uma base para o espaço $\mathcal{L}(15P_\infty)$

é dada pelo conjunto

$$\left\{1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{X^3}{Z^3}, \frac{X^4}{Z^4}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}, \frac{X^3Y}{Z^4}, \frac{X^4Y}{Z^5}, \frac{Y^2}{Z^2}, \frac{XY^2}{Z^3}, \frac{X^2Y^2}{Z^4}, \frac{Y^3}{Z^3}\right\}.$$

O polinômio

$$P(X,Y,Z) = (X+Y)(Y^2+YZ+Z^2) = XY^2+XYZ+X^2Z+XZ^2+Y^3+Y^2Z+YZ^2,$$

se anula nos pontos da curva onde $X = Y$ ou $Y = \alpha^5,\ \alpha^{10}$. Assim sendo, o elemento

$$\frac{XY^2}{Z^3} + \frac{XY}{Z^2} + \frac{X^2}{Z^2} + \frac{X}{Z} + \frac{Y^3}{Z^3} + \frac{Y^2}{Z^2} + \frac{Y}{Z},$$

gera uma palavra-código com peso 17. Logo, $d = 17$.

- $D = 16P_\infty$

  Neste caso, os parâmetros do código são: $n = 32,\ k = 15,\ 16 \leq d$. Uma base para o espaço $\mathcal{L}(16P_\infty)$ é dada pelo conjunto

$$\left\{1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{X^3}{Z^3}, \frac{X^4}{Z^4}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}, \frac{X^3Y}{Z^4}, \frac{X^4Y}{Z^5}, \frac{Y^2}{Z^2}, \frac{XY^2}{Z^3}, \frac{X^2Y^2}{Z^4}, \frac{X^3Y^2}{Z^5}, \frac{Y^3}{Z^3}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (Y^2+YZ+Z^2)(X^2+XZ+Z^2)X,$$

  se anula nos pontos da curva onde $X = 0,\ \alpha^5,\ \alpha^{10}$ ou $Y = \alpha^5,\ \alpha^{10}$. Assim, o elemento

$$\frac{X^3Y^2}{Z^5} + \frac{X^3Y}{Z^4} + \frac{X^3}{Z^3} + \frac{X^2Y^2}{Z^4} + \frac{X^2Y}{Z^3} + \frac{X^2}{Z^2} + \frac{XY^2}{Z^3} + \frac{XY}{Z^2} + \frac{X}{Z},$$

  gera uma palavra-código com peso 16. Portanto, $d = 16$.

- $D = 17P_\infty$

  Os parâmetros do código são: $n = 32,\ k = 16,\ 15 \leq d$. Uma base para o espaço $\mathcal{L}(17P_\infty)$ é dada pelo conjunto

$$\left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}, \frac{XY}{Z^2}, \frac{Y^2}{Z^2}, \frac{X^3}{Z^3}, \frac{X^2Y}{Z^3}, \frac{XY^2}{Z^3}, \frac{Y^3}{Z^3}, \frac{X^4}{Z^4}, \frac{X^3Y}{Z^4}, \frac{X^2Y^2}{Z^4}, \frac{XY^3}{Z^4}, \frac{X^4Y}{Z^5}, \frac{X^3Y^2}{Z^5}\right\}.$$

  O polinômio

$$P(X,Y,Z) = X(Y+\alpha^5Z)(Y+\alpha^{10}Z)(Y+\alpha Z),$$

se anula nos pontos da curva onde $X = 0$ ou $Y = \alpha,\ \alpha^5,\ \alpha^{10}$. Portanto, o elemento

$$\frac{XY^3}{Z^4} + \alpha^4\frac{XY^2}{Z^3} + \alpha^4\frac{XY}{Z^2} + \alpha\frac{X}{Z},$$

gera uma palavra-código com peso 15. Logo, $d = 15$.

Os códigos obtidos anteriormente são todos subcódigos do código derivado a seguir. Este código é visto como a modulação a ser utilizada no sistema de comunicações.

- $D = 31P_\infty$
  Os parâmetros do código são: $n = 32,\ k = 30,\ 1 \leq d$. Uma base do espaço $\mathcal{L}(31P_\infty)$ é dada pelo conjunto

$$\left\{\frac{X^iY^j}{Z^{i+j}},\ (i,j) \in \{0,1,2,3,4\} \times \{0,1,2,3,4\}\right\} \cup \left\{\frac{X^iY^5}{Z^{i+5}},\ i = 0,1,2,3\right\} \cup \left\{\frac{Y^6}{Z^6}\right\}.$$

Lema 4.1.2 *A distância mínima do código associado ao divsor $D = 31P_\infty$ é $d = 2$.*

Demonstração: Vamos mostrar que $d = 2$ em duas etapas.
Afirmação 1: Não existe palavra-código com peso 1 neste código.
De fato, da distribuição dos pontos racionais, vemos que existem 5 pontos da forma $(- : \alpha : 1)$, 5 pontos da forma $(- : \alpha^2 : 1)$, 5 pontos da forma $(- : \alpha^4 : 1)$, 5 pontos da forma $(- : \alpha^8 : 1)$, 5 pontos da forma $(- : \alpha^5 : 1)$ e 5 pontos da forma $(- : \alpha^{10} : 1)$.

Se existir uma palavra-código com peso 1 neste código, então existe um polinômio da forma

$$F(X,Y,Z) = X^4A_1(Y,Z) + X^3A_2(Y,Z) + X^2A_3(Y,Z) + XA_4(Y,Z) + A_5(Y,Z),$$

com
$A_1(Y,Z) = a_1Y^4 + a_2Y^3Z + a_3Y^2Z^2 + a_4YZ^3 + a_5Z^4,$

$A_2(Y,Z) = b_1Y^5 + b_2Y^4Z + b_3Y^3Z^2 + b_4Y^2Z^3 + b_5YZ^4 + b_6Z^5,$

$A_3(Y,Z) = c_1Y^5Z + c_2Y^4Z^2 + c_3Y^3Z^3 + c_4Y^2Z^4 + c_5YZ^5 + c_6Z^6,$

$A_4(Y,Z) = d_1Y^5Z + d_2Y^4Z^2 + d_3Y^3Z^3 + d_4Y^2Z^4 + d_5YZ^5 + d_6Z^6,$

$A_5(Y,Z) = e_1Y^6Z^2 + e_2Y^5Z^3 + e_3Y^4Z^4 + e_4Y^3Z^5 + e_5Y^2Z^6 + e_6YZ^7 + e_7Z^8,$
que se anula em 31 pontos da curva. Para isso, vamos analisar 2 situações.

1. O polinômio $F(X, Y, Z)$ se anula nos pontos $P_i,\ i = 3, 4, ..., 32$.
   Neste caso, de acordo com a Tabela 4.1, para cada $\alpha^i,\ i \in \{1, 2, 4, 8, 5, 10\}$, os polinômios
   $$F_i(X) = F(X, \alpha^i, 1),$$
   têm 5 raízes distintas. Como $gr(F_i(X)) = 4$, temos que $F_i(X)$ é o polinômio nulo. Desta forma, dado $j \in \{1, 2, 3, 4, 5\}$ temos que
   $$A_j(\alpha^i, 1) = 0,\ \forall\ i \in \{1, 2, 4, 8, 5, 10\},$$
   isto é, os polinômios
   $$A_j(Y) = A_j(Y, 1),\ j = 1, 2, 3, 4, 5,$$
   têm como raízes os elementos $\alpha^i,\ i \in \{1, 2, 4, 8, 5, 10\}$. Como $gr(A_1(Y)) = 4$ e $gr(A_2(Y)) = gr(A_3(Y)) = gr(A_4(Y)) = 5$ temos que
   $$A_1(Y) = A_2(Y) = A_3(Y) = A_4(Y) = 0.$$
   Assim,
   $$F(X, Y, Z) = A_5(Y, Z).$$
   Como $gr(\mathcal{C}) = 5$, pelo Teorema de Bezout, este polinômio só pode se anular em 30 pontos racionais. (absurdo!!).

2. Existe $k \in \{3, 4, ..., 32\}$ tal que $F(P_k) \neq 0$.
   Neste caso, existe $j \in \{1, 2, 4, 8, 5, 10\}$ tal que F se anula em 4 dos 5 pontos
   $$(u_1 : \alpha^i : 1), (u_2 : \alpha^i : 1), (u_3 : \alpha^i : 1), (u_4 : \alpha^i : 1), (u_5 : \alpha^i : 1).$$
   Temos também que, se $i \in \{1, 2, 4, 8, 5, 10\},\ i \neq j$ então os polinômios
   $$F_i(X) = F(X, \alpha^i, 1),$$
   têm 5 raízes distintas. Como no caso anterior, $F_i(X) = 0$. Considerando o grau dos polinômios $A_j(Y) = A_j(Y, 1)$, temos
   $$A_1(Y) = 0,\ A_2(Y) = A_3(Y) = A_4(Y) = a\prod_{i \neq j}(Y - \alpha^i).$$

Desta forma,

$$F(X,Y,Z) = \prod_{i \neq j}(Y - \alpha^i Z)(w_3X^3 + w_2X^2 + w_1X) + A_5(Y,Z).$$

Considerando $Y = \alpha^j$, o polinômio

$$F_j(X) = F(X, \alpha^j, 1),$$

tem quatro raízes entre os elementos $\{u_1, u_2, u_3, u_4, u_5\}$. Como $gr(F_j(X)) = 3$, então $w_3 = w_2 = w_1 = 0$ e $A_5(\alpha^j) = 0$. Portanto,

$$F(X,Y,Z) = A_5(Y,Z).$$

Como $gr(\mathcal{C}) = 5$, pelo Teorema de Bezout, este polinômio só pode se anular em 30 pontos racionais. (absurdo!!).

Afirmação 2: O código possui distância $d = 2$.
Tendo como base a distribuição dos pontos racionais, dada pela Tabela 4.1, basta observar que o elemento

$$\frac{Y^6}{Z^6} + \frac{Y^5}{Z^5} + \frac{Y^4}{Z^4} + \frac{Y^3}{Z^3} + 1$$

faz parte de $\mathcal{L}(D)$ e se anula nos pontos da forma $(- : \alpha^k : 1),\ k \in \{1, 2, 4, 8, 5, 10\}$, ou seja, em 30 pontos. Logo, $d = 2$. ■

4.2 Quártica de Klein

Nesta seção, calcularemos os parâmetros dos códigos associados à quártica de Klein.

A quártica de Klein é uma curva não singular $\mathcal{C}$, de gênero 3, cuja equação é

$$ZY^3 + X^3Y + Z^3X = 0. \tag{4.2}$$

Esta curva possui 24 pontos racionais em $\mathbb{F}_8$, como ilustra a Tabela 4.2.

Além disso, temos

$$\mathcal{C} \cap X = \{P \in \mathcal{C} |\ X = 0\} = \{P_2, P_3\},$$
$$\mathcal{C} \cap Y = \{P \in \mathcal{C} |\ Y = 0\} = \{P_1, P_3\},$$
$$\mathcal{C} \cap Z = \{P \in \mathcal{C} |\ Z = 0\} = \{P_1, P_2\},$$

$P_1 = (1:0:0)$	$P_2 = (0:1:0)$	$P_3 = (0:0:1)$
$P_4 = (1:\alpha^3:1)$	$P_5 = (1:\alpha^6:1)$	$P_6 = (1:\alpha^5:1)$
$P_7 = (\alpha:\alpha:1)$	$P_8 = (\alpha:\alpha^3:1)$	$P_9 = (\alpha:\alpha^4:1)$
$P_{10} = (\alpha^2:\alpha^2:1)$	$P_{11} = (\alpha^2:\alpha^6:1)$	$P_{12} = (\alpha^2:\alpha:1)$
$P_{13} = (\alpha^3:1:1)$	$P_{14} = (\alpha^3:\alpha^4:1)$	$P_{15} = (\alpha^3:\alpha^6:1)$
$P_{16} = (\alpha^4:\alpha^4:1)$	$P_{17} = (\alpha^4:\alpha^5:1)$	$P_{18} = (\alpha^4:\alpha^2:1)$
$P_{19} = (\alpha^5:1:1)$	$P_{20} = (\alpha^5:\alpha^2:1)$	$P_{21} = (\alpha^5:\alpha^3:1)$
$P_{22} = (\alpha^6:1:1)$	$P_{23} = (\alpha^6:\alpha:1)$	$P_{24} = (\alpha^6:\alpha^5:1)$

Tab. 4.2: Pontos $\mathbb{F}_8$-racionais da quártica de Klein.

e os divisores de intersecção são dados por:

$$div(\mathcal{C} \cap X) = 3P_3 + P_2;$$
$$div(\mathcal{C} \cap Y) = 3P_1 + P_3;$$
$$div(\mathcal{C} \cap Z) = 3P_2 + P_1.$$

Portanto,

$$div\left(\frac{X^iY^j}{Z^{i+j}}\right) = (3i+j)P_3 - (2i+3j)P_2 + (2j-i)P_1. \tag{4.3}$$

Tendo como base as informações anteriores, vamos considerar divisores da forma $D = rP_2 + sP_1$ e procurar bases para os espaços $\mathcal{L}(D)$ da forma $\dfrac{X^iY^j}{Z^{i+j}}$.
De (4.3), temos

$$\frac{X^iY^j}{Z^{i+j}} \in \mathcal{L}(D) \quad \Longleftrightarrow \quad 2i+3j \leq r \text{ e } i \leq s+2j.$$

De acordo com o Teorema A.2.4, e considerando $\mathcal{P} = \{P_3, ..., P_{24}\}$, se

$$2g-2 = 4 < gr(D) = r+s < n = 22, \tag{4.4}$$

então o código de Goppa associado terá parâmetros

$$(n,k,d) = (22, gr(D)+1-g = gr(D)-2, d), \text{com} \quad 22-gr(D) \leq d \leq 22-gr(D)+1.$$

Vamos calcular os parâmetros dos códigos associados aos divisores $D = rP_2 + sP_1$. De acordo com (4.4), precisamos considerar os seguintes casos:

1. $\boldsymbol{r+s=5}$

   Os parâmetros dos códigos associados são: $n = 22, k = 3, 17 \leq d$. Neste caso, é possível

obter bases da forma $\frac{X^iY^j}{Z^{i+j}}$ para os espaços associados aos seguintes divisores:

- $\boldsymbol{D_1=3P_2+2P_1}$ e $\boldsymbol{D_2=4P_2+P_1}$.
  Os espaços $\mathcal{L}(D_1)$ e $\mathcal{L}(D_2)$ possuem uma base dada pelo conjunto

$$\left\{1, \frac{X}{Z}, \frac{Y}{Z}\right\}.$$

Lema 4.2.1 *A distância mínima dos códigos associados aos divisores D_1 e D_2 é $d = 18$.*

Demonstração: Sejam $a, b, c \in \mathbb{F}_8$ e $\mathcal{C}_1$ a curva dada pela equação

$$aX + bY + cZ = 0.$$

Se existir uma palavra-código com peso 17 no código, então

$$\mathcal{C}_1 \cap \mathcal{C} = \{P_{i_1}, P_{i_2}, P_{i_3}, P_{i_4}, P_{i_5}\},$$

o que é um absurdo pois $gr(\mathcal{C}) = 4$ e $gr(\mathcal{C}_1) = 1$ (contraria o Teorema de Bezout). Portanto, não existem palavras-códigos com peso 17 neste código.

Pela afirmação anterior, temos então que $18 \leq d$. O polinômio

$$P(X, Y, Z) = X + Y,$$

se anula nos pontos da curva onde $X = Y$. Desta forma, o elemento

$$\frac{X}{Z} + \frac{Y}{Z},$$

gera uma palavra-código com peso 18. Logo, $d = 18$. ■

- $\boldsymbol{D_3=5P_2}$
  Neste caso, uma base para o espaço $\mathcal{L}(D_3)$ é dada pelo conjunto

$$\left\{1, \frac{Y}{Z}, \frac{XY}{Z^2}\right\}.$$

Lema 4.2.2 *A distância mínima do código associado ao divisor D_3 é $d = 18$.*

Demonstração: Sejam $(a, b, c) \in \mathbb{F}_8^3$, e $(a, b, c) \neq (0, 0, 0)$. Considere a curva dada

pela equação

$$\mathcal{C}_1 : aZ^2 + bYZ + cXY = 0. \tag{4.5}$$

Se existir uma palavra-código com peso 17, então a curva (4.5) tem, pelo menos, 5 pontos distintos em comum com a curva $\mathcal{C}$. Vamos mostrar que isto é impossível, analisando os seguintes casos:

- $a = 0,\ b = 0,\ c \neq 0.$
  Neste caso, a equação (4.5) se reduz a $cXY = 0$ e, assim, só temos o ponto $P_3 = (0 : 0 : 1)$ em comum.
- $a = 0,\ c = 0,\ b \neq 0$
  Neste caso, a equação (4.5) se reduz a $bY = 0$ e, novamente, só temos o ponto P_3 em comum.
- $a = 0,\ b \neq 0,\ c \neq 0.$
  Nesse caso, a equação (4.5) é da forma

  $$bY + cXY = Y(b + cX) = 0. \tag{4.6}$$

  Assim, os pontos que satisfazem a equação (4.6) são da forma:

  $$(u : 0 : 1),\ u \in \mathbb{F}_8 \text{ ou } \left(\frac{b}{c} : u : 1\right),\ u \in \mathbb{F}_8.$$

  Pela Tabela 4.2, só existem 4 pontos da curva $\mathcal{C}$ satisfazendo a equação anterior, que são:

  $$(0 : 0 : 1), \left(\frac{b}{c} : u_1 : 1\right), \left(\frac{b}{c} : u_2 : 1\right), \left(\frac{b}{c} : u_3 : 1\right)$$

  onde u_1, u_2, u_3 são as raízes do polinômio

  $$Y^3 + \left(\frac{b}{c}\right)^3 Y + \frac{b}{c}.$$

- $a \neq 0,\ b \neq 0,\ c = 0.$
  Neste caso, a equação (4.5) é da forma

  $$a + bY = 0,$$

  que é a equação de uma reta. Assim, usando o Teorema de Bezout, só poderemos ter 4 pontos em comum com a curva $\mathcal{C}$.

– $a \neq 0,\ c \neq 0,\ b = 0.$
Nesse caso, a equação (4.5) é da forma $a + cXY = 0$, ou seja,

$$XY = \frac{a}{c}. \tag{4.7}$$

Sendo a, c elementos em $\mathbb{F}_8$, temos que

$$\frac{a}{c} = \alpha^i, i \in \{0, 1, 2, 3, 4, 5, 6\}.$$

Assim, para sabermos quantos pontos da curva $\mathcal{C}$ satisfazem a equação (4.7), precisamos saber quantos elementos possuem os seguintes conjuntos

$$A_i = \{P = (x : y : z) \in \mathcal{C} |\ xy = \alpha^i\},\ \text{para} \quad i = 0, 1, 2, 3, 4, 5, 6.$$

De acordo com a Tabela 4.2, temos

$$\begin{array}{lll} A_0 = \{P_{14}, P_{20}, P_{23}\}, & A_1 = \{P_{11}, P_{16}, P_{21}\}, & A_2 = \{P_7, P_{15}, P_{17}\}, \\ A_3 = \{P_4, P_{12}, P_{13}\}, & A_4 = \{P_8, P_{10}, P_{24}\}, & A_5 = \{P_6, P_9, P_{19}\}, \\ A_6 = \{P_5, P_{18}, P_{22}\}. & & \end{array}$$

Logo, só teremos 3 pontos em comum entre as curvas.

– $a \neq 0,\ b \neq 0,\ c \neq 0.$
Neste caso, buscamos as soluções da forma

$$(u : v : 1) \in \mathcal{C} \cap \mathcal{C}_1,\ v \neq 0\ (v = 0 \Rightarrow a = 0).$$

Porém, note que

$$a+bv+cuv = 0 \Leftrightarrow avv^{-1}+bv+cuv = 0 \Leftrightarrow v(av^{-1}+b+cu) = 0 \Leftrightarrow av^{-1}+b+cu = 0.$$

Desta forma, temos que

$$(u : v : 1) \text{ satisfaz } a + bY + cXY \Leftrightarrow (u : v^{-1} : 1) \text{ satisfaz } aY + cX + b = 0.$$

Como, novamente, temos a equação de uma reta, só poderemos ter 4 pontos em comum.

De acordo com a afirmação anterior, o código possui distância mínima $18 \leq d$. O

polinômio

$$P(X, Y, Z) = (X + Z)Y = XY + YZ,$$

se anula nos pontos da curva para os quais $X = 1$ ou $Y = 0$. Assim, o elemento

$$\frac{XY}{Z^2} + \frac{Y}{Z},$$

gera uma palavra-código com peso 18. Portanto, $d = 18$. ■

2. $\boldsymbol{r+s=6}$.
Os parâmetros dos códigos associados são: $n = 22,\ k = 4,\ 16 \leq d$. Neste caso, é possível obter bases da forma $\dfrac{X^iY^j}{Z^{i+j}}$ para os espaços associados aos seguintes divisores:

- $\boldsymbol{D=6P_2+0P_1}$.
Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{Y^2}{Z^2}\right\}.$$

O polinômio

$$P(X, Y, Z) = (Y + Z)(Y + \alpha Z) = Y^2 + \alpha^5 YZ + Z^2,$$

se anula nos pontos da curva onde $Y = 1,\ \alpha$. Desta forma, o elemento

$$\frac{Y^2}{Z^2} + \alpha^5\frac{Y}{Z} + 1,$$

gera uma palavra-código com peso 16. Portanto, $d = 16$.

- $\boldsymbol{D=5P_2+1P_1}$.
Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{Y}{Z},\ \frac{XY}{Z^2}\right\}.$$

O polinômio

$$P(X, Y, Z) = (X + Z)(Y + \alpha Z) = XY + \alpha XZ + YZ + \alpha Z^2,$$

se anula nos pontos da curva onde $X = 1$ ou $Y = \alpha$. Desta forma, o elemento

$$\frac{XY}{Z^2} + \alpha\frac{X}{Z} + \frac{Y}{Z} + \alpha,$$

gera uma palavra-código com peso 16. Portanto, $d = 16$.

- $\boldsymbol{D=4P_2+2P_1}$.
  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{Y}{Z}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X+Z)(X+\alpha Z) = X^2 + \alpha^5 XZ + \alpha Z^2,$$

  se anula nos pontos da curva onde $X = 1,\ \alpha$. Desta forma, o elemento

$$\frac{X^2}{Z^2} + \alpha^5\frac{X}{Z} + \alpha,$$

  gera uma palavra-código com peso 16. Portanto, $d = 16$.

3. $\boldsymbol{r+s=7}$.
   Os parâmetros dos códigos associados são: $n = 22,\ k = 5,\ 15 \leq d$. Neste caso, é possível obter bases da forma $\dfrac{X^iY^j}{Z^{i+j}}$ para os espaços associados aos seguintes divisores:

   - $\boldsymbol{D=7P_2+0P_1}$
     Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2}\right\}.$$

     O polinômio

$$P(X,Y,Z) = Y(X+Z)(X+\alpha Z) = X^2Y + \alpha^5 XYZ + \alpha YZ^2,$$

     se anula nos pontos da curva onde $X = 1,\ \alpha$ ou $Y = 0$. Desta forma, o elemento

$$\frac{X^2Y}{Z^3} + \alpha^5\frac{XY}{Z^2} + \alpha\frac{Y}{Z},$$

gera uma palavra-código com peso 15. Portanto, $d = 15$.

- $\boldsymbol{D=6P_1+1P_1}$
  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{Y^2}{Z^2}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X+Y)(Y+\alpha^6 Z) = XY + \alpha^6 XZ + Y^2 + \alpha^6 YZ,$$

  se anula nos pontos da curva onde $X = Y$ ou $Y = \alpha^6$. Desta forma, o elemento

$$\frac{XY}{Z^2} + \alpha^6\frac{X}{Z} + \frac{Y^2}{Z^2} + \alpha^6\frac{Y}{Z},$$

  gera uma palavra-código com peso 15. Portanto $d = 15$.

- $\boldsymbol{D=5P_2+2P_1}$
  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{Y}{Z},\ \frac{XY}{Z^2}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X+Y)(X+\alpha^5 Z) = X^2 + \alpha^5 XZ + XY + \alpha^5 YZ,$$

  se anula nos pontos da curva onde $X = Y$ ou $X = \alpha^5$. Desta forma, o elemento

$$\frac{X^2}{Z^2} + \alpha^5\frac{X}{Z} + \frac{XY}{Z^2} + \alpha^5\frac{Y}{Z},$$

  gera uma palavra-código com peso 15. Portanto, $d = 15$.

4. $\boldsymbol{r+s=8}$.
   Os parâmetros dos códigos associados são: $n = 22,\ k = 6,\ 14 \leq d$. Neste caso, é possível obter bases da forma $\dfrac{X^iY^j}{Z^{i+j}}$ para os espaços associados aos seguintes divisores:

- $\boldsymbol{D=8P_2+0P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

  $$\left\{1,\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3}\right\}.$$

  O polinômio

  $$P(X,Y,Z) = (X+Y)(X+Z)Y = X^2Y + XYZ + XY^2 + Y^2Z,$$

  se anula nos pontos da curva onde $X = Y$ ou $X = 1$ ou $Y = 0$. Desta forma, o elemento

  $$\frac{X^2Y}{Z^3} + \frac{XY}{Z^2} + \frac{XY^2}{Z^3} + \frac{Y^2}{Z^2},$$

  gera uma palavra-código com peso 14. Portanto, $d = 14$.

- $\boldsymbol{D=7P_2+1P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

  $$\left\{1,\ \frac{X}{Z},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2}\right\}.$$

  Com os elementos

  $$1,\ \frac{X}{Z},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{Y^2}{Z^2},$$

  é possível formar uma palavra-código com peso 15 (ver $D = 6P_2 + P_1$). Desta forma, o código possui distância mínima $14 \leq d \leq 15$.

- $\boldsymbol{D=6P_2+2P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

  $$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{Y^2}{Z^2}\right\}.$$

  Com os elementos

  $$1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{Y}{Z},\ \frac{XY}{Z^2},$$

  é possível formar uma palavra-código com peso 15 (ver $D = 5P_2 + 2P_1$). Desta forma, o código possui distância míniuma $14 \leq d \leq 15$.

5. $\boldsymbol{r+s=9}$.

   Os parâmetros dos códigos associados são: $n = 22,\ k = 7,\ 13 \leq d$. Neste caso, é possível

obter bases da forma $\dfrac{X^iY^j}{Z^{i+j}}$ para os espaços associados aos seguintes divisores:

- $\boldsymbol{D=9P_2+0P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

  $$\left\{1,\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{Y^3}{Z^3}\right\}.$$

  O polinômio

  $$P(X,Y,Z) = Y^3 + Y^2Z + Z^3,$$

  se anula nos pontos da curva onde $Y = \alpha,\ \alpha^2,\ \alpha^4$. Desta forma, o elemento

  $$\frac{Y^3}{Z^3} + \frac{Y^2}{Z^2} + 1,$$

  gera uma palavra-código com peso 13. Portanto, $d = 13$.

- $\boldsymbol{D=8P_2+1P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

  $$\left\{1,\ \frac{X}{Z},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3}\right\}.$$

  O polinômio

  $$P(X,Y,Z) = (Y + \alpha Z)(Y + \alpha^2 Z)(X + \alpha^3 Z),$$

  se anula nos pontos da curva onde $Y = \alpha,\ \alpha^2$ ou $X = \alpha^3$. Desta forma, o elemento

  $$\frac{XY^2}{Z^3} + \alpha^6\frac{XY}{Z^2} + \alpha^3\frac{X}{Z} + \alpha^3\frac{Y^2}{Z^2} + \alpha^2\frac{Y}{Z} + \alpha^6$$

  gera uma palavra-código com peso 13. Portanto, $d = 13$.

- $\boldsymbol{D=7P_2+2P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

  $$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2}\right\}.$$

  O polinômio

  $$P(X,Y,Z) = (X + \alpha Z)(X + \alpha^2 Z)(Y + \alpha^5 Z),$$

se anula nos pontos da curva onde $X = \alpha,\ \alpha^2$ ou $Y = \alpha^5$. Desta forma, o elemento

$$\frac{X^2Y}{Z^3} + \alpha^6\frac{XY}{Z^2} + \alpha^3\frac{Y}{Z} + \alpha^5\frac{X^2}{Z^2} + \alpha^4\frac{X}{Z} + \alpha,$$

gera uma palavra-código com peso 13. Portanto, $d = 13$.

- $\boldsymbol{D=6P_2+3P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

  $$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{X^3}{Z^3},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{Y^2}{Z^2}\right\}.$$

  O polinômio

  $$P(X, Y, Z) = X^3 + X^2Z + Z^3,$$

  se anula nos pontos da curva onde $X = \alpha,\ \alpha^2,\ \alpha^4$. Desta forma, o elemento

  $$\frac{X^3}{Z^3} + \frac{X^2}{Z^2} + 1,$$

  gera uma palavra-código com peso 13. Portanto, $d = 13$.

6. $\boldsymbol{r+s=10}$.

   Os parâmetros dos códigos associados são: $n = 22,\ k = 8,\ 12 \leq d$. Neste caso, é possível obter bases da forma $\dfrac{X^iY^j}{Z^{i+j}}$ para os espaços associados aos seguintes divisores:

   - $\boldsymbol{D=10P_2+0P_1}$

     Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

     $$\left\{1,\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{X^2Y^2}{Z^4},\ \frac{Y^3}{Z^3}\right\}.$$

     O polinômio

     $$P(X, Y, Z) = Y(Y + Z)(X + Z)(X + \alpha Z),$$

     se anula nos pontos da curva onde $Y = 0, 1$ ou $X = 1,\ \alpha$. Desta forma, o elemento

     $$\frac{X^2Y^2}{Z^4} + \alpha^5\frac{XY^2}{Z^3} + \alpha\frac{Y^2}{Z^2} + \frac{YX^2}{Z^3} + \alpha^5\frac{XY}{Z^2} + \alpha\frac{Y}{Z},$$

     gera uma palavra-código com peso 12. Portanto, $d = 12$.

- $\boldsymbol{D=9P_2+1P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{Y^3}{Z^3}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X+Y)(Y+1)(Y+\alpha^5),$$

  se anula nos pontos da curva onde $X = Y$ ou $Y = 1,\ \alpha^5$. Desta forma, o elemento

$$\frac{XY^2}{Z^3} + \alpha\frac{XY}{Z^2} + \alpha^5\frac{X}{Z} + \frac{Y^3}{Z^3} + \alpha\frac{Y^2}{Z^2} + \alpha^5\frac{Y}{Z},$$

  gera uma palavra-código com peso 12. Portanto, $d = 12$.

- $\boldsymbol{D=8P_2+2P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X+Y)(X+Z)(Y+Z) = X^2Y + X^2Z + XZ^2 + XY^2 + Y^2Z + YZ^2,$$

  se anula nos pontos da curva onde $X = Y$ ou $X = 1$ ou $Y = 1$. Desta forma, o elemento

$$\frac{X^2Y}{Z^3} + \frac{X^2}{Z^2} + \frac{X}{Z} + \frac{XY^2}{Z^3} + \frac{Y^2}{Z^2} + \frac{Y}{Z},$$

  gera uma palavra-código com peso 12. Portanto, $d = 12$.

- $\boldsymbol{D=7P_2+3P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{X^3}{Z^3},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X+Y)(X+Z)(X+\alpha^3Z)$$

se anula nos pontos da curva onde $X = Y$ ou $X = 1,\ \alpha^3$. Desta forma, o elemento

$$\frac{X^3}{Z^3} + \alpha^2\frac{X^2}{Z^2} + \alpha^3\frac{X}{Z} + \frac{X^2Y}{Z^3} + \alpha^2\frac{XY}{Z^2} + \alpha^3,$$

gera uma palavra-código com peso 12. Portanto, $d = 12$.

7. $\boldsymbol{r}+\boldsymbol{s}=\mathbf{11}$.
   Os parâmetros dos códigos associados são: $n = 22,\ k = 9,\ 11 \leq d$. Neste caso, é possível obter bases da forma $\dfrac{X^iY^j}{Z^{i+j}}$ para os espaços associados aos seguintes divisores:

   - $\boldsymbol{D}=\mathbf{11}\boldsymbol{P_2}+\mathbf{0}\boldsymbol{P_1}$
     Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

     $$\left\{1,\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{X^2Y^2}{Z^4},\ \frac{Y^3}{Z^3},\ \frac{XY^3}{Z^4}\right\}.$$

     Com os elementos

     $$1,\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{X^2Y^2}{Z^4},\ \frac{Y^3}{Z^3},$$

     é possível formar uma palavra-código com peso 12 (ver $10P_2 + 0P_1$). Desta forma, a distância mínima satisfaz $11 \leq d \leq 12$, o que não altera a quantidade de erros corrigidos pelo código.

   - $\boldsymbol{D}=\mathbf{10}\boldsymbol{P_2}+\mathbf{1}\boldsymbol{P_1}$
     Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

     $$\left\{1,\ \frac{X}{Z},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{X^2Y^2}{Z^4},\ \frac{Y^3}{Z^3}\right\}.$$

     Com os elementos

     $$1,\ \frac{X}{Z},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{Y^3}{Z^3},$$

     é possível formar uma palavra-código com peso 12 (ver $9P_2 + 1P_1$). Desta forma, a distância mínima satisfaz $11 \leq d \leq 12$, o que não altera a quantidade de erros corrigidos pelo código.

- $\boldsymbol{D=9P_2+2P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

  $$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{Y^3}{Z^3}\right\}.$$

  Com os elementos

  $$1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},$$

  é possível formar uma palavra-código com peso 12 (ver $8P_2 + 2P_1$). Desta forma, a distância mínima satisfaz $11 \leq d \leq 12$, o que não altera a quantidade de erros corrigidos pelo código.

- $\boldsymbol{D=8P_2+3P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

  $$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{X^3}{Z^3},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3}\right\}.$$

  Com os elementos

  $$1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{X^3}{Z^3},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},$$

  é possível formar uma palavra-código com peso 12 (ver $7P_2 + 3P_1$). Desta forma, a distância mínima satisfaz $11 \leq d \leq 12$, o que não altera a quantidade de erros corrigidos pelo código.

8. $\boldsymbol{r+s=12}$.

   Os parâmetros dos códigos associados são: $n = 22,\ k = 10,\ 10 \leq d$. Neste caso, é possível obter bases da forma $\dfrac{X^iY^j}{Z^{i+j}}$ para os espaços associados aos seguintes divisores:

   - $\boldsymbol{D=12P_2+0P_1}$

     Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

     $$\left\{1,\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{X^2Y^2}{Z^4},\ \frac{Y^3}{Z^3},\ \frac{XY^3}{Z^4},\ \frac{Y^4}{Z^4}\right\}.$$

     O polinômio

     $$P(X,Y,Z) = (Y^3 + Y^2Z + Z^3)(Y + Z) = Y^4 + Y^2Z^2 + YZ^3 + Z^4,$$

se anula nos pontos da curva onde $Y = 1,\ \alpha,\ \alpha^2,\ \alpha^4$. Desta forma, o elemento

$$\frac{Y^4}{Z^4} + \frac{Y^2}{Z^2} + \frac{Y}{Z} + 1,$$

gera uma palavra-código com peso 10. Portanto, $d = 10$.

- $\boldsymbol{D = 11P_2 + 1P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{X^2Y^2}{Z^4},\ \frac{Y^3}{Z^3},\ \frac{XY^3}{Z^4}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (Y^3 + Y^2Z + Z^3)(X + Z) = XY^3 + XY^2Z + XZ^3 + Y^3Z + Y^2Z^2 + Z^4,$$

  se anula nos pontos da curva onde $Y = \alpha,\ \alpha^2,\ \alpha^4$ ou $X = 1$. Desta forma, o elemento

$$\frac{XY^3}{Z^4} + \frac{XY^2}{Z^3} + \frac{X}{Z} + \frac{Y^3}{Z^3} + \frac{Y^2}{Z^2} + 1,$$

  gera uma palavra-código com peso 10. Portanto, $d = 10$.

- $\boldsymbol{D = 10P_2 + 2P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{X^2Y^2}{Z^4},\ \frac{Y^3}{Z^3}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X + Z)(X + \alpha Z)(Y + Z)(Y + \alpha^2 Z),$$

  se anula nos pontos da curva onde $Y = 1,\ \alpha^2$ ou $X = 1,\ \alpha$. Desta forma, o elemento

$$\frac{X^2Y^2}{Z^4} + \alpha^3\frac{X^2Y}{Z^3} + \alpha^2\frac{X^2}{Z^2} + \alpha^5\frac{XY^2}{Z^3} + \alpha\frac{XY}{Z^2} + \frac{X}{Z} + \alpha\frac{Y^2}{Z^2} + \alpha^4\frac{Y}{Z} + \alpha^3,$$

  gera uma palavra-código com peso 10. Portanto, $d = 10$.

- $\boldsymbol{D=9P_2+3P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{X^3}{Z^3},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{X^3Y}{Z^4},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X^3+X^2Z+Z^3)(Y+Z) = X^3Y+X^3Z+X^2YZ+X^2Z^2+YZ^3+Z^4,$$

  se anula nos pontos da curva onde $X = \alpha,\ \alpha^2,\ \alpha^4$ ou $Y = 1$. Desta forma, o elemento

$$\frac{X^3Y}{Z^4}+\frac{X^3}{Z^3}+\frac{X^2Y}{Z^3}+\frac{X^2}{Z^2}+\frac{Y}{Z}+1,$$

  gera uma palavra-código com peso 10. Portanto, $d = 10$.

- $\boldsymbol{D=8P_2+4P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{X^3}{Z^3},\ \frac{X^4}{Z^4},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X^3+X^2Z+Z^3)(X+Z) = X^4+X^2Z^2+XZ^3+Z^4,$$

  se anula nos pontos da curva onde $X = 1,\ \alpha,\ \alpha^2,\ \alpha^4$. Desta forma, o elemento

$$\frac{X^4}{Z^4}+\frac{X^2}{Z^2}+\frac{X}{Z}+1,$$

  gera uma palavra-código com peso 10. portanto, $d = 10$.

9. $\boldsymbol{r+s=13}$.

   Os parâmetros dos códigos associados são: $n = 22,\ k = 11,\ 9 \leq d$. Neste caso, é possível obter bases da forma $\dfrac{X^iY^j}{Z^{i+j}}$ para os espaços associados aos seguintes divisores:

   - $\boldsymbol{D=13P_2+0P_1}$

     Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{X^2Y^2}{Z^4},\ \frac{X^3Y^2}{Z^5},\ \frac{Y^3}{Z^3},\ \frac{XY^3}{Z^4},\ \frac{X^2Y}{Z^3}\right\}.$$

O polinômio

$$P(X,Y,Z) = (X^3 + X^2Z + Z^3)(Y^2 + YZ),$$

se anula nos pontos da curva onde $X = \alpha,\ \alpha^2,\ \alpha^4$ ou $Y = 0, 1$. Desta forma, o elemento

$$\frac{X^3Y^2}{Z^5} + \frac{X^3Y}{Z^4} + \frac{X^2Y^2}{Z^4} + \frac{X^2Y}{Z^3} + \frac{Y^2}{Z^2} + \frac{Y}{Z},$$

gera uma palavra-código com peso 9. Portanto, $d = 9$.

- $\boldsymbol{D = 12P_2 + 1P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{X^2Y^2}{Z^4},\ \frac{Y^3}{Z^3},\ \frac{XY^3}{Z^4},\ \frac{Y^4}{Z^4}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X + Y)(Y^3 + YZ^2 + Z^3),$$

  se anula nos pontos da curva onde $X = Y$ ou $Y = \alpha^3,\ \alpha^6,\ \alpha^5$. Desta forma, o elemento

$$\frac{XY^3}{Z^4} + \frac{XY}{Z^2} + \frac{X}{Z} + \frac{Y^4}{Z^4} + \frac{Y^2}{Z^2} + \frac{Y}{Z},$$

  gera uma palavra-código com peso 9. Portanto, $d = 9$.

- $\boldsymbol{D = 11P_2 + 2P_1}$

  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{X^3Y}{Z^4},\ \frac{X^4Y}{Z^5},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{X^2Y^2}{Z^4}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X^2 + XZ)(X + \alpha Z)(X + \alpha^2 Z)(Y + Z),$$

  se anula nos pontos da curva onde $X = 0,\ 1,\ \alpha,\ \alpha^2$ ou $Y = 1$. Desta forma, o elemento

$$\frac{X^4Y}{Z^5} + \alpha^4\frac{X^3Y}{Z^4} + \alpha^5\frac{X^2Y}{Z^3} + \alpha^3\frac{XY}{Z^2} + \frac{X^4}{Z^4} + \alpha^4\frac{X^3}{Z^3} + \alpha^5\frac{X^2}{Z^2} + \alpha^3\frac{X}{Z},$$

  gera uma palavra-código com peso 9. Portanto, $d = 9$.

- $\boldsymbol{D=10P_2+3P_1}$
  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{X^3}{Z^3},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{X^3Y}{Z^4},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3},\ \frac{X^2Y^2}{Z^4}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X+\alpha^3 Z)(X+\alpha^6 Z)(X+Y)(Y+\alpha^3 Z),$$

  se anula nos pontos da curva onde $X = \alpha^3,\ \alpha^6$ ou $X = Y$ ou $Y = \alpha^3$. Desta forma, o elemento

$$\frac{X^3Y}{Z^4}+\alpha^3\frac{X^3}{Z^3}+\frac{X^2Y^2}{Z^4}+\alpha^6\frac{X^2Y}{Z^3}+\alpha\frac{X^2}{Z^2}+\alpha^5\frac{XY^2}{Z^3}+\alpha^6\frac{XY}{Z^2}+\alpha^5\frac{X}{Z}+\alpha^2\frac{Y^2}{Z^2}+\alpha^5\frac{Y}{Z},$$

  gera uma palavra-código com peso 9. Portanto, $d = 9$.

- $\boldsymbol{D=9P_2+4P_1}$
  Uma base para o espaço $\mathcal{L}(D)$ é dada pelo conjunto

$$\left\{1,\ \frac{X}{Z},\ \frac{X^2}{Z^2},\ \frac{X^3}{Z^3},\ \frac{X^4}{Z^4},\ \frac{Y}{Z},\ \frac{XY}{Z^2},\ \frac{X^2Y}{Z^3},\ \frac{X^3Y}{Z^4},\ \frac{Y^2}{Z^2},\ \frac{XY^2}{Z^3}\right\}.$$

  O polinômio

$$P(X,Y,Z) = (X^3+XZ^2+Z^3)(X+Y) = X^4+X^3Y+X^2Z^2+XYZ^2+XZ^3+YZ^3,$$

  se anula nos pontos da curva onde $X = \alpha^3,\ \alpha^6,\ \alpha^5$ ou $X = Y$. Dessa forma, o elemento

$$\frac{X^4}{Z^4}+\frac{X^3Y}{Z^4}+\frac{X^2}{Z^2}+\frac{XY}{Z^2}+\frac{X}{Z}+\frac{Y}{Z},$$

  gera uma palavra-código com peso 9. Portanto, $d = 9$.

Nosso objetivo é sempre gerar códigos que sejam subcódigos de códigos universais ($d = 1$ ou $d = 2$). Todos os códigos obtidos anteriormente são subcódigos do seguinte código universal:

- $\boldsymbol{D=14P_2+7P_1}$.
  Os parâmetros deste código são $n = 22,\ k = 19,\ 1 \leq d$. Um conjunto gerador para o espaço $\mathcal{L}(D)$ é:

$$\left\{ \begin{array}{cccccccccccc} 1 & \frac{X}{Z} & \frac{X^2}{Z^2} & \frac{X^3}{Z^3} & \frac{X^4}{Z^4} & \frac{X^5}{Z^5} & \frac{X^6}{Z^6} & \frac{X^7}{Z^7} & \frac{Y}{Z} & \frac{XY}{Z^2} & \frac{X^2Y}{Z^3} & \frac{X^3Y}{Z^4} \\ \frac{X^4Y}{Z^5} & \frac{X^5Y}{Z^6} & \frac{Y^2}{Z^2} & \frac{XY^2}{Z^3} & \frac{X^2Y^2}{Z^4} & \frac{X^3Y^2}{Z^5} & \frac{X^4Y^2}{Z^6} & \frac{Y^3}{Z^3} & \frac{XY^3}{Z^4} & \frac{X^2Y^3}{Z^6} & \frac{Y^4}{Z^4} & \frac{XY^4}{Z^5} \end{array} \right\}$$

Tendo como base a equação (4.2) podemos eliminar os elementos

$$\frac{X^3Y}{Z^4}, \frac{X^4Y}{Z^5}, \frac{X^5Y}{Z^6}, \frac{X^3Y^2}{Z^5}, \frac{X^4Y^2}{Z^6}.$$

Os 19 elementos restantes são linearmente independentes pois, tomando-se a ordem $X > Y > Z$, nenhum dos elementos restantes é divisível por X^3Y (termo líder do polinômio que gera a curva). A matriz geradora deste código tem como linhas

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 (relativa ao gerador 1)

0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 (relativa ao gerador $\frac{X^7}{Z^7}$).

Desta forma, somando-se essas duas linhas, teremos uma palavra-código com peso 1. Portanto, $d = 1$.

4.3 Códigos Multiníveis

Um dos objetivos de se fazer concatenação de códigos, é a obtenção de códigos com comprimento grande através de códigos de comprimento menor e também com distâncias mínimas grandes. Nesta seção, vamos mostrar que os códigos de Goppa podem ser utilizados na construção de códigos multiníveis, usando as idéias desenvolvidas em [12]. No final da seção, apresentaremos uma tabela de códigos obtidos pelo processo de concatenação usando os códigos racionais estudados no Capítulo 2. Esta tabela reproduz os resultados em [12], porém sem a necessidade de se fazer uso de códigos estendidos.

Uma **cadeia de partição** é uma sequência de códigos lineares, $A_1, A_2, ..., A_{m+1}$, de comprimento n_1 sobre $\mathbb{F}_q$, satisfazendo as condições

$$A_{i+1} \subset A_i, \quad |A_i/A_{i+1}| = q, \text{ para } \quad i = 1, 2, ..., m, \text{ com } \quad m \leq n_1.$$

Assumimos que $A_{m+1} = \{0\}$ com distância de Hamming ∞. Como os códigos em consideração

são lineares, a partição pode ser expressa na seguinte forma

$$A_i = \bigcup_{y^{(i)} \in \mathbb{F}_q} (y^{(i)} a_i + A_{i+1}), \text{ para } \quad i = 1, 2, ..., m, \quad a_i \in A_i, \quad a_i \notin A_{i+1},$$

onde a_i é um representante de uma classe de equivalência de A_{i+1} em A_i. Portanto, todas as palavras-código de A_1 podem ser completamente descritas pelo conjunto dos números q-ários $y^{(1)}, y^{(2)}, ...y^{(m)}$. Os códigos A_i são chamados **códigos internos**.

Para construirmos códigos multiníveis, vamos usar m códigos q-ários $C_i,\ i = 1, 2, ..., m$ com comprimento n_2, chamados **códigos externos**. Considere a matriz onde cada linha consiste de uma palavra-código de cada um dos códigos externos, respectivamente, isto é,

$$\begin{pmatrix} y_1^{(1)} & y_2^{(1)} & ... & y_{n_2}^{(1)} \\ y_1^{(2)} & y_2^{(2)} & ... & y_{n_2}^{(2)} \\ ... & ... & ... & ... \\ y_1^{(m)} & y_2^{(m)} & ... & y_{n_2}^{(m)} \end{pmatrix},$$

onde a i-ésima linha é uma palavra-código do código C_i. Desta forma, uma palavra do código multinível é representada da forma $(S_1, S_2, ..., S_{n_2})$, onde

$$S_j = y_j^{(1)} a_1 + y_j^{(2)} a_2 + ... + y_j^{(m)} a_m.$$

A distância mínima desses códigos satisfaz

$$d_{min} \geq min\{d_a^{(i)} d_c^{(i)},\ 1 \leq i \leq m\},$$

onde $d_a^{(i)}$ e $d_c^{(i)}$ denotam as distâncias mínimas dos códigos interno e externo, respectivamente.

Exemplo 4.3.1 *No Exemplo 2.3.5, Seção 2.3, foram construídos os seguintes códigos:*

- A_1 *com parâmetros* $(4, 4, 1)$ *e matriz geradora*

$$G_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

- *A_2 com parâmetros $(4, 3, 2)$ e matriz geradora*

$$G_2 = \begin{bmatrix} 0 & 1 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

- *A_3 com parâmetros $(4, 2, 3)$ e matriz geradora*

$$G_3 = \begin{bmatrix} 0 & 1 & \alpha & \alpha^2 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Vamos considerar A_4 como sendo o código com parâmetros $(4, 1, 4)$ e matriz geradora

$$G_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$$

Dessa forma, temos que $A_1 \supset A_2 \supset A_3 \supset A_4 \supset A_5 = \{0\}$ e também que

$$A_1 = \bigcup_{y^{(i)} \in \mathbb{F}_4} (y^{(i)}(0, 1, 1, 1) + A_2)$$

$$A_2 = \bigcup_{y^{(i)} \in \mathbb{F}_4} (y^{(i)}(0, 1, \alpha^2, \alpha) + A_3)$$

$$A_3 = \bigcup_{y^{(i)} \in \mathbb{F}_4} (y^{(i)}(0, 1, \alpha, \alpha^2) + A_4)$$

$$A_4 = \bigcup_{y^{(i)} \in \mathbb{F}_4} (y^{(i)}(1, 1, 1, 1) + A_5)$$

Portanto, a matriz geradora do código A_1 é também a matriz geradora do código multinível.

No Exemplo 2.3.1, Seção 2.3, construímos um código com parâmetros $(5, 5, 1)$. Pelo processo descrito na Seção (2.4) podemos construir subcódigos deste código com parâmetros $(5, 4, 2)$, $(5, 3, 3)$, $(5, 2, 4)$ e $(5, 1, 5)$. A Tabela 4.3 ilustra os códigos multiníveis obtidos utilizando-se estes subcódigos como códigos externos. Esta tabela reproduz os resultados apresentados em [12], porém sem a necessidade de se fazer uso de códigos estendidos.

C_1	C_2	C_3	C_4	código multinível
$\{0\}$	$\{0\}$	$\{0\}$	$(5, 1, 5)$	$(20, 1, d = 20)$
$\{0\}$	$\{0\}$	$\{0\}$	$(5, 2, 4)$	$(20, 2, d \geq 16)$
$\{0\}$	$\{0\}$	$(5, 1, 5)$	$(5, 2, 4)$	$(20, 3, d \geq 15)$
$\{0\}$	$\{0\}$	$(5, 2, 4)$	$(5, 3, 3)$	$(20, 5, d \geq 12)$
$\{0\}$	$(5, 1, 5)$	$(5, 2, 4)$	$(5, 3, 3)$	$(20, 6, d \geq 10)$
$\{0\}$	$(5, 1, 5)$	$(5, 3, 3)$	$(5, 3, 3)$	$(20, 7, d \geq 9)$
$\{0\}$	$(5, 2, 4)$	$(5, 3, 3)$	$(5, 4, 2)$	$(20, 9, d \geq 8)$
$\{0\}$	$(5, 3, 3)$	$(5, 4, 2)$	$(5, 4, 2)$	$(20, 11, d \geq 6)$
$(5, 1, 5)$	$(5, 3, 3)$	$(5, 4, 2)$	$(5, 4, 2)$	$(20, 12, d \geq 5)$
$(5, 2, 4)$	$(5, 4, 2)$	$(5, 4, 2)$	$(5, 1, 5)$	$(20, 15, d \geq 4)$
$(5, 3, 3)$	$(5, 4, 2)$	$(5, 5, 1)$	$(5, 5, 1)$	$(20, 17, d \geq 3)$

Tab. 4.3: Códigos multiníveis obtidos de códigos racionais.

4.4 Conclusões

Neste capítulo, por meio de dois exemplos, apresentamos a construção de códigos provenientes de curvas com gêneros 2 e 3, usando as mesmas idéias apresentadas no Capítulo 3 e na Observação A.2.1. Mostramos também que os códigos de Goppa podem ser usados, de uma maneira bem simples, na construção de códigos multiníveis.

Capítulo 5

Conclusões

Em pesquisas anteriores sobre sistemas de comunicação digital, cada um dos blocos do diagrama de blocos que compõem o sistema (ver Figura I) eram estudados separadamente. Nestes estudos, cada um dos blocos do diagrama foram associados a estruturas matemáticas como espaços métricos provenientes de espaços vetorias e, mais recentemente, espaços topológicos. Desta última associação, um novo conceito matemático passou a ser de grande importância no estudo de sistemas de comunicação: o conceito de gênero de uma superfície. Pesquisas recentes mostraram que o desempenho de sistemas de comunicação digital está associado ao gênero da superfície na qual o canal pode ser mergulhado ([1], [2]). Os códigos de Goppa, ou códigos algébrico-geométricos, formam uma classe de códigos com um bom desempenho e estão associados a curvas algébricas. Um dos conceitos fundamentais no estudo de curvas é o conceito de gênero da curva. Curvas algébricas e superfícies de Riemann estão relacionadas através do gênero (da curva ou da superfície) como pode ser visto no Capítulo B.

Neste trabalho, motivados por esta relação entre desempenho de sistemas, gênero de superfícies e curvas algébricas, nossa proposta foi fazer um estudo dos sistemas de uma forma conjunta, propondo uma integração entre modulação e codificação de canal, baseados em um único conceito matemático: o gênero de uma superfície na qual o canal pode ser mergulhado. Para fazer esta integração, nossa proposta foi: fixado um gênero g ($g = 0, 1, 2, 3$), encontrar curvas com este gênero e fazer uma análise dos parâmetros dos códigos associados a esta curva, a fim de se obter uma modulação, ou seja, um código com parâmetros $(n, n, 1)$ ou $(n, n-1, 2)$, e um subcódigo desta modulação, com parâmetros (n, k, d), $k < n$, para ser utilizado na codificação de canal. Além disto buscamos, sempre que possível, curvas maximais, isto é, curvas com o maior número de pontos racionais possíveis.

Os resultados obtidos estão assim distribuídos:

- no Capítulo 2, estudamos os códigos racionais ($g = 0$). Apresentamos uma maneira

diferente de se estudar códigos racionais, usando as idéias presentes em [4]. Com este processo, dado um corpo finito $\mathbb{F}_q$, podemos obter códigos racionais com parâmetros $n = q + 1$, $k \leq n$ e $d = n - k + 1$, isto é, códigos MDS. Entretanto, ao escolhermos subcódigos destes códigos estes podem perder esta propriedade. Desta forma, no final do capítulo, apresentamos um algoritmo para obtenção de subcódigos MDS de modulações racionais com parâmetros $(n, n, 1)$;

- no Capítulo 3, estudamos códigos provenientes de curvas elípticas ($g = 1$). Calculamos, como exemplos, os parâmetros dos códigos associados às curvas Hermitiana e de Hurwitz, que são duas curvas maximais de gênero um. Uma diferença entre estas curvas é que a curva Hermitiana possui um único ponto no infinito, enquanto que a curva de Hurwitz possui dois pontos no infinito. Assim, de acordo com a observação A.2.1, precisamos usar divisores com um ponto base, no caso da Hermitiana, e com dois pontos base, no caso da curva de Hurwitz. Tendo como base os parâmetros dos códigos encontrados nestes dois exmplos, no final apresentamos um resultado sobre os parâmetros dos códigos provenientes de curvas elípticas maximais;

- no Capítulo 4, estudamos códigos provenientes de curvas de gênero $g = 2$ e $g = 3$. As dificuldades são a escassez de exemplos e o fato de se ter que trabalhar com curvas singulares (no caso $g = 2$). Por meio de dois exemplos, obtidos em [11] e [9], calculamos os parâmetros dos códigos associados a estas duas curvas. No final, mostramos que os códigos de Goppa podem ser utilizados para fazer concatenação de códigos.

5.1 Propostas de trabalhos futuros

Durante o desenvolvimento deste trabalho, surgiram alguns tópicos interessantes para estudos futuros. Podemos destacar os seguintes tópicos:

- Estudo de códigos algébricos geométricos por meio de semigrupos;

- Estudo de códigos algébrico geométricos provenientes de ordens;

- Puncionamento de códigos de Goppa por meio de ramificações.

Referências Bibliográficas

[1] Rodrigo G. Cavalcante, Henrique Lazari, João de Deus Lima, Reginaldo Palazzo, Jr. A New Approach to the Design of Digital Communication Systems. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 68:145–177, 2005.

[2] João de Deus Lima. Identificação e Estrutura Algébrica das Superfícies Compactas com e sem Bordos Provenientes de Mergulhos de Canais Discretos sem Memória . Tese de doutorado, Faculdade de Engenharia Elétrica e de Computação, UNICAMP, Março 2002.

[3] Henry McKean, Victor Moll. *Elliptic Curves: Function Theory, Geometry, Arithmetic*. Cambridge University Press, 1997.

[4] Abramo Hefez, Maria Lúcia T. Villela. *Códigos Corretores de Erros*. IMPA, 2002.

[5] Judy L. Walker. *Codes and Curves*. AMS Press, 2000.

[6] David Cox, John Little, Donal O'Shea. *Ideals, Varieties and Algorithms*. Springer Verlag, 1992.

[7] William Fulton. *Algebraic Curves*. W. A. Benjamin, INC., 1969.

[8] Kenji Ueno. *An Introduction to Algebraic Geometry*. AMS Press, 1997.

[9] Arnaldo Garcia. *Pontos Racionais em Curvas Sobre Corpos Finitos*. IMPA, 1995.

[10] Angela Aguglia, Gábor Korchmáros, Fernando Torres . Plane Maximal Curves. *Acta Arithmetica*, 98(2):165–179, 2001.

[11] Miriam Abdón, Fernando Torres . On Maximal curves in characteristic two. *Manuscripta Math.*, 99:39–53, 1999.

[12] Jiantian Wu, Daniel J. Costello, Jr. New Multilevel Codes over GF(q). *IEEE Transactions on Information Theory*, 38(3):933–939, Maio 1992.

[13] Miriam Abdón, Fernando Torres . On a characterization of certain maximal curves. *Finite Fields and Their Applications*, 10:133–158, 2004.

[14] Gábor Korchmáros, Fernando Torres . On the genus of a maximal curve. *Mathematische Annalen*, 323:589–608, 2002.

[15] Gregory J. Pottie, Desmond P. Taylor. Multilevel Codes Based on Patitioning. *IEEE Transactions on Information Theory*, 35(1):87–98, Janeiro 1989.

[16] A. R. Calderbank. Multilevel Codes and Multistage Decoding. *IEEE Transactions on Communications*, 37(3):222–229, Março 1989.

[17] A. Cossidente, J. W. P. Hirschfeld, Gábor Korchmáros, Fernando Torres . On Plane Maximal Curves. *Compositio Mathematica*, 121:163–181, 2000.

[18] Hideki Imai, Shuji Hirakawa. A New Multilevel Coding Method Using Error-Correcting Codes. *IEEE Transactions on Information Theory*, IT-23(3):371–377, 1997.

[19] José Felipe Voloch. *Códigos Corretores de Erros*. IMPA, 1987.

[20] Givaldo Oliveira dos Santos. Caracterização Geométrica do Processo de Decodificação da Classe dos Códigos Alternantes Cíclicos Através de Polinômios Absolutamente Irredutíveis. Tese de doutorado, Faculdade de Engenharia Elétrica e de Computação, UNICAMP, Abrila 2003.

[21] Rick Miranda. *Algebraic Curves and Riemann Surfaces*. American Mathematical Society, 1995.

[22] Yoichi Ymayoshi, Masahiko Taniguchi. *An Introduction to Teichmüller Spaces*. Springer, 1992.

Índice Remissivo

Apêndice A

Pré-Requisitos

Neste capítulo, veremos os conceitos e resultados principais que serão necessários para a compreensão da teoria utlizada neste trabalho.

Este capítulo está organizado da seguinte forma. Na Seção A.1, serão apresentados alguns conceitos sobre anéis de polinômios em duas e três indeterminadas. Na Seção A.2, apresentaremos os conceitos e resultados sobre curvas algébricas e códigos de Goppa. Na Seção A.3, apresentaremos os conceitos relacionados às ordens monomiais e bases de Groebner.

A.1 O Anel de Polinômios

Sejam k um corpo e $k[X,Y]$, $k[X,Y,Z]$ os anéis de polinômios em duas e três indeterminadas sobre k. Estes dois anéis são fundamentais na teoria de curvas algébricas.

Um **polinômio homogêneo** de grau r, ou uma **forma** de grau r, é um polinômio da forma

$$F(X,Y,Z) = \sum_{i_0+i_1+i_2=r} a_{i_0 i_1 i_2} X^{i_0} Y^{i_1} Z^{i_2},\ a_{i_0 i_1 i_2} \in k$$

Formas são utilizadas na definição de curvas algébricas.

Seja $F(X,Y,Z) = \sum_{i_0+i_1+i_2=r} a_{i_0 i_1 i_2} X^{i_0} Y^{i_1} Z^{i_2}$ uma forma de grau r. A **desomogeneização** de F com respeito a Z é o polinômio

$$F_*(X,Y) = F(X,Y,1) \in k[X,Y]$$

Da mesma forma, dado $f(X,Y) \in k[X,Y]$ um polinômio de grau r, definimos a **homogeneiza-**

ção de f como sendo a forma

$$f^*(X,Y,Z) = Z^r f(\frac{X}{Z}, \frac{Y}{Z}) \in k[X,Y,Z]$$

A respeito dos processos descritos anteriormente, valem os seguintes resultados.

Proposição A.1.1 ([4]) *Sejam $F, G \in k[X,Y,Z]$ formas de grau r e $f, g \in k[X,Y]$. Então:*

1. $(fg)^* = f^* g^*,\ (f^*)_* = f$.

2. $(FG)_* = F_* G_*,\ F = Z^t (F_*)^*$, *onde t é a maior potência de Z que divide F.*

Seja $\overline{k}$ o fecho algébrico do corpo k. Um polinômio $f \in k[X,Y]$ é **absolutamente irredutível** se for um polinômio irredutível em $\overline{k}[X,Y]$. Polinômios irredutíveis também são utilizados na definição de curvas algébricas.

Em geral não é simples saber quando um determinado polinômio é absolutamente irredutível ou não. Se o polinômio for da forma especial

$$f(X,Y) = a_0 Y^n + a_1(X) Y^{n-1} + ... + a_n(X),\ a_i(X) \in k[X],\ a_0 \neq 0, \tag{A.1}$$

podemos utilizar o seguinte critério para verificar se o mesmo é absolutamente irredutível.

Teorema A.1.1 ([9]) *Seja $f(X,Y)$ um polinômio escrito na forma A.1. Suponha que $gr(a_n(X)) = m$ é relativamente primo com n e também que*

$$\frac{m}{n} > \frac{gr(a_i(X))}{i},\ i = 1, 2, ..., n-1.$$

Então o polinômio $f(X,Y)$ é absolutamente irredutível.

A.2 Curvas e Códigos de Goppa

Sejam k um corpo e $\overline{k}$ seu fecho algébrico. Nesta seção veremos as definições do espaço projetivo, o espaço onde as curvas algébricas são definidas, de curvas algébricas e outros conceitos fundamentais à teoria dos códigos de Goppa.

O **plano projetivo** $\mathbb{P}^2(k)$ é definido como o conjunto quociente de $k^3 \setminus (0,0,0)$ por uma relação de equivalência $\sim$, ou seja,

$$\mathbb{P}^2(k) = \frac{k^3 \setminus (0,0,0)}{\sim},$$

onde

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \Longleftrightarrow \exists\ a \in k^*;\ x_1 = ax_2,\ y_1 = ay_2,\ z_1 = az_2.$$

Como os pontos de $\mathbb{P}^2(k)$ são classes de equivalência, vamos usar a notação $(x : y : z)$ para representar estes elementos.

Seja $F(X, Y, Z) \in k[X, Y, Z]$ um polinômio homogêneo de grau d, e tal que $f(X, Y) = F(X, Y, 1)$ seja absolutamente irredutível. Definimos a **curva plana projetiva** de grau d associada ao polinômio F, denotada por $\mathcal{X}$ ou por $\mathcal{X}_F$, como sendo o conjunto

$$\mathcal{X} = \{(x : y : z) \in \mathbb{P}^2(k) |\ F(x, y, z) = 0\},$$

ou simplesmente

$$\mathcal{X} : F(X, Y, Z) = 0.$$

Dada uma curva podemos associar o seu **gênero**, denotado por $g(\mathcal{X})$, que satisfaz a seguinte desigualdade

$$g(\mathcal{X}) \leq \frac{(d-1)(d-2)}{2}.$$

Esta desigualdade passa a ser uma igualdade quando a curva for **não singular**, isto é, quando vale a condição

$$F(x, y, z) = F_X(x, y, z) = F_Y(x, y, z) = F_Z(x, y, z) = 0 \Longrightarrow (x, y, z) = (0, 0, 0),$$

onde F_X, F_Y, F_Z denotam as derivadas parciais de F com relação às variáveis X, Y, Z, respectivamente.

Teorema A.2.1 (Teorema de Bezout,[7]) *Seja k um corpo algebricamente fechado e consideremos F, $G \in k[X, Y, Z]$ polinômios homogêneos, sem fatores em comum, de grau m e n, respectivamente. As curvas projetivas $\mathcal{X}_F$, $\mathcal{X}_G$ definidas pelos polinômios acima se encontram em mn pontos. Em outras palavras vale*

$$\sum_P I(P, F, G) = mn,$$

onde $I(P, F, G)$ é a multiplicidade de intersecção das curvas definidas por F e G no ponto P.

O Teorema de Bezout estabelece que duas curvas, de graus m e n, respectivamente, têm mn pontos em comum (levando-se em conta as multiplicidades). Este teorema também é utilizado para o cálculo de divisores de intersecção.

Seja $\mathcal{X}$ uma curva plana projetiva definida por um polinômio homogêneo F e seja K um corpo qualquer contendo k. Um $K-$**ponto racional** em $\mathcal{X}$ é um ponto $(x:y:z) \in \mathbb{P}^2(K)$ tal que $F(x,y,z)=0$. Denotamos o conjunto dos $K-$pontos racionais da curva $\mathcal{X}$ como

$$\mathcal{X}(K) = \{(x:y:z) \in \mathbb{P}^2(K) |\ F(x,y,z)=0\}.$$

Com relação aos conjuntos $\mathcal{X}(K)$ vale o seguinte resultado.

Teorema A.2.2 ([5],[9],[19]) *Seja $\mathcal{X}$ uma curva projetiva não singular definida sobre um corpo finito $k=\mathbb{F}_q$. Então*

$$\#\mathcal{X}(\mathbb{F}_q) \leq 1+q+2g\sqrt{q},$$

onde $g=g(\mathcal{X})$, $\#\mathcal{X}(\mathbb{F}_q)$ denota a cardinalidade do conjunto $\mathcal{X}(\mathbb{F}_q)$ e q é um primo ou potência de primo.

Seja $k=\mathbb{F}_p$ um corpo finito com p elementos, p primo. Sabemos que, a menos de isomorfismos, existe um único corpo com p^n elementos, que denotaremos por $\mathbb{F}_{p^n}$. Sabemos também que $\mathbb{F}_{p^n} |\ \mathbb{F}_p$ é uma extensão finita de grau n, o grupo de Galois desta extensão é cíclico de ordem n e é gerado pelo chamado **automorfismo de Frobenius** dado por

$$\begin{array}{rccc} \sigma_{p,n}: & \mathbb{F}_{p^n} & \longrightarrow & \mathbb{F}_{p^n} \\ & \alpha & \longmapsto & \sigma_{p,n}(\alpha)=\alpha^p. \end{array}$$

Se $\mathcal{X}$ é uma curva plana projetiva definida sobre $\mathbb{F}_p$, podemos fazer este automorfismo agir nos pontos de $\mathbb{F}_{p^n}$ da seguinte forma

$$\sigma_{p,n}((x_0:y_0:z_0)) = (x_0^p : y_0^p : z_0^p).$$

O automorfismo de Frobenius pode ser usado para encontrar os pontos racionais de uma curva.

Seja $\mathcal{X}$ uma curva plana projetiva não singular. Um **ponto de grau** n em $\mathcal{X}$ sobre $\mathbb{F}_p$ é um conjunto $P=\{P_0, P_1, ..., P_{n-1}\}$ de n pontos distintos em $\mathcal{X}(\mathbb{F}_{p^n})$ tal que

$$P_i = \sigma_{p,n}^i(P_0),\ i=1,2,...,n-1.$$

Seja $\mathcal{X}$ uma curva definida em $\mathbb{F}_q$. Um **divisor** D em $\mathcal{X}$ é uma soma formal de pontos da curva com coeficientes inteiros, isto é, um divisor é um elemento da forma

$$D = \sum n_Q Q,$$

onde $n_Q \in \mathbb{Z}$ e Q são pontos (de grau arbitrário) em $\mathcal{X}$.

Se $n_Q \geq 0 \ \forall Q$, dizemos que o divisor D é **efetivo** e denotamos por $D \geq 0$. Definimos o **grau** de um divisor como sendo

$$gr(D) = \sum n_Q gr(Q),$$

e o **suporte** de um divisor D, denotado por $Supp(D)$, como sendo o conjunto dos pontos Q da curva que aparecem com coeficientes não nulos no divisor D, isto é,

$$Supp(D) = \{Q|\ n_Q \neq 0\}.$$

O conceito de divisor é importante pois, por meio de divisores, podemos associar espaços vetoriais a uma determinada curva e, por meio destes espaços, podemos definir os códigos de Goppa.

Seja $F(X, Y, Z)$ um polinômio que define uma curva plana projetiva $\mathcal{X}$ sobre $\mathbb{F}_q$ e seja

$$E = \left\{ \frac{G(X,Y,Z)}{H(X,Y,Z)} | G,\ H \text{ são homogêneos de mesmo grau} \right\} \cup \{0\}.$$

O **corpo das funções racionais** em $\mathcal{X}$, denotado por $\mathbb{F}_q(\mathcal{X})$ é o conjunto quociente de E por uma relação de equivalência $\sim$, isto é,

$$\mathbb{F}_q(\mathcal{X}) = \frac{E}{\sim},$$

onde

$$\frac{G}{H} \sim \frac{G'}{H'} \Longleftrightarrow GH' - G'H \in \langle F \rangle, \tag{A.2}$$

com $\langle F \rangle$ representando o ideal gerado pelo polinômio F em $k[X, Y, Z]$.

Seja $\mathcal{X}$ uma curva definida pelo polinômio F, e $f = \dfrac{G}{H} \in \mathbb{F}_q(\mathcal{X})$. O **divisor de** f é definido como

$$div(f) = \sum_{P \in \mathcal{X}_F \cap \mathcal{X}_G} I(P, F, G)P - \sum_{Q \in \mathcal{X}_F \cap \mathcal{X}_H} I(Q, F, H)Q. \tag{A.3}$$

Seja D um divisor sobre uma curva não singular. O **espaço das funções racionais associadas a** D é o conjunto

$$\mathcal{L}(D) = \{f \in \mathbb{F}_q(\mathcal{X})|\ div(f) + D \geq 0\} \cup \{0\}.$$

Este conjunto é um espaço vetorial finitamente gerado sobre $\mathbb{F}_q$ e vale o seguinte resultado.

Teorema A.2.3 (Teorema de Riemann-Roch,[5]) *Seja $\mathcal{X}$ uma curva plana projetiva não*

singular de gênero g definida sobre $\mathbb{F}_q$ e D um divisor em $\mathcal{X}$. Então $dim\mathcal{L}(D) \geq gr(D)+1-g$. Mais ainda, se $gr(D) > 2g-2$, então $dim\mathcal{L}(D) = gr(D)+1-g$.

Agora podemos definir os códigos algébricos-geométricos da seguinte forma. Considere $\mathcal{X}$ como uma curva plana projetiva definida sobre $\mathbb{F}_q$, D um divisor em $\mathcal{X}$ e $\mathcal{P} = \{P_1, ..., P_n\}$ um conjunto de n pontos $\mathbb{F}_q$-racionais distintos em $\mathcal{X}$. Suponha que $\mathcal{P} \cap Supp(D) = \emptyset$.

O **código algébrico-geométrico** associado à curva $\mathcal{X}$, ao conjunto $\mathcal{P}$ e ao divisor D é o conjunto

$$\mathcal{C}(\mathcal{X}, \mathcal{P}, D) = \{(f(P_1), ..., f(P_n))|\ f \in \mathcal{L}(D)\} \in \mathbb{F}_q^n. \tag{A.4}$$

Os parâmetros do código definido em (A.4) são dados pelo seguinte resultado.

Teorema A.2.4 ([5],[19]) *Seja $\mathcal{X}$ uma curva plana, projetiva, de gênero g, definida sobre $\mathbb{F}_q$. Seja $\mathcal{P} \subset \mathcal{X}(\mathbb{F}_q)$ um conjunto de n pontos $\mathbb{F}_q-$racionais distintos, e seja D um divisor tal que $2g-2 < gr(D) < n$. Então o código algébrico-geométrico $\mathcal{C}(\mathcal{X}, \mathcal{P}, D)$ é linear de comprimento n, dimensão $k = gr(D)+1-g$ e distância mínima $d \geq n - gr(D)$.*

Observação A.2.1 *Como foi visto nesta seção, para o cálculo dos parâmetros de um código de Goppa, precisamos conhecer os espaços $\mathcal{L}(D)$. Para sabermos se uma função racional pertence a um determinado espaço $\mathcal{L}(D)$, precisamos calcular seu divisor e isto não é uma tarefa fácil, pois envolve o conceito de multiplicidade de intersecção (ver A.3). Desta forma, durante este trabalho, buscaremos bases para os espaços $\mathcal{L}(D)$ da forma $\frac{X^iY^j}{Z^{i+j}}$ pois, com elementos desta forma, o cálculo dos divisores é mais simples. Por este motivo, quando uma curva possuir um único ponto da forma $(\alpha : \beta : 0)$ (chamado ponto no infinito), usaremos divisores com um único ponto base, como na Seção 3.1 e, caso a curva tenha mais de um ponto desta forma, usaremos divisores com mais de um ponto base, como na Seção 3.2.*

O Teorema A.2.4 nos dá um limitante inferior para a distância mínima de códigos associados a curvas algébricas. Para o cálculo das distâncias mínimas dos códigos, em muitos casos (ver Seções 3.2, 4.1, 4.2), adotaremos o seguinte procedimento: tendo uma base do espaço $\mathcal{L}(D)$ e conhecendo os pontos racionais da curva, buscaremos polinômios homogêneos

$$P(X,Y,Z) = \sum_{i_0+i_1+i_2=r} a_{i_0i_1i_2} X^{i_0}Y^{i_1}Z^{i_2},\ a_{i_0i_1i_2} \in k,$$

tais que $\frac{X^{i_0}Y^{i_1}}{Z^{r-i_2}} \in \mathcal{L}(D)$ e que se anulem em $gr(D)$ pontos racionais da curva pois, desta forma, a função racional $f = \sum_{i_0+i_1+i_2=r} a_{i_0i_1i_2} \frac{X^{i_0}Y^{i_1}}{Z^{r-i_2}}$ dá origem a uma palavra código de peso $n-gr(D)$. Desta forma, $d = n - gr(D)$.

A.3 Ordem Monomial e Bases de Groebner

Nesta seção, veremos alguns conceitos relacionados à ordens monomiais e bases de Groebner. Por meio destes conceitos, podemos estender o algoritmo da divisão para polinômios de mais de uma variável. Estes conceitos podem ser utilizados para mostrar independência linear de funções racionais e, assim, obter bases dos espaços vetoriais associados a divisores. Usaremos as seguintes notações:

- $k[X_1, X_2, ..., X_n] = k[\underline{X}]$;
- $X_1^{a_1} X_2^{a_2} ... X_n^{a_n} = \underline{X}^a,\ a = (a_1, a_2, ..., a_n) \in \mathbb{N}^n$.
- $a = (a_1, a_2, ..., a_n) \in \mathbb{N}^n,\ |a| = a_1 + a_2 + ... + a_n$.

Para fazermos divisões entre polinômios com uma variável usamos, de uma forma implícita, uma ordem monomial bastante natural, isto é, dados $i, j \in \mathbb{N}$ temos

$$X^i > X^j \Leftrightarrow i > j.$$

Para fazermos divisões com polinômios com mais de uma variável, precisamos do conceito de ordens monomiais.

Uma **ordem monomial** em $k[\underline{X}]$ é qualquer relação $>$ em $\mathbb{N}^n$ que satisfaz:

1. $>$ é uma relação de ordem total em $\mathbb{N}^n$, isto é, $\forall\ \alpha, \beta \in \mathbb{N}^n$ temos $\alpha = \beta$ ou $\alpha > \beta$ ou $\beta > \alpha$;
2. se $\alpha > \beta$ e $\gamma \in \mathbb{N}^n$ então vale $\alpha + \gamma > \beta + \gamma$;
3. a relação é boa ordem, isto é, todo subconjunto não vazio de $\mathbb{N}^n$ tem menor elemento.

Vejamos alguns exemplos de ordens monomiais.

Exemplo A.3.1 (Ordem Lexicográfica) *Sejam $\alpha = (a_1, \ldots, a_n),\ \beta = (b_1, \ldots, b_n)$ elementos de $\mathbb{N}^n$. Então*

$$\alpha >_{lex} \beta \Longleftrightarrow \exists\ i \in \{1, 2, ..., n\};\ a_i > b_i\ e\ a_k = b_k,\ k = 1, 2, ..., i-1.$$

Esta ordem é estendida para monômios da seguinte forma:

$$\underline{X}^\alpha >_{lex} \underline{X}^\beta \Longleftrightarrow \alpha >_{lex} \beta.$$

Exemplo A.3.2 (Ordem Lexicográfica Graduada) *Sejam $\alpha, \beta \in \mathbb{N}^n$. Então*

$$\alpha >_{grlex} \beta \Longleftrightarrow |\alpha| > |\beta| \text{ ou } |\alpha| = |\beta| \text{ e } \alpha >_{lex} \beta.$$

Esta ordem é estendida para monômios da seguinte forma:

$$\underline{X}^{\alpha} >_{grlex} \underline{X}^{\beta} \Longleftrightarrow \alpha >_{grlex} \beta.$$

Exemplo A.3.3 (Ordem Lexicográfica Graduada Reversa) *Sejam $\alpha, \beta \in \mathbb{N}^n$. Então*

$\alpha >_{grevlex} \beta \Longleftrightarrow |\alpha| > |\beta|$ *ou* $|\alpha| = |\beta|$ *e* $\exists\, i \in \{1, 2, ..., n\};\ a_i > b_i$ *e* $a_k = b_k,\ k = i{+}1, i{+}2, ..., n.$

Esta ordem é estendida para monômios da seguinte forma:

$$\underline{X}^{\alpha} >_{grevlex} \underline{X}^{\beta} \Longleftrightarrow \alpha >_{grevlex} \beta.$$

Seja $f = \sum a_{\alpha} \underline{X}^{\alpha}$ um polinômio não nulo em $k[\underline{X}]$, e seja $>$ uma ordem qualquer. Definimos:

- **multidegree** de f como, $mult(f) = max\{\alpha \in \mathbb{N}^n; a_{\alpha} \neq 0\}$;
- **coeficiente líder** de f como, $LC(f) = a_{mult(f)} \in k$;
- **monômio líder** de f como, $LM(f) = \underline{X}^{mult(f)}$;
- **termo líder** de f como, $LT(f) = LC(f)LM(f)$.

Assim, como no caso de polinômios em uma variável, temos um algoritmo de divisão para polinômios em mais de uma variável, descrito a seguir.

Teorema A.3.1 ([6]) *Fixe uma ordem qualquer em $\mathbb{N}^n$. Seja $(f_1, \ldots, f_s)$ uma s-upla ordenada de polinômios em $k[X_1, \ldots, X_n]$. Então, dado $f \in k[\underline{X}]$, existem $a_1, \ldots, a_s, r \in k[\underline{X}]$, tais que*

$$f = a_1 f_1 + \ldots + a_s f_s + r,$$

onde $r = 0$ ou r é uma combinação linear de monômios, nenhum dos quais é divisível por $LT(f_1), \ldots, LT(f_s)$. Tal r é chamado resto da divisão de f por $f_1, \ldots, f_s$.

Fixe uma ordem monomial. Seja $I \subseteq k[\underline{X}]$ um ideal não nulo. Definimos:

- o **conjunto dos termos líderes** do ideal I como, $LT(I) = \{c\underline{X}^{\alpha}; \exists\ f \in I, LT(f) = c\underline{X}^{\alpha}\}$;

- **ideal gerado** pelo conjunto $LT(I)$ como, $\langle LT(I)\rangle$.

Fixe uma ordem monomial. Um subconjunto finito $G = \{g_1, \ldots, g_s\}$ de um ideal I é uma **base de Groebner** para I se

$$\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle.$$

Teorema A.3.2 ([6]) *Fixe uma ordem. Todo ideal não nulo I de $k[\underline{X}]$ possui uma base de Groebner. Mais ainda, toda base de Groebner é uma base para o ideal I.*

Teorema A.3.3 ([6]) *Seja $G = \{g_1, \ldots, g_s\}$ uma base de Groebner do ideal I e $f \in k[\underline{X}]$. Então existe um único $r \in k[\underline{X}]$ com as seguintes propriedades:*

1. *Existe $g \in I$ tal que $f = g + r$;*

2. *Nenhum termo de r é divisível por $LT(g_1), \ldots, LT(g_s)$.*

Em particular, o resto da divisão de f por G, não importando a ordem como os elementos são listados, é sempre o mesmo.

Corolário A.3.3.1 ([6]) *Seja G uma base de Groebner de um ideal I e $f \in k[\underline{X}]$. Então*

$$f \in I \iff \text{o resto da divisão de } f \text{ por } G \text{ é } 0$$

Por meio do Corolário A.3.3.1 é possível saber quando um polinômio pertence a um ideal. Para isto, basta dividir este polinômio pela base de Groebner do ideal e observar o resto da divisão. No exemplo a seguir, vamos mostrar como utilizar os conceitos e resultados vistos nesta seção.

Exemplo A.3.4 *Seja k um corpo. Gostaríamos de saber se o polinômio $X^4Y + X^2Y^3 + XY^2 + Y$ pertence ao ideal gerado pelo polinômio $Y^2 + X^3$. Para isto, vamos usar a ordem lexicográfica $X > Y$. Como o ideal é gerado por um único elemento, este elemento é a base de Groebner do ideal. Além disso, temos que $LT(X^4Y + X^2Y^3 + XY^2 + Y) = X^4Y$ e $LT(Y^2 + X^3) = X^3$. Seguindo o procedimento de divisão temos*

$$\begin{array}{l|l} X^4Y + X^2Y^3 + XY^2 + Y & Y^2 + X^3 \\ \cline{2-2} -X^4Y - XY^3 & XY \\ \cline{1-1} X^2Y^3 - XY^3 + XY^2 + Y & \end{array}$$

Como nenhum dos monômios de $X^2Y^3 - XY^3 + XY^2 + Y$ é divisível por X^3, temos que o resto da divisão acima é $X^2Y^3 - XY^3 + XY^2 + Y$. Como o resto é não nulo, o polinômio $X^4Y + X^2Y^3 + XY^2 + Y$ não pertence ao ideal gerado por $Y^2 + X^3$.

Observação A.3.1 *Para aqueles que se interessarem em saber mais sobre os assuntos aqui tratados, recomendamos a leitura de [4], [5], [6] e [7].*

Apêndice B

Conexões entre Superfície de Riemann, Funções Algébricas e Topologia

Um dos resultados mais importantes conectando superfícies de Riemann, funções algébricas e topologia é o Teorema da Uniformização (Koebe-Poincaré) e que será fundamental no contexto em que esta pesquisa se insere. Os capítulos deste trabalho envolvendo a determinação de códigos de Goppa para gêneros $g = 0, 1, 2, 3$ seguem estritamente os fundamentos do referido teorema. Todavia, é importante que se apresentem tais fundamentos, mesmo que informalmente, como uma forma de se estabelecer e de se realizar as devidas conexões de conceitos.

Dessa forma, nas próximas seções apresentamos os elementos essenciais para uma melhor compreensão dos fundamentos utilizados neste trabalho.

B.1 Superfícies de Riemann

Uma superfície de Riemann é um espaço topológico que, localmente, se parece com um conjunto aberto do plano complexo. Vamos, nesta seção, ver os conceitos básicos para a definição precisa de uma superfície de Riemann.

Uma **carta complexa**, ou simplesmente carta, em um espaço topológico X, é um homeomorfismo $\phi : U \to V$, onde U e V são conjuntos abertos em X e $\mathbb{C}$, respectivamente. O conjunto U é chamado de domínio da carta ϕ e dizemos que ϕ é centrada em $p \in U$ se $\phi(p) = 0$. Usaremos a seguinte notação para cartas complexas.

$$\begin{array}{rccc} \phi: & U & \longrightarrow & V \\ & x & \longmapsto & z = \phi(x) \end{array}$$

Sejam $\phi_1 : U_1 \to V_1$ e $\phi_2 : U_2 \to V_2$ duas cartas complexas. Dizemos que ϕ_1 e ϕ_2 são **compatíveis** se $U_1 \cap U_2 = \emptyset$ ou, caso $U_1 \cap U_2 \neq \emptyset$, então $\phi_2 \circ \phi_1^{-1} : \phi_1(U_1 \cap U_2) \to \phi_2(U_1 \cap U_2)$ é uma aplicação holomorfa. A função $T = \phi_2 \circ \phi_1^{-1}$ é chamada função de transição entre as duas cartas.

Um **atlas complexo** $\mathcal{A}$ em X, ou simplesmente atlas, é uma coleção $\mathcal{A} = \{\phi_a : U_a \to V_a\}$ de cartas complexas, compatíveis 2 a 2, e cujos domínios cobrem todo o espaço, isto é, $X = \bigcup_a U_a$. Dois atlas complexos $\mathcal{A}$ e $\mathcal{B}$ são **equivalentes** se toda carta de um é compatível com todas as cartas do outro. Uma **estrutura complexa** em X é um atlas complexo maximal em X ou, uma classe de equivalência de atlas complexos.

Uma **superfície de Riemann** é um espaço topológico X conexo, e_2, Hausdorff com uma estrutura complexa.

Exemplos de superfícies de Riemann são apresentados a seguir.

Exemplo B.1.1 *Seja $X = \mathbb{R}^2$, $U \subsetneqq X$ conjunto aberto qualquer. As aplicações*

$$\begin{array}{rccl} \phi: & U & \longrightarrow & \mathbb{C} \\ & (x,y) & \longmapsto & \phi(x,y) = x + yi \end{array}$$

formam uma estrutura complexa em X. Assim, identificando topologicamente o conjunto $\mathbb{C}$ com $\mathbb{R}^2$, temos que $\mathbb{C}$ é uma superfície de Riemann, chamada plano complexo.

Exemplo B.1.2 *Seja $X = \{(x,y,w) \in \mathbb{R}^3 |\ x^2 + y^2 + w^2 = 1\}$. Vamos considerar a estrutura complexa dada pelas seguinte cartas:*

$$\begin{array}{rccl} \phi_1: & X - \{(0,0,1)\} & \longrightarrow & \mathbb{C} \\ & (x,y,w) & \longmapsto & \phi_1(x,y,w) = \frac{x}{1-w} + i\frac{y}{1-w} \end{array}$$

$$\begin{array}{rccl} \phi_2: & X - \{(0,0,-1)\} & \longrightarrow & \mathbb{C} \\ & (x,y,w) & \longmapsto & \phi_2(x,y,w) = \frac{x}{1+w} - i\frac{y}{1-w} \end{array}$$

Note que, sendo $z = \phi_1(x,y,w)$ temos que $\phi_2(x,y,w) = \frac{1}{z}$. Além disso, temos que $X - \{(0,0,\pm 1)\}$ é levado, tanto por ϕ_1 quanto por ϕ_2 em $\mathbb{C}^*$. O ponto $(0,0,1)$ é denotado por ∞ e esta superfície de Riemann é denotada por $\mathbb{C}_\infty$ e conhecida como Esfera de Riemann.

Podemos construir outras superfícies de Riemann seguindo o seguinte roteiro:

- Tome X um conjunto;
- encontre uma coleção enumerável $\{U_a\}$ de subconjuntos de X que cobrem X;

- para cada a, encontre uma bijeção ϕ_a de U_a em um subconjunto aberto V_a de $\mathbb{C}$;
- mostre que dados a e b, $\phi_a(U_a \cap U_b)$ é um conjunto aberto em V_a. Desta forma, podemos definir uma topologia em X de modo que ϕ_a seja uma carta complexa;
- mostre que as cartas ϕ_a são duas a duas compatíveis;
- mostre que X é conexo e Hausdorff.

Por meio deste roteiro, podemos apresentar agora outros exemplos importantes de superfícies de Riemann.

Exemplo B.1.3 *(Reta Projetiva) Seja $\mathbb{CP}^1$ a reta projetiva definida como*

$$\mathbb{CP}^1 = \{[z : w],\ z, w \in \mathbb{C}, \textit{não nulos simultaneamente}\}$$

Temos que $[z : w] = [\lambda z : \lambda w],\ \forall\ \lambda \in \mathbb{C}^*$.
Em $\mathbb{CP}^1$, considere

$$U_0 = \{[z : w];\ z \neq 0\}, \quad U_1 = \{[z : w];\ w \neq 0\}$$

e as bijeções

$$\begin{array}{rccl} \phi_0 : & U_0 & \longrightarrow & \mathbb{C} \\ & [z : w] & \longmapsto & \phi_0([z : w]) = \frac{w}{z} \end{array}$$

$$\begin{array}{rccl} \phi_1 : & U_1 & \longrightarrow & \mathbb{C} \\ & [z : w] & \longmapsto & \phi_1([z : w]) = \frac{z}{w} \end{array}$$

Com estas estruturas, a reta projetiva $\mathbb{CP}^1$ é uma superfície de Riemann.

Exemplo B.1.4 *(Toro complexo) Sejam w_1, w_2 números complexos linearmente independentes sobre $\mathbb{R}$. Seja $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$ o reticulado gerado por estes dois elementos. O grupo quociente $X = \frac{\mathbb{C}}{L}$ pode ser transformado em um espaço topológico por meio da aplicação projeção*

$$\pi : \mathbb{C} \longrightarrow L.$$

Neste espaço podemos definir cartas complexas transformando-o em uma superfície de Riemann, chamada de Toro Complexo.

Exemplo B.1.5 *(Plano Projetivo) O plano projetivo é definido como*

$$\mathbb{CP}^2 = \{[x : y : z],\ x, y, z \in \mathbb{C}, \textit{não nulos simultaneamente}\}$$

onde $[x : y : z] = [\lambda x : \lambda y : \lambda z],\ \forall\ \lambda \in \mathbb{C}^*$. *Este conjunto também tem uma estrutura de superfície de Riemann, onde os abertos considerados são*

$$U_0 = \{[x : y : z];\ x \neq 0\},\ U_1 = \{[x : y : z];\ y \neq 0\},\ U_2 = \{[x : y : z];\ z \neq 0\}$$

e os homomorfismos considerados são

$$\begin{array}{rccl} \phi_0 : & U_0 & \longrightarrow & \mathbb{C}^2 \\ & [x : y : z] & \longmapsto & \phi_0([x : y : z]) = (\frac{y}{x}, \frac{z}{x}) \\ \\ \phi_1 : & U_1 & \longrightarrow & \mathbb{C}^2 \\ & [x : y : z] & \longmapsto & \phi_1([x : y : z]) = (\frac{x}{y}, \frac{z}{y}) \\ \\ \phi_2 : & U_2 & \longrightarrow & \mathbb{C}^2 \\ & [x : y : z] & \longmapsto & \phi_2([x : y : z]) = (\frac{x}{z}, \frac{y}{z}). \end{array}$$

Exemplo B.1.6 *(Curva Projetiva) Seja* $F(X, Y, Z)$ *um polinômio homogêneo. A curva plana projetiva definida por* F *é o conjunto*

$$X = \{[x : y : z] \in \mathbb{CP}^2 |\ F(x, y, z) = 0\}.$$

Se F *é um polinômio não singular,* X *possui uma estrutura de superfície de Riemann, com abertos da forma* $X_0 = X \cap U_0,\ X_1 = X \cap U_1,\ X_2 = X \cap U_2$.

B.2 Funções e Aplicações

Nesta seção, consideraremos X como sendo uma superfície de Riemann, $p \in X$ e f uma função complexa definida em uma vizinhança W de p.

Dizemos que f é **holomorfa** em p se existe uma carta $\phi : U \to V$ $(p \in U)$ tal que a composição $f \circ \phi^{-1}$ é holomorfa em $\phi(p)$. Dizemos que f é holomorfa em W se for holomorfa em todos os pontos de W.

O lema a seguir nos fornece mais informações sobre funções holomorfas.

Lema B.2.1 ([21]) *Seja* X *uma superfície de Riemann,* $p \in X$, $f : W \to C$ *uma função com* $p \in W$. *Então,*

(i) f *é holomorfa em* p *se, e somente se, para toda carta* $\phi : U \to V$ $(p \in U)$, $f \circ \phi^{-1}$ *é holomorfa em* $\phi(p)$;

(ii) *f é holomorfa em W se, e somente se, existe um conjunto de cartas $\{\phi_i : Ui \to Vi\}$, com $W \subseteq \bigcup Ui$, tais que $f \circ \phi^{-1}$ é holomorfa em $\phi_i(W \cap Ui)$;*

(iii) *se f é holomorfa em p então f é holomorfa em uma vizinhança de p.*

Seja $W \subseteq X$ um conjunto aberto em uma superfície de Riemann X. O conjunto de todas as funções holomorfas em W será denotado por $\mathcal{O}_X(W)$. Portanto,

$$\mathcal{O}_X(W) = \{f : W \to \mathbb{C};\ f \text{ é holomorfa em } W\}.$$

Veremos agora os tipos de singularidades que funções holomorfas em superfícies de Riemann possuem. Estes conceitos são semelhantes aos conceitos de singularidades de funções de uma variável complexa.

Uma **vizinhança pontual** de $p \in X$ é um conjunto da forma $U - \{p\}$, onde U é uma vizinhança de p.

Seja f uma função holomorfa em uma vizinhança pontual de p. Dizemos que f possui uma **singularidade removível** em p se, e somente se, existe uma carta $\phi : U \to V$, $p \in U$ tal que a composição $f \circ \phi^{-1}$ tem singularidade removível em $\phi(p)$. Dizemos que f possui um **pólo** em p se, e somente se, existe uma carta $\phi : U \to V$, $p \in U$ tal que a composição $f \circ \phi^{-1}$ tem um pólo em $\phi(p)$. Dizemos que f possui uma **singularidade essencial** em p se, e somente se, existe uma carta $\phi : U \to V$, $p \in U$ tal que a composição $f \circ \phi^{-1}$ tem singularidade essencial em $\phi(p)$.

O lema a seguir é análogo ao lema B.2.1.

Lema B.2.2 ([21]) *Com as notações vistas, temos que f tem singularidade removível (pólo, essencial) se, e somente se, para toda carta $\phi : U \to V$, com $p \in U$, a composição $f \circ \phi^{-1}$ tem singularidade removível (pólo, essencial) em $\phi(p)$.*

Uma função f em uma superfície de Riemann X é **meromorfa** em um ponto $p \in X$ se f é uma função holomorfa e possui singularidade removível em p ou se f possui um pólo em p. Dizemos que f é meromorfa em um aberto W se for meromorfa em todos os pontos de W. O conjunto de todas as funções meromorfas em W será denotado por $\mathcal{M}_X(W)$. Portanto,

$$\mathcal{M}_X(W) = \{f : W \to \mathbb{C}; f \text{ meromorfa em } W\}.$$

Seja f uma função meromorfa em um ponto p de uma superfície de Riemann X. Sendo z uma coordenada local em X próximo a p, isto é, $z = \phi(x)$ com ϕ carta local e x próximo a p,

temos que $f \circ \phi^{-1}$ pode ser escrita como uma série de potência em torno de $z_0 = \phi(p)$. Desta forma,

$$f(\phi^{-1}(z)) = \sum_n c_n (z - z_0)^n.$$

A **ordem** de f em p, denotada por $ord_p(f)$, é o menor expoente com coeficiente não nulo, isto é, $ord_p(f) = min\{n;\ c_n \neq 0\}$. Esta definição de ordem é independente da escolha das coordenadas locais.

Vamos, agora, voltar a alguns exemplos da seção B.1 e caracterizar como são as funções meromorfas das superfícies de Riemann apresentadas.

- **Esfera de Riemann**: As funções meromorfas na Esfera de Riemann são da forma

$$f(z) = \frac{p(z)}{q(z)},$$

  com $p(z)$ e $q(z)$ polinômios.

- **A Reta Projetiva** $\mathbb{CP}^1$: As funções meromorfas na reta projetiva são da forma

$$f(z, w) = \frac{p(z, w)}{q(z, w)},$$

  onde $p(z, w)$ e $q(z, w)$ são polinômios homogêneos de mesmo grau.

- **Curva Plana Projetiva**: Se X for uma curva projetiva definida por um polinômio homogêneo, irredutível e não singular $F(X, Y, Z)$, então as funções meromorfas são da forma

$$F(X, Y, Z) = \frac{G(X, Y, Z)}{H(X, Y, Z)},$$

  onde G e H são polinômios homogêneos de mesmo grau e F não é um fator de H.

- **Toro complexo**: Seja $\tau \in \mathbb{C}$, com $Im(\tau) > 0$. Podemos definir uma função analítica em $\mathbb{C}$ dada por

$$\theta(z) = \sum_{n=-\infty}^{\infty} e^{\pi i[n^2\tau + 2nz]}.$$

  Definimos também

$$\theta^{(x)}(z) = \theta\left(z - \left(\frac{1}{2}\right) - \left(\frac{\tau}{2}\right) - x\right).$$

  Desta forma, dado um número natural d e dois conjuntos de números complexos $\{x_i\}, \{y_i\}$, com d elementos, tais que $\sum x_i - \sum y_i$ seja inteiro, então as funções meromorfas do toro

complexo são da forma

$$R(z) = \frac{\prod_i \theta^{(x_i)}(z)}{\prod_j \theta^{(y_j)}(z)}.$$

B.3 Divisores e Funções Meromorfas

Seja X uma superfície de Riemann. Denotaremos por $\mathbb{Z}^X$ o grupo aditivo de todas as funções de X em $\mathbb{Z}$. Dada uma função $D : X \to \mathbb{Z}$, o **suporte** de D é o conjunto dos pontos $p \in X$ tais que $D(p) \neq 0$. Um **divisor** em X é uma função $D : X \to \mathbb{Z}$ cujo suporte é um subconjunto discreto de X. O grupo dos divisores é denotado por $Div(X)$. Se X for uma superfície compacta e D um divisor, então seu suporte é finito. Assim, o grupo $Div(X)$ coincide com o grupo abeliano livre dos pontos de X. Desta forma, representaremos um divisor em X da seguinte maneira:

$$D = \sum_{p \in X} D(p).p, \ D(p) \neq 0 \text{ para um número finito de pontos.}$$

O **grau** de um divisor D é definido como

$$gr(D) = \sum_{p \in X} D(p).$$

Seja X uma superfície de Riemann e f uma função meromorfa em X não identicamente nula. O **divisor de** f, denotado por $div(f)$, é o divisor definido por

$$div(f) = \sum_{p \in X} ord_p(f).p.$$

Qualquer divisor da forma $div(f)$, f função meromorfa, é chamado **divisor principal** em X. O conjunto de todos os divisores principais é denotado por $PDiv(X)$.

Lema B.3.1 ([21]) *Seja X uma superfície compacta e f uma função meromorfa em X. Então,*

$$gr(div(f)) = 0.$$

Sendo f uma função meromorfa em X, definimos o **divisor de zeros** de f como

$$div_0(f) = \sum_{p \in X, \ ord_p(f) > 0} ord_p(f).p,$$

e o **divisor de pólos** de f como

$$div_\infty(f) = \sum_{p\in X,\ ord_p(f)<0} ord_p(f).p.$$

Desta forma, temos que $div(f) = div_0(f) - div_\infty(f)$.

Seja D uma divisor em uma superfície de Riemann. Dizemos que $D \geq 0$ se $D(p) \geq 0,\ \forall\ p$. Escrevemos $D > 0$ se $D \geq 0$ e $D \neq 0$. Também podemos escrever $D_1 \geq D_2$ se $D_1 - D_2 \geq 0$, o mesmo valendo para $D_1 > D_2$. Com isto, o conjunto $Div(X)$ é um conjunto parcialmente ordenado. Neste conjunto podemos também definir uma relação de equivalência. Para isto, dizemos que dois divisores, D_1 e D_2, são linearmente equivalentes, e usamos a notação $D_1 \sim D_2$, se $D_1 - D_2 \in PDiv(X)$ (conjunto dos divisores principais).

O resultado a seguir nos fornece informações sobre divisores em superfícies de Riemann.

Lema B.3.2 ([21]) *Seja X uma superfície de Riemann.*

1. *$D \sim 0$ se, e somente se D é um divisor principal;*
2. *se X é compacta então $D_1 \sim D_2 \Leftrightarrow gr(D_1) = gr(D_2)$;*
3. *se f é uma função meromorfa não identicamente nula então $div_0(f) \sim div_\infty(f)$. Se X é compacta, então $gr(div_0(f)) = gr(div_\infty(f))$.*

B.4 Espaço de Funções Associados a um Divisor

Nesta seção, definiremos e apresentaremos alguns resultados relacionados aos espaços $\mathcal{L}(D)$, espaços associados a divisores em superfícies de Riemann. Para isto, vamos definir $ord_p(f) = \infty$ quando f for uma função meromorfa identicamente nula em uma vizinhança do ponto p. Também consideraremos $n < \infty$ para qualquer número inteiro n.

Seja D um divisor em uma superfície de Riemann X. O **espaço das funções meromorfas** com pólos limitados por D, denotado por $\mathcal{L}(D)$, é o seguinte conjunto

$$\mathcal{L}(D) = \{f \in \mathcal{M}_X;\ div(f) \geq -D\}.$$

O resultado a seguir nos fornece informações importantes sobre estes espaços.

Lema B.4.1 ([21]) *Seja X uma superfície de Riemann e D um divisor em X.*
(i) $\mathcal{L}(D)$ é um espaço vetorial;
(ii) $D_1 \leq D_2 \Rightarrow \mathcal{L}(D_1) \subseteq \mathcal{L}(D_2)$;

(iii) $\mathcal{L}(0) = \{$*funções holomorfas*$\}$;
(iv) Se X *é compacta, então* $\mathcal{L}(0) = \{$*funções constantes*$\} \simeq \mathbb{C}$. *Além disso, se* $gr(D) < 0$ *então* $\mathcal{L}(D) = \{0\}$;
(v) Se X *é compacta então* $\mathcal{L}(D)$ *é espaço vetorial complexo de dimensão finita. Mais ainda, se* $D = P - N$, *onde* P *e* N *são divisores não negativos com suportes disjuntos, então* $dim(\mathcal{L}(D)) \leq 1 + gr(P)$.

Os resultados a seguir trazem informações sobre os espaços $\mathcal{L}(D)$ para duas superfícies especiais.

Teorema B.4.1 ([21]) *Seja* D *um divisor na esfera de Riemann. Então*

$$dim(\mathcal{L}(D)) = \begin{cases} 0 \text{ se } gr(D) < 0; \\ 1 + gr(D), \text{ se } gr(D) \geq 0. \end{cases}$$

Teorema B.4.2 ([21]) *Seja* D *um divisor no toro complexo.*
(i) Se $gr(D) < 0$ *então* $\mathcal{L}(D) = \{0\}$;
(ii) Se $gr(D) = 0$ *e* $D \sim 0$ *então* $dim(\mathcal{L}(D)) = 1$;
(iii) Se $gr(D) = 0$ *e* $D \nsim 0$ *então* $\mathcal{L}(D) = \{0\}$;
(iv) Se $gr(D) > 0$ *então* $dim(\mathcal{L}(D)) = gr(D)$.

B.5 Curvas Algébricas

Nesta seção, veremos a definição geral de curvas algébricas e como relacionar as superfícies de Riemann estudadas na seção B.2.

Seja X uma curva projetiva suave definida por um polinômio $F(X, Y, Z)$ homogêneo de grau d (ver exemplo B.1.6). O **grau** da curva projetiva é o grau do polinômio que a define. O **gênero** da curva suave X, denotado por $g(X)$, é definido como

$$g(X) = \frac{(d-1)(d-2)}{2},$$

onde d é o grau da curva.

Seja X uma superfície de Riemann compacta e S um conjunto de funções meromorfas em X. Dizemos que S **separa pontos** de X se, para quaisquer dois pontos distintos p e q de X, existe uma função meromorfa f em S tal que $f(p) \neq f(q)$. Dizemos que S **separa tangentes** de X se, para qualquer ponto p em X, existe uma função meromorfa f em S que tem multiplicidade um em p. Uma superfície de Riemann compacta X é uma **curva algébrica** se o corpo das funções meromorfas globais $\mathcal{M}(X)$ separa pontos e tangentes de X.

Exemplo
As seguintes superfícies são curvas algébricas:

- A Esfera de Riemann $\mathbb{C}_\infty$;
- Qualquer toro complexo $\mathbb{C}/L$;
- Curvas projetivas suaves planas.

Um dos resultados mais importantes sobre curvas algébricas é o teorema que segue.

Teorema B.5.1 (Teorema de Riemann-Roch,[21]) *Seja X uma curva algébrica de gênero g. Então, para qualquer divisor D e para qualquer divisor canônico K, temos que*

$$dim(\mathcal{L}(D)) - dim(\mathcal{L}(K - D)) = gr(D) + 1 - g.$$

Além disso, se D é um divisor de grau no mínimo $2g - 1$, então

$$dim(\mathcal{L}(D)) = gr(D) + 1 - g.$$

Como consequência do Teorema de Riemann-Roch, temos o seguinte resultado.

Teorema B.5.2 ([21]) *Seja X uma curva algébrica de gênero g,*

(i) Se $g = 0$, então X é isomorfa à esfera de Riemann $\mathbb{C}_\infty$;

(ii) Se $g = 1$, então X é isomorfa a um toro complexo $\mathbb{C}/L$;

(iii) Se $g \geq 2$, então X é isomorfa a um g-toro complexo.

B.6 Conexões entre Superfície de Riemann, Funções Algébricas e Topologia

Seja $\mathcal{X}$ uma curva projetiva definida pelo anulamento de um polinômio irredutível $P(x, y)$. Os pontos desta curva são triplas $(x, y, z) \in \mathbb{C}^3 - 0$ com identificações projetivas, fazendo sentido, portanto, a notação $\mathbf{x} = \frac{x}{z}$, $\mathbf{y} = \frac{y}{z}$. Elas são funções de carater racional em $\mathcal{X}$ e os zeros de P expressam uma relação entre elas, especificando $\mathbf{y}$ como função multivalorada de $\mathbf{x}$ e vice-versa. Essas funções podem ser alçadas para o recobrimento universal $\mathcal{K}$ de $\mathcal{X}$ onde elas se identificam como funções $\mathbf{x}$, $\mathbf{y}$ de caráter racional, invariante sob a ação do grupo de recobrimento. Deste modo, $\mathcal{X}$ é uniformizada por $\mathcal{K}$ em que a totalidade dos pontos de $\mathcal{X}$ é

evidenciada por meio de funções assumindo um único valor em $\mathcal{K}$, onde $\mathcal{K}$ é a esfera, plano ou o semi-plano superior.

B.6.1 Caso $g = 0$

Como, neste caso, a curva $\mathcal{X}$ não possui alças, então $\mathcal{X}$ é a reta projetiva $\mathbb{P}^1$ e, consequentemente, o seu próprio recobrimento universal. Assim, $\mathbf{x}$ e $\mathbf{y}$ são vistos como funções racionais em relação ao parâmetro w de $\mathbb{P}^1$ e a aplicação $w \mapsto (\mathbf{x}, \mathbf{y})$ é uma equivalência conforme entre $\mathbb{P}^1$ e $\mathcal{X}$. O exemplo mais simples e não trivial é o circulo projetivo $\mathcal{X} : \mathbf{x}^2 + \mathbf{y}^2 = 1$, com sua uniformização dada por

$$\mathbf{x} = \frac{1}{2}(w + w^{-1}), \quad \mathbf{y} = \frac{1}{2\sqrt{-1}}(w - w^{-1}).$$

Curvas Racionais

Se $\mathcal{X}$ é uma curva racional, no sentido de que existe uma aplicação não constante de caráter racional de $\mathbb{P}^1$ em $\mathcal{X}$, então $\mathcal{X}$ já é de gênero 0 e portanto a reta projetiva. A argumentação aqui é a seguinte: como $\mathbb{P}^1$ é simplesmente conexo, então uma aplicação de caráter racional de $\mathbb{P}^1$ em $\mathcal{X}$ pode ser levantada para uma aplicação de $\mathbb{P}^1$ em $\mathcal{K}$. Porém, isto é impossível se $\mathcal{K}$ não for a reta projetiva.

B.6.2 Caso $g = 1$

Se $\mathcal{X}$ é o toro complexo (gênero $g = 1$), sabemos que $\mathcal{X}$ não pode ser uniformizada por funções racionais, já que seu recobrimento universal não é a reta projetiva. Neste caso, $\mathcal{K} = \mathbb{C}$, $\mathcal{X}$ é o quociente de $\mathbb{C}$ pelo reticulado $\mathbb{L}$ e $\mathbf{x} = \dfrac{x}{z}$ e $\mathbf{y} = \dfrac{y}{z}$ podem ser levantadas à funções de caráter racional em $\mathbb{C}$ tendo todo número complexo $w \in \mathbb{L}$ como período. Estas funções uniformizam $\mathcal{X}$, são invariantes sob a ação do grupo das translações e não são funções racionais. São conhecidas como funções elípticas.

B.6.3 Caso $g \geq 2$

No caso de a esfera conter mais de uma alça, seu recobrimento universal $\mathcal{K}$ é o semi plano superior. Nestas condições, as funções $\mathbf{x}$ e $\mathbf{y}$, quando levantadas para $\mathcal{K}$, são invariantes sob o grupo $PSL(2, \mathbb{R})$. Estas funções são chamadas funções automorfas.

B.6.4 Exemplos

Como exemplos da interconexão de superfícies de Riemann, funções algébricas e topologia, iremos considerar os casos em que $g = 0, 1$. É sabido que todo domínio no plano complexo é uma superfície de Riemann. A esfera de Riemann, denotada por $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, entendida como uma compactificação do plano complexo, é uma superfície de Riemann, com uma estrutura complexa definida por meio de duas vizinhanças coordenadas $(\widehat{\mathbb{C}}, z)$, $(\widehat{\mathbb{C}} - \{0\}, \frac{1}{z})$. Considere a função algébrica $w = \sqrt{z}$. Esta é a superfície de Riemann na qual a função inversa da função analítica $z = f(w) = w^2$ assume valor único. Uma maneira de se ver isto é a seguinte: a função $z = w^2$ mapeia o semi-plano superior $H = \{w \in \mathbb{C};\ Im(w) > 0\}$ e o semi-plano inferior $H^* = \{w \in \mathbb{C};\ Im(w) < 0\}$ biholomorficamente no domínio $D = \mathbb{C} - L$, onde $L = \{x \in \mathbb{R};\ x \geq 0\}$ é um corte no plano z. Considere duas cópias D_1 e D_2 de D e cole, de forma cruzada, os cortes L_1 e L_2. Deste modo, obtemos uma superfície de recobrimento R, composta por duas folhas sobre a z-esfera. Como a função $f(w) = w^2$ induz um homeomorfismo sobrejetor F da w-esfera em R, podemos definir a estrutura complexa de R a partir da estrutura complexa da w-esfera, de modo que $F : \widehat{\mathbb{C}} \to R$ seja um mapeamento biholomorfo. Desta forma, R é a superfície de Riemann da função $w = \sqrt{z}$. Note que esta superfície de Riemann pode ser vista como a curva algébrica $w^2 = z$.

Com relação às curvas elípticas ($g = 1$), consideremos R a curva algébrica definida por

$$w^2 = z(z-1)(z-\lambda),\ \lambda \in \mathbb{C},\ \lambda \neq 0, 1. \tag{B.1}$$

R consiste de todos os pontos da forma $(z, w) \in \mathbb{C} \times \mathbb{C}$ satisfazendo (B.1), além do ponto (∞, ∞). Define-se a estrutura complexa de R por meio da estrutura complexa da z-esfera, de modo que a projeção $\pi : R \to \widehat{\mathbb{C}},\ \pi(z, w) = z$ seja analítica. R é a superfície de recobrimento ramificada de duas folhas sobre a z-esfera com pontos de ramificação $0,\ 1,\ \lambda,\ \infty$. O mapeamento $f : R \to \widehat{\mathbb{C}},\ f(z, w) = w$ é analítico, sendo dado por $w = \sqrt{z(z-1)(z-\lambda)}$ e R é a superfície de Riemann na qual tal função assume valores únicos.

Topológicamente, a superfície de Riemann R, definida por (B.1), é obtida da seguinte forma: considere duas cópias da esfera de Riemann S_1 e S_2, com cortes entre 0 e 1 e λ e ∞. Coloque-as frente a frente e una-as ao longo dos cortes. A superfície resultante é homeomorfa à superfície de Riemann R. Tal superfície é um toro.