Universidade Estadual de Campinas - UNICAMP
Faculdade de Engenharia Elétrica e de Computação - FEEC

Tese de Doutorado

Área de Concentração:
Eletrônica e Comunicações

Caracterização Geométrica do Processo de Decodificação da Classe dos Códigos Alternantes Cíclicos Através de Polinômios Absolutamente Irredutíveis

Givaldo Oliveira dos Santos

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

CAMPINAS - SP
ABRIL DE 2003

Este exemplar corresponde a redação final da tese defendida por Givaldo Oliveira dos Santos e aprovada pela Comissão julgada em 28 / 04 / 2003

Orientador

Universidade Estadual de Campinas - UNICAMP
Faculdade de Engenharia Elétrica e de Computação - FEEC
Departamento de Telemática - DT

Caracterização Geométrica do Processo de Decodificação da Classe dos Códigos Alternantes Cíclicos Através de Polinômios Absolutamente Irredutíveis

Givaldo Oliveira dos Santos

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

Banca Examinadora:
Prof. Dr. Fernando E. Torres Orihuela - IMECC-UNICAMP
Prof. Dr. Orlando Stanley Juriaans - IME-USP
Prof. Dr. Trajano Pires da Nobrega Neto - D.Mat-IBILCE-UNESP
Prof. Dr. João de Deus Lima - D.Mat-FANAT-UERN-RN
Prof. Dr. Antônio Aparecido de Andrade - D.Mat-IBILCE-UNESP

Tese de Doutorado apresentada à 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**.

CAMPINAS - SP
ABRIL DE 2003

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

Sa59c

Santos, Givaldo Oliveira dos
Caracterização geométrica do processo de decodificação da classe dos códigos alternantes cíclicos através de polinômios absolutamente irredutíveis / Givaldo Oliveira dos Santos. --Campinas, SP: [s.n.], 2003.

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

1. Curvas algébricas. 2. Corpos finitos (Álgebra). 3. Códigos de controle de erros (Teoria da informação). 4. Teoria da codificação. 5. Riemann, Superficies de. I. Palazzo Jr., Reginaldo. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Com muito amor e carinho a minha esposa
Auriene,
e a minha linda e maravilhosa filha
Ana Luiza,
que, com sua beleza, graça e inocência, deu um novo sentido à minha vida.

Com muito amor e carinho aos meus queridos pais
José Muniz dos Santos e *Helena Oliveira dos Santos,*
por tudo que fizeram e fazem por mim. Sem eles nada aqui seria realidade.
Aos meus queridos irmãos:
Gilson, Ednaldo, Edvaldo, Eliane, Josinaldo e Luciana.

Agradecimentos

A Deus e a Nossa Senhora Aparecida pela imensa generosidade demonstrada durante todas as etapas difíceis desta longa jornada e de toda a minha vida.

Em especial, ao Prof. Dr. Reginaldo Palazzo Jr., meu orientador de tese e amigo, pelo constante apoio ao trabalho realizado. O seu estímulo e atenção foram decisivos para que eu seguisse em frente na conquista de cada pequena etapa; a sua orientação direcionada aos objetivos permitiu que eu não me afastasse do tema central, reconduzindo-me de volta ao caminho seguro; além disso, pelas valiosas discussões, pela rigorosa correção nos textos e cálculos, como também por sua genialidade, amizade, paciência e atenção.

Em especial, ao Prof. Dr. João de Deus Lima, meu grande amigo irmão, pelo constante apoio durante o doutorado. Seu estímulo e atenção foram fundamentais para chegar à conquista de cada etapa; além disso, pelas valiosas discussões, ajuda na correção de textos mais específicos, como também pela sua paciência e atenção.

Em especial, ao Prof. Dr. Trajano Pires, pelo constante apoio durante o doutorado. Seu incentivo para seguir sempre em frente na conquista de cada etapa e também pelas valiosas discussões, ajuda na discussão dos textos, e ainda pela sua amizade, paciência e atenção.

Aos professores da banca examinadora: Prof. Dr. João de Deus Lima (D. Mat.-FANAT-UERN - Mossoró - RN), Prof. Dr. Fernando Torres (IMEC - UNICAMP), Prof. Dr. Trajano Pires (D. Mat-IBILCE-UNESP - São J. R. Preto), Prof. Dr. Antônio Andrade (D. Mat-IBILCE-UNESP - São J. R. Preto) e o Prof. Dr. Orlando Stanley Juriaans (IME-USP).

Às famílias Amauri & Regina e Vânio & Elizabete, por tudo que fizeram por mim, especialmente pela convivência e amizade que tiveram início na graduação.

Aos casais Cristiane & Marcel e João de Deus & Zuleica, pela grande amizade, pela força e carinho a mim dispensados, tanto no mestrado quanto agora no doutorado.

Aos casais Gilson & Carmem, Edvaldo & Joseane e Josemilton & Noêmia, pela grande amizade, pela força e carinho a mim dispensados nesta caminhada.

Às famílias Antônio & Ana, Sr. Antônio & Da. Vilma e Emerson & Joseane, pela amizade e apoio durante esta caminhada na cidade de Campinas.

Ao amigo Rodrigo Gusmão, tanto pela amizade quanto pelo apoio às questões computacionais.

Ao amigo Ercílio Carvalho da Silva, tanto pela amizade quanto pelas valiosas discussões e correções dos textos matemáticos.

Ao casal Juliene & Edson, tanto pela amizade quanto pelas correções dos textos relacionados a este trabalho.

Aos amigos que contribuíram de diversas formas: Marinaldo, Edson Donizete, Raulison Alves Resende, Diogo Robles, Alessandro, José Barros, Tatiana, Vanessa, Mário, Luciano, Mércio e Karine.

Aos amigos da UNED-MD que contribuíram de diversas formas: Feliciano, Carmen, Lemberg, Nádia, Adriana, Josemilton, Sandra, Marilucia, Professor Josiel, Valdomiro e demais amigos, pela convivência amigável e apoio neste empreendimento.

Aos professores e funcionários da Faculdade de Engenharia Elétrica e de Computação, especialmente os Professores do Departamento de Telemática e de Comunicação: Prof. Dr. Lee Luan Ling, Prof. Dr. Max Henrique M. Costa, Prof. Dr. Jaime Portugheis e Prof. Dr. Walter C. Borelli.

À Fundação de Amparo à Pesquisa do Estado de Alagoas - FAPEAL, pelo apoio financeiro durante três anos de doutorado. Processo No. 99/0315-0.

Ao Centro Federal de Educação Tecnológica de Alagoas (CEFET-AL) e a Unidade de Ensino Descentralizada de Marechal Deodoro (UNED-MD), pelo respaldo financeiro e apoio irrestrito durante todo o período de doutorado.

Resumo

Este trabalho tem como objetivo estabelecer uma relação entre curvas algébricas e o processo de decodificação da classe de códigos alternantes, conhecidos como subcódigos dos códigos de Reed-Solomon generalizado. O procedimento utilizado para alcançar tal objetivo consiste dos seguintes passos: 1) Propor uma construção de polinômios absolutamente irredutíveis que gerem curvas algébricas sobre corpos finitos $GF(q)$ (isto é, irredutível sobre o fecho algébrico de $GF(q)$, denotado por $\overline{GF(q)}$) com possíveis curvas com número máximo de pontos racionais; 2) Incorporar ao algoritmo de Berlekamp-Massey e ao algoritmo de Peterson-Gorenstein-Zierler uma estrutura geométrica de curvas algébricas na caracterização do processo de localização dos erros através da construção de polinômios absolutamente irredutíveis, que se dará por meio dos pontos racionais da curva associada a esta construção. Estabelecemos, assim, uma estrutura geométrica ao decodificador universal para os códigos alternantes a partir desses conceitos e propriedades.

Abstract

The aim of this research is to establish a relationship between algebraic curves and the decoding process of the class of Alternant codes, known as subcodes of the generalized Reed-Solomon codes. The procedure we used to achieve such a goal consists of the following steps: 1) to propose a construction of absolutely irreducible polynomials which generate algebraic curves over finite fields $GF(q)$ (that is, irreducible over the algebraic closure of $GF(q)$, denoted by $\overline{GF(q)}$) with maximal rational whenever possible; 2) to introduce to the Berlekamp-Massey and the Peterson-Gorenstein-Zierler algorithms a geometric structure of algebraic curves in the characterization of the error locator process by use of the construction of absolutely irreducible polynomials. This characterization is realized by means of the rational points associated with such curves. Therefore, we have established a geometric structure to the decoding process of the alternant codes from these concepts and properties.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Símbolos

Simbologia	Significado do Símbolo	Número da Página
T_m	aplicação traço	10
$\theta_{P_i}(\mathcal{X})$	anel local do ponto P_i	92
v_{P_i}	aplicação valorização discreta	92
Φ :	aplicação linear de $L(G)$ em $(GF(q))^n$	94
ϕ :	aplicação de $\mathbb{K}^3 - 0$ no plano projetivo $\mathbb{P}^2$	59
$\varphi : \mathrm{X} \rightarrow \mathrm{Y}$	aplicação diferenciável do X em Y	97
$\mathrm{f} : \mathrm{X} \rightarrow \mathrm{Y}$	bijeção contínua	97
$A(\alpha, y)$	código alternante de α e y	11
MDS	código com máxima distância de separação	8
$[n, n - rm]$	código de comprimento n e $n - rm$ símbolos de informação	10
$GBCH(P, G)$	código BCH generalizado dos polinômios P e G	34
$[n, k]$	código de comprimento n e k simbolos de informação	8
$[n, k, d]$	código de comprimento n, k simbolos de informação e distância d	10
$\mathfrak{C}(D, G)$	código linear associado aos divisores D e G	94
$GRS_k(\alpha, v)$	código de Reed-Solomon generalizado	8
$GRS_{n-k}(\alpha, v)$	código dual do código de Reed-Solomon generalizado	8
$\mathfrak{C}$	código sobre $GF(q)$	9
$\mathfrak{C}^*$	código sobre $GF(q^m)$	10
$T_m(\mathfrak{C}^*)$	código sobre $GF(q)$	10
$\Gamma(L, g)$	código de Goppa	17
n	comprimento de um código	8
$\mathbb{X}$	conjunto algébrico afim	50
$\mathfrak{X}$	conjunto dos pontos $(x : y : z) \in \mathbb{P}^2$ tal que $F(x, y, z) = 0$	59
$\mathcal{X}_f(\mathbb{K})$	conjunto das soluções da equação $f(x, y) = 0$	51
$\mathbb{C}$	conjunto dos números complexos	41
$\mathbb{Q}$	conjunto dos números racionais	41
$\mathbb{R}$	conjunto dos números reais	41

LISTA DE SÍMBOLOS

Capítulo 1

Introdução

Antes de procedermos à descrição do problema a ser analisado neste trabalho, apresentaremos um breve histórico sobre codificação e decodificação de códigos lineares.

Os códigos binários descobertos por R. C. Bose e D. K. Chaudhuri (1960) e independentemente por A. Hocquenghem (1959) foram chamados de códigos BCH e representam uma importante generalização dos códigos de Hamming, permitindo múltipla correção de erros. A generalização dos códigos BCH binários para códigos sobre $GF(q)$ foi feita por Gorenstein e Zierler, em 1961. Entre os códigos BCH não-binários, a subclasse mais importante é formada pelos códigos de Reed-Solomon (RS), os quais foram introduzidos por Reed e Solomon em 1960, independentemente dos trabalhos de Hocquenghem, Bose e Chaudhuri. Em 1967, J. N. Srivastava propôs uma nova classe de códigos lineares, chamada códigos de Srivastava, [5]. Em 1970, V. D. Goppa introduziu uma nova classe de códigos corretores de erros que incluem, como subclasses desses códigos, os códigos BCH e os códigos de Srivastava, [21]. Em 1972, H. J. Helgert apresentou uma generalização dos códigos BCH e dos códigos de Srivastava, [28]. Para uma discussão mais detalhada desses códigos, indicamos os livros de Belerkamp [5] e de MacWilliams-Sloane [57].

A classe dos códigos alternantes foi definida e estudada por Helgert em uma série de trabalhos [27]-[31]. Os resultados mais importantes foram compilados por Delsarte em [11]. Através desses resultados, essa classe de códigos é conhecida pelo nome de códigos de Reed-Solomon generalizado. O nome código alternante é baseado no fato de que a matriz ou determinante da forma

$$\begin{bmatrix} f_0(x_0) & f_1(x_0) & \cdots & f_{n-1}(x_0) \\ \vdots & \vdots & & \vdots \\ f_0(x_{r-1}) & f_1(x_{r-1}) & \cdots & f_{n-1}(x_{r-1}) \end{bmatrix}$$

é chamado de alternante [41]. Alguns dos códigos mais importantes usados na prática, como os códigos BCH e os códigos clássicos de Goppa, podem ser representados como subcódigos de subcorpos dos códigos de Reed-Solomon generalizado de uma maneira natural, portanto, são códigos alternantes.

Os códigos alternantes formam uma grande e poderosa família de códigos que podem ser obtidos por uma simples modificação na matriz verificação de paridade do código BCH, [57]. Essa classe consiste da união de vários códigos conhecidos, entre eles, estão os códigos

BCH, Reed-Solomon, códigos clássicos de Goppa, Srivastava, Srivastava generalizado e BCH generalizado. Por ser uma classe muito extensa de códigos, muito resta ainda a ser explorado sobre eles, veja [57].

Um dos fatos mais importantes na Teoria de Códigos Corretores de Erros nos últimos anos foi a introdução de métodos baseados em curvas algébrico-geométricas para a construção de códigos lineares. Esses códigos, denominados **algébrico-geométricos (AG)**, foram introduzidos por Goppa, [23]-[25]. Em 1982, Tsfasman, Vlădut e Zink [62] obtiveram um resultado importante quanto à existência de uma sucessão de códigos AG que excediam o limitante de Gilbert-Varshamov, impulsionando um importante desenvolvimento na teoria de códigos para correção de erros. Os códigos de Reed-Solomon são, então, um caso particular dos códigos AG quando a curva algébrica adotada é apenas uma reta, de forma que os códigos AG podem apresentar comprimento muito maior que os códigos de Reed-Solomon. Desde então, vários trabalhos foram publicados sobre os códigos AG. Estes códigos estão baseados na Teoria de Curvas Algébrico-Geométricas, [39]. Em [34], Justesen *et al* propuseram uma descrição dos códigos AG considerando somente monômios. Seguindo essa descrição de códigos AG, Feng e Rao, [15], construiram códigos AG, através de uma aproximação simples, utilizando três tipos de curvas planas afins irredutíveis sobre $GF(q)$.

O objetivo era construir uma classe de códigos lineares, que por sua vez são bem parecidos com os códigos AG atuais, porém, a construção não está diretamente baseada na Teoria de Curvas Algébrico-Geométricas. Dessa aproximação simples, resulta a construção de códigos AG em uma classe muito grande de curvas planas afins irredutíveis, sem usar a Teoria de Curvas Algébrico-Geométricas diretamente. Em alguns casos, a distância mínima projetada, obtida por esta aproximação, é mais precisa que a obtida usando o Teorema de Riemann-Roch.

No começo dos anos 80, Ihara [32], Tsfasman, Vlădut e Zink [61][62], provaram a existência de curvas sobre corpos finitos com muitos pontos racionais, possibilitando a construção de bons códigos quando n tende a infinito. Portanto, os melhores códigos são construídos através de curvas com muitos pontos racionais, uma vez que o comprimento das palavras-código está diretamente relacionado à quantidade de pontos racionais.

O problema de decodificação, para um dado código C, consiste em encontrar uma palavra-código em C tal que a distância para uma dada palavra recebida y seja mínima. Uma estratégia para realizar esta tarefa consiste de dois passos: inicialmente, determinar o suporte do vetor erro e, em seguida, determinar os valores dos erros correspondentes, isto é, as magnitudes dos erros. Decodificar pela localização de erro é o princípio básico da maioria dos algoritmos de decodificação para códigos lineares.

A idéia de expressar o passo fundamental na decodificação para obter a recorrência mais curta que produzirá uma determinada sequência é atribuída a Berlekamp e a Massey (BM) [5], isto é, utilizar relações de recursão lineares (registradores de deslocamentos) em uma variável, relações estas válidas para as síndromes da palavra recebida, para determinar um polinômio localizador de erros ocorridos. Helgert em [31], apresentou a equação fundamental para decodificar os códigos alternantes. O uso do algoritmo de Euclides para resolver a equação fundamental deve-se a Sugiyama *et al.,* [60]. Um algoritmo de decodificação diferente, também baseado no algoritmo de Euclides, foi determinado por Mandelbaum [37]. Ainda outro algoritmo de decodificação foi proposto por

Peterson-Gorenstein-Zierler, [7]. A função básica desse algoritmo é determinar, usando as propriedades de sistemas lineares, as funções simétricas elementares.

Um código BCH primitivo binário de comprimento n e taxa R pode ser decodificado até sua distância projetada em $O(n \log n)$ operações aritméticas. Esses resultados são melhores que aqueles obtidos com o algoritmo de Euclides, mas infelizmente só serão válidos para valores excessivamente grandes de n. Um algoritmo computacionalmente eficiente para decodificar a classe de códigos alternantes para propósitos práticos é o algoritmo de decodificação de Berlekamp-Massey, o qual é provavelmente o mais rápido.

Embora nosso objetivo, neste trabalho, não seja a decodificação de códigos algébrico-geométricos, pensamos ser válidas algumas citações para maiores esclarecimentos. Um algoritmo computacionalmente eficiente para decodificar esses códigos foi inicialmente descrito por Justesen *et al.*, em [34], e consistia numa generalização do algoritmo de Arimoto e Peterson-Gorenstein-Zierler para códigos de Reed-Solomon. Uma abordagem baseada em um tipo do algoritmo de Berlekamp-Massey bidimensional foi introduzida por Sakata em [48]. Sakata *et al.*, em [49], estenderam o algoritmo para permitir uma decodificação eficiente até a metade da distância mínima projetada. O algoritmo em [49] trata em detalhes de códigos em curvas hermitianas e necessita de uma certa complexidade, número de multiplicações no corpo de interesse, o qual é limitado superiormente pelo termo $An^{7/3}$ para uma constante A suficientemente grande. Aqui n denota o comprimento do código de uma curva hermitiana e a constante A é independente do comprimento do código. Além de [48] e [49], existe uma vasta literatura sobre algoritmos computacionalmente eficientes para decodificar códigos AG, veja [33] e [35].

Tendo como base o algoritmo de Berlekamp-Massey Köter, [36], usando de paralelismo, propos um algoritmo de decodificação rápida para determinar a função localizadora de erros para a classe de códigos algébrico-geométricos $C_\Omega(D, mP_\infty)$ de um ponto. Esse algoritmo é descrito por um conjunto de equações recursivas e funciona para ambas as decodificações, isto é, decodificar somente erro e decodificar erro-apagamento. O resultado principal desse trabalho é um algoritmo de localização de erro de implementação relativamente simples. Tal implementação paralela determina o localizador de erro para um código algébrico-geométrico que usa as mesmas exigências de execução que o algoritmo básico de Berlekamp-Massey em uma dimensão aplicado à decodificação de códigos de Reed-Solomon. Além disso, o algoritmo pode ser implementado eficazmente e pode requerer um tempo de execução que é essencialmente igual ao tempo de execução requerido pelo BM para um código de RS. Na implementação paralela proposta, a exigência de tempo para um código algébrico-geométrico que corrige t erros e definido sobre uma curva de gênero g é essencialmente igual às exigências de tempo de um código de Reed-Solomon corretor de $t + 2g$ erros. Essas observações são importantes para construir códigos AG e, em muitas aplicações, é uma alternativa razoável quando se trata de códigos de RS. Em particular, uma implementação paralela, simples e regular do algoritmo de decodificação é essencial para construir códigos AG, que é uma opção razoável em aplicações de engenharia.

A geometria algébrica é, enfim, uma ferramenta matemática que tem se mostrado útil ao desenvolvimento de soluções em diversas áreas da engenharia, como a codificação para controle de erros, a criptografia, a robótica, entre outras, veja, por exemplo, [10]. A geometria algébrica estabelece uma série de relações entre estruturas algébricas, como

espaços e ideais de funções, estruturas geométricas e variedades.

1.1 Descrição do Problema

O presente trabalho visa estabelecer uma relação entre curvas algébricas e os processos de codificação e decodificação de códigos lineares (códigos alternantes). Assim, apresentaremos uma proposta de construção de polinômios absolutamente irredutíveis geradores de curvas algébricas sobre corpos finitos, sendo que certas classes dessas curvas contém muitos pontos racionais. Tais curvas são bastante utilizadas na construção de códigos AG. Apresentaremos também aos processos de localização e de determinação da magnitude dos erros dos algoritmos de decodificação de códigos alternantes sobre corpos finitos esta estrutura geométrica, utilizando a construção de polinômios absolutamente irredutíveis. Os códigos alternantes podem ser decodificados através de qualquer uma das técnicas de decodificação dos códigos BCH. No entanto, existem bons algoritmos para decodificação de códigos BCH e Reed-Solomon, mas são específicos para estas duas classes. No âmbito dessa discussão, incorporaremos, ao algoritmo de Berlekamp-Massey (BM) e ao algoritmo de Peterson-Gorenstein-Zierler (PGZ), passos para estabelecer uma estrutura geométrica (curvas algébricas) na caracterização do processo de localização e determinação das magnitudes dos erros.

O problema em foco teve como ponto de partida, a busca de uma estrutura geométrica decorrente da relação entre o polinômio irredutível,

$$P(z,w) = p_0(z)w^n + p_1(z)w^{n-1} + \cdots + p_n(z),$$

gerador de uma superfície de Riemann compacta e a saída do algoritmo de Berlekamp-Massey (BM), isto é, construir um polinômio de duas variáveis (z,w), tal que para um determinado valor $z = z_0$ tenhamos o polinômio

$$P(z_0,w) = w^n + \sigma_1 w^{n-1} + \cdots + \sigma_n$$

como a saída do algorítmo de BM ou, equivalentemente, a superfície de erros.

O polinômio irredutível $P(z,w)$ apresenta algumas características interessantes que serão destacadas a seguir:

1. Dado z_0 e considerando que $w_1, w_2, \ldots, w_n$ são as raízes distintas de $P(z_0,w)$, então as funções simétricas elementares são obtidas da seguinte maneira

$$\begin{aligned}
\sigma_1 &= -(w_1 + w_2 + \ldots + w_n) \\
\sigma_2 &= \textstyle\sum_{i<j} w_i w_j \\
&\vdots \\
\sigma_n &= (-1)^n w_1 w_2 \ldots w_n;
\end{aligned}$$

2. A matriz formada pelas raízes $w_1, w_2, \ldots, w_n$ de $P(z_0,w)$ é a matriz de Vandermonde, dada por

$$M^* = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ w_1 & w_2 & \cdots & w_n \\ \vdots & \vdots & \cdots & \vdots \\ w_1^{n-1} & w_2^{n-1} & \cdots & w_n^{n-1} \end{bmatrix},$$

cujo determinante é dado por $\det M^* = \pm \prod_{i>j}(w_i - w_j)$;

3. Cabe observar também que $(w-w_1)(w-w_2)\ldots(w-w_n) = w^n + \sigma_1 w^{n-1} + \sigma_2 w^{n-2} + \cdots + \sigma_n$.

A partir dessas observações, conjecturamos que seria possível encontrar uma relação entre o polinômio irredutível $P(z,w)$ e o polinômio localizador de erros resultante do Passo 2 do algoritmo de BM, como também a determinação das magnitudes dos erros para os códigos cíclicos, tendo em vista que o polinômio localizador e a determinação das magnitudes dos erros apresentam as três características descritas.

Este trabalho tem como objetivo identificar uma estrutura geométrica associada ao processo de decodificação. Dessa maneira, apresentaremos como é possível construir polinômios irredutíveis $P(z,w)$ sobre corpos finitos $GF(q)$, onde $q = p^m$, p é um número primo, geradores das curvas algébricas e que, estejam relacionadas às correspondentes superfícies de Riemann compactas. Isso se deve ao fato de que a classe de superfícies de Riemann é equivalente à classe de curvas algébricas que, por sua vez, é equivalente à classe de corpos de funções algébricas. Como resultado, apresentaremos uma proposta de construção de polinômios absolutamente irredutíveis $P(z,w)$ sobre corpos finitos $GF(q)$, definidos para a decodificação dos códigos alternantes baseados na capacidade de correção de erros desses códigos. A condição de polinômio absolutamente irredutível garante que a curva algébrica sobre $GF(q)$ é conexa. Em termos práticos, quando a curva está definida por um modelo afim $f(x,y)$, absolutamente irredutível, implica que o anel de coordenadas $GF(q)[x,y]/(f)$ é um domínio de integridade e permanece assim quando o corpo é substituído por qualquer extensão finita. Isso resulta que o corpo quociente é um corpo de função de grau de transcendência 1.

Para desenvolver essas questões, este trabalho está organizado em capítulos, cujos conteúdos são descritos da seguinte maneira:

No Capítulo 2, apresentaremos uma abordagem sobre códigos alternantes e suas subclasses. Esses códigos são resultados dos subcódigos dos subcorpos dos códigos de Reed-Solomon Generalizados, chamados códigos alternantes. Mostraremos também suas várias subclasses de códigos com exemplos.

No Capítulo 3, apresentaremos uma proposta de construção de polinômios absolutamente irredutíveis sobre corpos finitos, como também, exemplos de curvas algébricas construídas através destes polinômios com número máximo de pontos racionais. A curva algébrica associada a construção para $n = 2$, gera uma curva não-singular. Além disso, daremos um exemplo de código AG construído através de uma curva algébrica gerada pela construção mencionada, para mostrar a sua importância nesse contexto. Trataremos, ainda, da relação entre curvas algébricas e superfícies de Riemann compactas.

No Capítulo 4, apresentaremos uma estrutura geométrica, através de curvas algébricas, relacionada aos processos de localização e de determinação da magnitude dos erros dos algoritmos de decodificação de códigos alternantes cíclicos sobre corpos finitos. Nesse contexto, incorporaremos, ao algoritmo de Berlekamp-Massey (BM) e ao algoritmo de Peterson-Gorenstein-Zierler (PGZ), novos passos através desta estrutura geométrica, utilizando curvas algébricas na caracterização do processo de localização e determinação das magnitudes dos erros.

No Capítulo 5, apresentaremos as conclusões e temas para estudos futuros.

Capítulo 2

Códigos Alternantes e suas Subclasses

Neste capítulo faremos uma descrição da classe de códigos alternantes, conhecidos como subcódigos dos códigos de Reed-Solomon generalizado, destacando as propriedades necessárias para o entendimento deste e dos demais capítulos. A principal motivação é estabelecer uma estrutura geométrica ao decodificador universal para os códigos alternantes[1] a partir desses conceitos e propriedades. Essa classe de códigos será apresentada através das matrizes geradora e verificação de paridade. Nessa categoria, enquadram-se os códigos BCH, Reed-Solomon e de Goppa[2]. Nas Seções 2.3 a 2.5 serão apresentadas as subclasses de códigos alternantes, como: códigos de Goppa e suas subclasses (Seção 2.3); códigos de Srivastava generalizado (Seção 2.4) e na Seção 2.5, baseado nos polinômios de Mattson-Solomon, apresentaremos os códigos BCH generalizados, incluíndo a sua relação com os códigos BCH, RS, Goppa e Srivastava.

2.1 Código Reed-Solomon Generalizado

Uma classe ligeiramente mais geral de códigos do que a dos códigos de RS são obtidos se

$$c = (u(1), u(\alpha), \ldots, u(\alpha^{q-1})) \tag{2.1}$$

é substituído por

$$\mathbf{c} = (v_1 u(1), v_2 u(\alpha), \ldots, v_{q-1} u(\alpha^{q-1})), \tag{2.2}$$

onde os v_i são elementos não-nulos de $GF(q)$. A equação (2.1) é o caso particular de (2.2) quando todos os $v_i = 1$. Isso sugere a seguinte generalização:

Sejam $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)$, onde os α_i são elementos distintos de $GF(q^m)$ e $\mathbf{v} = (v_1, v_2, \cdots, v_n)$, onde os v_i são elementos não-nulos (não necessariamente distintos) de $GF(q^m)$ e q é uma potência de um número primo p. Então o **código de Reed-Solomon**

[1] O leitor interessado em uma discussão mais completa sobre essa classe de códigos poderá consultar os livros de Muir, [40], e Muir-Metzler, [41].

[2] Ao mencionarmos código de Goppa, entenda que estamos nos referindo aos códigos clássicos de Goppa.

generalizado, denotado por $GRS_k(\alpha, \mathbf{v})$, consiste de todos os vetores

$$(v_1 f(\alpha_1), \cdots, v_n f(\alpha_n)),$$

onde $f(z) \in GF(q^m)[z]$ é qualquer polinômio cujo grau é menor que k com coeficientes em $GF(q^m)$. Neste caso, diremos que esse é um $[n, k]$-código sobre $GF(q^m)$.

Como f tem, no máximo, $k-1$ zeros, a distância mínima é pelo menos $n-k+1$, isto é, $d \geq n-k+1$. Por outro lado, pelo limitante de Singleton, a distância é, no máximo, $n-k+1$, consequentemente, $d = n-k+1$. Portanto, o código é dito ser um **código com máxima distância de separação** (MDS). A **matriz verificação de paridade** deste código é

$$\begin{aligned} H &= \begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ \alpha_1 y_1 & \alpha_2 y_2 & \cdots & \alpha_n y_n \\ \alpha_1^2 y_1 & \alpha_2^2 y_2 & \cdots & \alpha_n^2 y_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} y_1 & \alpha_2^{k-1} y_2 & \cdots & \alpha_n^{k-1} y_n \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix} \begin{bmatrix} y_1 & 0 & 0 & \cdots & 0 \\ 0 & y_2 & 0 & \cdots & 0 \\ 0 & & y_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & y_n \end{bmatrix} = XY, \end{aligned} \tag{2.3}$$

onde y $= (y_1, \ldots, y_n)$, com $y_i \in GF(q^m)$ e $y_i \neq 0$.

Uma característica dos códigos cujas palavras são geradas por matrizes é a existência do **código dual,** o qual corresponde ao espaço nulo da matriz H, isto é, o conjunto dos vetores $GRS_{n-1}(\alpha, v)$, tais que $vH^T = 0$, onde H^T denota a matriz transposta da matriz H.

Teorema 2.1.1 *[57] O dual do código $GRS_{k_0}(\alpha, v)$ é o código $GRS_{n-k_0}(\alpha, v')$ para algum $v' = (v'_1, v'_2, \cdots, v'_n)$, onde os $v'_i \in GF(q^m)$.*

Demonstração. *Suponha que $k_0 = n-1$. Seja $\mathcal{D}$ o código dual de $GRS_{n-1}(\alpha, v)$. Então, $\mathcal{D}$ tem dimensão 1 e, portanto, consiste de todos os múltiplos escalares de algum vetor fixado $v' = (v'_1, v'_2, \cdots, v'_n)$. Devemos mostrar que $v'_i \neq 0$, para todo $i = 1, 2, \cdots, n$. De fato, v' satisfaz*

$$\begin{aligned} &v_1 v'_1 + v_2 v'_2 + \cdots + v_n v'_n = 0 \\ &\alpha_1 v_1 v'_1 + \alpha_2 v_2 v'_2 + \cdots + \alpha_n v_n v'_n = 0 \\ &\quad \vdots \qquad\quad \vdots \qquad\qquad \vdots \qquad \vdots \\ &\alpha_1^{n-2} v_1 v'_1 + \alpha_2^{n-2} v_2 v'_2 + \cdots + \alpha_n^{n-2} v_n v'_n = 0 \end{aligned}$$

ou, equivalentemente,

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \cdots & \alpha_n^{n-2} \end{bmatrix} \begin{bmatrix} v_1 v'_1 \\ v_2 v'_2 \\ v_3 v'_3 \\ \vdots \\ v_n v'_n \end{bmatrix} = 0. \tag{2.4}$$

Suponha que algum $v'_i = 0$. Então, o sistema linear (2.4) é homogêneo para os outros $v_i v'_i$ cuja matriz dos coeficientes é a matriz de Vandermonde. Logo, o sistema possui somente a solução trivial, isto é, $v_i v'_i = 0$ e, assim, todos os $v'_i = 0$, o que é uma contradição. Portanto, os $v'_i \neq 0$, para todo i. Por outro lado, suponha que $k_0 < n-1$, então $GRS_{k_0}(\alpha, v)$ é o código dual de $GRS_{n-k_0}(\alpha, v')$, para todo $k_0 < n-1$, desde que

$$\sum_{i=1}^{n} (\alpha_i^s v_i)(\alpha_i^t v'_i) = \sum_{i=1}^{n} \alpha_i^{s+t} v_i v'_i = 0$$

para $s \leq k_0 - 1$ e $t \leq n - k_0 - 1$. ∎

Segue do Teorema 2.1.1 que $GRS_{k_0}(\alpha, v)$ tem matriz verificação de paridade igual à matriz geradora de $GRS_{n-k_0}(\alpha, v')$, isto é,

$$\begin{bmatrix} v'_1 & v'_2 & \cdots & v'_n \\ \alpha_1 v'_1 & \alpha_2 v'_2 & \cdots & \alpha_n v'_n \\ \alpha_1^2 v'_1 & \alpha_2^2 v'_2 & \cdots & \alpha_n^2 v'_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-k_o-1} v'_1 & \alpha_2^{n-k_0-1} v'_2 & \cdots & \alpha_n^{n-k_0-1} v'_n \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-k_0-1} & \alpha_2^{n-k_0-1} & \cdots & \alpha_n^{n-k_0-1} \end{bmatrix} \begin{bmatrix} v'_1 & 0 & \cdots & 0 \\ 0 & v'_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & v'_n \end{bmatrix}.$$

A seguir, descrevemos como uma matriz no corpo maior $GF(q^m)$ que pode ser usada para definir um código em um corpo menor $GF(q)$.

Inicialmente, suponha que o código seja definido por uma matriz verificação de paridade H em $GF(q^m)$. Mais precisamente, seja $H = (H_{ij})$, onde $H_{ij} \in GF(q^m)$ para $1 \leq i \leq r$, $1 \leq j \leq n$, uma matriz $r \times n$ de posto r em $GF(q^m)$. Então, $\mathfrak{C}$ é o código sobre $GF(q)$ consistindo de todos os vetores $\mathfrak{a} = (\mathfrak{a}_1, ..., \mathfrak{a}_n)$, $\mathfrak{a}_i \in GF(q)$, tal que $H\mathfrak{a}^T = 0$.

Outro modo de obtermos $\mathfrak{C}$ é como segue. Escolha uma base $\alpha_1, \ldots, \alpha_m$ para $GF(q^m)$ sobre $GF(q)$, e escreva

$$H_{ij} = \sum_{l=1}^{m} H_{ijl} \alpha_l, \quad H_{ijl} \in GF(q).$$

Defina $\widetilde{H}$ como sendo a matriz $rm \times n$ obtida de H substituindo cada entrada H_{ij} pelo vetor coluna correspondente $(H_{ij1}, \ldots, H_{ijm})^T$ de $GF(q)$. Assim,

$$\widetilde{H} = \begin{pmatrix} H_{111} & H_{121} & \cdots & H_{1n1} \\ H_{112} & H_{122} & \cdots & H_{1n2} \\ \vdots & \vdots & & \vdots \\ H_{11m} & H_{12m} & \cdots & H_{1nm} \\ \vdots & \vdots & & \vdots \\ H_{r1m} & H_{r2m} & \cdots & H_{rnm} \end{pmatrix}.$$

Então,

$$\begin{aligned} \mathfrak{a} \in \mathfrak{C} &\Leftrightarrow \sum_{j=1}^{n} H_{ij}\mathfrak{a}_j = 0 \quad \text{para} \quad i = 1, \ldots, r \\ &\Leftrightarrow \sum_{j=1}^{n} H_{ijl}\mathfrak{a}_j = 0 \quad \text{para} \quad i = 1, \ldots, r; l = 1, \ldots, m \\ &\Leftrightarrow \widetilde{H}\mathfrak{a}^T = 0. \end{aligned}$$

Assim, H ou $\widetilde{H}$ podem ser usadas para definir $\mathfrak{C}$. O posto de $\widetilde{H}$ sobre $GF(q)$ é, no máximo, rm, logo $\mathfrak{C}$ é um $[n, k \geq n - rm]$-código, assumindo $rm \leq n$.

Claro que também poderíamos considerar o código $\mathfrak{C}^*$ sobre $GF(q^m)$ consistindo de todos os vetores $\mathfrak{b} = (b_1, \ldots, b_n)$, $b_i \in GF(q^m)$, tais que $H\mathfrak{b}^T = 0$. Então, $\mathfrak{C}^*$ é um $[n, n - r]$-código sobre $GF(q^m)$. Como $GF(q) \subset GF(q^m)$, toda palavra-código em $\mathfrak{C}$ está em $\mathfrak{C}^*$. Na realidade $\mathfrak{C}$ consiste das palavras-código de $\mathfrak{C}^*$, que têm componentes em $GF(q)$. Representamos essa relação por

$$\mathfrak{C} = \mathfrak{C}^* \mid_{GF(q)},$$

o qual será chamado **subcódigo do subcorpo** de $\mathfrak{C}^*$ (ou a restrição de $\mathfrak{C}^*$ a $GF(q)$), isto é, $\mathfrak{C}^* \mid_{GF(q)}$ é um código sobre $GF(q)$.

Em geral, se $\mathfrak{C}^*$ é qualquer $[n, k^*, d^*]$-código sobre $GF(q^m)$, o subcódigo do subcorpo $\mathfrak{C}^* \mid_{GF(q)}$ consiste das palavras-código de $\mathfrak{C}^*$ que têm componentes em $GF(q)$. Então, $\mathfrak{C}^* \mid_{GF(q)}$ é um $[n, k, d]$-código com $n - m(n - k^*) \leq k \leq k^*$ e $d \geq d^*$. [57].

Por exemplo, seja $\mathfrak{C}^*$ o código BCH $[n, k, d] = [7, 6, 2]$ sobre $GF(2^3)$ com polinômio gerador $x + \alpha$, onde $\alpha \in GF(2^3)$ e satisfaz $\alpha^3 + \alpha + 1 = 0$. Seja $\mathfrak{C}$ o subcódigo do subcorpo $\mathfrak{C}^* \mid_{GF(2)}$. A palavra-código $a(x) = (x + \alpha)(x + \alpha^2)(x + \alpha^4) = x^3 + x + 1$ está em $\mathfrak{C}^*$ e portanto em $\mathfrak{C}$. Assim, $\mathfrak{C}$ contém o $[7, 4, 3]$-código de Hamming.

A aplicação traço T_m de $GF(q^m)$ para $GF(q)$ pode ser usada para expressar o dual de $\mathfrak{C}^* \mid_{GF(q)}$ em termos do dual de $\mathfrak{C}^*$. Esta aplicação é definida como a soma $T_m(\beta) = \beta + \beta^q + \cdots + \beta^{q^{m-1}} = \sum_{i=0}^{m-1} \beta^{p^i}$, onde $\beta \in GF(q^m)$. Seja $T_m(\mathfrak{C}^*)$ o código sobre $GF(q)$ consistindo de todos os vetores distintos

$$T_m(\mathfrak{b}) = (T_m(b_1), \ldots, T_m(b_n)), \quad \text{para } b \in \mathfrak{C}^*.$$

Então $T_m(\mathfrak{C}^*)$ é um $[n, k, d]$-código sobre $GF(q)$ com $k^* \leq k \leq mk^*$ e $d \leq d^*$.

Teorema 2.1.2 (Delsarte) *[57] O dual de um subcódigo do subcorpo é o traço do dual do código original, ou*

$$(\mathfrak{C}^* \mid_{GF(q)})^{\perp} = T_m((\mathfrak{C}^*)^{\perp}).$$

2.2 Códigos Alternantes

Os códigos alternantes consistem da união de várias famílias de códigos e são obtidos através de uma modificação na matriz verificação de paridade do código BCH, [57]. Por ser uma classe muito estensa de códigos, muito resta ainda a ser explorado sobre os códigos alternantes. Lembramos que um código BCH de comprimento n e distância de projeto δ sobre $GF(q)$ tem matriz verificação de paridade $H = (H_{ij})$, onde $H_{ij} = \alpha^{ij}$ $(1 \leq i \leq \delta - 1, 0 \leq j \leq n - 1)$ e $\alpha \in GF(q^m)$ é uma raiz n-ésima primitiva da unidade. Considerando os elementos de H_{ij} como o produto $\alpha_j^{i-1} y_j$, onde $\alpha = (\alpha_1, \cdots, \alpha_n)$ é um vetor com

componentes distintas em $GF(q^m)$ e $\mathrm{y} = (y_1, \cdots, y_n)$ é um vetor com componentes não-nulas em $GF(q^m)$, obtemos o **código alternante** $A(\alpha, \mathrm{y})$. As propriedades desta classe de códigos são resumidas na Figura 2.1. A partir desta figura, fica claro que os códigos BCH são casos especiais dos códigos alternantes.

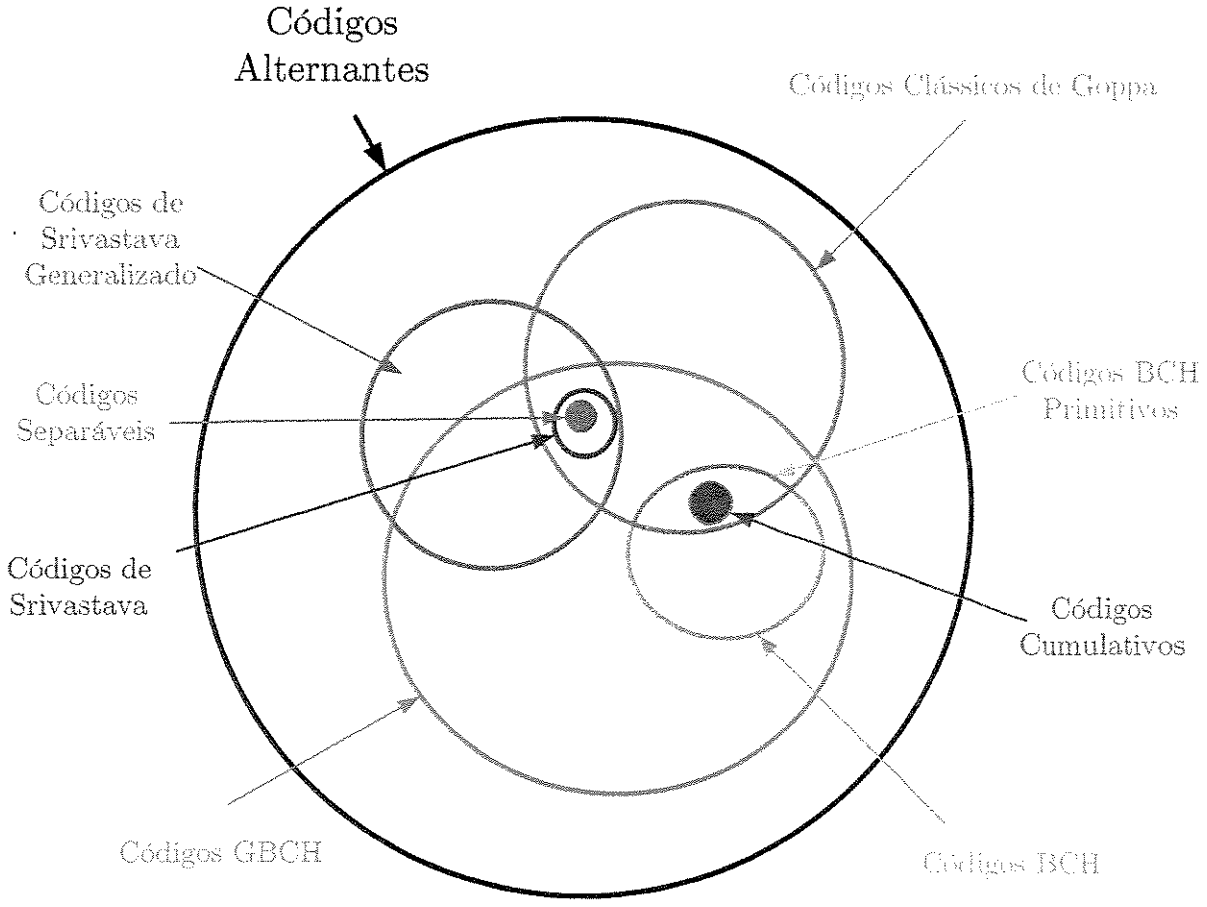


Figura 2.1: *Relação entre as várias subclasses dos códigos alternantes*

A seguir, definiremos várias subclasses da classe de códigos alternantes, tais como, códigos de Goppa, códigos de Srivastava generalizado e a generalização da classe dos códigos BCH, apresentada em [8]. A relação existente entre essas classes de códigos e a classe dos códigos alternantes foi mostrada na Figura 2.1.

O processo de codificação e decodificação dos códigos alternantes é semelhante ao dos códigos BCH. O elemento fundamental no processo de decodificação é o algoritmo de Berlekamp-Massey. Este algoritmo é usado para determinar o polinômio localizador de erro.

O código alternante $A(\alpha, \mathrm{y})$ consiste de todas as **palavras-código** de $GRS_k(\alpha, v)$ com componentes em $GF(q)$, isto é, $A(\alpha, \mathrm{y})$ é a restrição de $GRS_k(\alpha, v)$ a $GF(q)$. Assim, $A(\alpha, \mathrm{y})$ consiste de todos os vetores w sobre $GF(q)$ tais que $Hw^T = 0$, onde H é dada por (2.3). Em particular, o código alternante $A(\alpha, \mathrm{y})$ tem distância mínima $d \geq r + 1$, onde $r = n - k$.

Uma matriz verificação de paridade $\overline{H}$ com elementos em $GF(q^m)$ pode ser obtida substituindo cada elemento de H pelo vetor coluna correspondente de comprimento m de $GF(q)$, da mesma maneira que é feito para os códigos BCH. Como $A(\alpha, \mathrm{y})$ é um subcorpo do subcódigo de $GRS_k(\alpha, v)$, segue que $A(\alpha, \mathrm{y})$ é um código $[n, k, d]$ sobre $GF(q)$, com $n - mr \leq k \leq n - r$ e $d \geq r + 1$. Desse modo, é também possível obter a estimativa do limitante de d diretamente da matriz verificação de paridade.

Seja $\mathbf{C} = (c_{ij})$, $c_{ij} \in GF(q^m)$ com $1 \leq i, j \leq r$, qualquer matriz inversível. Então, a matriz verificação de paridade para $A(\alpha, \mathrm{y})$ é dada por

$$
\begin{aligned}
H &= \mathbf{CXY} \\
&= \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1r} \\ c_{21} & c_{22} & \cdots & c_{2r} \\ \vdots & \vdots & & \vdots \\ c_{r1} & c_{r2} & \cdots & c_{rr} \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_n^{r-1} \end{bmatrix} \begin{bmatrix} y_1 & 0 & \cdots & 0 \\ 0 & y_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & y_n \end{bmatrix} \qquad (2.5) \\
&= \begin{bmatrix} y_1 g_1(\alpha_1) & y_2 g_1(\alpha_2) & \cdots & y_n g_1(\alpha_n) \\ y_1 g_2(\alpha_1) & y_2 g_2(\alpha_2) & \cdots & y_n g_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ y_1 g_r(\alpha_1) & y_2 g_r(\alpha_2) & \cdots & y_n g_r(\alpha_n) \end{bmatrix}, \qquad (2.6)
\end{aligned}
$$

onde

$$g_i(x) = c_{i1} + c_{i2}x + c_{i3}x^2 + \cdots + c_{ir}x^{r-1}, \ i = 1, \cdots, r,$$

é um polinômio de grau menor ou igual a $r - 1$ com coeficientes em $GF(q^m)$.

Das igualdades (2.3) ou (2.6) concluímos que é natural rotular as coordenadas das palavras-código por $\alpha_1, \cdots, \alpha_n$.

Se $\mathbf{C}$ é não-singular, então H é a matriz verificação de paridade de um código linear com distância mínima pelo menos $r+1$. O número de símbolos de verificação de paridade é no máximo mr.

Se escolhermos qualquer submatriz de ordem r de H e computarmos seu determinante, obtemos o produto do determinante de $\mathbf{C}$ pelo determinante de Vandermonde, com elementos distintos, e pelo determinante de uma submatriz diagonal de $\mathbf{Y}$. Determinantes desse tipo são conhecidos como alternantes, [41], e, por esta razão, os códigos correspondentes a (2.5) são chamados **códigos alternantes**.

Por exemplo, se $\alpha = (1, \alpha, \alpha^2, \cdots, \alpha^6)$ e $\mathrm{y} = (1, 1, \cdots, 1)$ onde α é um elemento primitivo de $GF(2^3)$, então, para $r = 2$, o código alternante $A(\alpha, \mathrm{y})$ tem matriz verificação de paridade iqual a

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{bmatrix}.$$

Substituindo cada entrada de H pelo vetor binário correspondente de comprimento 3,

obtemos

$$\overline{H} = \left[\begin{array}{ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right].$$

Assim, $A(\alpha, \mathrm{y})$ é um código de Hamming $[7, 3, 4]$.

Por outro lado, se $\alpha = (1, \alpha, \alpha^2, \cdots, \alpha^6)$ e $\mathrm{y} = (1, \alpha, \alpha^2, \cdots, \alpha^6)$, onde α é um elemento primitivo de $GF(2^3)$, então, para $r = 2$, o código alternante $A(\alpha, \mathrm{y})$ tem matriz verificação de paridade igual a

$$H = \left[\begin{array}{ccccccc} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{array}\right].$$

A segunda linha dessa matriz é redundante e, portanto, pode ser desconsiderada, isto é, se tomarmos o quadrado dos elementos da 1^a linha teremos a 2^a, por causa disso se $\sum_{i=1}^{n} h_i a_i = 0$, onde $h_i \in GF(2^m)$ e $a_i = 0$ ou $a_i = 1$ então,

$$\sum_{i=1}^{n} h_i^2 a_i = \left(\sum_{i=1}^{n} h_i a_i = \right)^2 = 0.$$

Assim, podemos optar por

$$\overline{H} = \left[\begin{array}{ccccccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right].$$

Neste caso, $A(\alpha, \mathrm{y})$ é um código de Hamming $[7, 4, 3]$. Sendo assim, o efeito de y foi diminuir a distância mínima e aumentar o número de símbolos de informação.

Considere agora a classe de códigos alternantes obtida da matriz (2.6), conforme os seguintes procedimentos.

Sejam $r = ts$, onde t e s são inteiros positivos, z_i um elemento não-nulo de $GF(q^m)$ e w_j's elementos distintos de $GF(q^m)$ e para todo j, w_j é diferente de todos os $\alpha_i's$. Para $i = 1, 2, \cdots, n$, $l = 1, 2, \cdots, s$ e $k = 1, 2, \cdots, t$ considere

$$y_i = \frac{z_i}{\prod_{j=1}^{s}(\alpha_i - w_j)^t} \quad \text{e} \quad g_{(l-i)t+k}(\alpha_i) = \frac{z_i}{y_i(\alpha_i - w_l)^k}.$$

Substituindo y_i e $g_{(l-i)t+k}(\alpha_i)$ em (2.6), obtemos a matriz H dada por

$$H = \left[\begin{array}{c} H_1 \\ H_2 \\ \vdots \\ H_s \end{array}\right], \tag{2.7}$$

onde

$$H_l = \begin{bmatrix} \frac{z_1}{\alpha_1 - w_l} & \frac{z_2}{\alpha_2 - w_l} & \cdots & \frac{z_n}{\alpha_n - w_l} \\ \frac{z_1}{(\alpha_1 - w_l)^2} & \frac{z_2}{(\alpha_2 - w_l)^2} & \cdots & \frac{z_n}{(\alpha_n - w_l)^2} \\ \vdots & \vdots & & \vdots \\ \frac{z_1}{(\alpha_1 - w_l)^t} & \frac{z_2}{(\alpha_2 - w_l)^t} & \cdots & \frac{z_n}{(\alpha_n - w_l)^t} \end{bmatrix}.$$

Mas todo determinante de ordem ts é não-nulo, logo, esta classe de códigos tem distância mínima pelo menos igual a $ts+1$. O número de símbolos de verificação de paridade é, no máximo, mts e, como os z_i's em (2.7) devem ser distintos e diferentes dos w's, também distintos, o comprimento n do código não pode exceder $q^m - s$.

2.2.1 Códigos alternantes não-primitivos

A seguir, apresentaremos os códigos alternantes não-primitivos, de acordo com a definição em [29].

Seja $m = \lambda\mu$, onde λ e μ são inteiros maiores que 1. Então $GF(q^\lambda)$ é um subcorpo próprio de $GF(q^m)$. Em (2.7), considere $s = \mu$, $n \leq q^\lambda$, $\alpha_i \in GF(q^\lambda)$, $i = 1, 2, \ldots, n$, $z_i \in GF(q^\lambda) - 0$ e $w_j = w^{q^{\lambda(j-1)}}$, $j = 1, 2, \cdots, \mu$, onde w é um elemento arbitrário de $GF(q^m)$ que não está contido em qualquer subcorpo próprio de $GF(q^m)$. A condição em w assegura que os w_j's são distintos e diferentes dos α_i's. Esta escolha de parâmetros satisfaz, portanto, à condição dos códigos alternantes.

Considere agora os elementos

$$\frac{z_i}{(\alpha_i - w_1)^l} = \frac{z_i}{(\alpha_i - w)^l} \tag{2.8}$$

na l-ésima linha e i-ésima coluna de H_1. Elevando, ambos os membros de (2.8) a $q^{\lambda(j-1)}$-ésima potência, resulta que

$$\left(\frac{z_i}{(\alpha_i - w)^l}\right)^{q^{\lambda(j-1)}} = z_j \left(\frac{1}{(\alpha_i - w)^{q^{\lambda(j-1)}}}\right)^l = \frac{z_i}{(\alpha_i - w_j)^l},$$

para todo $j = 2, 3, \cdots, \mu$. Assim, para $l = 1, 2, \cdots, t$ e $j = 2, 3, \cdots, \mu$, a l-ésima linha em H_j é a $q^{\lambda(j-1)}$-ésima potência da l-ésima linha de H_1. Nestas condições, definimos a seguinte classe de códigos alternantes.

Seja $m = \lambda\mu$, onde λ e μ são inteiros maiores que 1. **Os códigos alternantes não-primitivos** são definidos pela matriz verificação de paridade

$$H = \begin{bmatrix} \frac{z_1}{\alpha_1 - w} & \frac{z_2}{\alpha_2 - w} & \frac{z_3}{\alpha_3 - w} & \cdots & \frac{z_n}{\alpha_n - w} \\ \frac{z_1}{(\alpha_1 - w)^2} & \frac{z_2}{(\alpha_2 - w)^2} & \frac{z_3}{(\alpha_3 - w)^2} & \cdots & \frac{z_n}{(\alpha_n - w)^2} \\ \vdots & \vdots & \vdots & & \vdots \\ \frac{z_1}{(\alpha_1 - w)^t} & \frac{z_2}{(\alpha_2 - w)^t} & \frac{z_3}{(\alpha_3 - w)^t} & \cdots & \frac{z_n}{(\alpha_n - w)^t} \end{bmatrix}, \tag{2.9}$$

onde $n \leq q^\lambda$, cada α_i é um elemento diferente de $GF(q^\lambda)$, $z_i \in GF(q^\lambda) - \{0\}$ e w é qualquer elemento de $GF(q^m)$ não contido em um subcorpo próprio de $GF(q^m)$.

Como conseqüência imediata da discussão acima, deduzimos que a distância mínima e o número máximo de símbolos de paridade dos códigos alternantes não-primitivos, são dados por

Teorema 2.2.1 *[29] Os códigos alternantes não-primitivos de comprimento $n \leq q^\lambda$ têm distância mínima $d \geq \mu t + 1$ e, no máximo, mt símbolos de paridade.*

Exemplo 2.2.2 *Seja $q = 2$, $m = 6$, $\mu = 2$, $\lambda = 3$, $t = 2$ e $n = 8$. Escolha $z_i = 1$, $i = 1, 2, \cdots, 8$, e w igual ao elemento primitivo de $GF(2^6)$ que é uma raiz de $x^6 + x + 1$. Então, fazendo as substituições na matriz (2.9), obtemos*

$$H = \begin{bmatrix} \frac{1}{0-w} & \frac{1}{1-w} & \frac{1}{\alpha^9-w} & \frac{1}{\alpha^{18}-w} & \cdots & \frac{1}{\alpha^{54}-w} \\ \frac{1}{(0-w)^2} & \frac{1}{(1-w)^2} & \frac{1}{(\alpha^9-w)^2} & \frac{1}{(\alpha^{18}-w)^2} & \cdots & \frac{1}{(\alpha^{54}-w)^2} \end{bmatrix}.$$

A segunda linha é o quadrado da primeira linha e, consequentemente, redundante. Expandindo a primeira linha em $GF(2)$, temos a matriz

$$\widetilde{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Assim, $\widetilde{H}$ é a matriz verificação de paridade de um código ($n = 2^3, k \geq 2^3 - 6, d \geq 2 \cdot 2 + 1 = 5$), isto é, um código $[8, 2, 5]$. As palavras-código são

$$\{00000000, 11110001, 01011110, 10101111\}.$$

Note que este código não é cíclico. Em termos da primeira formulação de códigos alternantes, igualdade (2.5), temos para este código que

$$\mathbf{C} = \begin{bmatrix} w^{17} & w^{16} & w & 1 \\ w^{16} & 0 & 1 & 0 \\ w^{10} & w^2 & w^8 & 1 \\ w^2 & 0 & 1 & 0 \end{bmatrix}, \quad \mathbf{X} = \begin{bmatrix} w^0 & w^0 & w^0 & w^0 & w^0 & w^0 & w^0 & w^0 \\ 0 & w^0 & w^9 & w^{18} & w^{27} & w^{36} & w^{45} & w^{54} \\ 0 & w^0 & w^{18} & w^{36} & w^{54} & w^9 & w^{27} & w^{45} \\ 0 & w^0 & w^{27} & w^{54} & w^{18} & w^{45} & w^9 & w^{36} \end{bmatrix} \quad e$$

$$\mathbf{Y} = \begin{bmatrix} w^{45} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & w^{18} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & w^0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & w^{18} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & w^{45} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & w^0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & w^9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & w^9 \end{bmatrix}.$$

Como o determinante de $\mathbf{C}$, $|\mathbf{C}| = (w + w^8)^4$, *é não-nulo, segue que* $\mathbf{CXY}$ *e* $\mathbf{XY}$ *são matrizes verificação de paridade do mesmo código. Mas* $\mathbf{X}$ *é a matriz verificação de paridade do código BCH primitivo estendido* $[8, 1]$ *com* $m_0 = 0$, *distância de projeto* 8 *e distância real* 8. *O efeito de* $\mathbf{Y}$ *é, portanto, diminuir a distância mínima para* 5 *e aumentar o número de símbolos de informação para* 2.

Casos particulares de códigos alternantes não-primitivos

Se $z_i = z$ para todo i, pelo Apêndice 2.6, podemos multiplicar cada linha da matriz H em (2.9) por z^{-1} resultando que o espaço linha de H permanecerá invariante. Assim, sem perda de generalidades, podemos assumir daqui em diante que $z = 1$. Se também considerarmos $t = rq$, para algum inteiro positivo r, então a (lq)-ésima linha de H é igual a q-ésima potência da l-ésima linha de H, para todo $l = 1, 2, \cdots, r$. Para sermos mais exatos, o comentário acima pode ser expresso na forma do seguinte resultado.

Teorema 2.2.3 *[29] Se* $z_i = 1$, $i = 1, 2, \cdots, n$, *então os códigos alternantes não-primitivos de comprimento* q^λ *têm distância mínima* $d \geq \mu rq + 1$ *e, no máximo,* $(q-1)rm$ *símbolos verificação de paridade, para qualquer inteiro positivo* $r = t/q$.

O próximo teorema resulta dos seguintes fatos: se os valores de q, m, r e λ são constantes inteiras, então os códigos alternantes não-primitivos são completamente determinados pelo parâmetro w; além disso, pelo Apêndice 2.6 deste capítulo, $GF(q^\lambda)$ é invariante sobre adição e multiplicação por qualquer elemento não-nulo e, também sobre potenciação, isto é, elevando todos os elementos da q-ésima linha de H à potência l, $l = 1, 2, \cdots, \lambda$.

Teorema 2.2.4 *[29] Se* q, m, r *e* λ *são constantes inteiras então, para* $l = 1, 2, \cdots, \lambda$ *e qualquer* $\beta \in GF(q^\lambda) - \{0\}$, *os códigos alternantes não-primitivos, com parâmetros da forma* w, $w + \beta$, $w\beta$ *e* w^q, *são equivalentes.*

Considere, portanto, o polinômio $f(x) = x^n - \tau x^{n-1} + \tau$, onde $\tau = (w^n - w)^{-1}$. Através de substituições simples podemos mostrar que as raízes de $f(x)$ são os elementos da primeira linha de H. Dividindo a l-ésima linha de H por $(-\tau)^l$, $l = 1, 2, \cdots, t$, pelo Apêndice 2.6, esta operação deixa o código invariante. Assim, para $\lambda = 2$, temos que $\tau^n = -\tau$. Donde concluímos que, independentemente de τ, os elementos da primeira linha da nova matriz verificação de paridade são as raízes de $x^n + x^{n-1} + 1$. Por conseguinte, temos o seguinte resultado.

Teorema 2.2.5 *[29] Se* q, m *e* t *são constantes inteiras e* $\lambda = 2$, *então todos os códigos alternantes não-primitivos são equivalentes.*

2.2.2 O dual de um código alternante

Teorema 2.2.6 *[57] O dual do código alternante* $A(\alpha, \mathrm{y})$ *é o código* $T_m(GRS_{n-k}(\alpha, \mathrm{y})) = T_m(GRS_k(\alpha, \mathrm{y})^\perp)$.

Demonstração. A demonstração é consequência dos Teoremas 2.1.1 e 2.1.2. ∎

2.3 Códigos de Goppa

Goppa [21, 22] introduziu uma ampla classe de códigos corretores de erros que incluem, como subclasses desses códigos, os códigos BCH e os códigos de Srivastava. Os códigos de Goppa formam uma das mais importantes classes dos códigos alternantes. Da mesma maneira que os códigos cíclicos são especificados em termos de um polinômio gerador, os códigos de Goppa são descritos em termos de um polinômio gerador $g(z)$, denominado polinômio de Goppa. Ao contrário dos códigos cíclicos, onde é difícil estimar a distância mínima d a partir do polinômio gerador, os códigos de Goppa têm a propriedade de que $d \geq \deg g + 1$, onde $\deg g$ denota o grau do polinômio $g(z)$.

Seja $L = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ um subconjunto dos elementos de $GF(q^m)$, onde q é uma potência de um número primo p e m é um inteiro positivo não-nulo. Seja $g(z)$ um polinômio em z sobre $GF(q^m)$ tal que $g(z)$ não contém raiz em L e o grau de $g(z)$ é menor que n.

O conjunto das n-uplas $(a_1, a_2, \cdots, a_n)$, com $a_i \in GF(q)$ tal que

$$\sum_{i=1}^{n} \frac{a_i}{z - \alpha_i} \equiv 0 \bmod g(z) \tag{2.10}$$

é chamado **código de Goppa** e é denotado por $\Gamma(L, g)$.

Na congruência (2.10), assumimos que todos os α_i's são distintos. Assim, o código é definido completamente por L e $g(z)$.

Observe no Exemplo 2.2.2 que para $y_i = h^{-1}(\alpha_i)$ temos $h(z) = (z + w)^{18}$ como sendo o polinômio de Goppa do código.

Para códigos binários, $d \geq 2 \deg g + 1$, se $g(z)$ não tem fator irredutível repetido. Em geral, $g(z)$ tem raízes em uma extensão de $GF(q^m)$, embora o corpo de localização do código seja $GF(q^m)$.

2.3.1 Matriz verificação de paridade do código de Goppa

Como todos os códigos lineares, o código de Goppa também pode ser definido por uma matriz verificação de paridade H. Várias formas desta matriz foram determinadas em [21] e [22].

Para o vetor código $\mathfrak{a} = (a_1, a_2, \cdots, a_n)$ temos

$$R_{\mathfrak{a}}(z) = \sum_{i=1}^{n} \frac{a_i}{z - \alpha_i} \equiv 0 \bmod g(z).$$

Essa comparação é equivalente a

$$\sum_{i=1}^{n} a_i \left[(z - \alpha_i)^{-1}\right]_m \equiv 0,$$

onde $[(z - \alpha_i)^{-1}\}]_m$ é o elemento inverso de $(z - \alpha_i)^{-1}$ na álgebra dos polinômios mod $g(z)$. Esse elemento é determinado do seguinte modo:

$$\left[(z - \alpha_i)^{-1}\right]_m = \frac{g(z) - g(\alpha_i)}{z - \alpha_i} g^{-1}(\alpha_i),$$

assim, o lado direito contém um polinômio de grau menor que o grau de $g(z)$, e

$$\frac{1}{z-\alpha_i} \equiv \frac{g(z)-g(\alpha_i)}{z-\alpha_i} g^{-1}(\alpha_i) \bmod g(z).$$

Portanto, a **matriz verificação de paridade do código de Goppa** consiste de uma única linha

$$\left(\frac{g(z)-g(\alpha_1)}{z-\alpha_1} g^{-1}(\alpha_1) \quad \frac{g(z)-g(\alpha_2)}{z-\alpha_2} g^{-1}(\alpha_2) \quad \cdots \quad \frac{g(z)-g(\alpha_n)}{z-\alpha_n} g^{-1}(\alpha_n) \right).$$

Iremos assumir que $g(z) = \sum g_i z^i$, com $g_i \in GF(q^m)$, $g_r \neq 0$ e $\deg\{g(z)\} = r$. Então, a matriz H' pode ser representada por:

$$\begin{aligned} H' &= \begin{bmatrix} g_r g^{-1}(\alpha_1) & \cdots & g_r g^{-1}(\alpha_n) \\ (g_{r-1} + g_r\alpha_1) g^{-1}(\alpha_1) & \cdots & (g_{r-1} + g_r\alpha_n) g^{-1}(\alpha_n) \\ \vdots & & \vdots \\ (g_1 + g_2\alpha_1 + \cdots + g_r\alpha_1^{r-1}) g^{-1}(\alpha_1) & \cdots & (g_1 + g_2\alpha_n + \cdots + g_r\alpha_n^{r-1}) g^{-1}(\alpha_1) \end{bmatrix} \\ &= \begin{bmatrix} g_r & 0 & \cdots & 0 \\ g_{r-1} & g_r & \cdots & 0 \\ g_{r-2} & g_{r-1} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ g_1 & g_2 & \cdots & g_r \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_n^{r-1} \end{bmatrix} \begin{bmatrix} g^{-1}(\alpha_1) & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & g^{-1}(\alpha_n) \end{bmatrix} \\ &= \mathbf{CXY}. \end{aligned}$$

Como $\mathbf{C}$ é uma matriz inversível, fica claro que H' é uma transformação linear das linhas da matriz

$$H = \begin{bmatrix} g^{-1}(\alpha_1) & \cdots & g^{-1}(\alpha_1) \\ \alpha_1 g^{-1}(\alpha_1) & \cdots & \alpha_n g^{-1}(\alpha_1) \\ \vdots & & \vdots \\ \alpha_1^{r-1} g^{-1}(\alpha_1) & \cdots & \alpha_n^{r-1} g^{-1}(\alpha_1) \end{bmatrix}. \tag{2.11}$$

Assim, a matriz verificação de paridade de $\Gamma(L, g)$ é a matriz de Vandermonde multiplicada à direita por uma matriz diagonal, isto é,

$$\begin{aligned} H &= \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \alpha_3^{r-1} & \cdots & \alpha_n^{r-1} \end{bmatrix} \begin{bmatrix} g^{-1}(\alpha_1) & 0 & \cdots & 0 \\ 0 & g^{-1}(\alpha_2) & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & g^{-1}(\alpha_n) \end{bmatrix} \\ &= \mathbf{XY}. \end{aligned}$$

Comparando (2.11) com (2.6) verificamos que $\Gamma(L, g)$ é um código alternante $A(\alpha, y)$ com $\alpha = (\alpha_1, \cdots, \alpha_n)$ e $\mathrm{y} = (g^{-1}(\alpha_1), \cdots, g^{-1}(\alpha_n))$.

Teorema 2.3.1 *[57] O código dual de um código de Goppa é dado por* $\Gamma(L, g)^{\perp} = T_m(GRS_r(\alpha, \mathrm{y}))$, *onde* $y_i = g^{-1}(\alpha_i)$.

Apresentaremos, agora, uma outra forma da matriz verificação de paridade do código de Goppa e mostraremos que a mesma é equivalente à matriz (2.11), [63].

Sejam $\beta_i \in GF(q^m)$ e r_i um inteiro maior ou igual a 1 com $1 \leq i \leq s$, onde os β_i são os zeros de

$$g(z) = (z-\beta_1)^{r_1}(z-\beta_2)^{r_2}\cdots(z-\beta_s)^{r_s}.$$

A matriz H é então dada por

$$H = \begin{bmatrix} (\beta_1-\alpha_1)^{-1} & (\beta_1-\alpha_2)^{-1} & \cdots & (\beta_1-\alpha_n)^{-1} \\ (\beta_1-\alpha_1)^{-2} & (\beta_1-\alpha_2)^{-2} & \cdots & (\beta_1-\alpha_n)^{-2} \\ \vdots & \vdots & & \vdots \\ (\beta_1-\alpha_1)^{-r_1} & (\beta_1-\alpha_2)^{-r_1} & \cdots & (\beta_1-\alpha_n)^{-r_1} \\ (\beta_2-\alpha_1)^{-1} & (\beta_2-\alpha_2)^{-1} & \cdots & (\beta_2-\alpha_n)^{-1} \\ (\beta_2-\alpha_1)^{-2} & (\beta_2-\alpha_2)^{-2} & \cdots & (\beta_2-\alpha_n)^{-2} \\ \vdots & \vdots & & \vdots \\ (\beta_2-\alpha_1)^{-r_2} & (\beta_2-\alpha_2)^{-r_2} & \cdots & (\beta_2-\alpha_n)^{-r_2} \\ \vdots & \vdots & & \vdots \\ (\beta_s-\alpha_1)^{-1} & (\beta_s-\alpha_2)^{-1} & \cdots & (\beta_s-\alpha_n)^{-1} \\ (\beta_s-\alpha_1)^{-2} & (\beta_s-\alpha_2)^{-2} & \cdots & (\beta_s-\alpha_n)^{-2} \\ \vdots & \vdots & & \vdots \\ (\beta_s-\alpha_1)^{-r_s} & (\beta_s-\alpha_2)^{-r_s} & \cdots & (\beta_s-\alpha_n)^{-r_s} \end{bmatrix} \tag{2.12}$$

As matrizes (2.11) e (2.12) são equivalentes. Como apresentado a seguir:

Seja $\Gamma(L,g)$ um código de Goppa com polinômio $g_l(z) = (z-\beta_l)^{r_1}$. Aplicando este polinômio na matriz (2.11) temos

$$H_l = \begin{bmatrix} (\alpha_1-\beta_l)^{-r_1} & (\alpha_2-\beta_l)^{-r_1} & \cdots & (\alpha_n-\beta_l)^{-r_1} \\ (\alpha_1-\beta_l)^{-r_1}\alpha_1 & (\alpha_2-\beta_l)^{-r_1}\alpha_2 & \cdots & (\alpha_n-\beta_l)^{-r_1}\alpha_n \\ \vdots & \vdots & & \vdots \\ (\alpha_1-\beta_l)^{-r_1}\alpha_1^{r_1-1} & (\alpha_2-\beta_l)^{-r_1}\alpha_2^{r_1-1} & \cdots & (\alpha_n-\beta_l)^{-r_1}\alpha_n^{r_1-1} \end{bmatrix}.$$

Demonstração. Por operações elementares sobre matrizes, podemos substituir h_2 por $h_2 - \beta h_1$, onde h_i é a i-ésima linha de H, para obter a matriz semelhante de H

$$H_l' = \begin{bmatrix} (\alpha_1-\beta_l)^{-r_1} & (\alpha_2-\beta_l)^{-r_1} & \cdots & (\alpha_n-\beta_l)^{-r_1} \\ (\alpha_1-\beta_l)^{-r_1}(\alpha_1-\beta_l) & (\alpha_2-\beta_l)^{-r_1}(\alpha_2-\beta_l) & \cdots & (\alpha_n-\beta_l)^{-r_1}(\alpha_n-\beta_l) \\ \vdots & \vdots & & \vdots \\ (\alpha_1-\beta_l)^{-r_1}\alpha_1^{r_1-1} & (\alpha_2-\beta_l)^{-r_1}\alpha_2^{r_1-1} & \cdots & (\alpha_n-\beta_l)^{-r_1}\alpha_n^{r_1-1} \end{bmatrix}.$$

Pela mesma razão, podemos substituir h_3 por $h_3 - \beta_1^2 - 2\beta_1$ para obter a matriz semelhante

$$H_l'' = \begin{bmatrix} (\alpha_1-\beta_l)^{-r_1} & (\alpha_2-\beta_l)^{-r_1} & \cdots & (\alpha_n-\beta_l)^{-r_1} \\ (\alpha_1-\beta_l)^{-r_1}(\alpha_1-\beta_l) & (\alpha_2-\beta_l)^{-r_1}(\alpha_2-\beta_l) & \cdots & (\alpha_n-\beta_l)^{-r_1}(\alpha_n-\beta_l) \\ (\alpha_1-\beta_l)^{-r_1}(\alpha_1-\beta_l)^2 & (\alpha_2-\beta_l)^{-r_1}(\alpha_2-\beta_l)^2 & \cdots & (\alpha_n-\beta_l)^{-r_1}(\alpha_n-\beta_l)^2 \\ \vdots & \vdots & & \vdots \\ (\alpha_1-\beta_l)^{-r_1}\alpha_1^{r_1-1} & (\alpha_2-\beta_l)^{-r_1}\alpha_2^{r_1-1} & \cdots & (\alpha_n-\beta_l)^{-r_1}\alpha_n^{r_1-1} \end{bmatrix},$$

que é semelhante, após as devidas simplificações, à matriz

$$H_l'' = \begin{bmatrix} (\alpha_1-\beta_l)^{-r_1} & (\alpha_2-\beta_l)^{-r_1} & \cdots & (\alpha_n-\beta_l)^{-r_1} \\ (\alpha_1-\beta_l)^{-(r_1-1)} & (\alpha_2-\beta_l)^{-(r_1-1)} & \cdots & (\alpha_n-\beta_l)^{-(r_1-1)} \\ \vdots & \vdots & & \vdots \\ (\alpha_1-\beta_l)_1^{-1} & (\alpha_2-\beta_l)^{-1} & \cdots & (\alpha_n-\beta_l)^{-1} \end{bmatrix}.$$

Consequentemente, se $g(z) = \prod_{l=1}^{s}(z-\beta_l)^{r_1} = \prod_{l=1}^{s} g_l(z)$, então o código de Goppa será a interseção dos códigos com $g_l(z) = (z-\beta_l)^{r_1}$, para $l = 1, 2, \cdots, s$. Donde,

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_s \end{bmatrix}$$

que é igual à matriz (2.12). ■

2.3.2 Códigos de Goppa reversíveis

Se o conjunto localização L é ordenado de tal forma que $\alpha_{n+1-i} = \beta_1 + \beta_2 - \alpha_i$, então este código de Goppa é chamado de **reversível**, isto é, se $(c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \in \Gamma(L, g)$, então $(c_{n-1}, c_{n-2}, \ldots, c_1, c_0) \in \Gamma(L, g)$. Por exemplo, $\{000, 110, 101, 011\}$ é um código reversível.

Considere que o código de Goppa é dado pelo polinômio $g(z) = [(z-\beta_1)(z-\beta_2)]^a$, onde a é um inteiro maior ou igual a 1, [63]. Consideremos os seguintes casos:

1) Se $\beta_1, \beta_2 \in GF(q^m)$ e $L = GF(q^m) - \{\beta_1, \beta_2\}$, então $n = q^m - 2$;

2) Se $L = GF(q^m)$ e $(z-\beta_1)(z-\beta_2)$ é irredutível sobre $GF(q^m)$, então, $\beta_1, \beta_2 \in GF(q^{2m})$ com $\beta_1 = \beta_2^{q^m}$, $\beta_2 = \beta_1^{q^m}$ e $n = q^m$.

Em ambos os casos, a matriz H associada ao código de Goppa é dada por

$$H = \begin{bmatrix} (\beta_1-\alpha_1)^{-1} & (\beta_1-\alpha_2)^{-1} & \cdots & (\beta_1-\alpha_n)^{-1} \\ (\beta_1-\alpha_1)^{-2} & (\beta_1-\alpha_2)^{-2} & \cdots & (\beta_1-\alpha_n)^{-2} \\ \vdots & \vdots & & \vdots \\ (\beta_1-\alpha_1)^{-a} & (\beta_1-\alpha_2)^{-a} & \cdots & (\beta_1-\alpha_n)^{-a} \\ (\beta_2-\alpha_1)^{-1} & (\beta_2-\alpha_2)^{-1} & \cdots & (\beta_2-\alpha_n)^{-1} \\ (\beta_2-\alpha_1)^{-2} & (\beta_2-\alpha_2)^{-2} & \cdots & (\beta_2-\alpha_n)^{-2} \\ \vdots & \vdots & & \vdots \\ (\beta_2-\alpha_1)^{-a} & (\beta_2-\alpha_2)^{-a} & \cdots & (\beta_2-\alpha_n)^{-a} \end{bmatrix}.$$

Observe que, para qualquer i,j, $1 \leq i, j \leq n$, a condição $\beta_1 - \alpha_i = -(\beta_2 - \alpha_j)$ implica $\beta_1 - \alpha_j = -(\beta_2 - \alpha_i)$. Disso segue que $(\beta_1-\alpha_i)^k = [-(\beta_2-\alpha_j)]^k$ e $(\beta_1-\alpha_j)^k = [-(\beta_2-\alpha_i)]^k$,

para $k = 2, 3, \cdots, a$. Para os dois casos considerados acima, temos $\beta_1 + \beta_2 \in GF(q^m)$. Assim, para cada $\alpha_i \in L$, existe um único $\alpha_j = \beta_1 + \beta_2 - \alpha_i \in L$ tal que $\beta_1 - \alpha_i = -(\beta_2 - \alpha_j)$. Se o conjunto L é ordenado de modo que $\alpha_{n+1-i} = \beta_1 + \beta_2 - \alpha_i$, então estes códigos de Goppa tornam-se reversíveis. A distância mínima deste código é pelo menos $2a + 1$ desde que $\deg g(z) = 2a$.

2.3.3 Códigos de Goppa reversíveis estendidos

Seja C um $[n, k, d]$-código binário no qual algumas palavras-código têm peso ímpar. Construa um novo código $\widehat{C}$ acrescentando um 0 ao final de toda palavra-código de C com peso par, e um 1 ao final de toda palavra-código com peso ímpar. $\widehat{C}$ tem a propriedade de que toda palavra-código tem peso par, isto é, satisfaz à nova equação de verificação de paridade

$$x_1 + x_2 + \ldots + x_{n+1} = 0,$$

a **verificação de paridade "global"**. Esta técnica de adicionar mais símbolos de verificação é geralmente chamada de **extensão do código.**

Se C tem matriz verificação de paridade H, $\widehat{C}$ tem matriz de verificação de paridade

$$\widehat{H} = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ 0 & & & \\ \vdots & & H & \\ 0 & & & \end{bmatrix}.$$

Suponha que os códigos de Goppa são reversíveis e estendidos através de verificação de paridade global. Neste caso, a matriz verificação de paridade dos códigos de Goppa estendidos será dada por

$$H_E = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & (\beta_1 - \alpha_1)^{-1} & (\beta_1 - \alpha_2)^{-1} & \cdots & (\beta_1 - \alpha_n)^{-1} \\ 0 & (\beta_1 - \alpha_1)^{-2} & (\beta_1 - \alpha_2)^{-2} & \cdots & (\beta_1 - \alpha_n)^{-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & (\beta_1 - \alpha_1)^{-a} & (\beta_1 - \alpha_2)^{-a} & \cdots & (\beta_1 - \alpha_n)^{-a} \\ 0 & (\beta_2 - \alpha_1)^{-1} & (\beta_2 - \alpha_2)^{-1} & \cdots & (\beta_2 - \alpha_n)^{-1} \\ 0 & (\beta_2 - \alpha_1)^{-2} & (\beta_2 - \alpha_2)^{-2} & \cdots & (\beta_2 - \alpha_n)^{-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & (\beta_2 - \alpha_1)^{-a} & (\beta_2 - \alpha_2)^{-a} & \cdots & (\beta_2 - \alpha_n)^{-a} \end{bmatrix}.$$

Para mostrar que H_E define um código cíclico, é suficiente observar que H_E é linha

equivalente à seguinte matriz:

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 1+\frac{\beta_2-\beta_1}{\beta_1-\alpha_1} & 1+\frac{\beta_2-\beta_1}{\beta_1-\alpha_2} & \cdots & 1+\frac{\beta_2-\beta_1}{\beta_1-\alpha_n} \\ 1 & (1+\frac{\beta_2-\beta_1}{\beta_1-\alpha_1})^2 & (1+\frac{\beta_2-\beta_1}{\beta_1-\alpha_2})^2 & \cdots & (1+\frac{\beta_2-\beta_1}{\beta_1-\alpha_n})^2 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & (1+\frac{\beta_2-\beta_1}{\beta_1-\alpha_1})^a & (1+\frac{\beta_2-\beta_1}{\beta_1-\alpha_2})^a & \cdots & (1+\frac{\beta_2-\beta_1}{\beta_1-\alpha_n})^a \\ 1 & 1-\frac{\beta_2-\beta_1}{\beta_2-\alpha_1} & 1-\frac{\beta_2-\beta_1}{\beta_2-\alpha_2} & \cdots & 1-\frac{\beta_2-\beta_1}{\beta_2-\alpha_n} \\ 1 & (1-\frac{\beta_2-\beta_1}{\beta_2-\alpha_1})^2 & (1-\frac{\beta_2-\beta_1}{\beta_2-\alpha_2})^2 & \cdots & (1-\frac{\beta_2-\beta_1}{\beta_2-\alpha_n})^2 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & (1-\frac{\beta_2-\beta_1}{\beta_2-\alpha_1})^a & (1-\frac{\beta_2-\beta_1}{\beta_2-\alpha_2})^a & \cdots & (1-\frac{\beta_2-\beta_1}{\beta_2-\alpha_n})^a \end{bmatrix}. \tag{2.13}$$

Como

$$1+\frac{\beta_2-\beta_1}{\beta_1-\alpha_i}=\frac{\beta_2-\alpha_i}{\beta_1-\alpha_i}$$

e

$$1-\frac{\beta_2-\beta_1}{\beta_2-\alpha_i}=\frac{\beta_1-\alpha_i}{\beta_2-\alpha_i}=\left(1+\frac{\beta_2-\beta_1}{\beta_1-\alpha_i}\right)^{-1}.$$

Também

$$\frac{\beta_2-\alpha_i}{\beta_1-\alpha_i}\neq\frac{\beta_2-\alpha_j}{\beta_1-\alpha_j}, \quad \text{para } i\neq j.$$

Além disso, para o caso **1)** $[\beta_2-\alpha_i/\beta_1-\alpha_i]\in GF(q^m)$, e, assim, $[\beta_2-\alpha_i/\beta_1-\alpha_i]^{q^m-1}=1$. Para o caso **2)**, como β_1 e β_2 são conjugados em $GF(q^m)$, temos então que

$$\begin{aligned}\left(\frac{\beta_2-\alpha_i}{\beta_1-\alpha_i}\right)^{q^m+1} &= \left(\frac{\beta_2^{q^m}-\alpha_i^{q^m}}{\beta_1^{q^m}-\alpha_i^{q^m}}\right)\left(\frac{\beta_2-\alpha_i}{\beta_1-\alpha_i}\right) \\ &= \left(\frac{\beta_1-\alpha_i}{\beta_2-\alpha_i}\right)\left(\frac{\beta_2-\alpha_i}{\beta_1-\alpha_i}\right)=1.\end{aligned}$$

Se $N=n+1$, então $N=q^m-1$ para o caso **1)** e $N=q^m+1$ para o caso **2)**. Como, para ambos os casos, $[\beta_2-\alpha_i/\beta_1-\alpha_i]^N=1$ e $[\beta_2-\alpha_i/\beta_1-\alpha_i]\neq[\beta_2-\alpha_j/\beta_1-\alpha_j]$, para $i\neq j$, $1\leq i,j\leq N-1$ e, além disso, $[\beta_2-\alpha_i/\beta_1-\alpha_i]\neq 1$ quando $\beta_1\neq\beta_2$, segue que os elementos $[\beta_2-\alpha_i/\beta_1-\alpha_i]$, para $1\leq i\leq N-1$ são exatamente as $(N-1)$ raízes N-ésimas distintas da unidade que não são iguais a um. Consequentemente, o conjunto L pode ser ordenado da seguinte forma

$$\frac{\beta_2-\alpha_i}{\beta_1-\alpha_i}=\alpha^i,$$

onde, para o caso **1)**, α é um elemento primitivo de $GF(q^m)$ enquanto que, para o caso **2)**, $\alpha=\beta^{q^m-1}$, onde β é primitivo em $GF(q^{2m})$.

Devemos notar que tal ordenação também satisfaz à exigência inicial de que $\alpha_{n+1-i} = \beta_1 + \beta_2 - \alpha_i$, visto que

$$\begin{aligned}\alpha_i + \alpha_{n+1-i} &= \tfrac{\beta_2-\beta_1\alpha^i}{1-\alpha^i} + \tfrac{\beta_2-\beta_1\alpha^{n+1-i}}{1-\alpha^{n+1-i}} \\ &= \tfrac{\beta_2-\beta_1\alpha^i}{1-\alpha^i} + \tfrac{\beta_2-\beta_1\alpha^{-i}}{1-\alpha^{-i}} \\ &= \tfrac{\beta_2-\beta_1\alpha^i}{1-\alpha^i} + \tfrac{\beta_1-\beta_2\alpha^i}{1-\alpha^i} \\ &= \beta_1 + \beta_2.\end{aligned}$$

Assim, segue que H_E é linha equivalente à matriz (2.13), que define uma classe de códigos cíclicos reversíveis gerados por $g(x)$ tendo $1, \alpha^{\pm 1}, \alpha^{\pm 2}, \ldots, \alpha^{\pm a}$ como raízes e, portanto, com distância mínima $d \geq 2a + 2$.

Por exemplo, considere um código de Goppa com $L = GF(3) = \{0, 1, 2\}$, $g(z) = z^2 + z + 2 = (z - \alpha)(z - \alpha^3)$, onde α é primitivo em $GF(3^2)$ e $\alpha^2 + \alpha + 2 = 0$. Assim, $\alpha^2 = 2\alpha + 1$, $\alpha^3 = 2\alpha + 2, \alpha^4 = 2$, $\alpha^5 = 2\alpha$, $\alpha^6 = \alpha + 2$, $\alpha^7 = \alpha + 1$ e $\alpha^8 = 1$. Sejam $\alpha_1 = 0$, $\alpha_2 = 1$ e $\alpha_3 = 2$. Então

$$\begin{aligned}H &= \begin{bmatrix} (\alpha-\alpha_1)^{-1} & (\alpha-\alpha_2)^{-1} & (\alpha-\alpha_3)^{-1} \\ (\alpha^3-\alpha_1)^{-1} & (\alpha^3-\alpha_2)^{-1} & (\alpha^3-\alpha_3)^{-1} \end{bmatrix} \\ &= \begin{bmatrix} (\alpha-0)^{-1} & (\alpha-1)^{-1} & (\alpha-2)^{-1} \\ (\alpha^3-0)^{-1} & (\alpha^3-1)^{-1} & (\alpha^3-2)^{-1} \end{bmatrix} \\ &= \begin{bmatrix} (\alpha)^{-1} & (\alpha^6)^{-1} & (\alpha^7)^{-1} \\ (\alpha^3)^{-1} & (\alpha^2)^{-1} & (\alpha^5)^{-1} \end{bmatrix} = \begin{bmatrix} \alpha^7 & \alpha^2 & \alpha \\ \alpha^5 & \alpha^6 & \alpha^3 \end{bmatrix}.\end{aligned}$$

Assim,

$$H_E = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & \alpha^7 & \alpha^2 & \alpha \\ 0 & \alpha^5 & \alpha^6 & \alpha^3 \end{bmatrix}.$$

Conseqüentemente, o código de Goppa é o código linear $[3, 1]$ sobre $GF(3)$, consistindo de três palavras-código $(0, 0, 0), (1, 2, 1)$ e $(2, 1, 2)$. É também um código reversível com distância $d \geq 2 \deg g(z) + 1 = 2.2 + 1 = 5$. O código de Goppa estendido é o código cíclico reversível $[4, 1]$ sobre $GF(3)$ gerado pelo polinômio $g(x) = (x-1)(x^2+1) = 2+x+2x^2+x^3$ com palavras-código $(0, 0, 0, 0), (2, 1, 2, 1)$ e $(1, 2, 1, 2)$.

Exemplo 2.3.2 *Sejam $L = GF(2^4) - \{\alpha, \alpha^3\}$ e $g(z) = (z - \alpha)(z - \alpha^3)$, onde α é um elemento primitivo em $GF(2^4)$ e $\alpha^4 + \alpha + 1 = 0$. Suponha que L é o conjunto localizador dado pela ordem*

$$\alpha_i = \frac{\alpha^3 - \alpha\alpha^i}{1 - \alpha^i}, \ 1 \leq i \leq 14$$

e obtida da relação $(\beta_2 - \alpha_i)(\beta_2 - \alpha_i)^{-1} = \alpha^i$. Assim,

$$\begin{array}{lllllll} \alpha_1 = \alpha^2, & \alpha_2 = 0, & \alpha_3 = \alpha^8, & \alpha_4 = \alpha^{10}, & \alpha_5 = \alpha^7, & \alpha_6 = \alpha^6, & \alpha_7 = \alpha^4, \\ \alpha_8 = \alpha^{14}, & \alpha_9 = \alpha^5, & \alpha_{10} = 1, & \alpha_{11} = \alpha^{13}, & \alpha_{12} = \alpha^{12}, & \alpha_{13} = \alpha^9, & \alpha_{14} = \alpha^{11}. \end{array}$$

Então,

$$H = \begin{bmatrix} \alpha^{10} & \alpha^{14} & \alpha^5 & \alpha^7 & \alpha & \alpha^4 & 1 & \alpha^8 & \alpha^{13} & \alpha^{11} & \alpha^3 & \alpha^2 & \alpha^{12} & \alpha^9 \\ \alpha^9 & \alpha^{12} & \alpha^2 & \alpha^3 & \alpha^{11} & \alpha^{13} & \alpha^8 & 1 & \alpha^4 & \alpha & \alpha^7 & \alpha^5 & \alpha^{14} & \alpha^{10} \end{bmatrix}$$

define um código linear reversível $[14, 6]$ *com distância* $d = 5$. *Agora, como* $\alpha^3 - \alpha = \alpha^9$, *então a matriz*

$$H_E = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{14} \\ 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \cdots & \alpha^{-14} \end{bmatrix}$$

define um código cíclico reversível $[15, 6]$ *gerado por* $g(x) = (x+1)(x^4+x+1)(x^4+x^3+1)$. *Este código é conhecido como sendo um* ***código de Melas expurgado.***

Exemplo 2.3.3 *Seja* L *o mesmo conjunto definido no Exemplo 2.3.2 e seja* $g(z) = [(z - \alpha)(z - \alpha^3)]^3$. *Então a matriz*

$$H = \begin{bmatrix} (\alpha - \alpha^2)^{-1} & (\alpha - 0)^{-1} & \cdots & (\alpha - \alpha^{11})^{-1} \\ (\alpha - \alpha^2)^{-2} & (\alpha - 0)^{-2} & \cdots & (\alpha - \alpha^{11})^{-2} \\ (\alpha - \alpha^2)^{-3} & (\alpha - 0)^{-3} & \cdots & (\alpha - \alpha^{11})^{-3} \\ (\alpha^3 - \alpha^2)^{-1} & (\alpha^3 - 0)^{-1} & \cdots & (\alpha^3 - \alpha^{11})^{-1} \\ (\alpha^3 - \alpha^2)^{-2} & (\alpha^3 - 0)^{-2} & \cdots & (\alpha^3 - \alpha^{11})^{-2} \\ (\alpha^3 - \alpha^2)^{-3} & (\alpha^3 - 0)^{-3} & \cdots & (\alpha^3 - \alpha^{11})^{-3} \end{bmatrix} = \begin{bmatrix} \alpha^{10} & \alpha^{14} & \cdots & \alpha^9 \\ \alpha^5 & \alpha^{13} & \cdots & \alpha^3 \\ 1 & \alpha^{12} & \cdots & \alpha^{12} \\ \alpha^9 & \alpha^{12} & \cdots & \alpha^{10} \\ \alpha^3 & \alpha^9 & \cdots & \alpha^5 \\ \alpha^{12} & \alpha^6 & \cdots & 1 \end{bmatrix}$$

define um código linear reversível $[14, 2]$ *com distância* $d = 7$. *Portanto, a matriz*

$$H_E = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{14} \\ 1 & (\alpha) & (\alpha^2)^2 & (\alpha^3)^2 & \cdots & (\alpha^{14})^2 \\ 1 & (\alpha)^3 & (\alpha^2)^3 & (\alpha^3)^3 & \cdots & (\alpha^{14})^3 \\ 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \cdots & \alpha^{-14} \\ 1 & (\alpha^{-1})^2 & (\alpha^{-2})^2 & (\alpha^{-3})^2 & \cdots & (\alpha^{-14})^2 \\ 1 & (\alpha^{-1})^3 & (\alpha^{-2})^3 & (\alpha^{-3})^3 & \cdots & (\alpha^{-14})^3 \end{bmatrix}$$

define um código cíclico reversível $[15, 2]$ *gerado por* $g(x) = (x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$.

2.3.4 Códigos de Goppa especiais

Consideraremos a seguir alguns códigos de Goppa particulares e relacionados na Figura 2.2.

A classificação de tais códigos é baseada na forma do polinômio gerador. Códigos cumulativos são do mesmo tipo que os códigos BCH. Códigos separáveis têm um esquema de decodificação próprio. Para ambas as classes de códigos é possível melhorar os limitantes de seus parâmetros no caso binário: $n \leq 2^m$, $k \geq n - mt$, $d \geq 2t + 1$. (Os códigos de Srivastava, dos quais trataremos adiante, foram obtidos em 1967. Dentro da classe dos códigos separáveis, os códigos irredutíveis têm uma estrutura algébrica mais "forte".)

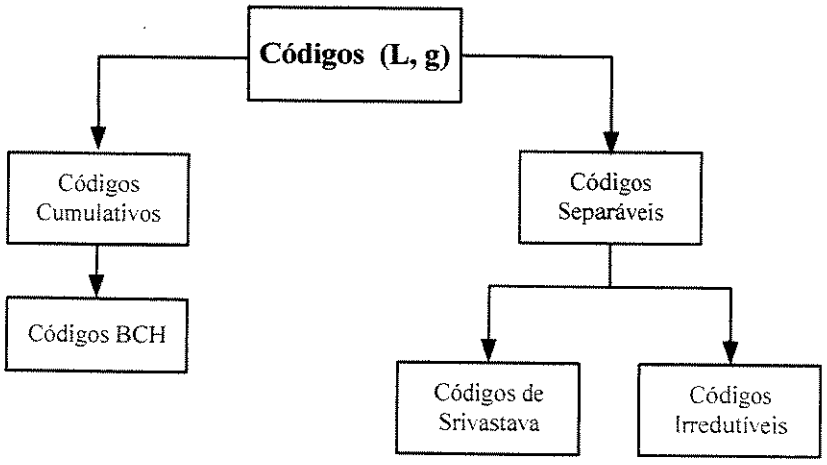


Figura 2.2: *Códigos de Goppa particulares*

Códigos Cumulativos

Os **códigos cumulativos** são códigos cujo polinômio gerador tem uma única raiz, isto é, $g(z) = (z - \alpha)^r$.

O conjunto máximo L que pode ser encontrado para tais códigos corresponde a $GF(q^m) - \{\alpha\}$, de forma que o comprimento máximo da palavra-código é igual a $q^m - 1$. Um caso particular de códigos comulativos é quando $g(z) = z^r$, correspondente ao código BCH.

Teorema 2.3.4 *[22] Todos os códigos cumulativos com o mesmo parâmetro r têm o mesmo espectro de pesos.*

Teorema 2.3.5 *[22] Seja $\mathfrak{C}$ um código de Goppa da classe $\Gamma(L, g)$, com $L = \{1, \alpha, \cdots, \alpha^{n-1}\}$, onde $\alpha \in GF(2^m)$ é uma raiz primitiva n-ésima da unidade. Se $\mathfrak{C}$ é cíclico, então $\mathfrak{C}$ é um código BCH e $g(z) = z^r$ para algum r. Os códigos BCH são os únicos códigos $\Gamma(L, g)$ cíclicos.*

Exemplo 2.3.6 *Para o código BCH de comprimento $n = q - 1 = 15$ e $d = 5$, temos o código de Goppa $C(L, g)$, onde $L = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}$, $g(z) = z^{d-1} = z^4$ e $t = 2$. A matriz geradora do código de Goppa é dada por*

$$H = \begin{bmatrix} g^{-1}(\alpha_1) & g^{-1}(\alpha_2) & \cdots & g^{-1}(\alpha_n) \\ g^{-1}(\alpha_1)\alpha_1 & g^{-1}(\alpha_2)\alpha_2 & \cdots & g^{-1}(\alpha_n)\alpha_n \\ \vdots & \vdots & & \vdots \\ g^{-1}(\alpha_1)\alpha_1^{d-2} & g^{-1}(\alpha_2)\alpha_2^{d-2} & \cdots & g^{-1}(\alpha_n)\alpha_n^{d-2} \end{bmatrix}.$$

Assim,

$$H = \begin{bmatrix} 1 & \alpha^{11} & \alpha^7 & \alpha^3 & \alpha^{14} & \alpha^{10} & \alpha^6 & \alpha^2 & \alpha^{13} & \alpha^9 & \alpha^5 & \alpha & \alpha^{12} & \alpha^8 & \alpha^4 \\ 1 & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & 1 & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & 1 & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 \\ 1 & \alpha^{13} & \alpha^{11} & \alpha^9 & \alpha^7 & \alpha^5 & \alpha^3 & \alpha & \alpha^{14} & \alpha^{12} & \alpha^{10} & \alpha^8 & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^{14} & \alpha^{13} & \alpha^{12} & \alpha^{11} & \alpha^{10} & \alpha^9 & \alpha^8 & \alpha^7 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{bmatrix}.$$

Códigos Separáveis

Os códigos cujo polinômio gerador não tem raízes múltiplas, isto é, $g(z) = (z-z_1)(z-z_2)\cdots(z-z_r)$ são chamados de **códigos separáveis.**

Os códigos separáveis binários, da mesma maneira que os códigos BCH, admitem uma melhoria nos limitantes de seus parâmetros. Assim, para $\deg g = t$ temos que $n \leq 2^m$, $k \geq n - mt$ e $d \geq 2t+1$.

Definição 2.3.7 *Os códigos separáveis têm a seguinte forma específica da matriz verificação de paridade (matriz de Cauchy)*

$$H_C = \left\| (z_i - \alpha_j)^{-1} \right\|,$$

onde $i = 1, 2, \cdots, r$, $j = 1, 2, \cdots, n$ *e* z_i, α_j *são elementos distintos de* $GF(q^m)$ *ou de uma extensão deste corpo.*

Códigos de Srivastava Os códigos cujo polinômio gerador se decompõe em um corpo minimal contendo L, são chamados de **códigos de Srivastava.** Os parâmetros n, k e d destes códigos são, $n \leq q^m - 2t$, $k \geq n - 2mt$, $d \geq 2t+1$.

Pouco é conhecido sobre quantos símbolos de informação os códigos de Srivastava de fato contém. Na pior das hipóteses, eles só são ligeiramente inferiores aos códigos BCH. Na melhor das hipóteses, eles podem ter uma taxa de informação consideravelmente melhor. Os códigos de Srivastava definitivamente merecem pesquisa adicional.

Códigos de Goppa Irredutíveis Um código de Goppa separável é denominado **código de Goppa irredutível** se o polinômio $g(z)$ é irredutível sobre um corpo minimal contendo L.

A matriz verificação de paridade de um código de Goppa irredutível consiste da matriz linha

$$T_H = \left((z_0 - \alpha_1)^{-1} (z_0 - \alpha_2)^{-1} \cdots (z_0 - \alpha_n)^{-1} \right),$$

onde z_0 é uma raiz de $g(z)$.

A seguir apresentaremos alguns exemplos:

1). Considere $g(z) = z^3 + z + 1$, que é irredutível sobre $GF(2)$. Os zeros de $g(z)$ estão em $GF(2^3)$ e, assim, estão em $GF(2^6), GF(2^9), \cdots$. Entretanto, como m não é um múltiplo de 3, podemos considerar $L = GF(2^m)$ e obter um código de Goppa irredutível com parâmetros

$$[n = 2^m,\ k \geq 2^m - 3m,\ d \geq 7]. \tag{2.14}$$

Quando $m = 5$, os parâmetros para n, k e d são exatamente $[32, 17, 7]$. De uma outra maneira, podemos escolher $g(z)$ como sendo um polinômio cúbico irredutível sobre $GF(2^m)$, resultando em um código de Goppa com os parâmetros dados em (2.14), para qualquer valor de m. Geralmente, escolhendo $g(z)$ como sendo um polinômio

irredutível de grau r sobre $GF(2^m)$, obtemos um código de Goppa irredutível com parâmetros

$$[n = 2^m,\ k \geq 2^m - rm,\ d \geq 2r + 1], \tag{2.15}$$

quaisquer que sejam r e m. O código BCH primitivo comparado com o código de Goppa tem parâmetros

$$[n = 2^m - 1,\ k \geq 2^m - 1 - rm,\ d \geq 2r + 1].$$

Analisando os parâmetros k e d em (2.14) e (2.15), deduzimos que o código BCH primitivo possui um símbolo de informação a menos.

2). Consideremos $g(z) = z^2 + z + 1$, $L = GF(2^3) = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^6\}$, onde α é um elemento primitivo de $GF(2^3)$, $q = 2$ e $q^m = 8$. Se $\beta \in GF(8)$ e os zeros de z^2+z+1 pertencem a $GF(2^2), GF(2^4), GF(2^6), \cdots$ e não pertencem a $GF(2^3)$, então $g(\beta) \neq 0$. Neste caso, obtemos um código de Goppa irredutível Γ de comprimento $n = |L| = 8$, dimensão $k \geq 8 - 2.3 = 2$ e distância mínima $d \geq 5$. Logo, a matriz verificação de paridade é

$$H = \begin{bmatrix} \frac{1}{g(0)} & \frac{1}{g(1)} & \frac{1}{g(\alpha)} & \cdots & \frac{1}{g(\alpha^6)} \\ \frac{0}{g(0)} & \frac{1}{g(1)} & \frac{\alpha}{g(\alpha)} & \cdots & \frac{\alpha^6}{g(\alpha^6)} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{bmatrix}.$$

Assim, na forma binária, H é dada por

$$H = \left[\begin{array}{cccccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right].$$

As palavras-código são

$$\{0\,0\,0\,0\,0\,0\,0\,0,\ 0\,0\,1\,1\,1\,1\,1\,1,\ 1\,1\,0\,0\,1\,0\,1\,1,\ 1\,1\,1\,1\,0\,1\,0\,0\}.$$

Este é um código de Goppa com parâmetros $[8, 2, 5]$. Acrescentando um dígito de paridade e reordenando as colunas, obtemos o código com parâmetros $[9, 2, 6]$, cujas palavras-código são

$$\{0\,0\,0\,0\,0\,0\,0\,0\,0,\ 0\,1\,1\,0\,1\,1\,0\,1\,1,\ 1\,0\,1\,1\,0\,1\,1\,0\,1,\ 1\,1\,0\,1\,1\,0\,1\,1\,0\}.$$

Observamos que este código é cíclico, $n - r = 8 - 2 = 6$ e $v_i = g(\alpha_i) = \alpha^{2i} + \alpha^i + 1$. Como $\prod_{j \neq i}(\alpha_j - \alpha_i) = 1$, para todo i, então é um código de Goppa $[8, 2, 5]$, restrição para $GF(2)$ do código sobre $GF(2^3)$ com matriz geradora

$$\begin{bmatrix} 1 & 1 & \alpha^5 & \alpha^3 & \alpha^5 & \alpha^6 & \alpha^6 & \alpha^3 \\ 0 & 1 & \alpha^6 & \alpha^5 & \alpha & \alpha^3 & \alpha^4 & \alpha^2 \\ 0 & 1 & 1 & 1 & \alpha^4 & 1 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 & 1 & \alpha^4 & 1 & 1 \\ 0 & 1 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha & \alpha^5 & \alpha^6 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^6 & \alpha^5 & \alpha^3 & \alpha^5 \end{bmatrix}.$$

Observe que

$$\begin{aligned} &linha\ 1 + linha\ 2 + linha\ 6 = 11110100, \\ &linha\ 1 + linha5 + linha6 = 11001011, \\ &linha2 + linha5 = 00111111. \end{aligned}$$

3). Consideremos $g(z) = z^3 + z + 1$ e $L = GF(2^5)$. Temos que $g(\beta) \neq 0$ para $\beta \in L$. Então, $\Gamma(L, g)$ é um código de Goppa irredutível com parâmetros $[32, 17, 7]$, com matriz verificação de paridade dada por: (Aqui α é um elemento primitivo de $GF(2^5)$).

$$H = \begin{bmatrix} \frac{1}{g(0)} & \frac{1}{g(1)} & \frac{1}{g(\alpha)} & \cdots & \frac{1}{g(\alpha^{30})} \\ \frac{0}{g(0)} & \frac{1}{g(1)} & \frac{\alpha}{g(\alpha)} & \cdots & \frac{\alpha^{30}}{g(\alpha^{30})} \\ \frac{0^2}{g(0)} & \frac{1^2}{g(1)} & \frac{\alpha^2}{g(\alpha)} & \cdots & \frac{\alpha^{60}}{g(\alpha^{30})} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \alpha^4 & \alpha^8 & \alpha^{14} & \cdots & \alpha^{26} \\ 0 & 1 & \alpha^5 & \alpha^{10} & \alpha^{17} & \cdots & \alpha^{25} \\ 0 & 1 & \alpha^6 & \alpha^{12} & \alpha^{20} & \cdots & \alpha^{24} \end{bmatrix}.$$

4). Os coeficientes de $g(z)$ não precisam ser restritos a 0's e 1's. Por exemplo, podemos considerar $g(z) = z^2 + z + \alpha^3$, onde α é um elemento primitivo de $GF(2^4)$. Observe que $g(z)$ é irredutível sobre $GF(2^4)$, pois $T_4(\alpha^3) = \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^9 = 1$, onde $T_4(\alpha^3)$ é o traço de α^3. Portanto, podemos considerar $L = GF(2^4)$ e obter um código de Goppa irredutível com parâmetros $[16, 8, 5]$.

Corolário 2.3.8 *[57] Seja $\Gamma(L, g)$ um código de Goppa binário com $L = \{1, \alpha, \cdots, \alpha^{n-1}\}$, onde $\alpha \in GF(2^m)$ é uma raiz n-ésima da unidade. Então,*

$$\Gamma(L, g) = \left\{ \mathfrak{a}(x) : [z^{n-1} A(z)]_n \equiv 0 \bmod g(z) \right\}.$$

Exemplo 2.3.9 *Considere o código de Goppa $\Gamma(L, g)$ onde $g(z) = z^3 + z + 1$, $L = \{1, \alpha, \cdots, \alpha^{14}\}$ e α é um elemento primitivo de $GF(2^4)$. A matriz verificação de paridade é então dada por*

$$H = \left[\begin{array}{cccccccccccccc} 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right].$$

Então, $\Gamma(L,g)$ é um código $[15,3,7]$ com matriz geradora

$$\begin{matrix} u_1 \\ u_2 \\ u_3 \end{matrix} \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Este é um código com pequena distância mínima, mas é uma boa ilustração do corolário.

Teorema 2.3.10 (Goppa) *[67] O código de Goppa sobre $GF(q)$ com polinômio de Goppa $g(z)$ satisfaz as condições*

$$n \leq q^m - s_0, \quad n - k \leq m \deg g \quad e \quad d \geq \deg g + 1,$$

onde s_0 é o número de raízes do polinômio $g(z)$ pertencentes a $GF(q^m)$.

2.3.5 Parâmetros das subclasses de códigos de Goppa binários

Considere os códigos $\Gamma(L,g)$ binários com polinômio $g(z)$ representado na forma

$$g(z) = 1 + \beta z + (\beta z)^{t-1} + z^t, \tag{2.16}$$

onde $\beta \in GF(2^m)$, $m = 2l$, $\beta^t \neq 1$, $t = 2^l + 1$ e l é um inteiro positivo maior que 1. É mostrado em [53] que todas as raízes do polinômio $g(z)$ estão no corpo $GF(2^m)$. Os elementos do corpo $GF(2^m)$ que não são raízes do polinômio $g(z)$ formam o subconjunto L. Tais códigos $\Gamma(L,g)$ têm comprimento $n = 2^{2l} - 2^l - 1$. Pode-se mostrar que para $\beta^t \neq 1$, estes códigos são separáveis, portanto, sua distância mínima é $d \geq 2^{2l+1} + 3$.

Lema 2.3.11 *[53] O polinômio $g(z)$ definido em (2.16) satisfaz a condição $g(\alpha^{-(t-1)}) = \alpha^{-t} g(\alpha)$, $t = 2^l+1$. Observe que a igualdade é verificada por substituição direta do elemento $\alpha^{-(t-1)}$ no valor de z em $g(z)$. Observamos que no corpo $GF(2^m)$, $\alpha^{2m} = \alpha$, onde $m = 2l$.*

Lema 2.3.12 *[53] Todos os valores $g(\alpha_i)$, $\alpha_i \in L \subset GF(2^m)$, do polinômio $g(z)$ definido em (2.16) estão contidos no corpo $GF(2^l) \subset GF(2^m)$, onde $m = 2l$.*

Demonstração. *Para provar este lema, basta aplicar o seguinte fato da teoria de corpos finitos: o elemento $\gamma \in GF(p^c)$ pertence ao subcorpo $GF(p^s) \subset GF(p^c)$ se, e somente se, $\gamma^{p^s} = \gamma$ no corpo $GF(p^c)$.*

Eleve o elemento $g(\alpha_i)$ à potência $2^l + 1$, resultando em

$$[g(\alpha_i)]^{2^l} = \left[1 + \beta\alpha_i + (\beta\alpha_i)^{2^l} + \alpha_i^{2^l+1}\right]^{2^l} = \left[1 + \beta\alpha_i + (\beta\alpha_i)^{2^{2l}} + \alpha_i^{2^{2l}+2^l}\right] = g(\alpha_i).$$

■

Proposição 2.3.13 *[53] A dimensão do código $\Gamma(L,g)$ separável binário definido em (2.16), com $n = 2^{2l} - 2^l - 1$ e $d \geq 2^{2l+1} + 3$, satisfaz a condição $k \geq n - m(t - \frac{5}{2})$, onde $m = 2l$ e $t = 2^l + 1$.*

2.3.6 Outros resultados sobre os códigos de Goppa

Reuniremos aqui as principais relações entre os parâmetros dos códigos de Goppa.

Teorema 2.3.14 (Goppa) *[67] O código de Goppa sobre $GF(q)$ com polinômio de Goppa $g(z)$ satisfaz as relações*

$$n \leq q^m - s_0, \;\; n - k \leq m \deg g \;\; e \;\; d \geq \deg g + 1,$$

Teorema 2.3.15 (Goppa) *[67] O código de Goppa sobre $GF(2)$ com polinômio de Goppa $g(z)$ que não contém raízes repetidas satisfaz*

$$n \leq 2^m - s_0, \;\; n - k \leq m \deg g \;\; e \;\; d \geq 2 \deg g + 1.$$

Teorema 2.3.16 (Goppa) *[67] O código de Goppa sobre $GF(2)$ com polinômio de Goppa $g(z) = (z - z_1)^{2t}$ satisfaz as relações*

$$n \leq 2^m - 1, \;\; n - k \leq mt \;\; e \;\; d \geq 2t + 1,$$

onde a raiz z_1 de $g(z)$ pertence a $GF(2^m)$.

Teorema 2.3.17 (Goppa) *[67] O código de Goppa binário com polinômio de Goppa da forma $\{\widetilde{g}(z)\}^2$ satisfaz as relações*

$$n \leq 2^m - s_0, \;\; n - k \leq m \,\text{grau}\, \widetilde{g} \;\; e \;\; d \geq 2 \,\text{grau}\, \widetilde{g} + 1,$$

onde $\widetilde{g}(z)$ é um polinômio arbitrário sobre $GF(2^m)$ e s_0 é o número de raízes distintas de $g(z)$ pertencentes a $GF(2^m)$.

Segue do Teorema 2.3.17, que todos os códigos de Goppa binários satisfazem a relação $2(n-k) \leq m(d-1)$. Observamos que nem todos os códigos de Goppa binários estão incluídos nos Teoremas 2.3.16 e 2.3.17. Por exemplo, quando $g(z) = \{(z-z_1)(z-z_2)^2(z-z_3)^3\}^2$, onde z_1, z_2 e z_3 são elementos em $GF(2^m)$, temos as relações $n < 2m-3$, $n-k < 6m$, $d > 13$ provenientes do Teorema 2.3.17, enquanto que as relações $n < 2m-3$, $n-k < 9m$, $d > 13$ são provenientes de teoremas que se encontram em [21], [22], [6].

2.4 Códigos de Srivastava Generalizado

O nosso objetivo aqui é definir e dar exemplos da classe de códigos alternantes denominada classe dos códigos de Srivastava generalizados.

Na matriz verificação de paridade do código alternante $A(\alpha, \mathrm{y})$, suponha que $r = st$, $\alpha_1, \alpha_2, \cdots, \alpha_n, w_1, w_2, \cdots, w_s$, sejam $n+s$ elementos distintos de $GF(q^m)$ e $z_1, z_2, \cdots, z_n$ sejam elementos não-nulos de $GF(q^m)$, [57]. Considere o polinômio na variável x,

$$g_{(l-1)t+k}(x) = \frac{\prod_{j=1}^{s}(x - w_j)^t}{(x - w_l)^k}, \;\; l = 1, \cdots s, k = 1, \cdots, t,$$

e

$$y_i = \frac{z_i}{\prod_{j=1}^{s}(\alpha_i - w_j)^t},\ i = 1, \cdots, n,$$

de tal forma que

$$y_i g_{(l-1)t+k}(\alpha_i) = \frac{z_i}{(\alpha_i - w_l)^k}.$$

Levando em consideração as relações anteriores, o código de Srivastava generalizado é definido como segue.

Definição 2.4.1 *O código resultante* $[n,\ k \geq n - mst,\ d \geq st + 1]$ *é definido como um* ***código de Srivastava generalizado sobre*** $GF(q^m)$. *Assim, a matriz verificação de paridade para este código é*

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_s \end{bmatrix},$$

onde

$$H_l = \begin{bmatrix} \frac{z_1}{\alpha_1 - w_l} & \frac{z_2}{\alpha_2 - w_l} & \cdots & \frac{z_n}{\alpha_n - w_l} \\ \frac{z_1}{(\alpha_1 - w_l)^2} & \frac{z_2}{(\alpha_2 - w_l)^2} & \cdots & \frac{z_n}{(\alpha_n - w_l)^2} \\ \vdots & \vdots & & \vdots \\ \frac{z_1}{(\alpha_1 - w_l)^t} & \frac{z_2}{(\alpha_2 - w_l)^t} & \cdots & \frac{z_n}{(\alpha_n - w_l)^t} \end{bmatrix},$$

e $l = 1, \cdots, s$.

Os códigos de Srivastava originais (1967) são casos particulares dos códigos da Definição 2.4.1, onde $t = 1$ e $z_i = \alpha_i^\mu$, para algum μ. A correspondente matriz verificação de paridade é

$$H = \begin{bmatrix} \frac{\alpha_1^\mu}{\alpha_1 - w_1} & \frac{\alpha_2^\mu}{\alpha_2 - w_1} & \cdots & \frac{\alpha_n^\mu}{\alpha_n - w_1} \\ \frac{\alpha_1^\mu}{\alpha_1 - w_2} & \frac{\alpha_2^\mu}{\alpha_2 - w_2} & \cdots & \frac{\alpha_n^\mu}{\alpha_n - w_2} \\ \vdots & \vdots & & \vdots \\ \frac{\alpha_1^\mu}{\alpha_1 - w_s} & \frac{\alpha_2^\mu}{\alpha_2 - w_s} & \cdots & \frac{\alpha_n^\mu}{\alpha_n - w_s} \end{bmatrix}. \tag{2.17}$$

Como existem s w_i's, pode haver, no máximo, $(q^m - s)$ elementos α_i's. Assim, o comprimento de um código de Srivastava generalizado é, no máximo, $q^m - s$.

Se $\alpha_1, \alpha_2, \cdots, \alpha_n$ são escolhidos como elementos de $GF(q^m)$, exceto os w_i's, então $n = q^m - s$ e os códigos são chamados **primitivos**.

Considerando que o código de Srivastava é um código alternante, um código de Srivastava generalizado tem parâmetros $k \geq n - mst$ e $d \geq st + 1$.

Observação 2.4.2 *Considere a matriz H equivalente à matriz em (2.17) dada por*

$$H = \begin{bmatrix} \frac{b_1^\mu}{1-a_1b_1} & \frac{b_2^\mu}{1-a_1b_2} & \frac{b_3^\mu}{1-a_1b_3} & \cdots & \frac{b_n^\mu}{1-a_1b_n} \\ \frac{b_1^\mu}{1-a_2b_1} & \frac{b_2^\mu}{1-a_2b_2} & \frac{b_3^\mu}{1-a_2b_3} & \cdots & \frac{b_n^\mu}{1-a_2b_n} \\ \vdots & \vdots & \vdots & & \vdots \\ \frac{b_1^\mu}{1-a_{\mathrm{d}-1}b_1} & \frac{b_2^\mu}{1-a_{\mathrm{d}-1}b_2} & \frac{b_3^\mu}{1-a_{\mathrm{d}-1}b_3} & \cdots & \frac{b_n^\mu}{1-a_{\mathrm{d}-1}b_n} \end{bmatrix}, \tag{2.18}$$

onde μ é qualquer inteiro, $a_1, a_2, \cdots, a_{\mathrm{d}-1}$ são elementos distintos de $GF(q^m)$ e $b_1, b_2, \cdots, b_n$ são os elementos em $GF(q^m) - \{0, a_1^{-1}, a_2^{-1}, \cdots, a_{\mathrm{d}-1}^{-1}\}$. Neste caso, o comprimento de bloco do código é $n = q^m - \mathrm{d}$, [5].

Observamos que se denominarmos, na matriz (2.18), $b_i = \alpha_i$ e $a_j = \frac{w_j - \alpha_i + 1}{\alpha_i}$ para $i = 1, \cdots, n$ e $j = 1, \cdots, \mathrm{d}-1$ obteremos a matriz (2.17). Portanto, fica claro que elas são matrizes equivalentes.

Exemplo 2.4.3 *Considere o código de Srivastava com $m = 4$, $s = 2$, $n = 14$, $w_1 = 0$ e $w_2 = 1$. Se α é um elemento primitivo de $GF(2^4)$ que é uma raiz de $f(x) = 1 + x + x^4$ e $z_i = 1$, $x_i = \alpha^i$ para $i = 1, 2, \cdots, 14$, a matriz H em $GF(2^4)$ assume a forma*

$$H = \begin{bmatrix} \frac{1}{\alpha} & \frac{1}{\alpha^2} & \frac{1}{\alpha^3} & \cdots & \frac{1}{\alpha^{14}} \\ \frac{1}{\alpha - 1} & \frac{1}{\alpha^2 - 1} & \frac{1}{\alpha^3 - 1} & \cdots & \frac{1}{\alpha^{14} - 1} \end{bmatrix}.$$

Considerando os elementos de H sobre $GF(2)$, temos

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Como todas as linhas de H são linearmente independentes, H é a matriz verificação de paridade de um código linear $[14, 6, 5]$, com distância mínima $d = 2s + 1 = 5$. O código dual é o código linear $[14, 8, 4]$ com distância mínima 4. Ambos são exemplos de códigos ótimos.

Observação 2.4.4 *Um código de Srivastava generalizado binário com $t = 1$ possue distância mínima $d \geq 2s + 1$.*

Exemplo 2.4.5 *Considere o código de Srivastava generalizado binário com* $m = 6$, $n = 8$, $r = 2$, $s = 1$, $t = 2$ *e* $\alpha_1, \alpha_2, \cdots, \alpha_8$ *elementos de* $GF(2^3)$ *contidos em* $GF(2^6)$, *isto é,*

$$\{\alpha_1, \alpha_2, \cdots, \alpha_8\} = \{0, 1, \alpha^9, \alpha^{18}, \alpha^{27}, \alpha^{36}, \alpha^{45}, \alpha^{54}\},$$

onde α *é um elemento primitivo de* $GF(2^6)$. *Considere também* $w_1 = \alpha$, $z_i = 1$, *para* $i = 1, \cdots, 8$. *Portanto,*

$$H = \begin{bmatrix} \frac{1}{0-\alpha} & \frac{1}{1-\alpha} & \frac{1}{\alpha^9-\alpha} & \frac{1}{\alpha^{18}-\alpha} & \cdots & \frac{1}{\alpha^{54}-\alpha} \\ \frac{1}{(0-\alpha)^2} & \frac{1}{(1-\alpha)^2} & \frac{1}{(\alpha^9-\alpha)^2} & \frac{1}{(\alpha^{18}-\alpha)^2} & \cdots & \frac{1}{(\alpha^{54}-\alpha)^2} \end{bmatrix}.$$

Observamos que a segunda linha é o quadrado da primeira e, portanto, redundante. Assim, na forma binária, H *é dada por*

$$\widetilde{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

As palavras-código são

$$\{0\,0\,0\,0\,0\,0\,0\,0,\ 1\,1\,1\,1\,0\,0\,0\,1,\ 0\,1\,0\,1\,1\,1\,1\,0,\ 1\,0\,1\,0\,1\,1\,1\,1\}.$$

Desse modo, $\widetilde{H}$ *é a matriz verificação de paridade de um código* $[n = 2^3, k \geq 2^3 - 6]$, *com distância mínima* $d \geq 2 \cdot 2 + 1 = 5$, *isto é, um código* $[8, 2, 5]$. *Observamos que este código não é cíclico.*

Exemplo 2.4.6 *Considere o código de Srivastava binário com* $m = 4$, $s = 2$, $t = 1$, $n = 13$, $w_1 = \alpha^{-1}$, $w_2 = \alpha^{-2}$,

$$\{\alpha_1, \alpha_2, \cdots, \alpha_{13}\} = GF(2^4) - \{0, \alpha^{-1}, \alpha^{-2}\},$$

e $\mu = 1$, *onde* α *é um elemento primitivo de* $GF(2^4)$. *Portanto, a matriz* H *em* $GF(2^4)$ *assume a forma*

$$\begin{aligned} H &= \begin{bmatrix} \frac{1}{1-0} & \frac{1}{\alpha-0} & \frac{1}{\alpha^2-0} & \cdots & \frac{1}{\alpha^{12}-0} \\ \frac{1}{1-\alpha^{-1}} & \frac{1}{\alpha-\alpha^{-1}} & \frac{1}{\alpha^2-\alpha^{-1}} & \cdots & \frac{1}{\alpha^{12}-\alpha^{-1}} \\ \frac{1}{1-\alpha^{-2}} & \frac{1}{\alpha-\alpha^{-2}} & \frac{1}{\alpha^2-\alpha^{-2}} & & \frac{1}{\alpha^{12}-\alpha^{-2}} \end{bmatrix} \\ &= \begin{bmatrix} 1 & \alpha^{14} & \alpha^{13} & \cdots & \alpha^3 \\ \alpha^{12} & \alpha^8 & \alpha^2 & \cdots & \alpha^{10} \\ \alpha^9 & \alpha^3 & \alpha & & \alpha^{14} \end{bmatrix}. \end{aligned}$$

Essa é matriz do código de Srivastava $[13, 5, 5]$.

Além do mais, o código de Srivastava generalizado binário com $z_i = 1$, para todo i, $s = 1$ e $n = 2^m - 1$ é um código BCH no sentido estrito.

2.5 Códigos BCH Generalizados

Descreveremos e forneceremos exemplos de uma classe de códigos alternantes denominada de classe de códigos BCH generalizados, [8]. Essa classe é definida em termos de dois polinômios $P(z)$ e $G(z)$.

Seja n relativamente primo a q, e seja o corpo $GF(q^m)$ a menor extensão de $GF(q)$ que contém todas as raízes n-ésimas da unidade.

Definição 2.5.1 *[57] O* ***polinômio de Mattson-Solomon*** *(MS) associado ao vetor* $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1})$, *onde* $\mathbf{a}(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ *e* $a_i \in GF(q^m)$ *é a forma polinomial de* $\mathbf{a}$ *dada por*

$$A(z) = \sum_{j=1}^{n} A_j z^{n-j},$$

onde $A_j = \mathbf{a}(\alpha^j) = \sum_{i=0}^{n-1} a_i \alpha^{ij}$, $j = 0, \pm 1, \pm 2, \cdots$. *As formas alternativas de* $A(z)$ *são*

$$A(z) = \sum_{j=0}^{n-1} A_{-j} z^j = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} (\alpha^{-i} z)^j.$$

O código BCH generalizado, denotado por $GBCH(P, G)$, é definido da seguinte maneira.

Definição 2.5.2 *[8] Sejam* $P(z)$ *e* $G(z)$ *polinômios com coeficientes em* $GF(q^m)$, *relativamente primos a* $z^n - 1$ *e tais que* $\deg P(z) \leq n-1$ *e* $r = \deg G(z) \leq n-1$. *Então o* ***código*** BCH ***generalizado de comprimento*** n ***sobre*** $GF(q)$ *com polinômios associados* $P(z)$ *e* $G(z)$, *denotado por* $GBCH(P, G)$, *consiste de todos os polinômios* $\mathbf{a}(x)$ *com coeficientes em* $GF(q)$ *e grau menor ou igual a* $n-1$. *Então o código* $GBCH(P, G)$ *consiste de todos os* $\mathbf{a}(x)$ *com coeficientes em* $GF(q)$ *e grau menor ou igual a* $n-1$ *para que o polinômio (MS)* $A(z)$, *satisfaça a seguinte condição de congruência*

$$[A(z)P(z)]_n \equiv 0 \mod G(z).$$

Desse modo, H é a matriz verificação de paridade do código $GBCH(P, G)$ e $a =$

$(a_0, a_1, \cdots, a_{n-1}) \in GBCH(P, G)$ se, e somente se, $aH^T = 0$, onde

$$H = \begin{bmatrix} \frac{p_0}{g_0} & \frac{p_1\alpha}{g_1} & \frac{p_2\alpha^2}{g_2} & \cdots & \frac{p_{n-1}\alpha^{n-1}}{g_{n-1}} \\ \frac{p_0}{g_0} & \frac{p_1\alpha^2}{g_1} & \frac{p_2\alpha^4}{g_2} & \cdots & \frac{p_{n-1}\alpha^{2(n-1)}}{g_{n-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ \frac{p_0}{g_0} & \frac{p_1\alpha^r}{g_1} & \frac{p_2\alpha^{2r}}{g_2} & \cdots & \frac{p_{n-1}\alpha^{r(n-1)}}{g_{n-1}} \end{bmatrix} \tag{2.19}$$

$$= \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{r-1} & \alpha^{2(r-1)} & \cdots & \alpha^{(r-1)(n-1)} \end{bmatrix} \begin{bmatrix} \frac{p_0}{g_0} & 0 & 0 & \cdots & 0 \\ 0 & \frac{p_1\alpha}{g_1} & 0 & \cdots & 0 \\ 0 & 0 & \frac{p_2\alpha^2}{g_2} & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \frac{p_{n-1}\alpha^{n-1}}{g_{n-1}} \end{bmatrix}.$$

Assim, H é a matriz verificação de paridade do código $GBCH$. Isso mostra que o código $GBCH(P, G)$ é um código alternante, onde $\alpha_1, \alpha_2, \cdots, \alpha_n$ são as raízes n-ésimas da unidade e $y_i = \frac{p_{i-1}\alpha^{i-1}}{g_{i-1}}$. Portanto, o código $GBCH(P, G)$ tem como parâmetros $[n, k \geq n - rm, d \geq r + 1]$, onde $r = \deg G(z)$.

Teorema 2.5.3 *[8] Sejam $P(z) = z^{b+\delta-2}$ e $G(z) = z^{\delta-1}$ polinômios com coeficientes em $GF(q^m)$. O código $GBCH$ associado a $(z^{b+\delta-2}, z^{\delta-1})$ é um código BCH com distância de projeto δ e α^{b+j}, b um inteiro maior ou igual a 0 e $j = 0, 1, \cdots, \delta - 2$, as $\delta - 1$ raízes consecutivas do polinômio gerador.*

Como α é uma raiz primitiva n-ésima da unidade, observamos que todos os códigos BCH pertencem a esta classe de códigos. Neste caso, a matriz verificação de paridade é dada por

$$\begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & (\alpha^b)^{n-1} \\ 1 & \alpha^{b+1} & (\alpha^{b+1})^2 & \cdots & (\alpha^{b+1})^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{b+\delta-2} & (\alpha^{b+\delta-2})^2 & \cdots & (\alpha^{b+\delta-2})^{n-1} \end{bmatrix},$$

onde α é um elemento não-nulo de $GF(q^m)$ de ordem n, b um inteiro maior ou igual a 0 e δ é a distância de projeto do código.

Teorema 2.5.4 *[57] Se $P(z) = z^{b_1+\delta-2} + z^{b_2+\delta-2}$ e $G(z) = z^{\delta-1}$, então o código $GBCH$ associado a $(z^{b_1+\delta-2} + z^{b_2+\delta-2}, z^{\delta-1})$ contém a intersecção dos correspondentes códigos BCH e, na verdade, pode ser igual a essa intersecção.*

Exemplo 2.5.5 *Consideremos o caso binário, isto é, quando* $q = 2$. *Se* $P(z) = z^{n-1}$ *então* $GBCH(P, G)$ *é o código de Goppa* $\Gamma(L, G)$, *onde* $L = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ *e* $\alpha \in GF(2^m)$ *é uma raiz primitiva n-ésima da unidade, ou seja,*

$$GBCH(z^{n-1}, G(z)) = \Gamma(L, G) = \{\mathbf{a}(x) : [z^{n-1}A(z)]_n \equiv 0 \mod G(z)\}.$$

Exemplo 2.5.6 *Sejam* $n = 15$, $P(z) = z$ *e* $G(z) = z^2$. *Assim, a matriz verificação de paridade do código* $GBCH(z, z^2)$ *é dada por*

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \end{bmatrix}.$$

Considerando os elementos de H *sobre* $GF(2)$, *temos*

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Observamos que esta matriz define o código BCH *com parâmetros* $[15, 10, 4]$.

Exemplo 2.5.7 *Sejam* $n = 15$, $P(z) = z^5$ *e* $G(z) = z^2$. *Assim, a matriz verificação de paridade do código* $GBCH(z^5, z^2)$ *é dada por*

$$H = \begin{bmatrix} 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha & \alpha^5 & \alpha^9 & \alpha^{13} & \alpha^2 & \alpha^6 & \alpha^{10} & \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^{11} \\ 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} \end{bmatrix}.$$

Sobre $GF(2)$, *temos*

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Esta matriz define o código BCH *com parâmetros* $[15, 7, 4]$.

Exemplo 2.5.8 *Sejam* $n = 15$, $P(z) = z + z^5$ *e* $G(z) = z^2$. *Assim, a matriz verificação de paridade do código* $GBCH(z + z^5, z^2)$ *é dada por*

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^{11} & \alpha^4 & \alpha^{10} & \alpha^7 & \alpha^6 & \alpha^8 & \alpha^{13} & \alpha^5 & \alpha^3 & \alpha^{14} & \alpha^9 & \alpha^{12} \\ 1 & \alpha^2 & \alpha^4 & \alpha^{14} & \alpha^8 & 1 & \alpha^{13} & \alpha^{13} & \alpha & \alpha^7 & 1 & \alpha^{14} & \alpha^{11} & \alpha^7 & \alpha^{11} \end{bmatrix}.$$

Teorema 2.5.9 *[8]A distância mínima de Hamming,* d, *para o código* $GBCH$ *associado a* $(P(z), G(z))$ *satisfaz a desigualdade* $d \geq \deg G(z) + 1$.

Este limite inferior para uma distância mínima d será muito útil na construção de códigos e ainda poderá ser considerada como a "distância de projeto" do código.

Teorema 2.5.10 *[8] Seja k o número de dígitos de informação em cada palavra-código de um código C. Então $n-k \leq m\tau$, onde $\tau = \deg G(z)$.*

Demonstração. Como a matriz H com entradas em $GF(q^m)$ tem τ linhas, então H pode ser re-escrita em termos dos elementos de $GF(q)$ com, no máximo, $m\tau$ linhas. Portanto, $n-k \leq m\tau$. ∎

A matriz sobre $GF(q^m)$ com a notação $\| \ \|$, dada por

$$G = \left\| \alpha^i h_i^{-1} \alpha^{-ij} \right\|, \quad 0 \leq i \leq n-1, \ 1 \leq j \leq n-\tau$$

é, de fato, a matriz geradora do código $GBCH$ q^m-ário associado a $(P(z), G(z))$. Observamos que este código pode ser considerado como um código de Reed-Solomon generalizado.

Teorema 2.5.11 *[8] Suponha que C seja o código $GBCH$ q-ário associado a $(P(z), G(z))$. Seja $[P(z)G^{-1}(z)]_n = \sum_{j\in J} \theta_j z^j$, $\theta_j \in GF(q^m) - \{0\}$. Além disso, seja C_j o código $GBCH$ q-ário associado a $(z^{\tau+j}, z^\tau)$, onde $\tau = \deg G(z)$. Então, $\overline{C} = \cap_{j\in J} Cj$ é um subcódigo cíclico de C. Além do mais, C é cíclico se, e somente se, $C = \overline{C}$. Isso implica que se C é cíclico e o seu polinômio gerador está definido pelo conjunto de raízes então $\{\cup_{j\in J}\{\alpha^{-(i+j)} \mid_{i=1,2,\cdots,\tau}\}$.*

Exemplo 2.5.12 *Seja $q = 2$, $m = 4$ e $n = 15$. Se α é uma raiz de $z^4 + z + 1$, então α é uma 15-ésima raiz primitiva de 1 em $GF(2^4)$. O código cíclico binário $\overline{C}(15, 8)$, gerado pelas raízes $\{\alpha^0, \alpha^5, \alpha^7\}$, não é um código BCH e pode ser definido alternativamente pelas raízes $\{\alpha^{-(i+j)} \mid_{i=1,2;j=0,3,14}\}$. Considere os polinômios $P(z) = z(z^4 + z + \alpha)$ e $G(z) = z^2$. Como $P(z)$ e $G(z)$ são polinômios sobre $GF(q^m)$ e $[P(z)G^{-1}(z)]_{15} = \alpha z^{14} + z^3 + 1$, então o Teorema 2.5.11 implica que $\overline{C} \subseteq C$, onde C é o código $GBCH$ binário associado a $(P(z), G(z))$. Porém, como C tem oito dígitos de informação, então $\overline{C} = C$. Conseqüentemente, a classe dos códigos $GBCH$ também contém alguns códigos cíclicos que não são códigos BCH.*

Corolário 2.5.13 *[8] Se $m = 1$, então um código $GBCH$ q-ário é cíclico se, e somente se, é um código de Reed-Solomon.*

2.5.1 Relação dos códigos GBCH com outros códigos

Discutiremos brevemente a relação entre os códigos $GBCH$ e alguns códigos existentes, isto é, códigos BCH, Reed-Solomon, Goppa e Srivastava.

Códigos BCH e códigos de Reed-Solomon.

É mostrado, no Teorema 2.5.3, que todos os códigos BCH pertencem à classe dos códigos $GBCH$. Uma situação ainda mais geral é: se $P(z) \equiv z^h G(z) \bmod(z^n - 1)$, então o código associado a $(P(z), G(z))$ é o código BCH definido pelo seguinte conjunto de raízes, $\{\alpha^{-(h+j)} \mid_{j=1,2,\cdots,\deg G(X)}\}$. Em particular, se $m = 1$ em $GF(q^m)$, temos os códigos de Reed-Solomon.

Códigos de Goppa.

A semelhança entre a matriz verificação de paridade H dos códigos $GBCH$ e a dos códigos de Goppa pode ser facilmente constatada. A matriz verificação de paridade do código de Goppa é dada por

$$H_{GP} = \left\| G^{-1}(\alpha^i)\alpha^{-ij} \right\|, \ i = 0, 1, \cdots, n-1, \ j = 0, 1, \cdots, \deg G(z) - 1,$$

onde $G(z) \in GF(q^m)[z]$. Porém, a matriz verificação de paridade do código $GBCH$ associada a $(z^{n-1}, G(z))$ é dada por

$$H_{GBCH} = \left\| p_i g^{-1} \alpha^{-ij} \right\| = \left\| \alpha^i G^{-1}(\alpha^i)\alpha^{-ij} \right\| = H_{GP},$$

onde $j = 1, \cdots, \deg G(z)$. Portanto, o código de Goppa gerado por $G(z)$ é o código $GBCH$ associado a $(z^{n-1}, G(z))$, pois os códigos $GBCH$ podem ser considerados como uma generalização dos códigos de Goppa. Além disso, se essa classe não contém todos os códigos BCH, então a classe dos códigos de Goppa é um subconjunto próprio dos códigos $GBCH$. Sabemos ainda que um código de Goppa é cíclico se, e somente se, é um código BCH. Porém, isto geralmente não é verdade para códigos $GBCH$.

Forneceremos, agora, um exemplo com o objetivo de ilustrar a igualdade entre as matrizes H_{GBCH} e H_{GP}.

Seja $q = 2$, $m = 4$, $n = 15$. Seja α uma raiz de $z^4 + z + 1$, então α é uma 15-ésima raiz primitiva da unidade em $GF(2^4)$. Considere os polinômios $P(z) = z^{14}$, $G(z) = z^3$ e $L = \{1, \alpha, \alpha^2, \cdots, \alpha^{14}\}$. Como o $\deg G(z) = 3$ e $n = 15$ temos, para o código de Goppa, que $i = 0, 1, \cdots, 14$ e $j = 0, 1, 2$. Assim, a matriz verificação de paridade do código de Goppa $\Gamma(L, G)$ é dada por

$$H_{GP} = \begin{bmatrix} \frac{\alpha^0}{\alpha^0} & \frac{\alpha^0}{\alpha^3} & \frac{\alpha^0}{\alpha^6} & \frac{\alpha^0}{\alpha^9} & \frac{\alpha^0}{\alpha^{12}} & \cdots & \frac{\alpha^0}{\alpha^9} & \frac{\alpha^0}{\alpha^{12}} \\ \frac{\alpha^0}{\alpha^0} & \frac{\alpha^{-1}}{\alpha^3} & \frac{\alpha^{-2}}{\alpha^6} & \frac{\alpha^{-3}}{\alpha^9} & \frac{\alpha^{-4}}{\alpha^{12}} & \cdots & \frac{\alpha^{-13}}{\alpha^9} & \frac{\alpha^{-14}}{\alpha^{12}} \\ \frac{\alpha^0}{\alpha^0} & \frac{\alpha^{-2}}{\alpha^3} & \frac{\alpha^{-4}}{\alpha^6} & \frac{\alpha^{-6}}{\alpha^9} & \frac{\alpha^{-8}}{\alpha^{12}} & \cdots & \frac{\alpha^{-11}}{\alpha^9} & \frac{\alpha^{-13}}{\alpha^{12}} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & \cdots & \alpha^6 & \alpha^3 \\ 1 & \alpha^{11} & \alpha^7 & \alpha^3 & \alpha^{14} & \cdots & \alpha^8 & \alpha^4 \\ 1 & \alpha^{10} & \alpha^5 & 1 & \alpha^{10} & \cdots & \alpha^{10} & \alpha^5 \end{bmatrix}.$$

No caso do código $GBCH$, $j = 1, 2, 3$, a matriz verificação de paridade do código H_{GBCH} é dada por

$$H_{GBCH} = \begin{bmatrix} \frac{\alpha^0}{\alpha^0\alpha^0} & \frac{\alpha}{\alpha^3\alpha} & \frac{\alpha^2}{\alpha^6\alpha^2} & \frac{\alpha^3}{\alpha^9\alpha^3} & \frac{\alpha^4}{\alpha^{12}\alpha^4} & \cdots & \frac{\alpha^{13}}{\alpha^9\alpha^{13}} & \frac{\alpha^{14}}{\alpha^{12}\alpha^{14}} \\ \frac{\alpha^0}{\alpha^0\alpha^0} & \frac{\alpha^1}{\alpha^3\alpha^2} & \frac{\alpha^2}{\alpha^6\alpha^4} & \frac{\alpha^3}{\alpha^9\alpha^6} & \frac{\alpha^4}{\alpha^{12}\alpha^8} & \cdots & \frac{\alpha^{13}}{\alpha^9\alpha^{11}} & \frac{\alpha^{14}}{\alpha^{12}\alpha^{13}} \\ \frac{\alpha^0}{\alpha^0\alpha^0} & \frac{\alpha}{\alpha^3\alpha^3} & \frac{\alpha^2}{\alpha^6\alpha^6} & \frac{\alpha^3}{\alpha^9\alpha^9} & \frac{\alpha^4}{\alpha^{12}\alpha^{12}} & \cdots & \frac{\alpha^{13}}{\alpha^9\alpha^9} & \frac{\alpha^{14}}{\alpha^{12}\alpha^{12}} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & \cdots & \alpha^6 & \alpha^3 \\ 1 & \alpha^{11} & \alpha^7 & \alpha^3 & \alpha^{14} & \cdots & \alpha^8 & \alpha^4 \\ 1 & \alpha^{10} & \alpha^5 & 1 & \alpha^{10} & \cdots & \alpha^{10} & \alpha^5 \end{bmatrix}.$$

Portanto, as duas matrizes são iguais.

Podemos ver também que, se a matriz do código de Goppa for dada por

$$H_{GP} = \left\| G^{-1}(\alpha^{-i})\alpha^{-ij} \right\|, \ i = 0, 1, \cdots, n-1, \ j = 0, 1, \cdots, \deg G(z) - 1,$$

então a matriz do código $GBCH$ associada a $(z^{n-1}, G(z))$ será dada por

$$H_{GBCH} = \left\| p_i g^{-1} \alpha^{-ij} \right\| = \left\| \alpha^i G^{-1}(\alpha^{-i})\alpha^{-ij} \right\|, \ j = 1, \cdots, \deg G(z).$$

Portanto, temos que $H_{GBCH} = H_{GP}$.

Códigos de Srivastava

Considerando que os códigos de Goppa contém os códigos de Srivastava, então os códigos de Srivastava são também códigos $GBCH$. Esta relação pode ser ilustrada como segue. Suponha que, para $j = 1, \cdots, \tau$,

$$\beta_j \in GF(q^m) - \{\alpha^i \mid_{i=0,1,\cdots n-1}\}$$

são elementos distintos em $GF(q^m)$ e $\tau = \deg G(z)$. Para qualquer inteiro l, o código $GBCH$, C_j, associado a $(z^{n-1}, z - \beta_j)$ é o espaço nulo da matriz

$$H_j = \left\| \frac{\alpha^{il}}{1 - \beta_j \alpha^i} \right\|, \ i = 0, 1, \cdots n-1.$$

Suponha, agora, que $G(z) = \prod_{j=1}^{\tau}(z - \beta_j)$. Então o código associado a $(z^{n-1}, G(z))$ é $\bigcap_{j=1}^{\tau} C_j$. Assim, este código é o espaço nulo da matriz

$$H = \begin{bmatrix} H_1 \\ \vdots \\ H_\tau \end{bmatrix} = \left\| \frac{\alpha^{il}}{1 - \beta_j \alpha^i} \right\|, \ i = 0, 1, \cdots n-1, \ j = 1, \cdots, \tau.$$

Esta matriz define o código de Srivastava. Consequentemente, somente os códigos de Srivastava, com $l = 1$, é que estão contidos na classe dos códigos de Goppa.

2.6 Apêndice

Propriedades de Matrizes

Seja α um elemento primitivo de $GF(q^m)$, raiz de algum polinômio primitivo de grau m e coeficientes em $GF(q)$. Então, todo elemento de $GF(q^m)$ pode ser expresso como uma expressão polinomial em α de grau, no máximo, $m-1$, com coeficientes em $GF(q)$.

Agora, se H é uma matriz de l linhas e n colunas com elementos em $GF(q^m)$, cada elemento pode ser representado por m coeficientes de seu polinômio correspondente organizado em uma coluna. Dessa maneira, dizemos que H se expande para uma matriz de ml linhas e n colunas, cujas linhas são n-uplas de elementos em $GF(q)$. O espaço linha V de H é o conjunto de todas as combinações lineares das linhas de H sobre $GF(q)$ e formam um subespaço vetorial cuja dimensão é igual ao número de linhas linearmente independentes em H.

O conjunto V satisfaz as seguintes propriedades:

i) V é invariante sob permutações de linhas de H;

ii) V é invariante sob a multiplicação dos elementos de uma linha de H por qualquer elemento não-nulo de $GF(q^m)$;

iii) V é invariante sob a adição de uma linha de H com um múltiplo de uma linha de H em $GF(q^m)$;

iv) V é invariante sob a operação de elevar a q-ésima potência, os elementos de uma linha H;

v) V é invariante sob a pré-multiplicação de H em $GF(q)$ por qualquer matriz não-singular $l \times l$ em $GF(q)$.

Omitiremos as demonstrações das propriedades acima, pois as mesmas não apresentam dificuldades.

Capítulo 3

Polinômios, Curvas e Superfícies de Riemann

O nosso objetivo principal neste capítulo é apresentar uma proposta de construção de curvas algébricas através de polinômios absolutamente irredutíveis sobre corpos finitos. Os mesmos serão utilizados nos processos de localização e de determinação da magnitude dos erros dos algoritmos de decodificação de códigos alternantes que apresentaremos no Capítulo 4. Apresentaremos também, algums exemplos de curvas algébricas com número máximo de pontos racionais definidas por esta construção. Na Seção 3.1, definiremos corpos algebricamente fechados. Na Seção 3.2, definiremos polinômios irredutíveis, absolutamente irredutíveis, apresentaremos o critério de Eisenstein para caracterizar polinômios absolutamente irredutíveis, e concluíremos a seção com a proposta de construção de polinômios absolutamente irredutíveis sobre corpos finitos. Na Seção 3.3, definiremos espaço afim e conjunto algébrico, curvas algébricas planas, gênero de uma curva, espaço projetivo e resolução de singularidades. Na Seção 3.4, definiremos pontos racionais e número de pontos racionais, apresentaremos as principais curvas algébricas mais conhecidas. Na Seção 3.5, apresentaremos as curvas associadas aos resultados obtidos na Seção 3.2 sobre corpos finitos. Apresentaremos algums exemplos de curvas com número máximo de pontos racionais. Na Seção 3.6, definiremos superfície de Riemann através do polinômio $f(x, y)$ e apresentaremos a relação entre superfície de Riemann compacta e curvas algébricas.

3.1 Corpos Algebricamente Fechados

Um corpo $\mathbb{K}$ é **algebricamente fechado** se todo polinômio em $\mathbb{K}[X]$ tem raiz em $\mathbb{K}$.

Por exemplo, o corpo $\mathbb{K} = GF(2)$ não é algebricamente fechado, pois $x^2 + x + 1$ é irredutível sobre $GF(2)$. Similarmente, $\mathbb{Q}$ e $\mathbb{R}$ não são algebricamente fechados, já que x^2+1 é irredutível sobre estes corpos. Porém, $\mathbb{C}$ é algebricamente fechado. Essa afirmação é o Teorema Fundamental da Álgebra.

Dado um corpo $\mathbb{K}$, é freqüentemente conveniente olhar para um corpo algebricamente fechado que contém $\mathbb{K}$.

Seja $\mathbb{K}$ um corpo. O **fecho algébrico** de $\mathbb{K}$ é um corpo $\mathcal{K}$ com $\mathbb{K} \subseteq \mathcal{K}$ satisfazendo

(i) $\mathcal{K}$ é algebricamente fechado, e

(*ii*) Se $\mathbb{L}$ é um corpo tal que $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathcal{K}$ e $\mathbb{L}$ é algebricamente fechado, então $\mathbb{L} = \mathcal{K}$.

Em outras palavras, um fecho algébrico de $\mathbb{K}$ é o "menor"corpo algebricamente fechado que contém $\mathbb{K}$. Como consequência, resulta o seguinte teorema.

Teorema 3.1.1 *[58] Todo corpo tem um único fecho algébrico.*

Notação 3.1.2 *Denotaremos de agora em diante $\mathcal{K}$ por $\overline{\mathbb{K}}$, isto é, $\mathcal{K} = \overline{\mathbb{K}}$.*

Por exemplo, $\overline{\mathbb{R}} = \mathbb{C}$. Por outro lado, é conhecido que π, por exemplo, não é a raiz de um polinômio sobre $\mathbb{Q}$, assim $\overline{\mathbb{Q}} \subset \mathbb{C}$ mas $\overline{\mathbb{Q}} \neq \mathbb{C}$. Também $\overline{GF(4)} = \overline{GF(2)}$ e, em geral, $\overline{GF(p^n)} = \overline{GF(p)}$.

O próximo teorema fornece uma propriedade fundamental de corpos algebricamente fechados.

Teorema 3.1.3 *[58] Seja $\mathbb{K}$ um corpo algebricamente fechado e seja $f(x) \in \mathbb{K}[x]$ um polinômio de grau n, então, existem $u \in \mathbb{K}^* := \mathbb{K}\backslash\{0\}$ e $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ (não necessariamente distintos) tais que $f(x) = u(x - \alpha_1)\ldots(x - \alpha_n)$. Em particular, contando multiplicidade, f tem exatamente n raízes em $\mathbb{K}$.*

Demonstração. Indução em n. Se $n = 0$, então f é constante, assim $f \in \mathbb{K}^*$. Assuma agora que todo polinômio de grau n pode ser escrito na forma do Teorema 3.1.3, e $f(x) \in \mathbb{K}[x]$ tem grau $n+1$. Então, como $\mathbb{K}$ é algebricamente fechado, f tem uma raiz α. Agora temos que $f(x) = (x - \alpha)g(x)$ para algum $g(x) \in \mathbb{K}[x]$ de grau n. Por hipótese, podemos escrever $g(x)$ na forma desejada, assim dando uma expressão apropriada para $f(x)$. ∎

Teorema 3.1.4 *[58] Todo corpo finito $GF(q)$ com $q = p^m$ elementos pode ser unicamente definido no fecho algébrico $\overline{GF(p)}$ do corpo $GF(p)$ como o corpo de raízes do polinômio $x^q - x$. Todo corpo finito é isomorfo a um e somente um dos corpos $GF(q)$.*

3.2 Irredutibilidade de Polinômios

Um polinômio

$$f(x, y) = f_0(x)y^n + f_1(x)y^{n-1} + \cdots + f_n(x),$$

em $\mathbb{K}[x, y]$, é chamado **redutível** se existem polinômios g e h tal que

$$f(x, y) = g(x, y)h(x, y),$$

com $1 \leq \deg(g(x, y)), \deg(h(x, y)) < \deg(f(x, y))$. Caso contrário, **irredutível.**

Os polinômios x, y e $x - y$ são todos irredutíveis. Mais ainda, o polinômio $x^3y + y^3 + x$ é irredutível sobre $\mathbb{Z}_2$.

O polinômio $f(x, y)$ com coeficientes no corpo $\mathbb{K}$ é dito ser **absolutamente irredutível** se $f(x, y)$ é irredutível sobre qualquer extensão algébrica do corpo $\mathbb{K}$, isto é, $f(x, y)$ é irredutível em $\overline{\mathbb{K}}$.

Os únicos polinômios da forma $f(x)$, que são absolutamente irredutíveis, têm a forma $f(x) = ax + b$ porque todo polinômio $f(x)$ se decompõe em fatores lineares em alguma extensão finita de corpos.

A proposição a seguir e seu corolário mostram que polinômios absolutamente irredutíveis se comportam mais como polinômios lineares com uma única indeterminada.

Proposição 3.2.1 *[47] Seja $f(x, y)$ um polinômio não-constante sobre um corpo $\mathbb{K}$. Então existe uma extensão finita de corpos $\mathbb{L}$ tal que $f(x, y)$ tem um fator absolutamente irredutível em $\mathbb{L}[x, y]$.*

Demonstração. A prova é por indução no grau de $f(x, y)$. Se o grau é 1, então $f(x, y)$ é absolutamente irredutível. Suponha que a proposição foi provada para todos os graus menores que n e que $f(x, y)$ tem grau n.

Se $f(x, y)$ é absolutamente irredutível não há nada o que provar. Caso contrário, existe uma extensão finita de corpos $\mathbb{J}$ tal que $f(x, y)$ não é irredutível em $\mathbb{J}[x, y]$ (obviamente que $\mathbb{J}$ pode ser $\mathbb{K}$). Então, em $\mathbb{J}[x, y]$,

$$f(x, y) = g(x, y)h(x, y),$$

onde g e h têm grau menor que n e nenhum deles é uma constante. Pela hipótese de indução segue que, para alguma extensão finita de corpos $\mathbb{L}$ de $\mathbb{J}$, $g(x, y)$ tem um fator absolutamente irredutível $p(x, y)$ em $\mathbb{L}[x, y]$. Agora, $p(x, y)$ é também um fator de $f(x, y)$ em $\mathbb{L}[x, y]$ e $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$. Assim, a proposição é verificada para $f(x, y)$ com grau n. ∎

Corolário 3.2.2 *[47] Seja $f(x, y)$ um polinômio não-constante sobre um corpo $\mathbb{K}$. Então existe uma extensão finita de corpos $\mathbb{L}$ tal que $f(x, y)$ se decompõe em um produto de fatores absolutamente irredutíveis em $\mathbb{L}[x, y]$.*

Demonstração. A prova é por indução no grau de $f(x, y)$. Se $f(x, y)$ é absolutamente irredutível não há nada que provar. Este é sempre o caso se $n = 1$. Caso contrário, pela Proposição 3.2.1, existe uma extensão finita de corpos $\mathbb{J}$ de $\mathbb{K}$ tal que

$$f(x, y) = p(x, y)q(x, y), \tag{3.1}$$

em $\mathbb{J}[x, y]$ e $p(x, y)$ é absolutamente irredutível. Então, o grau de $q(x, y)$ é menor que n e, assim, pela hipótese de indução, existe uma extensão finita de corpos $\mathbb{L}$ de $\mathbb{J}$ tal que $q(x, y)$ se divide em fatores absolutamente irredutíveis sobre $\mathbb{L}$. Então, pela equação (3.1), o mesmo acontece com $f(x, y)$. ∎

A proposição a seguir, que é um caso especial do critério de Eisenstein, fornece um modo fácil para construir polinômios absolutamente irredutíveis. O critério não é um meio necessário, porém existem muitos polinômios que o satisfaz (incluindo quase todos os exemplos considerados neste trabalho).

Proposição 3.2.3 (Critério de Eisenstein) *[47] Seja $f(x, y) \in \mathbb{K}[x, y]$ escrito como*

$$f(x, y) = \sum_{i=0}^{n} f_{n-i}(x)y^i.$$

Suponha que $mdc(f_0(x), f_1(x), \ldots, f_n(x)) = 1$ *e que exista um elemento* $\zeta \in \mathbb{L}$ *para alguma extensão de* $\mathbb{K}$ *tal que*

(*i*) ζ *não é raiz de* $f_0(x)$;

(*ii*) ζ *é uma raiz de* $f_{n-i}(x)$ *para todo* $i < n$; *e*

(*iii*) ζ *não é uma raiz dupla de* $f_n(x)$.

Então $f(x, y)$ *é absolutamente irredutível.*

Demonstração. Suponha que para alguma extensão $\mathbb{J}$ de $\mathbb{K}$, o polinômio $f(x, y)$ seja fatorável não-trivialmente. Seja $f(x, y) = g(x, y)h(x, y)$, onde $g(x, y) = \sum^r g_i(x)y^i$ e $h(x, y) = \sum^s h_i(x)y^i$, com $0 < r, s \leq n$ e $r + s = n$. Então, essa fatoração também será não-trivial em qualquer extensão finita de $\mathbb{J}$. Assim, podemos assumir que $\zeta \in \mathbb{J}$.

Como ζ não é uma raiz dupla de $f_n(x) = g_0(x)h_0(x)$, ela é uma raiz de um dos dois polinômios, isto é, de $g_0(x)$ ou de $h_0(x)$. Assumiremos que $g_0(\zeta) = 0 \neq h_0(\zeta)$. Se ζ não é uma raiz de $f_0(x) = g_r(x)h_s(x)$, então não será uma raiz nem de $g_r(x)$ e nem de $h_s(x)$. Agora, seja $k > 0$ o menor índice tal que ζ não é uma raiz de $g_k(x)$ e considere o coeficiente $f_{n-k}(x)$ como sendo

$$f_{n-k}(x) = \sum_{i=0}^{k} g_i(x)h_{k-i}(x) = g_k(x)h_0(x) + \sum_{i=0}^{k-1} g_i(x)h_{k-i}(x).$$

Se $k < n$, ζ é uma raiz de $f_{n-k}(x)$. Também é, pela definição de k, uma raiz de $g_i(x)$ para todo $i < k$, mas ζ não é uma raiz de $g_k(x)$ ou $h_0(x)$. Assim,

$$0 = f_{n-k}(\zeta) = g_k(\zeta)h_0(\zeta) + \sum_{i=0}^{k-1} g_i(\zeta)h_{k-i}(\zeta) = g_k(\zeta)h_0(\zeta) + 0 \neq 0.$$

Esta contradição prova que $k = n$. Como $f(x, y)$ não tem coeficientes $f_i(x)$ para $i > n$, segue que $h(x, y) = h_0(x)$. Conseqüentemente, $h_0(x)$ divide todo polinômio $f_i(x)$ para $i = 1, ..., n$. Do fato de que o maior fator comum entre os coeficientes $f_i(x)$, $0 \leq i \leq n$, é 1 implica que $h_0(x)$ é uma constante. Assim, em qualquer fatoração de $f(x, y)$, sobre qualquer extensão finita de $\mathbb{J}$, um dos fatores é uma constante, mostrando que $f(x, y)$ é absolutamente irredutível. ∎

Corolário 3.2.4 *[47] Existe um número infinito de polinômios absolutamente irredutíveis sobre qualquer corpo.*

Demonstração. Pela Proposição 3.2.3 (com $\zeta = 0$) todos os polinômios da forma $y^n - x$ são absolutamente irredutíveis. ∎

Observamos que o polinômio $y^2 - x$ é absolutamente irredutível sobre $\mathbb{R}$. Por outro lado, o polinômio $x^2 + y^2 - 1 = [y + (x + 1)][y + (x + 1)]$ sobre $GF(2)$ é redutível e, portanto, não atende ao critério de Eisenstein.

Consideremos agora a curva $x^3y+y^3+x=0$. Pelo critério de Eisenstein, este polinômio é absolutamente irredutível sobre $GF(2)$, quando a raiz $\zeta = 0$. Observe que no polinômio

$$f(x,y) = f_0(x)y^3 + f_1(x)y^2 + f_2(x)y + f_3(x),$$

temos que $f_0(x) = 1$, $f_1(x) = 0$, $f_2(x) = x^3$ e $f_3(x) = x$. Como $f_3(x) = x$ tem grau 1, então $\zeta = 0$ é a única raiz de $f_3(x)$ e satisfaz *iii)*. Como $\zeta = 0$ é raiz de f_1 e f_2 satisfaz *ii)*. Como $\zeta = 0$ não é raiz de f_0 satisfaz *i)*, logo $f(x,y)$ é absolutamente irredutível pelo critério de Eisenstein.

Pelo mesmo critério, a curva cúbica $x^3 + y^3 + 1 = 0$ é um polinômio absolutamente irredutível sobre $GF(2)$, considerando a raiz $\zeta = 1$. Observamos que no polinômio

$$f(x,y) = f_0(x)y^3 + f_1(x)y^2 + f_2(x)y + f_3(x),$$

temos que $f_3(x) = x^3+1$, $f_1(x) = f_2(x) = 0$ e $f_0(x) = 1$. Como $x^3+1 = (x+1)(x^2+x+1)$, então $\zeta = 1$ não é raiz dupla de $f_3(x)$. Portanto, satisfaz *i)*, *ii)* e *iii)* da Proposição 3.2.3.

De modo análogo, deduzimos que a curva quíntupla $x^5 + y^5 + 1 = 0$ é um polinômio absolutamente irredutível sobre $GF(2)$, considerando a raiz $\zeta = 1$. Observamos que no polinômio

$$f(x,y) = f_0(x)y^5 + f_1(x)y^4 + f_2(x)y^3 + f_3(x)y^2 + f_4(x)y + f_5(x),$$

temos que $f_5(x) = x^5 + 1$, $f_1(x) = f_2(x) = f_3(x) = f_4(x) = 0$ e $f_0(x) = 1$. Como $x^5 + 1 = (x+1)(x^4 + x^3 + x^2 + x + 1)$, então $\zeta = 1$ não é raiz dupla de $f_0(x)$. Portanto, satisfaz *i)*, *ii)* e *iii)* da Proposição 3.2.3.

Apresentamos agora, uma outra construção de polinômios absolutamente irredutíveis sobre corpos finitos.

Sejam $a_1, a_2, \ldots, a_n$, onde $a_i \in GF(q)$ e $n \leq q$, definidos através da equação

$$(Y - Y_1)(Y - Y_2)\ldots(Y - Y_n) = Y^n + a_1Y^{n-1} + \cdots + a_{n-1}Y + a_n$$

sobre $GF(q)$, onde

$$\begin{aligned} a_1 &= \textstyle\sum_{i=1}^{n} Y_i \\ a_2 &= \textstyle\sum_{i<j} Y_iY_j \\ a_3 &= \textstyle\sum_{i<j<k} Y_iY_jY_k \\ &\vdots \\ a_n &= Y_1Y_2\ldots Y_n = \textstyle\prod_{i=1}^{n} Y_i. \end{aligned} \tag{3.2}$$

Esses valores são conhecidos como as **funções simétricas elementares** de Y_i. Observamos que, se nem todos os Y_i's são nulos, então existe pelo menos um $a_i \neq 0$. Suponha que $a_i = 0$ para todo i, então provaremos, por indução, que os Y_i's são todos nulos. Tomando $a_n = 0$, isto é, $Y_1Y_2\ldots Y_n = 0$, sem perda de generalidade, podemos assumir que $Y_n = 0$. Suponha, agora, que é sempre verdade que $Y_i = 0$ para $1 < i \leq n$. Assim, para $a_1 = Y_1 + Y_2 + \ldots + Y_n = 0$, temos que $Y_1 = 0$. Portanto, se $a_i = 0$ para todo i, então os Y_i's são todos nulos.

Definição 3.2.5 *Seja $f(x,y)$ um polinômio a duas variáveis (x,y) sobre o corpo $GF(q)$ definido por*

$$f(x,y) = y^n + f_{j,b}(x)\sum_{i=j}^{n} g_i(x)y^{n-i}, \qquad \text{(Chavel)}$$

onde $j = \min\{k \in \{1,2,\ldots,n\}; a_k \neq 0\}$, $f_{j,b}(x) = x - b + a_j$, $b \in GF(q)$,

$$h_i(x) = \rho(x-b) + \frac{a_i}{a_j} - b^{i-1}, \rho = \begin{cases} 0, & se \begin{cases} i < n \quad ou\ i = n \quad e \\ \frac{a_n}{a_j} - b^{n-1} \neq -(b-a_j)^{n-1} \end{cases} \\ 1, & se\ i = n \quad e \quad \frac{a_n}{a_j} - b^{n-1} = -(b-a_j)^{n-1} \end{cases} \quad e$$

$g_i(x) = x^{i-1} + h_i(x), \quad i = j,\ldots,n.$

Teorema 3.2.6 *O polinômio da Definição 3.2.5, para $n > 0$ e $n \neq 2$, é absolutamente irredutível.*

Demonstração. Seja $\zeta = (b - a_j)$. Observe que ζ não é raiz de $p_0(x) = 1$, mas é raiz de $p_i(x) = f_{j,b}(x)g_i(x)$ para $j \leq i \leq n$, logo satisfaz (i) e (ii) da Proposição 3.2.3. Vamos provar agora que ζ não é raiz dupla de $p_n(x)$, isto é, não é raiz de $g_n(x)$. A prova será dividida em duas partes:

(i) Suponha que $a_n/a_j - b^{n-1} \neq -(b-a_j)^{n-1}$, $\rho = 0$ e que ζ é raiz de $g_n(x)$. Desta forma, calculando $g(\zeta) = g(b-a_j) = (b-a_j)^{n-1} + a_n/a_j - b^{n-1} = 0$, temos que $a_n/a_j - b^{n-1} = -(b-a_j)^{n-1}$, contradição. Logo, $f(x,y)$ é absolutamente irredutível pelo critério de Eisenstein.

(ii) De modo análogo, supondo que $a_n/a_j - b^{n-1} = -(b-a_j)^{n-1}$ e $\rho = 1$, devemos ter que ζ não é raiz de $g_n(x)$. Vamos supor que ζ é raiz de $g_n(x)$, consequentemente $g(\zeta) = g(b-a_j) = (b-a_j)^{n-1} + (b - a_j - b) + a_n/a_j - b^{n-1} = 0$, logo $a_j = 0$. Absurdo, pois $a_j \neq 0$ para algum j. Assim, $f(x,y)$ é absolutamente irredutível pelo critério de Eisenstein

Portanto, $f(x,y)$ é absolutamente irredutível pelo critério de Eisenstein. ∎

Como exemplos de polinômios absolutamente irredutíveis construídos a partir da Definição 3.2.5, citamos os seguintes:

1) Consideremos $\mathbb{K} = GF(9)$ como sendo o corpo de Galois gerado por α, raiz de $x^2 + 2x + 2 = 0$. Sejam $a_1 = 1, a_2 = 2, a_3 = 1, a_4 = 2$ e $b = 0$. Como $j = \min\{k \in \{1,2,3,4\}; a_k \neq 0\} = 1$ e $a_4/a_1 - b^3 = 2 \neq -(b-a_1)^3 = 1$, então temos pelo polinômio (Chavel), que $f_1(x) = x + a_1 - b = x + 1 - 0 = x + 1$, $g_1(x) = 1 + 0 = 1$, $g_2(x) = x + a_2/a_1 - b = x + 2$, $g_3(x) = x^2 + a_3/a_1 - b^2 = x^2 + 1$ e $g_4(x) = x^3 + a_4/a_1 - b^3 = x^3 + 2$. Assim,

$$f(x,y) = y^4 + (x+1)y^3 + (x+1)(x+2)y^2 + (x+1)(x^2+1)y + (x+1)(x^3+2)$$

é absolutamente irredutível sobre $GF(9)$, com $\zeta = 1$.

2) Consideremos $\mathbb{K} = GF(16)$ como sendo o corpo de Galois gerado por α, raiz de $x^4 + x + 1 = 0$. Sejam $a_1 = 1, a_2 = 1, a_3 = 0$ e $b = 0$, isto é, a_i,$b \in GF(16)$, $i = 1, 2, 3$. Assim, pelo polinômio (Chave1), temos que $f(x, y) = y^3 + (x + 1)y^2 + (x + 1)(x - 1)y + (x + 1)x^2$. Portanto, $f(x, y)$ é absolutamente irredutível sobre $GF(16)$, com $\zeta = 1$.

3) Sejam $a_1 = 1, a_2 = 0, a_3 = 0$ e $b = 1$, isto é, a_i,$b \in GF(16)$, $i = 1, 2, 3$, assim, pelo polinômio (Chave1), temos que $f(x, y) = y^3 + xy^2 + x(x - 1)y + x^3 - x$. Portanto, $f(x, y)$ é absolutamente irredutível sobre $GF(16)$, com $\zeta = 0$.

4) Sejam $a_1 = 0, a_2 = 0, a_3 = 1$ e $b = 1$, isto é, a_i,$b \in GF(16)$, $i = 1, 2, 3$, logo, pelo polinômio (Chave1), temos que $f(x, y) = y^3 + x^3 + x^2 - x$. Portanto, $f(x, y)$ é absolutamente irredutível sobre $GF(16)$, com $\zeta = 0$.

Teorema 3.2.7 *O polinômio*

$$f(x, y) = y^2 + f_1(x)y + g(x),$$

com $f_1(x) = x + c_1 - b$, *é absolutamente irredutível se uma das condições abaixo for satisfeita:*

(i) $g(x) = (x + c_1 - b)(x + c_2/c_1 - b)$, *se* $c_1 \neq 0$ *e* $c_2 \neq c_1^2$;

(ii) $g(x) = (x + c_1 - b)c_1$, *se* $c_1 \neq 0$ *e* $c_2 = c_1^2$;

(iii) $g(x) = (x + c_2 - b)$, *se* $c_1 = 0$.

Demonstração. Usando o fato de que $c_1 \neq 0$, então temos duas situações a considerar: *i)* $c_2 \neq c_1^2$; e *ii)* $c_2 = c_1^2$. Para ambas as situações, a Proposição 3.2.3 mostra que $f(x, y)$ é absolutamente irredutível.

Considerando agora $c_1 = 0$, temos duas situações a considerar: *i)* $c_2 \neq 0$; e *ii)* $c_2 = 0$. Para *i)* temos que

$$f(x, y) = y^2 + (x - b)y + (x + c_2 - b)$$

é absolutamente irredutível, visto que, não existe dois polinômios $h_1 = d_1x + e_1$ e $h_2 = d_2x + e_2$, tais que $h_1 + h_2 = x - b$ e $h_1h_2 = x + c_2 - b$. Agora, para *ii)*, temos que

$$f(x, y) = y^2 + (x - b)y + (x - b),$$

logo, $f(x, y)$ é absolutamente irredutível pela Proposição 3.2.3.

Portanto, $f(x, y)$ é absolutamente irredutível sobre qualquer corpo $GF(q)$, se uma das três condições for satisfeita. ∎

Proposição 3.2.8 *O polinômio*

$$f(x, y) = y^2 + f_1(x)y + g(x), \qquad \text{(Chave2)}$$

tal que um dos a_i*'s é diferente de zero, é absolutamente irredutível se uma das condições abaixo for satisfeita:*

(*i*) $f_1(x) = x + a_1 - b$ e $g(x) = (x + a_1 - b)(x + a_2/a_1 - b)$, *se* $a_1 \neq 0$ *e* $a_2 \neq a_1^2$;

(*ii*) $f_1(x) = x + a_1 - b$ e $g(x) = (x + a_1 - b)a_1$, *se* $a_1 \neq 0$ *e* $a_2 = a_1^2$;

(*iii*) $f_1(x) = 0$ *e* $g(x) = (x + a_2 - b)$, *se* $a_1 = 0$.

Demonstração. Pelo Teorema 3.2.7, temos que as condições (*i*) e (*ii*) mostram que $f(x, y)$ é absolutamente irredutível. Considerando agora, $a_1 = 0$ e $a_2 \neq 0$, temos que

$$f(x, y) = y^2 + (x + a_2 - b),$$

que é absolutamente irredutível, pela Proposição 3.2.3.

Portanto, $f(x, y)$ é absolutamente irredutível sobre qualquer corpo $GF(q)$, se uma das três condições é satisfeita. ∎

Por exemplo, considerando o corpo de Galois $GF(16)$ e $a_1 = \alpha$, $a_2 = \alpha^4$, $b = \alpha$. Como $a_2 \neq a_1^2$ e $a_1 \neq 0$, temos pela Proposição 3.2.8, que $f_1(x) = x + a_1 - b = x + \alpha - \alpha = x$ e $g(x) = (x + a_2/a_1 - b)(x + a_1 - b) = (x + \alpha^3 - \alpha)(x + \alpha - \alpha) = (x + \alpha^9)x$. Portanto, $f(x, y)$ é dado por

$$f(x, y) = y^2 + xy + (x + \alpha^9)x.$$

Dessa forma, pela Proposição 3.2.3, este polinômio é absolutamente irredutível sobre $GF(16)$, com $\zeta = 0$.

Considere agora, o corpo de Galois $GF(9)$ e $a_1 = 1$, $a_2 = \alpha^4$, $b = \alpha$. Como $a_2 \neq a_1^2$ e $a_1 \neq 0$, temos pela Proposição 3.2.8, que $f_1(x) = x + a_1 - b = x + 1 - \alpha = x + 1 + 2\alpha = x + \alpha^3$ e

$$g(x) = (x + a_2/a_1 - b)(x + a_1 - b) = (x + \alpha^4 - \alpha)(x + 1 - \alpha)$$
$$g(x) = (x + \alpha^4 + 2\alpha)(x + 1 + 2\alpha) = (x + \alpha^6)(x + \alpha^3).$$

Portanto, $f(x, y)$ é dado por

$$f(x, y) = y^2 + (x + \alpha^3)y + (x + \alpha^6)(x + \alpha^3).$$

Desse modo, pela Proposição 3.2.3, este polinômio é absolutamente irredutível sobre $GF(9)$, com $\zeta = \alpha^3$.

Observação 3.2.9 *Os polinômios (Chave1) e (Chave2), podem ser colocados sob a forma* $f(x, y) = x^n + y^n + g(x, y)$, *onde o grau de* $g(x, y)$ *é menor ou igual a* n.

3.3 Curvas Algébricas

A descoberta da conexão entre a Teoria da Equação Diofantina e outros campos da matemática, como álgebra, geometria e análise, teve início no século XIX. Isso foi comprovado pelas investigações executadas por Lagrange, Gauss, Dirichlet e Hermite na Teoria de formas quadráticas, investigações estas que culminaram na criação da aritmética de corpos quadráticos e serviram como uma base para aproximar grupos de matemáticos. Exemplos disso são os trabalhos de Kummer, que estudou a equação de Fermat $x^n + y^n = z^n$ e teve como resultado a criação da aritmética de corpos ciclotômicos, desenvolvendo, assim, a Teoria de Ideais para os corpos de números algébricos. Finalmente, os resultados

de Jacobi, relativos à aplicação dos teoremas de Euler e Abel na composição de integrais elípticas e abelianas para a adição de pontos racionais em curvas algébricas, estenderam os fundamentos para a aritmética de variedades Abelianas. Ao mesmo tempo, uma analogia próxima foi descoberta entre os corpos de números algébricos e os de funções algébricas, que conduziu, por um lado, à criação da teoria aritmética de corpos de funções e, por outro, à introdução em aritmética de números p-ádicos (Hensel), que representa a parte da expansão de Puiseus para as funções algébricas em corpos de números. Assim, os fundamentos foram estendidos para a álgebra comutativa em termos da geometria algébrica moderna[1].

Dado um polinômio com coeficientes inteiros ou racionais (uma equação Diofantina), um problema fundamental na Teoria dos Números é encontrar soluções desta equação que sejam inteiras, inteiras positivas, ou racionais. Por exemplo, o último Teorema de Fermat (recentemente provado por *Andrew Wiles*) mostra que não existe solução (x, y, z) inteira positiva para a equação $x^n + y^n = z^n$, quando $n \geq 3$. Kummer fez o seguinte: a equação de Fermat $x^n + y^n = z^n$ pode ser reescrita na forma produto

$$x^n = (z - y)(z - \zeta_n y) \ldots (z - \zeta_n^{n-1} y),$$

onde ζ_n é a raiz n-ésima primitiva da unidade $\cos(2\pi/n) + i \sin(2\pi/n)$, e descobriu que em $\mathbb{Z}[\zeta_n]$ existe uma lei chamada de fatoração única em ideais principais que substitui a fatoração única em números primos. Essa descoberta abriu caminho para a Teoria de Números Algébricos, possibilitando provar parcialmente o último Teorema de Fermat para valores de n relativamente grandes. Esse problema é freqüentemente abordado com relação às equações Diofantinas, com o objetivo de encontrar soluções geométricas através das equações módulo p. Se $f(x, y) = 0$ for um polinômio em duas variáveis, então a equação $f(x, y) = 0$ define uma curva $\mathcal{X}_f$ no plano. Por exemplo, as únicas soluções racionais para a curva elíptica $y^2 = x^3 - x$ são $(x, y) = (0, 0)$ e $(\pm 1, 0)$. Isso nos faz considerar neste trabalho **curvas algébricas** e **curvas algébricas sobre corpos finitos.**

3.3.1 Espaço Afim e Conjunto Algébrico

Seja $\mathbb{K}$ um corpo qualquer. Denotaremos por $\mathcal{A}^n(\mathbb{K})$, ou simplesmente por $\mathcal{A}^n$ (se $\mathbb{K}$ está subentendido), o **produto cartesiano** de n cópias de $\mathbb{K}$, isto é, $\mathcal{A}^n(\mathbb{K})$ é o conjunto das n-uplas de elementos de $\mathbb{K}$. $\mathcal{A}^n(\mathbb{K})$ é chamado o **espaço afim de dimensão** n **sobre** $\mathbb{K}$ e seus elementos são chamados **pontos.** $\mathcal{A}^1(\mathbb{K})$ é a reta afim.

Seja $f \in \mathbb{K}[X_1, X_2, \ldots, X_n]$. Um ponto $P = (a_1, \ldots, a_n) \in \mathcal{A}^n(\mathbb{K})$ é um zero de f se $f(P) = f(a_1, \ldots, a_n) = 0$. Se f não é uma constante, o conjunto de zeros de f é chamado a **variedade afim ou a hipersuperfície** $\mathtt{V}(f)$ **definida por** f e é, então, dada por

$$\mathtt{V}(f) = \{P \in \mathcal{A}^n \mid f(P) = 0\}.$$

Em outras palavras, uma variedade afim $\mathtt{V}(f) \subset \mathcal{A}^n$ é o conjunto de soluções para a equação $f(x_1, \ldots, x_n) = 0$.

Seja $\mathbb{K}$ um corpo. O plano afim sobre $\mathbb{K}$ é $\mathcal{A}^2(\mathbb{K}) = \mathbb{K}^2$.

[1] Para maiores detalhes veja [58].

Uma variedade afim em $\mathcal{A}^2(\mathbb{K})$ é chamada uma **curva plana afim**. Se f é um polinômio de grau 1, $\mathtt{V}(f)$ é chamado um **hiperplano** em $\mathcal{A}^n(\mathbb{K})$.

Considerando $\mathbb{K} = \mathbb{R}$, temos os seguintes exemplos:

a) $\mathtt{V}(Y^2 - X(X^2 - 1)) \subset \mathcal{A}^2$, mostrado na Figura 3.1-(a).

b) $\mathtt{V}(Y^2 - X^2(X + 1)) \subset \mathcal{A}^2$, mostrado na Figura 3.1-(b).

c) $\mathtt{V}(Z^2 - (X^2 + Y^2)) \subset \mathcal{A}^3$, mostrado na Figura 3.1-(c).

d) $\mathtt{V}(Y^2 - XY - X^2Y + X^3)) \subset \mathcal{A}^2$, mostrado na Figura 3.1-(d).

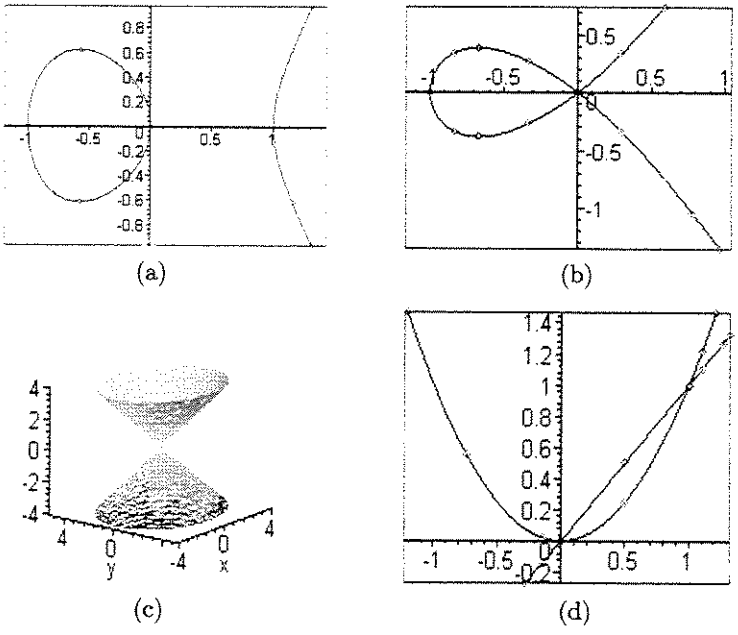


Figura 3.1: *Variedades Afins*

Mais geralmente, se $\mathtt{S}$ é qualquer conjunto de polinômios em $\mathbb{K}[X_1, X_2, \ldots, X_n]$, temos $\mathtt{V}(\mathtt{S}) = \{P \in \mathcal{A}^n \mid f(P) = 0 \text{ para todo } f \in \mathtt{S}\}$. Observe que $\mathtt{V}(\mathtt{S}) = \cap_{f \in S}\mathtt{V}(f)$. Se $\mathtt{S} = \{f_1, \ldots f_r\}$, usualmente escrevemos $\mathtt{V}(f_1, \ldots f_r)$, em vez de $\mathtt{V}(\{f_1, \ldots f_r\})$.

Um subconjunto $\mathbb{X} \subset \mathcal{A}^n(\mathbb{K})$ é um **conjunto algébrico afim**, ou simplesmente um **conjunto algébrico**, se $\mathbb{X} = \mathtt{V}(\mathtt{S})$, para algum $\mathtt{S}$. Se $\mathbb{K}$ é um corpo finito, todo subconjunto de $\mathcal{A}^n(\mathbb{K})$ é algébrico.

3.3.2 Curvas algébricas planas

Suponha que $\overline{\mathbb{K}}$ é um corpo algebricamente fechado e $\mathbb{K}_0$ é um subcorpo de $\overline{\mathbb{K}}$. Denotaremos por $\mathcal{A}^2$ o plano afim sobre $\overline{\mathbb{K}}$ consistindo do conjunto de todos os pares (a, b) de elementos a, b de $\overline{\mathbb{K}}$. Chamamos o par $P = (a, b)$ de um **ponto do plano** $\mathcal{A}^2$ e os elementos a e b, as **coordenadas do ponto** P.

Uma **curva algébrica plana** é o conjunto de todos os pontos $P = (a, b) \in \mathcal{A}^2$ cujas coordenadas satisfazem a equação

$$f(x, y) = 0, \tag{3.3}$$

onde $f(x, y)$ é um polinômio com coeficientes sobre $\overline{\mathbb{K}}$. Se os coeficientes do polinômio $f(x, y)$ pertencem a $\mathbb{K}_0$, então dizemos que a curva (3.3) é definida sobre $\mathbb{K}_0$.

As soluções simultâneas para duas equações polinomiais em duas variáveis, é a interseção destas duas curvas. Em particular, consideremos $f(x, y) = y - x^2$ e $g(x, y) = y - c$ para várias escolhas de c. Se considerarmos $\mathbb{K} = \mathbb{R}$, sabemos qual é o gráfico dessas duas equações e procuramos os pontos de interseção. Observamos que, às vezes, têm exatamente 2 pontos de interseção. Isso acontece, por exemplo, se $c = 4$. Se $c = 0$, encontramos só um ponto, e se $c < 0$, não encontramos nenhum ponto. Porém, se $c = 0$, as curvas são realmente tangentes no ponto de interseção e podemos dizer que existe um único ponto de multiplicidade 2. Mais adiante, veremos que se estendermos a $\mathbb{K} = \mathbb{C}$, encontramos 2 pontos de interseção exatamente para $c < 0$. Mais geralmente, se considerarmos retas da forma $y = mx + b$, obtemos 2, 1, ou 0 pontos de interseção sobre $\mathbb{R}$ e a situação é como antes. Se houver um ponto de interseção, então a reta é realmente uma reta tangente. Se não houver nenhum ponto de interseção, então encontramos dois pontos quando consideramos $\mathbb{C}$. Observamos que $\mathcal{X}_f$ e $\mathcal{X}_g$ sempre se cruzam em exatamente dois pontos, contando a multiplicidade e estendendo ao fecho algébrico.

Agora, substitua g pela reta vertical definida por $g(x, y) = x - c$. Qual deverá ser o valor de c para que haja só um ponto de interseção e a reta não seja tangente no ponto? A extensão de $\mathbb{R}$ para $\mathbb{C}$ não resolve o problema. Todavia, se o procedimento da contagem das interseções estiver correto deverá ocorrer dois pontos de interseção entre qualquer reta e a curva $\mathcal{X}_f$, onde $f(x, y) = y - x^2$.

Heuristicamente, as curvas $x = c$ e $y = x^2$ se cruzam também uma vez "no infinito". Em geral, uma curva $\mathcal{X}_f$ onde $f(x, y) \in \mathbb{K}[x, y]$ é chamada uma **curva afim**.

Uma **curva algébrica plana afim** (ou mais abreviadamente, **curva**) é uma classe de equivalência definida sobre os polinômios não constantes $f \in \mathbb{K}[x, y]$, onde dois polinômios são **equivalentes** se um é múltiplo do outro por uma constante.

Nesse contexto, a equação de uma curva é qualquer um dos polinômios nessa classse.

Dizemos que uma curva está definida sobre $\mathbb{K}_0$, subcorpo de $\overline{\mathbb{K}}$, se a mesma admite uma equação com coeficientes em $\mathbb{K}_0$.

Em geral, podemos procurar soluções $x, y \in \mathbb{K}_0 = GF(q)$, onde $GF(q)$ é um corpo de extensão de $GF(p)$. Chamamos tal solução de um **ponto na curva** $\mathcal{X}$. Se as coordenadas x e y das soluções de $f(x, y) = 0$ estão, em $GF(q)$, chamamos este ponto de **ponto racional**.

O ponto $P = (a, b)$ da curva (3.3) é um **ponto $\mathbb{K}_0$-racional** se suas coordenadas a, b pertencem a $\mathbb{K}_0 \subset \overline{\mathbb{K}}$. O conjunto das soluções da equação $f(x, y) = 0$ em $\mathbb{K}$ é denotado por $\mathcal{X}_f(\mathbb{K})$.

Se o polinômio $f(x, y)$ pode ser representado como o produto $f = gh$ dos polinômios $g(x, y)$ e $h(x, y)$, então a curva definida pelo polinômio $f(x, y)$ é a união de duas curvas definidas pelas equações $g(x, y) = 0$ e $h(x, y) = 0$. Se o polinômio $f(x, y)$ é irredutível, então a curva definida é **chamada curva irredutível**. Como todo polinômio pode ser fatorado num produto de um número finito de polinômios irredutíveis, segue que,

toda curva algébrica plana, definida sobre $\mathbb{K}_0$, é a união de um número finito de curvas irredutíveis sendo, portanto, suas componentes curvas irredutíveis.

Uma curva é chamada **racional** se é o conjunto de zeros de um polinômio que possui coeficientes racionais. Na terminologia usual de geometria algébrica, uma curva é chamada racional se é isomorfa a reta projetiva $\mathbb{P}^1$.

O **grau da curva irredutível** (3.3) é o grau do polinômio $f(x, y)$ que define a curva. Uma **curva de grau** 1 é uma reta; assim, falamos "da reta $ax + by + c$", ou "da reta $ax + by + c = 0$", que obviamente é uma **curva racional**.

Se $f = \prod f_i^{e_i}$, onde os f_i's são os fatores irredutíveis de f, então os f_i's são as componentes de f e e_i é a multiplicidade da componente f_i. Se $e_i = 1$, então dizemos que f_i é uma **componente simples**, caso contrário, dizemos que f_i é uma **componente múltipla**.

Se f é irredutível, então $\mathtt{V}(f)$ é uma **variedade** em $\mathcal{A}^2$.

Seja $\mathcal{X}_f$ uma curva, $P = (a, b) \in \mathcal{X}_f$. P é chamado um **ponto simples** de $\mathcal{X}_f$ se a derivada $f_X(P) \neq 0$ ou $f_Y(P) \neq 0$. Neste caso, a reta $f_X(P)(X - a) + f_Y(P)(Y - b) = 0$ é chamada a **reta tangente** de $\mathcal{X}_f$ no ponto P. Um ponto que não é simples é chamado **múltiplo** (ou **singular**).

Apresentaremos a seguir alguns exemplos de curvas algébricas planas bem conhecidas:

1) A **reta** que passa pelos pontos (a, b) e (c, d), $(b - d)x + (c - a)y + ad - bc = 0$.

2) O **círculo** de raio r e centro (a, b), isto é, o lugar dos pontos que satisfazem a equação $(X - a)^2 + (Y - b)^2 = r^2$.

3) A **elipse**, lugar dos pontos cujas distâncias a dois pontos fixos (por exemplo $(\pm c, 0)$) têm soma constante $2a$, isto é,

$$\sqrt{(X + c)^2 + Y^2} + \sqrt{(X - c)^2 + Y^2} = 2a. \tag{3.4}$$

Observamos que esta equação não é polinômial, mas é possível eliminar os radicais de (3.4), para obter

$$\frac{X^2}{a^2} + \frac{Y^2}{b^2} = 1. \tag{3.5}$$

Obviamente, (X, Y) é solução de (3.4) se, e somente se, também é solução de (3.5).

4) A **hipérbole**, lugar dos pontos cujas distâncias a dois pontos fixos, chamados focos, têm diferença constante $2a$. Assim, marcando os focos em $(\pm c, 0)$, a diferença das distâncias se expressa por

$$\sqrt{(X - c)^2 + Y^2} - \sqrt{(X + c)^2 + Y^2} = 2a.$$

Como $b^2 = c^2 - a^2$ e eliminando os radicais, obtemos a equação

$$\frac{X^2}{a^2} - \frac{Y^2}{b^2} = 1.$$

5) A **parábola**, lugar dos pontos equidistantes de um ponto fixo, chamado foco e de uma reta fixa, diretriz. Tomando $(0, b)$, $b > 0$ e $Y = -b$ como foco e diretriz, a sua equação é,

$$X^2 = 4bY, \quad \text{ou} \quad f = X^2 - 4bY.$$

6) A **cissóide de Diócles**, cuja equação é dada por

$$bX^2 - Y(Y^2 + X^2) = 0.$$

Tomando $b = 1$, a equação da cissóide é dada por $X^2 - Y(Y^2 + X^2) = 0$, cujo gráfico é mostrado na Figura 3.2 (a).

7) A **cúbica** definida pela equação $Y^2 - X^3 + X = 0$, cujo gráfico é mostrado na Figura 3.2 (b), possui duas componentes reais.

8) A **cúbica cuspidal** (Cúspide = ponto duplo com uma única tangente) definida pela equação $Y^2 - X^3 = 0$, cujo gráfico é mostrado na Figura 3.2 (c).

9) A **cúbica nodal** (Nó = ponto duplo com tangentes distintas) dada pela equação $Y^2 = X^3 + X^2$, cujo gráfico é mostrado na Figura 3.2 (d).

10) A **rosácea de 3 pétalas,** definida pela equação $(X^2 + Y^2)^2 = Y^3 - 3X^2Y$, cujo gráfico é mostrado na Figura 3.2 (e). A origem é um ponto triplo ordinário.

11) A **lemniscata,** definida pela equação $(X^2+Y^2)^2 = X^2-Y^2$, cujo gráfico é mostrado na Figura 3.2 (f), apresenta um nó na origem com tangentes $Y = \pm X$.

12) A **singularidade tacnodal,** definida pela equação $Y^2 - 3X^2Y - Y^3 + X^4 = 0$, cujo gráfico é mostrado na Figura 3.2 (g).

13) A **singularidade real isolada,** definida pela equação $X^2 + Y^2 = X^3$, cujo gráfico é mostrado na Figura 3.2 (h).

Observação 3.3.1 *A Figura 3.2 mostra apenas os gráficos reais das curvas planas, isto é, os pontos das curvas cujas coordenadas são números reais, contudo, o gráfico real dá uma idéia razoável do que está se passando.*

Observação 3.3.2 *Um cálculo com as derivadas mostra que a Figura 3.2 (b) é a única curva não-singular, e que $P = (0, 0)$ é o único ponto múltiplo nas Figuras 3.2 (a), (c), (d), (e), (f), e (g). No primeiro exemplo, o termo linear da equação para a curva é apenas a reta tangente à curva em $(0, 0)$.*

3.3.3 Espaço Projetivo

A idéia original de acrescentar ao plano usual uma reta no infinito, constituindo um plano projetivo, é devida a Desargues. Seu livro foi publicado em 1639 e pretendia dar uma fundamentação matemática aos métodos de perspectiva empregados pelos pintores e arquitetos.

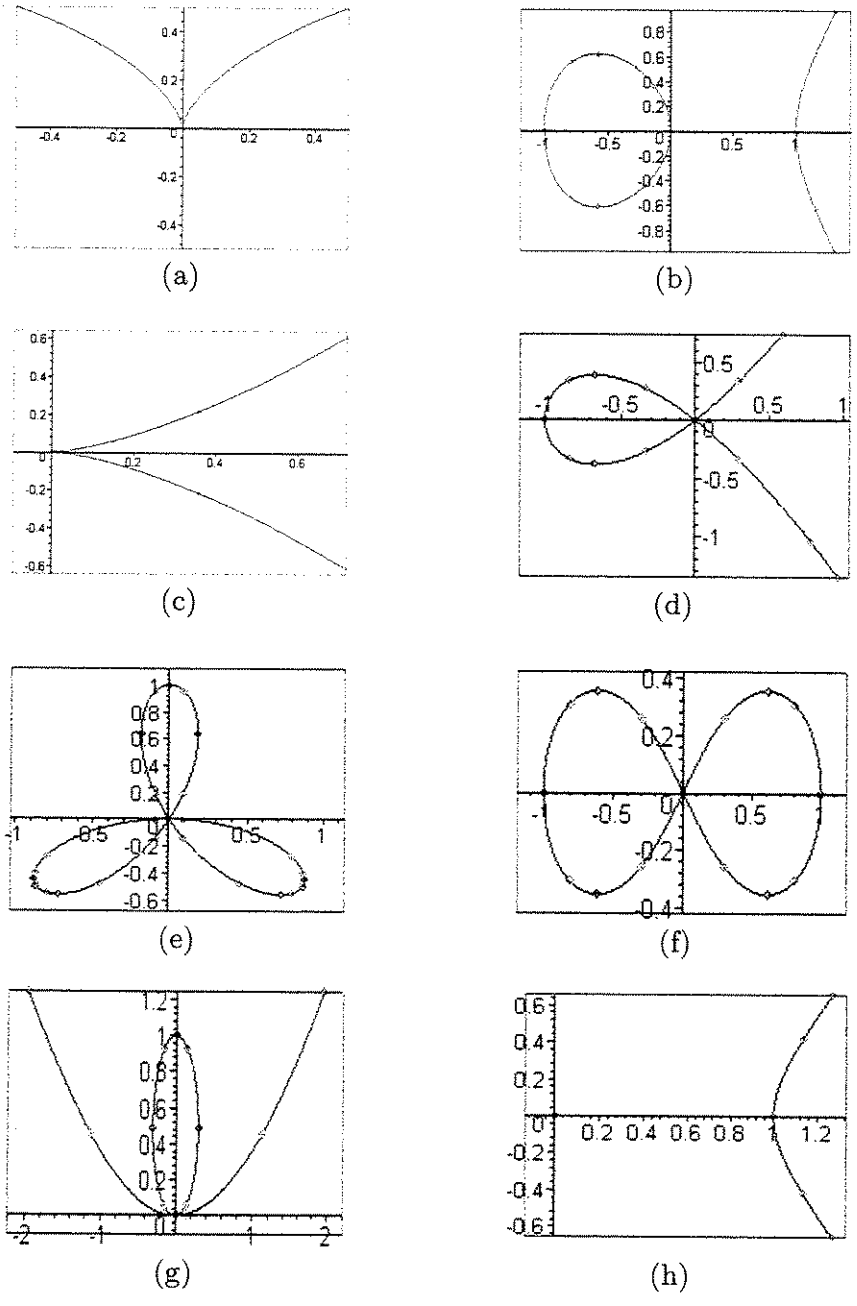


Figura 3.2: *Curvas algébricas planas*

Consideremos o plano afim mergulhado no espaço tridimensional como o plano Ψ de equação $Z = 1$. Cada ponto de Ψ determina uma reta passando pela origem. Cada reta de Ψ determina um plano passando pela origem. Se as retas r, $r' \in \Psi$ se intersectam, seu ponto de interseção dá lugar à reta de interseção dos dois planos associados as retas r e r'. Se as retas r, r' são paralelas, os correspondentes planos se intersectam, desta vez ao longo de uma reta passando pela origem e contida no plano $Z = 0$.

Definição 3.3.3 *Seja $\mathbb{K}$ um corpo. O* ***espaço projetivo*** *sobre $\mathbb{K}$, denotado por $\mathbb{P}^n(\mathbb{K})$, ou simplesmente $\mathbb{P}^n$, é definido como sendo o conjunto de todas as retas que passam pela origem $(0, 0, \ldots, 0)$ em $\mathcal{A}^{n+1}(\mathbb{K})$. Qualquer ponto $(x) = (x_1, x_2, \ldots, x_{n+1}) \neq (0, 0, \ldots, 0)$ determina uma única reta, isto é, $\{(\lambda x_1, \ldots, \lambda x_{n+1}) \mid \lambda \in \mathbb{K}\}$. Dois pontos (x) e (y) determinam a mesma reta se, e somente se, existe um $\lambda \in \mathbb{K}$, não-nulo, tal que $y_i = \lambda x_i$ para $i = 1, \ldots, n+1$. Desse modo, dizemos que (x) e (y) são* ***equivalentes.*** *Então $\mathbb{P}^n$ pode ser identificado com o conjunto de classes de equivalência de pontos em $\mathcal{A}^{n+1} - \{(0, 0, \ldots, 0)\}$ ou $\mathcal{A}^{n+1} \backslash \{(0, 0, \ldots, 0)\}$.*

Um elemento $P = (a_0 : \cdots : a_n) \in \mathbb{P}^n$ é chamado ponto e $a_0, \ldots, a_n \in \mathcal{A}^{n+1}$ são ditas as **coordenadas homogêneas de** P.

O conjunto $\mathcal{H} = \{(0 : a_1 : \cdots : a_n) \in \mathbb{P}^n\}$ é chamado de hiperplano no infinito e os pontos de $\mathcal{H}$, denotados por Q, são chamados pontos no infinito.

O **plano projetivo** $\mathbb{P}^2$ é o conjunto das retas do espaço tridimensional passando pela origem.

Do exposto acima, vemos que o plano Ψ se identifica naturalmente como um subconjunto de $\mathbb{P}^2$ que ainda denotaremos por Ψ. Os pontos de $\mathbb{P}^2 - \Psi$ são chamados de **pontos no infinito**. Tais pontos são obtidos através de certas transformações de coordenadas não-lineares chamadas "projetivas". Precisaremos somente de duas transformações: as transformações de coordenadas do sistema padrão (x, y) para os sistemas (u, v) e (w, z) dadas pelas regras

$$u = y/x, \quad v = 1/x \quad \text{e} \quad w = 1/y, \quad z = x/y \tag{3.6}$$

serão chamadas **mudanças de coordenadas projetivas.**

Note que a transformação do sistema (u, v) para o sistema (w, z) é do mesmo tipo. Note também que os pontos dados podem estar em qualquer dos três sistemas de coordenadas. Como consequência, a maioria dos pontos são representáveis nos três sistemas, mas alguns só são representáveis em dois deles e uns poucos só são representáveis em um sistema.

Por exemplo, o ponto $(x = 1, y = 1)$ é o mesmo que o ponto $(u = 1, v = 1)$, e o ponto $(x = a, y = b)$ para $a \neq 0$ é o mesmo que o ponto $(u = ba^{-1}, v = a^{-1})$. O ponto $(x = 0, y = 1)$ não tem nenhum equivalente no sistema (u, v), mas é o mesmo que $(w = 1, z = 0)$. O ponto $(u = 1, v = 0)$ não tem nenhum equivalente no sistema (x, y), mas é o mesmo que $(w = 0, z = 1)$. O ponto $(x = 0, y = 0)$ não tem nenhum equivalente no sistema (u, v) ou no sistema (w, z).

Normalmente, especificamos o sistema de coordenadas pela notação $P : (x = a, y = b)$. Os sistemas de coordenadas são usados na seguinte ordem de prioridade. Se um ponto pode ser representado no sistema (x, y), então usamos esse sistema. Falhando esse, se o

ponto pode ser representado no sistema $(u,\ v)$ (necessariamente com $v = 0$), usamos esse sistema. O único ponto restante $(w = 0,\ z = 0)$ é representado no sistema $(w,\ z)$.

Podemos considerar os pontos que não podem ser representados no sistema $(x,\ y)$ como formando uma reta no infinito ou **horizontal** com a equação $v = 0$. A horizontal intercepta toda reta ordinária em um único ponto. Assim, como verificaremos brevemente, $(u = a,\ v = 0)$ é a interseção da reta $y = ax + b$ com a horizontal, e $(w = 0,\ z = 0)$ é a interseção do eixo y $(x = 0)$ com a horizontal.

Como exemplos, destacamos os seguintes.

A equação $y = ax + b$ pode ser escrita como $y/x = a + b/x$. No sistema $(u,\ v)$ essa equação é transformada em $u = a + bv$, confirmando que $(u = a,\ v = 0)$ está na reta.

A hipérbole retangular $x^2 - y^2 = 1$ é transformada em $1/v^2 - u^2/v^2 = 1$. Para $x \neq 0$ também $1/v \neq 0$. Assim, podemos multiplicar esta equação por v^2 para obter a curva $1 = u^2 + v^2$. Esta é a equação de um círculo com a reta $v = 0$ como um diâmetro. Assim, a hipérbole retangular pode ser vista como um círculo com a horizontal como um diâmetro.

A parábola $2x = y^2 + 1$ é transformada em $2/v = u^2/v^2 + 1$. Novamente, multiplicando por v^2, resulta em $2v = u^2 + v^2$ ou $u^2 + (v - 1)^2 = 1$. Note que esta é também a equação de um círculo, mas desta vez $v = 0$ é uma tangente. Assim, a parábola pode ser vista como um círculo com a horizontal como uma tangente.

A curva $x^3 + y^3 - 1 = 0$ é transformada em $u/v^3 + 1^3/v^3 - 1 = 0$ ou $u^3 + 1 - v^3 = 0$. Se a característica do corpo é 2, então a equação permanece igual à equação original em x e y.

Observamos que, em todos os casos considerados, o grau da equação não muda pela transformação utilizada.

Seja $f(x, y)$ um polinômio absolutamente irredutível em $\mathbb{K}[x, y]$ de grau d e defina

$$g(u, v) = v^d f(\frac{1}{v}, \frac{u}{v}) \quad \text{e} \quad h(w, z) = w^d f(\frac{z}{w}, \frac{1}{w}).$$

Então, a **curva projetiva** $\mathcal{X}$ definida por $f(x, y)$ é a união das três curvas $\mathcal{X}_1 : f(x, y) = 0$, $\mathcal{X}_2 : g(u, v) = 0$ e $\mathcal{X}_3 : h(w, z) = 0$, os pontos são permitidos ter coordenadas em qualquer extensão finita $\mathbb{L}$ de $\mathbb{K}$. Chamamos estas três curvas de as **componentes afins de** $\mathcal{X}$, e denotaremos a curva completa por $\mathcal{X} : f(x, y) = 0$.

Se $f(x, y) = ax$, então $g(u, v) = a$ e a componente afim (u, v) é vazia. Isso ocorre porque $f(x, y)$ é a horizontal do sistema (u, v). Para outros casos temos que mostrar que as componentes afins juntas atendem às condições de mudanças de coordenadas projetivas, definidas em (3.6), e que g e h satisfazem às condições de curvas afins.

Proposição 3.3.4 *[47] Seja $f(x, y) \neq ax$ um polinômio absolutamente irredutível de grau d e seja $g(u, v) = v^d f(1/v, u/v)$. Então g é um polinômio absolutamente irredutível de grau d. Além disso, se um ponto P tem coordenadas $P : (x = a, y = b)$ e também $P : (u = c, v = d)$, então $f(a, b) = 0$ se, e somente se, $g(c, d) = 0$.*

Demonstração. Correspondendo a um termo $bx^r y^s$ de $f(x, y)$, o polinômio $g(u, v)$ tem um termo $bu^s v^{(d-r-s)}$. Como $f(x, y) \neq ax$ e $f(x, y)$ é absolutamente irredutível, x não divide $f(x, y)$. Conseqüentemente, pelo menos um termo de $f(x, y)$ tem $r = 0$. Isso prova que g tem grau d. Como o grau de $f(x, y)$ é d, existe um termo não-nulo $bx^r y^s$

com $r+s=d$. Esse termo é transformado em bu^s. Conseqüentemente, $g(u,v)$ não é um múltiplo de v. Suponha que, para alguma extensão de corpos, $g(u,v)=h(u,v)k(u,v)$, onde h e k têm graus r e s, respectivamente. Então nem $h(u,v)$, nem $k(u,v)$ é um múltiplo de v. Assim

$$f(x,y)=x^d g(\frac{y}{x},\frac{1}{x})=(x^r h(\frac{y}{x},\frac{1}{x}))(x^s k(\frac{y}{x},\frac{1}{x})),$$

e os dois fatores são polinômios de grau r e s, respectivamente. Considerando que f é absolutamente irredutível, segue que $r=0$ ou $s=0$. Mas isso implica que h ou k é uma constante. Assim, g é absolutamente irredutível.

Voltando às afirmações feitas sobre P temos, por hipótese, que $c=b/a$, $d=1/a$ e $a\neq 0$. Então, $g(c,d)=a^{-d}f(a,b)$. Assim, $g(c,d)=0$ se, e só se, $f(a,b)=0$. ∎

Apresentaremos a seguir uma outra forma de definição do plano projetivo.

Denotaremos por $(x:y:z)$ o ponto de $\mathbb{P}^2$ que representa a reta ligando a origem 0 a um ponto $(x,y,z)\neq O$. Dizemos que x,y,z são **coordenadas homogêneas** do ponto $(x:y:z)$ relativas à base canônica $\{(1,0,0),(0,1,0),(0,0,1)\}$.

Um polinômio $F(x,y,z)$ é um **polinômio homogêneo** se todo monômio tiver o mesmo grau nas variáveis x,y e z; este grau é o grau do polinômio homogêneo. Por exemplo, $F(x,y,z)=x^2y-2xyz+3z^3$ é homogêneo de grau 3 nas variáveis x,y,z.

Observe que a soma de dois polinômios homogêneos de diferentes graus não preserva a homogeneidade.

O polinômio homogêneo determinado por F é chamado equação da curva algébrica $\mathcal{X}\subset\mathbb{P}^2$. O processo de **projetivização** de uma curva plana em $\mathbb{K}^2$ consiste em considerar o fecho desta curva algébrica em $\mathbb{P}^2$. Do ponto de vista algébrico, o processo traduz-se pela "homogeneização" de polinômios de $\mathbb{K}[x,y]$ mediante a introdução de uma nova variável Z. Topologicamente, o que se está fazendo é acrescentar um número finito de pontos de $\mathbb{P}^2$ à curva original de $\mathbb{K}^2$, os chamados pontos no infinito. Tais pontos são facilmente determinados fazendo-se $Z=0$ na equação da curva projetivizada.

Ilustraremos os pontos no infinito com dois exemplos. Primeiro, considere a reta

$$\mathcal{L}:\alpha X+\beta Y+\gamma Z=0,$$

digamos que $\alpha=0$. A parte afim de $\mathcal{L}$ é a reta $L_0:\alpha x+\beta y+1=0$ em $\mathcal{A}^2$. Os pontos no infinito em $\mathcal{L}$ correspondem aos pontos onde $Z=0$. Há só um tal ponto, isto é $[-\beta,\alpha,0]\in\mathcal{L}$ que corresponde ao ponto no infinito $[-\beta,\alpha]\in\mathbb{P}^1$, que por outo lado, corresponde à direção $-\beta y=\alpha x$ em $\mathcal{A}^2$. Esta direção é exatamente a direção da reta L_0. Assim $\mathcal{L}$ consiste da reta afim L_0 junto com o único ponto no infinito que corresponde à direção de L_0.

Agora, olhamos para a curva projetiva

$$\mathcal{X}:X^2-Y^2-Z^2=0.$$

Há dois pontos em $\mathcal{X}$ com $Z=0$, isto é $[1,1,0]$ e $[1,-1,0]$. Esses dois pontos correspondem, respectivamente, aos pontos no infinito $[1,1]$,$[1,-1]\in\mathbb{P}^1$, ou equivalentemente às direções $y=x$ e $y=-x$ em $\mathcal{A}^2$. A parte afim de $\mathcal{X}$ é a hipérbole

$$\mathcal{X}_0:x^2-y^2-1=0.$$

Suponha agora que tomemos uma sucessão de pontos (r_1, s_1), (r_2, s_2), ... em $\mathcal{X}_0$ tal que estes pontos tendem a infinito, isto é, $|s_2| \to \infty$. Se reescrevemos $r_i^2 - s_i^2 - 1 = 0$ como

$$\left(\frac{r_i}{s_i} - 1\right)\left(\frac{r_i}{s_i} + 1\right) = \frac{1}{s_i^2},$$

então o termo do lado direito vai para 0 quando $i \to \infty$, assim vemos que ou

$$\lim_{i\to\infty} \frac{r_i}{s_i} = 1 \quad \text{ou} \quad \lim_{i\to\infty} \frac{r_i}{s_i} = -1,$$

dependendo, obviamente, de qual ramo da hipérbole utilizamos. (Veja Figura 3.3).

Seja L_i a reta tangente a $\mathcal{X}_0$ no ponto (r_i, s_i). Afirmamos que, quando $i \to \infty$, a direção da reta tangente L_i se aproxima da direção de uma das retas $y = \pm x$. Isto não é nada além da afirmação de que as retas $y = \pm x$ são assíntotas à curva $\mathcal{X}_0$. Para conferir esta afirmação analiticamente, diferenciamos implicitamente a equação $x^2 - y^2 - 1 = 0$ para adquirir

$$\frac{dy}{dx} = \frac{x}{y},$$

e assim

$$\text{(inclinação de } L_i) = \text{(inclinação de } \mathcal{X}_0 \text{ em } (r_i, s_i)) = \frac{r_i}{s_i} \longrightarrow_{i\to\infty} \pm 1.$$

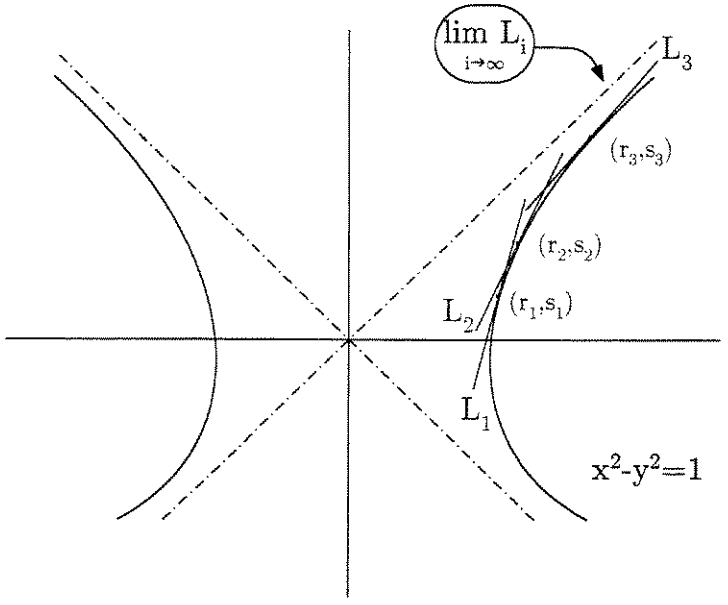


Figura 3.3: *Pontos no infinito são limites de direções tangentes*

Definição 3.3.5 *O conjunto de todas as razões* $(a_0 : a_1 : a_2)$ *é chamado* ***plano projetivo*** *e será denotado por* $\mathbb{P}^2(\mathbb{K})$. *Cada* $(a_0 : a_1 : a_2)$ *é chamado um* ***ponto*** *de* $\mathbb{P}^2(\mathbb{K})$.

Segue da Definição 3.3.5, que a igualdade

$$(a_0 : a_1 : a_2) = (a_0' : a_1' : a_2')$$

ocorre se, e somente se, existe uma constante $\lambda \neq 0$ tal que $(a_0, a_1, a_2) = \lambda(a_0', a_1', a_2')$. Em particular, se $a_0 \neq 0$, então

$$(a_0 : a_1 : a_2) = (1 : \frac{a_1}{a_0} : \frac{a_2}{a_0}).$$

Em vista disso, concluímos que as coordenadas homogêneas de um ponto de $\mathbb{P}^2$, relativas a uma base prefixada, estão bem definidas a menos de um fator escalar diferente de zero.

Uma topologia é introduzida em $\mathbb{P}^2$, a **topologia quociente**, considerando-se a seguinte aplicação,

$$\begin{aligned} \phi : \mathbb{K}^3 - \{0\} &\to \mathbb{P}^2 \\ (x, y, z) &\mapsto (x : y : z). \end{aligned}$$

Neste caso, dizemos que um subconjunto $\mathcal{U} \subset \mathbb{P}^2$ é aberto se $\phi^{-1}(\mathcal{U})$ é aberto em $\mathbb{K}^3 - \{0\}$, com a sua topologia usual. Estabelecendo, assim, em $\mathbb{P}^2$, uma **noção de vizinhança**, segundo a qual dois pontos de $\mathbb{P}^2$ estão "próximos" se as retas associadas em $\mathbb{K}^3$ formam um "pequeno" subconjunto de $\mathbb{P}^2$, $\mathcal{A}^2 = \{(x : y : z) \mid z \neq 0\}$ é aberto e denso em $\mathbb{P}^2$, pois $\phi^{-1}(\mathcal{A}^2)$ é o complementar do plano $z = 0$ em $\mathbb{K}^3$ e, é, evidentemente, aberto e denso em $\mathbb{K}^3 - \{0\}$.

Pode-se mostrar que a aplicação

$$\begin{array}{ccc} K^2 & \longrightarrow & \mathcal{A}^2 \subset \mathbb{P}^2 \\ (x, y) & \longmapsto & (x : y : 1) \end{array} \tag{3.7}$$

é uma bijeção. Desta forma, passamos a considerar o plano afim $\mathcal{A}^2$ como contido em $\mathbb{P}^2$, identificando-o com $\mathcal{A}^2$.

Consideremos o conjunto $\mathfrak{X} = \{(x : y : z) \in \mathbb{P}^2 : F(x, y, z) = 0\}$. O plano projetivo $\mathbb{P}^2$, pode ser **coberto** pelos três conjuntos abertos $\mathcal{U}_0 = \{(x : y : z) \in \mathbb{P}^2 \mid x \neq 0\}$, $\mathcal{U}_1 = \{(x : y : z) \in \mathbb{P}^2 \mid y \neq 0\}$ e $\mathcal{U}_2 = \{(x : y : z) \in \mathbb{P}^2 \mid z \neq 0\}$. É fácil verificar que a definição de U_i independe dos sistemas de coordenadas homogêneas dos pontos. É evidente que $\mathcal{U}_i$ é um aberto de $\mathbb{P}^2$ e que o espaço projetivo $\mathbb{P}^2 = \mathcal{U}_0 \cup \mathcal{U}_1 \cup \mathcal{U}_2$.

Em particular, se considerarmos $\mathcal{U}_0 = \{(x : y : z) \in \mathbb{P}^2(\mathbb{K}) \mid x \neq 0\}$, temos, por exemplo, que

$$\mathcal{X}_0 = \mathfrak{X} \cap \mathcal{U}_0 \cong \{(y, z) \in \mathbb{K}^2 \mid F(1, y, z) = 0\}$$

é a curva plana afim descrita pelo polinômio $f(y, z) = 0$, onde $f(y, z) = F(1, y, z)$.

Como conseqüencias imediatas, resultam as seguintes afirmações.

Afirmação 3.3.6 *Nas condições do conjunto $\mathfrak{X}$ e da aplicação definida em (3.7), valem as seguintes implicações:*

(i) $f(x_0, y_0) = 0 \iff F(x_0, y_0, 1) = 0$;

(*ii*) Para qualquer $\lambda \in \mathbb{K}^*$, temos

$$F(\lambda X, \lambda Y, \lambda Z) = (\lambda Z)^d f(\frac{\lambda X}{\lambda Z}, \frac{\lambda Y}{\lambda Z}) = \lambda^d F(X, Y, Z),$$

assim

$$F(X_0, Y_0, Z_0) = 0 \Longleftrightarrow F(\lambda X_0, \lambda Y_0, \lambda Z_0) = 0, \quad \forall\, \lambda \in \mathbb{K}^*.$$

(*iii*) Visto que F é homogêneo, $F(0,0,0) = 0$.

Em virtude da Afirmação 3.3.6(*iii*) , podemos ignorar a solução $(0,0,0)$ de $F = 0$. Por causa da implicação (*ii*) da mesma afirmação, é possível identificar as soluções (X_0, Y_0, Z_0) e (aX_0, aY_0, aZ_0).

Lembramos que pontos de $\mathbb{P}^2(\mathbb{K})$ são classes de equivalência, isto é, $(X_0 : Y_0 : Z_0)$ é a representação da classe de equivalência de (X_0, Y_0, Z_0) em $\mathbb{P}^2(\mathbb{K})$.

Como $f(x, y) = 0$ é um polinômio em duas variáveis, então a equação $f(x, y) = 0$ define uma curva $\mathcal{X}_f$ no plano. Definamos agora o fecho projetivo $\widehat{\mathcal{X}_f}$ de $\mathcal{X}_f$ cujo significado correspondente equivale a "somar pontos no infinito". Para isso, vamos introduzir o conceito de homogeneização de um polinômio.

Definição 3.3.7 *O polinômio F de grau d é chamado a* ***homogeneização de*** *f, quando F é obtido de f, através da computação de Z's nos monômios de graus inferiores de f, visando um polinômio F cujos monômios possuem o mesmo grau, determinado por* $F(X, Y, Z) = Z^d f(X/Z, Y/Z)$

Sejam $\mathbb{K}$ um corpo, $f(x, y) \in \mathbb{K}[x, y]$ um polinômio de grau d e $\mathcal{X}_f$ a curva associada a f. O **fecho projetivo da curva** $\mathcal{X}_f$ é $\widehat{\mathcal{X}_f} := \{(X_0, Y_0, Z_0) \in \mathbb{P}^2(\mathbb{K}) \mid F(X_0, Y_0, Z_0) = 0\}$, onde $F(X, Y, Z) = Z^d f(X/Z, Y/Z) \in \mathbb{K}[X, Y, Z]$ é a homogeneização de f.

Qualquer ponto $(X_0 : Y_0 : Z_0)$ com $Z_0 = 0$ é chamado um **ponto no infinito**. Todos os outros pontos são chamados **afins.**

Por exemplo, a curva definida pela equação polinomial $y^2 = x^3 + x + 1$ está em $\mathcal{X}_f$ onde $f(x, y) = y^2 - x^3 - x - 1$. Então

$$F(X, Y, Z) = Z^3((Y/Z)^2 - (X/Z)^3 - (X/Z) - 1) = Y^2Z - X^3 - XZ^2 - Z^3.$$

Note que todo monômio que aparece em F tem grau exatamente $3 = \deg(f)$, e que a tarefa de construir F equivale a computar e somar bastante Z's de forma que todo termo tenha grau 3. O polinômio F é chamado a homogeneização de f.

Em particular, $\mathbb{P}^0$ consiste de um só ponto. $\mathbb{P}^1$, **reta projetiva**, é a reta usual $\mathcal{A}^1$ com um ponto extra no infinito.

Quando $\mathbb{K} = \mathbb{R}$, podemos visualizar $\mathbb{P}^1(\mathbb{R})$ como a circunferência, com o ponto no infinito indicado na Figura 3.4.

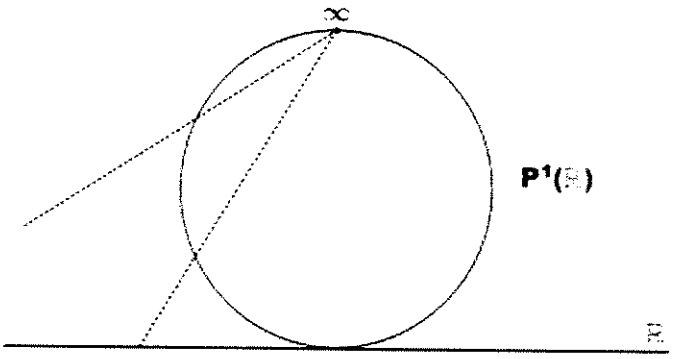


Figura 3.4: *Reta Projetiva,* $\mathbb{P}^1(\mathbb{R})$.

3.3.4 Resolução de singularidades

Partindo da hipótese de que estamos interessados em curvas planas, a única restrição a mais que necessitaremos é que as curvas sejam não-singulares. Como não-singularidade e diferenciabilidade são conceitos bastante relacionados, temos que entender primeiramente o que significa diferenciar sobre um corpo arbitrário $\mathbb{K}$.

Sejam $\mathbb{K}$ um corpo e $f(x,y) \in \mathbb{K}[x,y]$ um polinômio. Se $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, corpo de característica zero, sabemos o significado de derivada parcial f_x de f com respeito a x. Se $\mathbb{K}$ for um corpo de característica p, a definição tradicional de limite não se aplica, tendo-se que levar em consideração a redução mod p dos coeficientes. Porém, para $f(x,y) \in GF(q)[x,y]$, podemos definir a derivada parcial formal $f_x(x,y) \in \mathbb{K}[x,y]$ de f com respeito a x da mesma maneira que no corpo de característica zero. Por exemplo, se $f(x,y) = x^2 + y^3 + xy$, então $f_x(x,y) = 2x + y$ e $f_y(x,y) = 3y^2 + x$ sobre qualquer corpo $\mathbb{K}$. Em particular, se $\mathbb{K} = GF(2)$, então $f_x(x,y) = y$ e $f_y(x,y) = y^2 + x$. Por outro lado, se $\mathbb{K} = GF(3)$, então $f_x(x,y) = 2x + y$ e $f_y(x,y) = x$.

Definição 3.3.8 *Sejam* $\mathbb{K}$ *um corpo e* $f(x,y) \in \mathbb{K}[x,y]$. *Um* ***ponto singular*** *da curva* $\mathcal{X}_f$ *é um ponto* $(x_0,y_0) \in \mathbb{K} \times \mathbb{K}$ *tal que* $f(x_0,y_0) = 0$ *e* $f_x(x_0,y_0) = 0$ *e* $f_y(x_0,y_0) = 0$. *Se* $F(X,Y,Z)$ *é a homogeneização de* $f(x,y)$, *então* $(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(\mathbb{K})$ *é um* ***ponto singular*** *de* $\widehat{\mathcal{X}_f}$ *se o ponto está na curva e se todas as derivadas parciais forem nulas, isto é,*

$$\begin{aligned} F(X_0,Y_0,Z_0) &= F_X(X_0,Y_0,Z_0) \\ &= F_Y(X_0,Y_0,Z_0) \\ &= F_Z(X_0,Y_0,Z_0) \\ &= 0. \end{aligned}$$

Como exemplos de pontos não-sigulares destacamos os dois exemplos a seguir:

a) Seja $\mathcal{X}$ uma curva dada por $f(x,y) = y^3 - x^2 - 1$ e um ponto $P(0,1)$, tal que $f(P) = 0$. Assim,

$$f_x = -2x \Rightarrow f_x(P) = 0 \quad e \quad f_y = 3y^2 \Rightarrow f_y(P) \neq 0$$

logo, P é um ponto não-singular de $\mathcal{X}$.

b) Seja $\mathcal{X}$ uma curva dada por $F(X,Y,Z) = Z^2 - Z - Y^2 + Y$ e um ponto $P(0,0,0)$, tal que $F(P) = 0$. Assim,

$$\begin{array}{lll} F_X = 0 & \Rightarrow & F_X(P) = 0 \\ F_Y = -2Y + 1 & \Rightarrow & F_Y(P) \neq 0 \\ F_Z = 2Z - 1 & \Rightarrow & F_Z(P) \neq 0 \end{array}$$

logo, P é um ponto não-singular $\mathcal{X}$.

Sejam $\mathbb{K}$ um corpo e $f(x,y) \in \mathbb{K}[x,y]$. Uma curva $\mathcal{X}_f$ é chamada **não-singular**, **regular** ou **suave** se todos os pontos na curva $\mathcal{X}_f$ são não-sigulares. Seja $P = (a,b) \in \mathcal{X}_f$. A curva $\widehat{\mathcal{X}_f}$ é não-singular se a mesma não tem pontos singulares.

Como exemplo, suponha que $\mathcal{X}$ seja uma curva definida por $y^2 = 4x^3 - ax - b$, isto é, pelo polinômio

$$f(x,y) = y^2 - 4x^3 + ax + b.$$

Assumindo que a característica do corpo $\mathbb{K}$ é diferente de 2, então as derivadas parciais de f são $2y$ e $-12x^2 + a$. Assim, um ponto em $\mathcal{X}$ é um par (x,y) tal que $y = 0$ e x é uma raiz repetida de $4x^3 - ax - b$. Portanto, $\mathcal{X}_f$ é não-singular se, e somente se, as raízes de $4x^3 - ax - b$ são todas simples, que é verdade se, e somente se, seu discriminante $\Delta = a^3 - 27b^2 \neq 0$.

Se a Definição 3.3.8 faz sentido, espera-se que $\mathcal{X}_f$ seja não-singular, então os únicos possíveis pontos singulares de $\widehat{\mathcal{X}_f}$ estão no infinito. Isto é verdade e segue da definição da homogeneização de f e da regra da cadeia para derivadas parciais.

Intuitivamente, um ponto singular é um ponto onde a curva não tem uma reta tangente bem definida. Por exemplo, consideremos a curva $\mathcal{X}_f$, onde $f(x,y) = -x^3 + y^2 + x^4 + y^4$ sobre $\mathbb{C}$. Temos que $f_x(x,y) = -3x^2 + 4x^3 = x^2(-3 + 4x)$ e $f_y(x,y) = 2y + 4y^3 = 2y(1 + 2y^2)$. Para que (x_0, y_0) seja um ponto singular, decorre que $x_0 = 0$ ou $3/4$ e $y_0 = 0$, $\frac{1}{2}i$ ou $-\frac{1}{2}i$. Uma verificação rápida mostra que dos 6 possíveis pares (x_0, y_0) só $(0,0)$ está na curva, assim $(0,0)$ é a única singularidade afim. A homogeneização de f é

$$F(X,Y,Z) = -X^3Z + Y^2Z^2 + X^4 + Y^4.$$

Assim, $F_X = -3X^2Z + 4X^3$, $F_Y = 2YZ^2 + 4Y^3$ e $F_Z = -X^3 + 2Y^2Z$. Considerando que todas as singularidades afins foram determinadas, precisamos somente considerar o ponto no infinito, pela fixação de $Z = 0$. Deste modo, para que $(X_0 : Y_0 : 0)$ seja uma singularidade, teremos que ter

$$X_0^4 + Y_0^4 = 4X_0^3 = -4Y_0^3 = -X_0^3 = 0.$$

O único modo disso acontecer é se $X_0 = Y_0 = 0$, mas isso é impossível em $\mathbb{P}^2$ visto que Z_0 já é 0. Assim, o único ponto singular em $\widehat{\mathcal{X}_f}$ é o ponto $(0:0:1)$. Consequentemente, a curva $\mathcal{X}_f$ mostrada na Figura 3.5 é, de fato, cuspidal.

Afirmação 3.3.9 *Uma curva plana não-singular é absolutamente irredutível. Em outras palavras, isso quer dizer que, se $f(x,y) \in \mathbb{K}[x,y]$ define uma curva plana não-singular $\mathcal{X}_f$, e se $f = gh$ para algum $g, h \in \overline{\mathbb{K}}[x,y]$, com $\overline{\mathbb{K}}$ sendo o fecho algébrico de $\mathbb{K}$, então $g \in \overline{\mathbb{K}}$ ou $h \in \overline{\mathbb{K}}$.*

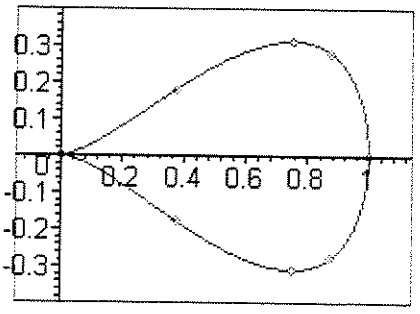


Figura 3.5: *Curva Cuspidal*

Modelo não-singular de curvas planas (Desingularização de curvas planas)

A desingularização de curvas planas está baseada no seguinte teorema clássico, provado por Riemann e Cayley.

Teorema 3.3.10 *[4] Toda curva plana pode ser biracionalmente transformada em uma curva destituída de singularidades.*

Entre as diferentes provas do teorema estão versões construtivas que necessariamente derivam transformações biracionais de uma sucessão de transformações quadráticas simples.

Teorema 3.3.11 *[4] Seja $\mathcal{X}$ uma curva projetiva. Então existe uma curva projetiva não-singular $\mathcal{X}'$ e um morfismo biracional f de $\mathcal{X}'$ sobre $\mathcal{X}$. Se $f' : \mathcal{Y} \longrightarrow \mathcal{X}$ é outra, então existe um único isomorfismo $g : \mathcal{X}' \longrightarrow \mathcal{Y}$ tal que $f'g = f$.*

Seja $\mathcal{X}$ qualquer curva projetiva, $f : \mathcal{X}' \longrightarrow \mathcal{X}$ como no Teorema 3.3.11. Dizemos que $\mathcal{X}'$ é o modelo não-singular de $\mathcal{X}$, ou de $K = k(\mathcal{X})$. Identificaremos $k(\mathcal{X})$ com K por meio de $\widetilde{f}$.

Apresentamos agora dois exemplos de desingularização de uma curva plana.

Considere a cúbica nodal $Y^2 - X^2 - X^3 = 0$. Se fizermos a transformação $X' = X$ e $Y' = Y/X$ de forma que $X = X'$ e $Y = X'Y'$, então obtemos $(Y^2 - X^2 - X^3) \longrightarrow (X'^2Y'^2 - X'^2 - X'^3 = X'^2(Y'^2 - 1 - X')$, conforme mostra a Figura (3.6). Retirando o fator externo X'^2, obtemos a parábola $Y'^2 - 1 - X' = 0$. Assim, a cúbica nodal é transformada em uma parábola pela transformação

$$\begin{cases} X' = X \\ Y' = Y/X \end{cases} \quad \text{ou} \quad \begin{cases} X = X' \\ Y = X'Y'. \end{cases}$$

Agora, as equações que definem esta transformação são ambas consideradas racionais. Tal transformação é chamada de transformação biracional. Assim, neste exemplo, podemos dizer que a cúbica nodal e a parábola são biracionalmente equivalentes. Agora, também podemos considerar a mesma transformação aplicada a cúbica cuspidal $Y^2 - X^3 = 0$,

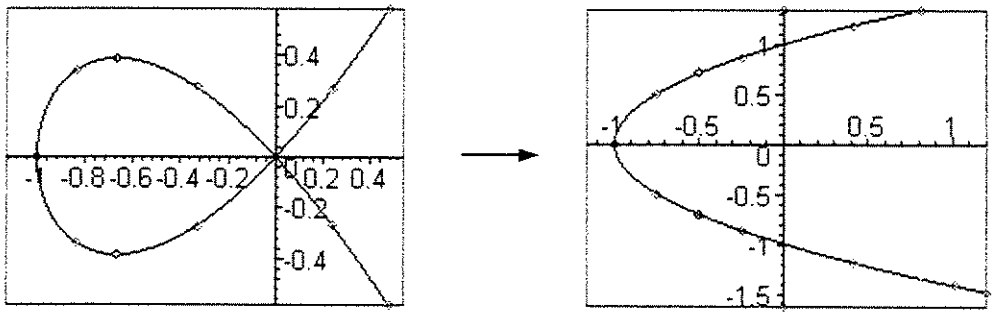


Figura 3.6: *Desingularização da cúbica nodal*

conforme mostra a Figura 3.7. Dessa forma, produz $X'^2(Y'^2 - X') = 0$ e, retirando o fator externo X'^2, obtemos a parábola $Y'^2 - X' = 0$. Assim, podemos concluir que a cúbica cuspidal e a parábola são biracionalmente equivalentes. Em particular, vemos que todas as curvas consideradas nestes exemplos têm o mesmo gênero, isto é, gênero zero.

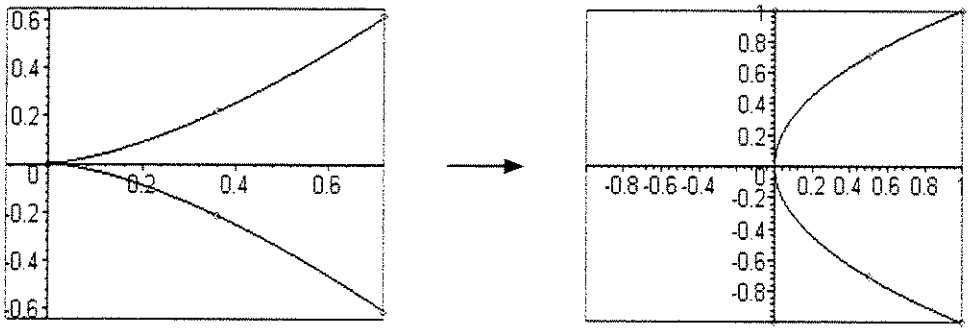


Figura 3.7: *Desingularização da cúbica cuspidal*

Gênero de curvas algébricas planas

Para qualquer curva algébrica plana $\mathcal{X}$, temos definido um número $\mathrm{g} = \mathrm{g}(\mathcal{X})$. Esse número é chamado o **gênero** de $\mathcal{X}$. Sua propriedade básica é que para qualquer outra curva plana irredutível $\mathcal{X}'$: $\mathcal{X}$ é biracionalmente equivalente a $\mathcal{X}' \Rightarrow \mathrm{g}(\mathcal{X}) = \mathrm{g}(\mathcal{X}')$.

Se a curva $\mathcal{X}$ é destituída de componentes múltiplas, isto é, se $f(x, y)$ não é divisível pelo quadrado de qualquer polinômio não-constante, então $\mathcal{X}$ tem no máximo $n(n-1)/2$ pontos duplos, onde n é o grau do polinômio $f(x, y)$. Além disso, se $\mathcal{X}$ é uma curva irredutível, isto é, se $f(x, y)$ é um polinômio irredutível, então $\mathcal{X}$ tem, no máximo, $(n-1)(n-2)/2$ pontos duplos. Novamente, os pontos duplos têm que ser contados corretamente.

Assim, no caso de $\mathcal{X}$ ser irredutível, definimos

$$\mathrm{g} = (n-1)(n-2)/2 - \delta,$$

onde δ indica o número de pontos duplos, os quais são contados com multiplicidade: neste caso, sempre temos $\mathrm{g} \geq 0$.

Teorema 3.3.12 *[2] Uma curva algébrica $\mathcal{X}$ tem gênero $\mathrm{g} = 0$ se, e somente se, $\mathcal{X}$ tem uma parametrização racional.*

Teorema 3.3.13 *[17] Se $\mathcal{X}$ é uma curva irredutível de grau n e m_P a multiplicidade de $\mathcal{X}$ no ponto P, então*

$$\mathrm{g}(\mathcal{X}) = \frac{(n-1)(n-2)}{2} - \sum_{P} \frac{m_P(m_P-1)}{2}. \tag{3.8}$$

Nos próximos exemplos determinaremos o gênero de algumas curvas:

a) O gênero de uma reta ou de uma cônica irredutível é zero;

b) Se $\mathcal{X}$ é uma cúbica $y^2 = x^3$, então temos que $\mathrm{g} = 0$;

c) Considere a curva $y^2 + x^2 = x^3$. O ponto singular é $(0:0:1)$ com múltiplicidade 2. Logo,
$$\mathrm{g} = \frac{(3-1)(3-2)}{2} - 1 = 0;$$

d) Considere a curva $y^2 = x^5$. Os pontos singulares são $(0:0:1)$ e $(0:1:0)$ com respectivas multiplicidades iguais a 2 e 3. Logo,
$$\mathrm{g} = \frac{(5-1)(5-2)}{2} - 1 - 3 = 2.$$

Seja P um ponto singular com multiplicidade $m = 2$, então P é chamado um **ponto duplo**. O ponto P é dito ser uma **singularidade ordinária** se as retas tangentes em P são todas distintas. Um ponto duplo ordinário é chamado um **nó**. Um ponto duplo P em uma curva é chamado um **cúspide** se existe uma única reta tangente para a curva em P.

Por exemplo, a curva $\mathcal{X} : y^2 = x^3 + ax^2$ tem um ponto singular em $(0,0)$. Se $a \neq 0$, ele é um nó e as retas tangentes em $(0,0)$ são $y = \pm\sqrt{ax}$. Elas estão definidas sobre um corpo $\mathbb{K}$ se, e somente se, a é uma raiz quadrada em $\mathbb{K}$. Se $a = 0$, o ponto singular é um cúspide.

Topologicamente, toda curva não-singular sobre $\mathbb{C}$ pode ser vista como uma superfície em $\mathbb{R}^3$. Por exemplo, uma curva elíptica tem uma equação da forma $y^2 = f(x)$, onde $f(x)$ é um polinômio cúbico em x sem raízes repetidas, e pode ser pensada como um toro em $\mathbb{R}^3$. Em geral, toda curva não-singular pode ser interpretada como uma esfera com um determinado número de asas. Este número de asas é chamado o gênero topológico da curva. Em particular, uma curva elíptica tem gênero 1. Em geral, se mostra que se $f(x,y)$ é um polinômio de grau d tal que a curva $\widehat{\mathcal{X}_f}$ é não-singular, então o gênero topológico de $\mathcal{X}_f$ é determinado pelo fórmula $\mathrm{g} = (d-1)(d-2)/2$. Essa fórmula é chamada a fórmula de Plücker.

Lema 3.3.14 (Fórmula de Plücker) *Seja $f(x,y) \in \mathbb{K}[x,y]$ um polinômio de grau n tal que $\widehat{\mathcal{X}_f}$ é não-singular, então o gênero da curva $\mathcal{X}_f$ (ou de $\widehat{\mathcal{X}_f}$) é dado por*

$$\mathrm{g}(\mathcal{X}_f) = \frac{(n-1)(n-2)}{2}. \tag{3.9}$$

3.4 Curvas Algébricas sobre Corpos Finitos

Consideraremos o corpo $\mathbb{K}_0$ como sendo o corpo $GF(q)$ consistindo de $q = p^r$ elementos e $\overline{\mathbb{K}} = \overline{GF(q)}$ o seu fecho algébrico. Nesse caso, o conjunto de pontos $GF(q)$-racionais da curva (3.3), definida sobre $GF(q)$, coincidem com o conjunto de soluções da equação (3.3) nos elementos x, y do corpo $GF(q)$. Em particular, para $GF(p)$, p primo, então a questão relativa aos pontos $GF(p)$-racionais da curva (3.3) é equivalente às soluções da congruência $f(x, y) \equiv 0 \,(\mathrm{mod}\, p)$.

3.4.1 Número de pontos racionais de uma curva algébrica sobre corpos finitos

Seja $\mathcal{X}$ uma curva definida sobre $GF(q)$, isto é, as equações definidas têm coeficientes em $GF(q)$. Então pontos em $\mathcal{X}$ com todas as suas coordenadas em $GF(q)$, tais que$f(x, y) \equiv 0$, são chamados **pontos racionais.**

Seja $\mathcal{X}$ uma curva determinada pela equação $f(x, y) = 0$, denotaremos o **conjunto de pontos racionais** desta curva por

$$\mathcal{X}(GF(q)) = \{(x, y) : x, y \in GF(q) \text{ e } f(x, y) = 0\}.$$

Como exemplo, considere a curva $y^2 = x^3 + x + 1$ sobre o corpo $GF(5)$. Como podemos achar os pontos racionais desta curva? Como x e y assumem valores em $GF(5)$, podemos somente escolher cada uma das cinco possibilidades para x, tomando-os no polinômio $x^3 + x + 1$, e observando quando o resultado é um quadrado em $GF(5)$. Fazendo isto, achamos nove pontos (inclusive o ponto $\mathbb{O}$ no infinito):

$$\mathcal{X}(GF(5)) = \{\mathbb{O}, (0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)\}.$$

Assim, a curva definida pela equação $f(x, y) = y^2 - x^3 - x - 1$ tem nove pontos racionais sobre $GF(5)$.

Denotaremos por $N_q(\mathrm{g})$ o número de pontos racionais da curva $\mathcal{X}$ de gênero g sobre $GF(q)$.

Por muitos anos, a pergunta sobre quantos pontos racionais uma curva de gênero g sobre um corpo finito com q elementos chamou a atenção de matemáticos. Em 1940, *A. Weil* [58] provou a hipótese de Riemann para curvas sobre corpos finitos. Como um corolário imediato obteve um limitante superior para o número de pontos racionais em uma curva geometricamente irredutível não-singular $\mathcal{X}$ de gênero g sobre um corpo finito de cardinalidade q, isto é

$$N_q(\mathrm{g}) \leq q + 1 + 2\mathrm{g}\sqrt{q}. \tag{3.10}$$

Este limitante foi provado para curvas elípticas (isto é, g = 1) por *H. Hasse* em 1933, [58]. Porém, a questão de achar o número máximo $N_q(\mathrm{g})$ de pontos racionais em uma curva irredutível não-singular de gênero g sobre um corpo finito $GF(q)$ não atraiu a atenção dos matemáticos até que Goppa introduziu os códigos geométricos em 1980, [24].

Em 1981, *Ihara* mostra em [32] que

$$N_q(\mathrm{g}) \leq q + 1 + \left\lfloor (\sqrt{(8q+1)\mathrm{g}^2 + 4(q^2 - q)\mathrm{g}} - \mathrm{g})/2 \right\rfloor, \tag{3.11}$$

onde $\lfloor a \rfloor$ denota a parte inteira de a. Para $\mathrm{g} > (q - \sqrt{q})/2$ o limitante (3.11) é melhor que o limitante (3.10). Em [50], *Serre* mostra que o limitante de Weil (3.10) pode ser melhorado para

$$N_q(\mathrm{g}) \leq q + 1 + \mathrm{g}\lfloor 2\sqrt{q} \rfloor .$$

No mesmo trabalho, Serre introduziu a idéia de "fórmula explicita"em analogia com a Teoria dos Números, para obter melhores limitantes superiores para $N_q(\mathrm{g})$.

Teorema 3.4.1 *[58] Seja $\mathcal{X}$ uma curva projetiva não-singular de gênero g definida sobre $GF(q^r)$. Se $N_{q^r}(\mathcal{X})$ denota o número de pontos racionais de $\mathcal{X}$, então*

$$|N_{q^r}(\mathcal{X}) - q^r - 1| \leq \mathrm{g}\lfloor 2q^{r/2} \rfloor,$$

onde $\lfloor a \rfloor$ denota a parte inteira de a.

Definição 3.4.2 *[58] Uma curva projetiva $\mathcal{X}$ é maximal quando*

$$N_{q^r}(\mathrm{g}) = q^r + 1 + \mathrm{g}\left\lfloor 2\sqrt{q^r} \right\rfloor .$$

Um exemplo conhecido de uma curva maximal é a chamada curva hermitiana que definiremos em breve.

A maioria das curvas que iremos abordar será representada através de equações envolvendo polinômios em duas variáveis sobre um corpo finito, objetivando sempre os modelos projetivos não-singulares das curvas.

Nesta subseção apresentamos as principais curvas algébricas mais conhecidas sobre corpos finitos. Os gráficos dos exemplos considerados são gráficos de curvas sobre o corpo dos números reais. Calcularemos todos os pontos com coordenadas nos corpos finitos $GF(2)$, $GF(4)$, $GF(5)$, $GF(9)$ e $GF(16)$, para as curvas aqui mencionadas.

Curvas de Fermat

A curva de Fermat $\mathcal{F}_m$ é uma curva plana projetiva sobre $GF(q)$ com equação definida por

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

onde $mdc(m, q) = 1$. As derivadas parciais de $X^m + Y^m + Z^m$ são mX^{m-1}, mY^{m-1}, e mZ^{m-1}. Seu gênero é $\mathrm{g} = (m-1)(m-2)/2$.

Por exemplo, a curva dada por $x^5 + y^5 + 1 = 0$ sobre o corpo $GF(4^2) = GF(16)$ é uma curva de Fermat não-singular com gênero 6. A equação homogênea $X^5 + Y^5 + Z^5 = 0$ é chamada de superfície quíntica com singularidade isolada ou cone de Fermat. A origem é o único ponto singular. As correspondentes curvas são mostradas na Figura 3.8.

Curvas Hermitianas

Seja $q = r^2$. A curva H_r sobre o corpo $GF(q)$ definida pelas equações afins $x^{r+1} + y^{r+1} + 1 = 0$ e $x^{r+1} - y^r - y = 0$, são chamadas curvas Hermitianas. As correspondentes equações homogêneas são,

$$X^{r+1} + Y^{r+1} + Z^{r+1} = 0 \quad \text{e} \quad X^{r+1} - Y^r Z - Y Z^r = 0. \tag{3.12}$$

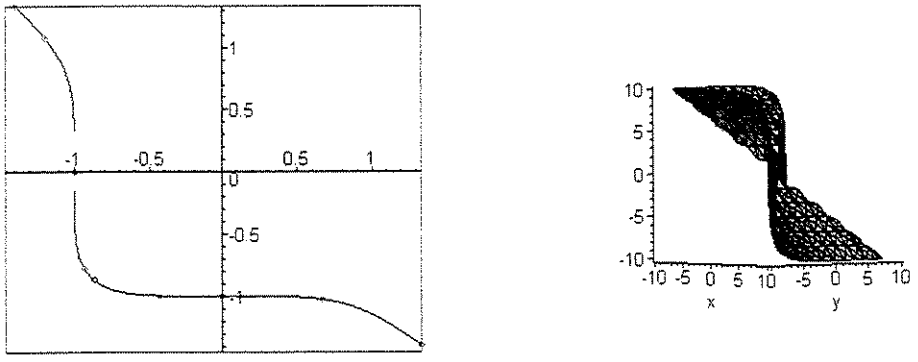


Figura 3.8: *Curvas de Fermat*

A equação afim $x^{r+1} - y^r - y = 0$ tem $(0:1:0)$ como seu único ponto no infinito e r^3 outros pontos racionais sobre $GF(r^2)$ no plano afim.

O gênero da curva H_r é dado por

$$\mathrm{g}(\mathsf{H}_r) = \frac{r(r-1)}{2}.$$

Observe que para todo $\alpha \in GF(r^2)$ existem r elementos $\beta \in GF(r^2)$ tal que $\beta^r + \beta = \alpha^{r+1}$.

A seguir, forneceremos vários exemplos de curvas hermitianas:

a) A curva dada por $x^5 - y^4 - y = 0$ é uma curva hermitiana não-singular de gênero 6. A equação homogênea é $X^5 - Y^4Z - YZ^4 = 0$ é chamada de superfície quíntica não-singular. As correspondentes curvas são mostradas na Figura 3.9 (a);

b) A curva dada por $x^3 - y^2 - y = 0$ é uma curva hermitiana não-singular de gênero 1. A equação homogênea é $X^3 - Y^2Z - YZ^2 = 0$;

c) Seja H_3 uma curva hermitiana dada pela equação $x^4 = y^3 + y$ sobre $\mathbb{K} = GF(9) = GF(3)/ < x^2+x+2 >$. O gênero desta curva é 3. Esta curva tem 27 pontos racionais. O polinômio homogêneo associado é $X^4 - ZY^3 - Z^3Y = 0$. As correspondentes curvas são mostradas na Figura 3.9 (b);

d) Seja H_4 uma curva hermitiana dada pela equação $x^5 + y^5 + 1 = 0$ sobre $\mathbb{K} = GF(16)$. O gênero desta curva é 6. O seu polinômio homogêneo associado é $X^5 + Y^5 + Z^5 = 0$. As correspondentes curvas são mostradas na Figura 3.8.

Curvas subhermitianas

Seja s um divisor de $\sqrt{q}+1$, onde q é um quadrado, e seja $\mathcal{X}_s$ a curva com equação afim $y^{\sqrt{q}} + y = x^s$. Se $s = \sqrt{q}+1$, então $\mathcal{X}_s$ é a curva hermitiana sobre $GF(q)$, para $s < \sqrt{q}+1$, as curvas $\mathcal{X}_s$ são fatores de $\mathcal{X}_{\sqrt{q}+1}$, isto é, existe uma aplicação sobrejetiva $f_s : \mathcal{X}_{\sqrt{q}+1} \longrightarrow \mathcal{X}_s$ (é dada por $(x, y) \mapsto (x^{(\sqrt{q}+1)/s}, y)$). Essas curvas são chamadas subhermitianas. É bem conhecido que a curva $\mathcal{X}_{\sqrt{q}+1}$ (e conseqüêntemente todas as $\mathcal{X}_s$) é maximal, isto é, $\mathcal{X}_{\sqrt{q}+1}$

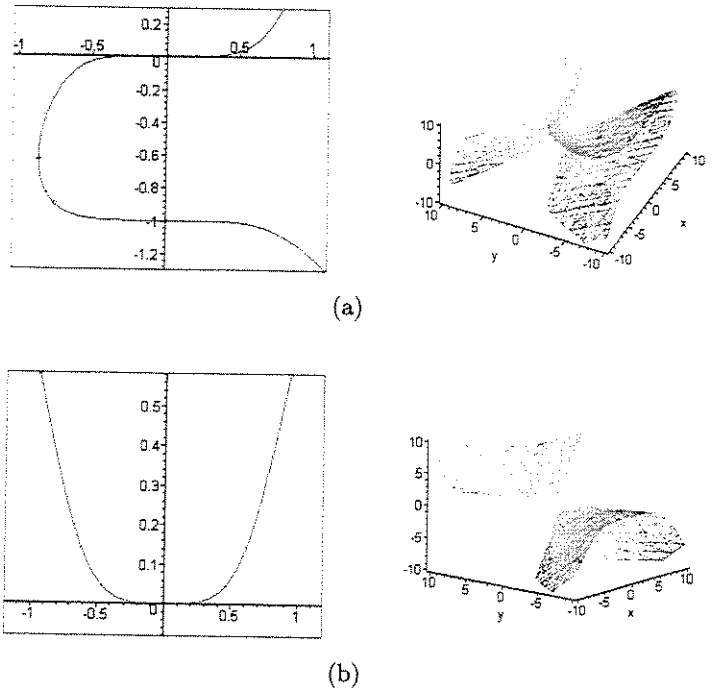


Figura 3.9: *Curvas Hermitianas*

tem o número máximo possível de pontos $GF(q)$-racionais para curvas do mesmo gênero, isto é,

$$N_q(\mathcal{X}_{\sqrt{q}+1}) = q\sqrt{q} + 1 = q + 1 + 2\mathrm{g}\sqrt{q},$$

onde $\mathrm{g} = (q - \sqrt{q})/2$ é o gênero de $\mathcal{X}_{\sqrt{q}+1}$. Em geral, os gêneros de $\mathcal{X}_s$ são iguais a $(\sqrt{q} - 1)(s - 1)/2$ e tem

$$N_q(\mathcal{X}_s) = q + 1 + 2\mathrm{g}_s\sqrt{q}.$$

Na curva $\mathcal{X}_s$ existe um único pólo em comum para x e y o qual é um ponto $GF(q)$-racional Q_∞.

Curvas Quasihermitianas

Estas curvas podem ser encontradas com maiores detalhes em [44].

Uma **curva quasihermitiana,** $C_{s,r}$, sobre $GF(q)$ (com $q = 2^m$) é uma curva plana projetiva, que tem por equação

$$Y^s Z^r + \beta_1 Y Z^{s+r-1} + \beta_2 X^{s+r} = 0,$$

onde $s, r \in \mathbb{N}$, $s \geq 2$, $r \geq 0$, $\beta_1, \beta_2 \in GF(q) \setminus \{0\}$.

O gênero da curva $C_{s,r}$ sobre qualquer corpo $\mathbb{K}$ de característica 2 é dado pelo seguinte resultado.

Teorema 3.4.3 *[44] Se ocorrerem as três seguintes condições*

i) $s+r = 2^n r_0$, *com* $n \geq 0$ *e* $r_0 \geq 1$ *ímpar,*

ii) $s-1 = 2^t s_0$, *com* $t \geq 0$ *e* $s_0 \geq 1$ *ímpar e*

iii) $a = mdc(r_0, s)$, $a = 2a_0 + 1$

então,

$$\mathrm{g}(C_{s,r}) = \frac{s_0(r_0-1)}{2} - a_0.$$

Proposição 3.4.4 *[44] São verdadeiras as seguintes afirmações:*

(*i*) As curvas de equações afins $y^s + y + x^{s+r} = 0$ e $y_1^s + \beta_1 y_1 + \beta_2 x_1^{s+r} = 0$ são isomorfas sobre $\overline{GF(q)}$;

(*ii*) Ambas as curvas têm o mesmo gênero;

(*iii*) Se $(s+r)$ e $(s-1)$ são primos em relação a $(q-1)$, então as curvas

$$y^s + y + x^{s+r} = 0 \quad e \quad y_1^s + \beta_1 y_1 + \beta_2 x_1^{s+r} = 0$$

são isomorfas sobre $GF(q)$;

(*iv*) Se $(s+r)$ e $(s-1)$ são primos em relação a $(q-1)$, então as curvas

$$y^s + y + x^{s+r} = 0 \quad e \quad y_1^s + \beta_1 y_1 + \beta_2 x_1^{s+r} = 0$$

têm o mesmo número de pontos racionais.

Como conseqüência da Proposição 3.4.4, Palanquez [44] considerou uma família de curvas planas projetivas $C_{s,r}$, absolutamente irredutíveis sobre o corpo finito $GF(q)$ de característica 2, definida conforme o próximo parágrafo.

Para cada par de números naturais $s \geq 2$ e $r \geq 0$ as curvas $C_{s,r}$ têm por equação $F_{s,r} = 0$, sendo que $F_{s,r} \in GF(q)[X,Y,Z]$ é o polinômio dado por

$$Y^s Z^r + Y Z^{s+r-1} + X^{s+r},$$

isto é, $\forall s \geq 2, \forall r \geq 0$, $C_{s,r} = V(Y^s Z^r + Y Z^{s+r-1} + X^{s+r})$.

Por exemplo, seja $\mathbb{K} = GF(16)$. Considere a curva $\mathcal{X}$ com equação $y^2 + yz + x^2 = 0$, onde $s = 2$ e $r = 0$. Essa é uma curva não-singular. A correspondente curva é mostrada na Figura 3.10 (a). Como $s = 2$ e $r = 0$, temos pelo Teorema 3.4.3, que $n = 1$, $r_0 = 1$, $t = 0$, $s_0 = 1$ e $a_0 = 0$. Logo, o gênero de $C_{2,0}$ é

$$\mathrm{g}(C_{2,0}) = \frac{1(1-1)}{2} - 0 = 0.$$

Os pontos racionais desta curva são:

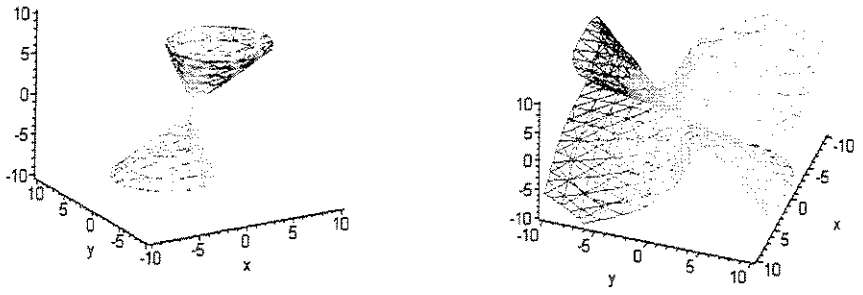
	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}
x	α	α	α^2	α^2	α^4	α^4	α^5	α^5	α^8	α^8	α^{10}	α^{10}	1	1	0	0
y	α^3	α^{14}	α^6	α^{13}	α^{11}	α^{12}	α^2	α^8	α^7	α^9	α	α^4	α^5	α^{10}	1	0
z	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Ainda no mesmo corpo, considere a curva $\mathcal{X}$ com equação $y^2z + yz^2 + x^3 = 0$, onde $s = 2$ e $r = 1$. Essa é uma curva não-singular. A correspondente curva é mostrada na Figura 3.10 (b). Como $s = 2$ e $r = 1$, temos pelo Teorema 3.4.3, que $n = 0$, $r_0 = 3$, $t = 0$, $s_0 = 1$ e $a_0 = 0$. Logo, o gênero de $C_{2,0}$ é

$$\mathrm{g}(C_{2,0}) = \frac{1(3-1)}{2} - 0 = 1.$$

Os pontos racionais desta curva são:

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
x	α^5	α^5	α^{10}	α^{10}	1	1	0	0
y	α^5	α^{10}	α^5	α^{10}	α^5	α^{10}	1	0
z	1	1	1	1	1	1	1	1



(a) (b)

Figura 3.10: *Curvas Quasihermitianas*

Curvas Elípticas

Uma curva sobre um corpo $\mathbb{K}$, com característica diferente de 2, dada por

$$y^2 = ax^3 + bx^2 + cx + d,$$

onde $a, b, c, d \in \mathbb{K}$ e o polinômio cúbico do lado direito não tem raízes múltiplas, é chamada **curva elíptica.**

Por exemplo, as curvas definidas por $y^2 = x^3 - x$, $y^2 = x^3 + 1$ e $y^2 = x^3 - 4$, são curvas elípticas. As correspondentes curvas são mostradas, respectivamente, na Figura 3.11.

As curvas definidas por $y^2 = x^3$ e $y^2 = x^2(x + 1)$ geram um cilindro cúbico cuspidal e um cilindro cúbico nodal, respectivamente. Não são curvas elípticas uma vez que os polinômios cúbicos têm raízes múltiplas. Isto pode ser visto na Figura 3.2 (c) e (d). Observe que elas são geometricamente diferentes das curvas elípticas, visto que cada uma delas tem um ponto singular em $(0, 0)$.

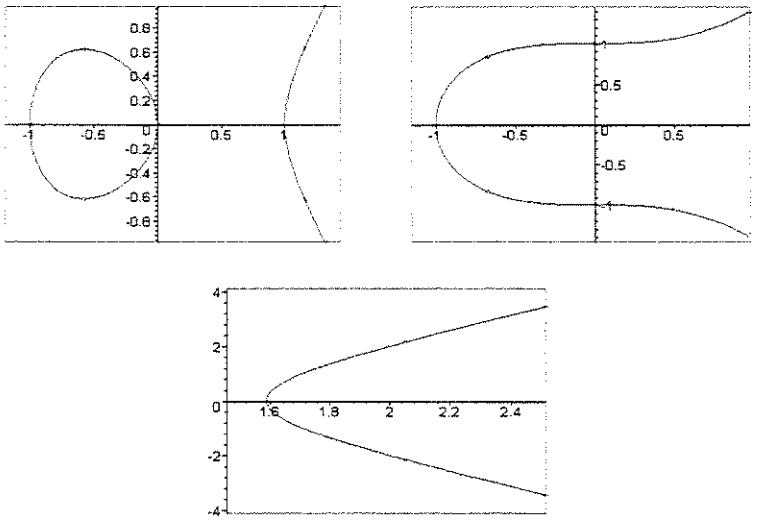


Figura 3.11: *Curvas Elípticas*

Curvas de Klein

A curva

$$x^m y + y^m + x = 0,$$

onde $m^2 - m + 1$ é relativamente primo a q, é definida como sendo a curva de Klein K_m. A correspondente equação homogênea é

$$X^m Y + Y^m Z + X Z^m = 0.$$

Observe que K_m é uma curva não-singular se $mdc(m^2 - m + 1, q) = 1$.

Seja $\mathbb{K} = GF(8)$. Considere a quártica de Klein, isto é, a curva $\mathcal{X}$ com equação $x^3y + y^3 + x = 0$, mostrada na Figura 3.12 (a). As correspondentes equações nos outros dois sistemas de coordenadas são $u^3v + v^3 + u = 0$ e $w^3z + z^3 + w = 0$. A equação homogênea é dada por

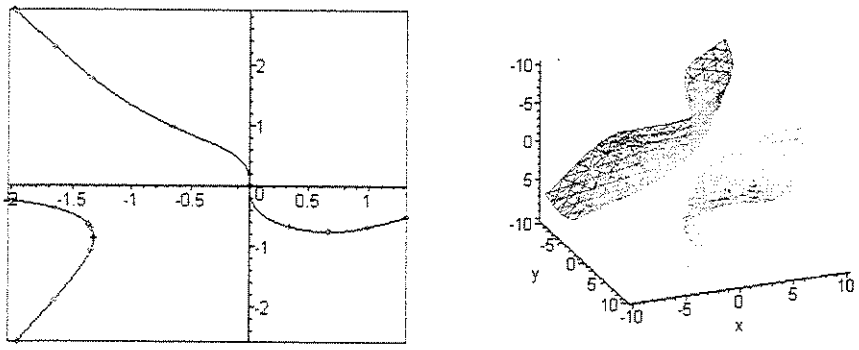
$$X^3Y + Y^3Z + XZ^3 = 0$$

e o seu grafico é mostrado na Figura 3.12 (b). Sobre o corpo $GF(2)$ os pontos racionais desta curva são $(1:0:0)$, $(0:1:0)$ e $(0:0:1)$. Em $GF(4)$, há mais dois pontos racionais, isto é, $(1:\alpha:1+\alpha)$ e $(1:1+\alpha:\alpha)$, se $GF(4) = \{0, 1, \alpha, \alpha^2\}$, onde $\alpha^2 = 1+\alpha$. Em $GF(8)$, há 24 pontos racionais.

Seja $GF(4) = \{0, 1, \alpha, \overline{\alpha}\}$, onde $\alpha^2 = 1 + \alpha = \overline{\alpha}$. Considere a curva de Klein sobre $GF(4)$, isto é, a curva $\mathcal{X}$ dada pela equação $x^2y + \alpha y^2 + \overline{\alpha}x = 0$. A equação homogênea é dada por

$$X^2Y + \alpha Y^2 Z + \overline{\alpha} X Z^2 = 0.$$

Essa é uma curva não-singular com gênero 1. Os nove pontos racionais desta curva são



(a) (b)

Figura 3.12: *Curvas de Klein*

dados pela tabela abaixo:

	P_1	P_2	P_3	P_4	P_5	P_6	Q_1	Q_2	Q_3
x	1	0	0	1	1	1	α	1	1
y	0	1	0	α	$\overline{\alpha}$	1	1	α	1
z	0	0	1	$\overline{\alpha}$	α	1	1	1	α

3.5 Curvas Associadas aos Polinômios (Chave1) e (Chave2)

Nesta seção utilizamos os resultados advindos da Seção 3.2. A condição de polinômio absolutamente irredutível garante que a curva está "conectada" em um certo sentido, isto é, a curva $\mathcal{X} : f(x, y) = 0$ é conexa. Na realidade, se $\mathcal{X}$ está definida como acima por uma forma homogênea F em $GF(q)[X, Y, Z]$, irredutibilidade significa simplesmente que F não é o produto de duas formas homogêneas não-constantes em $GF(q)[X, Y, Z]$ de grau menor. Absolutamente irredutível é uma propriedade geométrica que significa dizer que F é irredutível sobre qualquer extensão finita de $GF(q)$, isto é, a curva $\mathcal{X}$ quando vista sobre o fecho algébrico de $GF(q)$ não é a união disjunta de outras duas curvas. Em termos práticos, quando $\mathcal{X}$ está definida por um modelo afim $f(x, y)$, absolutamente irredutível implica que o anel de coordenadas $GF(q)[x, y]/(f)$ é um domínio de integridade e permanece assim se o corpo $GF(q)$ é substituído por qualquer extensão finita. Isso garante, em outras palavras, que o corpo quociente é um corpo de função de grau de transcendência 1. No que diz respeito ao gênero de $\mathcal{X}$, lembramos que é uma medida da complexidade da curva $\mathcal{X}$ quando comparada com a reta projetiva. Com isto, faz sentido falarmos agora em construção de curvas algébricas sobre corpos finitos associada aos polinômios (Chavel) e (Chave2) apresentados na Seção 3.2.

Observação 3.5.1 *Observe que a curva algébrica associada ao polinômio absolutamente irredutível (Chave2) sobre $GF(q)$ é não-singular.*

A seguir, apresentamos inúmeros exemplos de curvas algébricas com muitos pontos racionais advindas dos polinômios (Chavel) e (Chave2). Os gráficos das curvas consi-

deradas são sobre os reais. Calcularemos todos os pontos com coordenadas nos corpos finitos $GF(4)$, $GF(5)$, $GF(8)$, $GF(9)$ e $GF(16)$, para as curvas aqui mencionadas.

Exemplo 3.5.2 *Seja $GF(8) = GF(2)/\langle x^3+x+1\rangle$ o corpo de Galois gerado por α, raiz de x^3+x+1. Seja $\mathcal{X}_f$ a curva definida pela equação $y^2+xy+\alpha^5y+x^2+\alpha^4x+\alpha^5=0$ sobre $GF(8)$, onde $f(x,y)=y^2+xy+\alpha^5y+x^2+\alpha^4x+\alpha^5$. Esta curva é não-singular de gênero 0. O polinômio homogêneo de f é dado por*

$$\begin{aligned} F(X,Y,Z) = &\ Z^2\left((\tfrac{Y}{Z})^2+(\tfrac{XY}{Z^2})+(\tfrac{\alpha^5Y}{Z})+(\tfrac{X}{Z})^2+(\tfrac{\alpha^4X}{Z})+\alpha^5\right) \\ = &\ Y^2+XY+\alpha^5YZ+X^2+\alpha^4XZ+\alpha^5Z^2. \end{aligned}$$

Esta curva tem nove pontos racionais,como mostra a tabela seguinte:

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9
x	1	0	α^5	0	1	α	α	α^6	α^6
y	0	α^2	0	α^3	α^4	1	α^2	1	α^3
z	1	1	1	1	1	1	1	1	1

Pelo limitante da Definição 3.4.2 esta curva é maximal.

Exemplo 3.5.3 *Seja $GF(4)=\{0,1,\alpha,\overline{\alpha}\}$, onde $\alpha^2=\alpha+1=\overline{\alpha}$. Considere a curva $\mathcal{X}$ sobre $GF(4)$ dada pela equação $y^2+xy+x^2+\alpha xz=0$. Esta curva é não-singular com $\mathrm{g}=0$. Seus cinco pontos racionais são dados pela seguinte tabela:*

	P_1	P_2	P_3	P_4	P_5
x	α	α	1	1	0
y	α	0	α	$\overline{\alpha}$	0
z	1	1	0	0	1

Como esta curva possui 5 pontos racionais, pelo limitante da Definição 3.4.2, é uma curva maximal.

Exemplo 3.5.4 *Encontramos dois exemplos de curvas de $\mathrm{g}=0$ com 17 pontos racionais em seus modelos projetivos suaves (não-singulares) sobre $GF(16)$. Estas curvas são, portanto, definidas pelos seguintes polinômios:*

$$f_1(x,y)=y^2+xy+x^2+\alpha^9x \quad e \quad f_2(x,y)=y^2+xy+x^2+x.$$

Os respectivos polinômio homogêneos são:

$$F_1(X,Y,Z)=Y^2+XY+X^2+\alpha^9XZ \quad e \quad F_2(X,Y,Z)=Y^2+XY+X^2+XZ.$$

Os conjuntos dos pontos racionais de cada curva são dados, respectivamente, por $\{(\alpha^8,\ \alpha^{14},\ 1)$, $(\alpha^4,\ \alpha^{12},\ 1)$, $(\alpha^{14},\ \alpha^3,\ 1)$, $(\alpha,\ 1,\ 1)$, $(\alpha^5,\ \alpha^{12},\ 1)$, $(\alpha^8,\ \alpha^6,\ 1)$, $(\alpha^7,\ \alpha^3,\ 1)$, $(\alpha^5,\ \alpha^{14},\ 1)$, $(\alpha^4,\ \alpha^6,\ 1)$, $(\alpha,\ \alpha^4,\ 1)$, $(\alpha^{14},\ 1,\ 1)$, $(\alpha^7,\ \alpha^4,\ 1)$, $(\alpha^9,\ \alpha^9,\ 1)$, $(\alpha^9,\ 0,\ 1)$, $(\alpha^{10},\ 1,\ 0)$, $(\alpha^5,\ 1,\ 0)$, $(0,\ 0,\ 1)\}$ e $\{(\alpha^5,\ \alpha^6,\ 1)$, $(\alpha^5,\ \alpha^9,\ 1)$, $(\alpha^7,\ \alpha^6,\ 1)$, $(\alpha^7,\ \alpha^{10},\ 1)$, $(\alpha^{10},\ \alpha^3,\ 1)$, $(\alpha^{10},\ \alpha^{12},\ 1)$, $(\alpha^{11},\ \alpha^3,\ 1)$, $(\alpha^{11},\ \alpha^5,\ 1)$, $(\alpha^{13},\ \alpha^9,\ 1)$, $(\alpha^{13},\ \alpha^{10},\ 1)$, $(\alpha^{14},\ \alpha^5,\ 1)$, $(\alpha^{14},\ \alpha^{12},\ 1)$, $(1,\ 1,\ 1)$, $(1,\ 0,\ 1)$, $(\alpha^{10},\ 1,\ 0)$, $(\alpha^5,\ 1,\ 0)$, $(0,\ 0,\ 1)\}$. Como estas curvas possuem 17 pontos racionais e $\mathrm{g}=0$, então pelo limitante da Definição 3.4.2, são curvas maximais. As correspondentes curvas para f_1 e F_1 são mostradas, respectivamente, na Figura 3.13 (a).

Exemplo 3.5.5 *Seja $\mathcal{X}$ a curva definida pela equação $y^4+(x+1)y^3+(x+1)(x+2)y^2+(x+1)(x^2+1)y+(x+1)(x^3+2)=0$ sobre $GF(9)=GF(3)/<x^2+x+2>$. Observe que $\mathcal{X}$ é não-singular e seu gênero é 3. O polinômio homogêneo de f é dado por $F(X,Y,Z)=Y^4+(X+Z)Y^3+(X+Z)(X+2Z)Y^2+(X+Z)(X^2+Z^2)Y+(X+Z)(X^3+2Z^3)$. Os pontos racionais da curva são dados pela seguinte tabela:*

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}
x	α	α	α^2	α^3	α^3	α^5	α^5	α^6	α^7	α^7	1	0	1
y	α	1	α^7	α^3	1	α^3	α^5	α^5	α	α^7	0	α^4	0
z	1	1	1	1	1	1	1	1	1	1	α^4	1	1

As correspondentes curvas são mostradas, respectivamente, na Figura 3.13 (b). Esta curva não é maximal.

Exemplo 3.5.6 *Considere a curva $\mathcal{X}$ sobre $GF(4)$ dada pela equação $y^3+x^2y+xy^2+\alpha y^2z+\alpha yz^2+x^3+\overline{\alpha}x^2z=0$. Esta curva é não-singular com $\mathrm{g}=1$. Seus pontos racionais são dados pela seguinte tabela:*

	P_1	P_2	P_3	P_4	P_5	P_6	P_7
x	0	1	1	α	$\overline{\alpha}$	$\overline{\alpha}$	1
y	0	1	α	α	1	0	$\overline{\alpha}$
z	1	0	1	1	1	1	1

Exemplo 3.5.7 *Encontramos quatro exemplos de curvas de $\mathrm{g}=1$ com nove pontos racionais em seus modelos projetivos suaves (não-singulares) sobre $GF(4)$. Estas curvas são definidas pelos seguintes polinômios:*

$$\begin{aligned} f_1(x,y) &= y^3+x^3+1 \\ f_2(x,y) &= y^3+x(x^2+x-1) \\ f_3(x,y) &= y^3+xy^2+x^2y+x(x^2+x+1) \\ f_4(x,y) &= y^3+(x+1)y^2+(x+1)^2y+(x+1)(x^2+x+1) \\ &= y^3+(x+1)y^2+(x+1)^2y+x^3+1). \end{aligned}$$

Os respectivos polinômios homogêneos são:

$$\begin{aligned} F_1(X,Y,Z) &= Y^3+X^3+Z^3 \\ F_2(X,Y,Z) &= Y^3+X^3+X^2Z-XZ^2 \\ F_3(X,Y,Z) &= Y^3+XY^2+X^2Y+X^3+X^2Z+XZ^2 \\ F_4(X,Y,Z) &= Y^3+XY^2+ZY^2+X^2Y+Z^2Y+X^3+Z^3. \end{aligned}$$

Os pontos racionais de cada curva são dados, respectivamente, por

$$\begin{aligned} &\{(1,0,1),(\alpha,1,0),(1,0,\alpha),(\alpha^2,1,0),(1,0,\alpha^2),(1,1,0),(0,\alpha,1),(0,\alpha^2,1),(0,1,1)\}, \\ &\{(0,0,1),(1,\alpha,1),(1,0,\alpha),(1,\alpha^2,1),(1,0,\alpha^2),(1,1,0),(\alpha^2,1,0),(\alpha,1,0),(1,1,1)\}, \\ &\{(0,0,1),(\alpha,1,1),(1,0,\alpha),(\alpha^2,1,1),(1,0,\alpha^2),(1,1,0),(\alpha^2,\alpha,1),(\alpha,\alpha^2,1),(1,1,1)\}, \\ &\{(0,1,1),(\alpha,\alpha,1),(1,0,\alpha),(\alpha^2,1,1),(1,0,\alpha^2),(1,1,0),(\alpha,1,1),(\alpha^2,\alpha^2,1),(1,0,1)\}. \end{aligned}$$

Pelo limitante da Definição 3.4.2, estas curvas são maximais.

Exemplo 3.5.8 *Seja* $GF(5) = \{0, 1, 2, 3, 4\}$. *Para* $a_1 = 3$, $a_2 = 2$ *e* $a_3 = 0$, *temos, pelo Teorema 3.2.6, que a curva* $\mathcal{X}_f$ *sobre* $GF(5)$ *é definida pelo polinômio* $f(x, y) = y^3 + xy^2 + 3y^2 + x^2y + 2xy + 2y + x^3 + 3x^2$. *O polinômio homogêneo de* f *é dado por* $F(X, Y, Z) = Y^3 + XY^2 + 3Y^2Z + X^2Y + 2XYZ + 2YZ^2 + X^3 + 3X^2Z$. *Esta curva é não-singular de gênero* $\mathrm{g} = 1$. *Os dez pontos racionais desta curva são dados pela seguinte tabela:*

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}
x	2	0	0	0	3	4	4	1	1	4
y	0	0	3	4	2	2	3	2	3	1
z	1	1	1	1	1	1	1	0	0	0

Pelo limitante da Definição 3.4.2, esta curva é maximal.

Exemplo 3.5.9 *Encontramos dois exemplos de curvas de* $\mathrm{g} = 1$ *com 16 pontos racionais em seus modelos projetivos suaves (não-singulares) sobre* $GF(9)$. *Estas curvas são definidas pelos seguintes polinômios:*

$$\begin{aligned} f_1(x, y) &= y^3 + (x+1)(x+1)y + (x+1)(x^2+1) \quad e \\ f_2(x, y) &= y^3 + x^2y + x(x^2 + x - 1). \end{aligned}$$

Os respectivos polinômios homogêneos são:

$$\begin{aligned} F_1(X, Y, Z) &= XZ^2 + X^2Z + X^3 + YZ^2 + YX^2 + Z^3 + 2XYZ + Y^3 \quad e \\ F_2(X, Y, Z) &= Y^3 + X^2Y + X^3 + X^2Z - XZ^2. \end{aligned}$$

Os pontos racionais de cada curva são dados, respectivamente, por $\{(\alpha^7, 1, 0), (\alpha^6, \alpha^7, 1), (1, 1, 1), (\alpha^2, \alpha^5, 1), (\alpha^6, \alpha^3, 1), (\alpha^2, \alpha, 1), (1, \alpha, 1), (0, \alpha^3, 1), (0, 1, 1), (0, \alpha, 1), (\alpha^6, 0, 1), (\alpha^2, 0, 1), (\alpha^4, 0, 1), (\alpha^9, 0, 1), (\alpha^5, 1, 0), (1, 1, 0)\}$ *e* $\{(\alpha, \alpha^3, 1), (\alpha, \alpha^7, 1), (\alpha^3, \alpha^5, 1), (\alpha^4, \alpha, 1), (\alpha^4, \alpha^3, 1), (\alpha^4, 1, 1), (1, \alpha, 1), (1, \alpha^3, 1), (1, 1, 1), (\alpha^3, \alpha, 1), (\alpha^5, 1, 0), (1, 0, \alpha^5), (\alpha^7, 1, 0), (1, 0, \alpha^7), (0, 0, 1), (1, 1, 0)\}$. *Pelo limitante da Definição 3.4.2, estas curvas são maximais.*

Exemplo 3.5.10 *Seja* $\mathcal{X}_f$ *a curva definida pela equação* $y^3 + x^3 + x^2 - x = 0$ *sobre* $GF(16)$, *onde* $f(x, y) = y^3 + x^3 + x^2 - x$. *Esta curva é não-singular de gênero* 1. *O polinômio homogêneo de* $f(x, y)$ *é dado por* $F(X, Y, Z) = X^3 - XZ^2 + ZX^2 + Y^3$. *As correspondentes curvas são mostradas, respectivamente, na Figura 3.13 (c).*

O objetivo de apresentarmos estes exemplos de curvas algébricas maximais dadas pela Definição 3.2.5 e pela Proposição 3.2.8 é mostrar que existe a possibilidade de se utilizar estas curvas para possíveis construções de bons códigos lineares binários construídos através de curvas algébricas-geométricas, usando métodos conhecidos de concatenação. Esses códigos são chamados de códigos algébricos-geométricos (códigos AG) e foram introduzidos por Goppa, [24].

Observação 3.5.11 *Todas as curvas mencionadas nos Exemplos 3.5.2 a 3.5.10 são curvas suaves. A curva do Exemplo 3.5.10 é singular, se considerarmos definidas sobre o corpo* $GF(3^m)$. *As curvas dos Exemplos 3.5.2, 3.5.3, 3.5.4, 3.5.7, 3.5.8 e 3.5.9 são todas curvas máximais. A curva* f_1 *do Exemplo 3.5.7 é também uma curva Hermitiana, (veja equação (3.12)).*

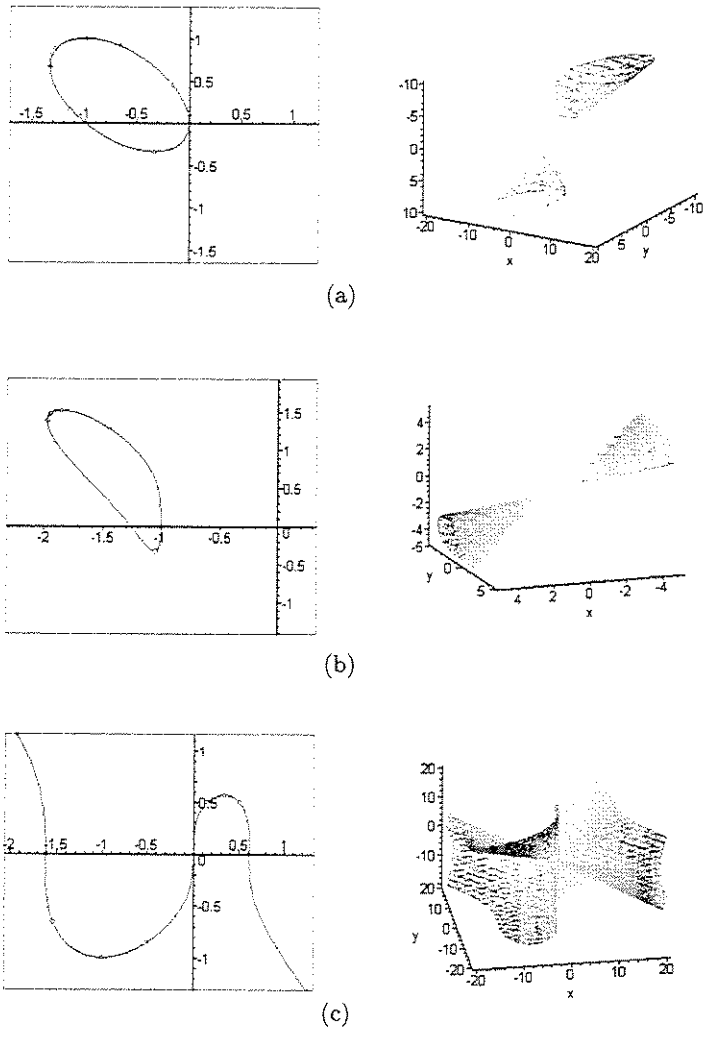


Figura 3.13: *Curvas construídas a partir dos polinômios (Chave1) e (Chave2)*

Como as curvas dos Exemplos 3.5.2, 3.5.3, 3.5.4, 3.5.7, 3.5.8 e 3.5.9 são todas curvas máximais, isto é, curvas com muitos pontos racionais que são bastante utilizadas na construção de códigos AG. Então, apresentaremos agora um exemplo de código AG construído a partir de uma destas curvas algébricas. Para uma noção básica de construção de códigos AG que será utilizado no exemplo abaixo, (veja Apêndice 3.7).

Exemplo 3.5.12 *Considere* Ξ *o fecho algébrico de* $GF(4)$. *Assim, consideramos que a curva* $\mathcal{X}$ *seja a curva em* $\mathbb{P}^2$ *do exemplo (3.5.7), onde* $\mathrm{g} = 1$. *Observe que a terceira potência de um elemento de* $GF(4)$ *é* 0 *ou* 1, *e que todos os pontos racionais têm uma coordenada* 0. *Em* $Q = (0:1:1)$, *podemos tomar* $\mathrm{t} = x/z$ *como parâmetro local. Observe que a expressão* $\gamma = x/(y+z)$ *parece uma função perfeitamente razoável e de fato é em boa parte da curva* $\mathcal{X}$. *Porém, em* Q *a fração não faz sentido. Temos, portanto, que encontrar uma forma equivalente para* γ *próximo de* Q. *Para entender melhor o comportamento de* γ *em* Q, *teremos que representar a função diferentemente. Para este fim, observamos que na curva* $\mathcal{X}$, *temos que* $(y+z)(y^2+yz+z^2) = x^3$, *isto é,* $(y+z) = x^3/(y^2+yz+z^2)$. *Assim, em* $\mathcal{X}$ *temos*

$$\begin{aligned}\gamma(x,y,z) &= \frac{x}{y+z} = \frac{x(y^2+yz+z^2)}{x^3} = \frac{1}{x^2}\cdot\frac{(y^2+yz+z^2)}{1} \\ &= \mathrm{t}^{-2}\cdot\frac{(y^2+yz+z^2)}{z^2}\end{aligned}$$

onde o segundo fator à direita é regular e não é 0 *em* Q. *Por nossas convenções anteriores, dizemos que* γ *tem um pólo de ordem* 2 *em* Q. *Similarmente,* $\eta = y/(y+z)$ *tem um pólo de ordem* 3 *em* Q, *visto que*

$$\begin{aligned}\eta(x,y,z) &= \frac{y}{y+z} = \frac{y(y^2+yz+z^2)}{x^3} = \frac{1}{x^3}\cdot\frac{y(y^2+yz+z^2)}{1} \\ &= \mathrm{t}^{-3}\cdot\frac{(y^2+yz+z^2)}{z^3}.\end{aligned}$$

Construiremos em seguida dois códigos.

Primeiro, tomando $\mathrm{gr}(\mathrm{G}) = 2$, *isto é,* $\mathrm{G} = 2Q$, *temos que o código* $\mathfrak{C}(D,\mathrm{G})$ *tem dimensão* 2. *Temos que determinar duas funções que formem uma base para* $\mathsf{L}(2Q)$. *Uma delas é a função constante* 1, *que produz* **1** *como um vetor da base para* $\mathfrak{C}(D,\mathrm{G})$. *A outra função deve ser definida em* $\mathcal{X}$ *com exceção de* Q *onde tem um pólo de ordem* 2. *Esta outra função é* γ. *Assim,* $\{1,\gamma\}$ *é uma base para* $\mathsf{L}(2Q)$ *sobre* $GF(4)$. *Isto nos dá a seguinte matriz geradora para o código* $\mathfrak{C}(D,\mathrm{G})$

$$\begin{pmatrix} 1(P_1) & \dots & 1(P_8) \\ \gamma(P_1) & \dots & \gamma(P_8) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & \overline{\alpha} & \alpha & \alpha & \overline{\alpha} \end{pmatrix}, \tag{3.13}$$

e realmente, vemos que $d = 6$, *isto é* $\mathrm{v} = (1,1,0,0,\overline{\alpha},\alpha,\alpha,\overline{\alpha}) \in \mathfrak{C}(D,\mathrm{G})$.

Segundo, se tomarmos $\mathrm{gr}(\mathrm{G}) = 3$, *isto é,* $\mathrm{G} = 3Q$, *então temos que acrescentar uma linha a matriz (3.13), correspondendo a uma função que tem um pólo de ordem* 3 *em* Q. *A função que corresponde ao acréscimo da linha é* η. *Como* $\gamma = x/(y+z)$ *e* $\eta = y/(y+z)$ *são regulares fora de* Q *e tem um pólo de ordem* 2 *e* 3, *respectivamente, em* $Q = (0:1:1)$.

Assim as funções 1, γ *e* η *têm ordens de pólo mutuamente distintas e são elementos de* $\mathrm{L}(3Q)$. *Conseqüentemente a dimensão de* $\mathrm{L}(3Q)$ *é pelo menos 3. Como a curva* $\mathcal{X}$ *tem gênero 1, o grau de* $W - 3Q$ *é negativo, assim* $\dim(W - 3Q) = 0$. *Através do Teorema 3.7.9, temos que* $\dim(3Q) = 3$. *Portanto, fica claro agora por que no exemplo o espaço* $\mathrm{L}(3Q)$ *tem dimensão* 3. *Assim,* $\{1, \gamma, \eta\}$ *forma umaa base para* $\mathrm{L}(3Q)$ *sobre* $GF(4)$. *Isto nos dá a seguinte matriz geradora para o código algébrico-geométrico* $\mathfrak{C}(D, \mathrm{G})$

$$\begin{pmatrix} 1(P_1) & \dots & 1(P_8) \\ \gamma(P_1) & \dots & \gamma(P_8) \\ \eta(P_1) & \dots & \eta(P_8) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & \overline{\alpha} & \alpha & \alpha & \overline{\alpha} \\ 0 & 1 & \overline{\alpha} & \alpha & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Desta forma, a distância mínima é no mínimo 5, *isto é,* $d \geq 5$, *claro que, se vê imediatamente na matriz geradora que* $d = 5$, *isto é,* $\mathrm{v} = (0, 1, \overline{\alpha}, \alpha, 0, 0, 1, 1)$ *é uma palavra-código de* $\mathfrak{C}(D, \mathrm{G})$ *de peso igual a* 5.

3.6 Curvas Algébricas e Superfícies de Riemann

Nesta seção, apresentaremos a construção de superfície de Riemann $\mathcal{S}$ associada a um polinômio irredutível $f \in \mathbb{C}[x, y]$ e as propriedades da projeção canônica $\pi : \mathcal{S} \to \mathbb{C}$ (que é uma aplicação de revestimento ramificado no sentido topológico). O objetivo é desenvolver o conceito de superfície de Riemann de uma função algébrica f. Em seguida, apresentaremos a resolução das singularidades de $\mathcal{S}$ para obter o modelo da superfície de Riemann, que é idêntico, em todos os aspectos, ao modelo de variedade analítica de dimensão complexa 1. Para noções básicas topológicas veja Apéndice 3.8.

Usaremos a notação $\mathcal{C}(f)$ para a curva determinada por $f \in \mathbb{C}[x, y]$.

Não é difícil verificar que $\mathcal{C}(f)$ é um subconjunto fechado na topologia de $\mathbb{C}^2$ dada por uma das métricas usuais. Identificando $\mathbb{C}^2$ por $\mathbb{R}^4$, tem-se que $\mathcal{C}(f)$ é um subconjunto de $\mathbb{R}^4$ de dimensão real 2. Resulta que $\mathcal{C}(f)$ é uma superfície diferenciável usual em todos os pontos, com exceção de um número finito de pontos – os pontos singulares de f. Observe que $\mathcal{C}(f)$ está contida em $\mathbb{R}^4$ e não em $\mathbb{R}^3$, dessa forma, temos que fazer uso do gráfico real de $\mathcal{C}(f)$ ou de qualquer de suas seções por um plano real em $\mathbb{R}^4$, para podermos visualizar.

Nesse sentido, podemos chamar $\mathcal{C}(f)$ de **superfície de Riemann** (com singularidade) associada a f.

Agora, consideremos a projeção de $\mathbb{C}^2$ sobre a primeira coordenada, $(x, y) \mapsto x$. Assim, a restrição desta projeção a $\mathcal{C}(f)$ será denotada por π, isto é, $\pi : \mathcal{C}(f) \to \mathbb{C}$. É evidente que π é contínua relativamente à topologia induzida de $\mathbb{C}^2$. Denominaremos π como sendo a **projeção estrutural** de $\mathcal{C}(f)$.

Por outro lado, escreveremos

$$f = f_0(x)y^n + f_1(x)y^{n-1} + \cdots + f_{n-1}(x)y + f_n(x), \tag{3.14}$$

onde $f_0(x) \neq 0$. Como $\mathbb{C}$ é um corpo algebricamente fechado, temos que para todo $\alpha \in \mathbb{C}$ tal que α não é simultaneamente raiz dos polinômios $f_0(x), \dots, f_1(x)$, $f(\alpha, y) = 0$ tem alguma raiz em $\mathbb{C}$. Consequentemente, se $n \geq 1$, com exceção de um conjunto finito de pontos, então $\mathbb{C}$ é imagem de algum ponto de $\mathcal{C}(f)$ (em particular, a imagem $\pi(\mathcal{C}(f))$ de

$\mathcal{C}(f)$ é um conjunto aberto e denso em $\mathbb{C}$ na topologia usual). Com isso, temos o seguinte resultado.

Proposição 3.6.1 *[55] Sejam $f \in \mathbb{C}[x,y]$, como em (3.14), um polinômio irredutível, $\mathcal{C}(f)$ a superfície de Riemann associada e $\pi : \mathcal{C}(f) \to \mathbb{C}$ a projeção estrutural. Então:*

a) π é constante se, e somente se, $n = 0$;

b) Se π não é constante, a imagem de $\mathcal{C}(f)$ é o complementar de um conjunto finito de pontos de $\mathbb{C}$;

c) Se π não é constante, a imagem inversa por π de qualquer ponto de $\pi(\mathcal{C}(f))$ é um conjunto finito de pontos de $\mathcal{C}(f)$. Com exceção de um conjunto finito de pontos, a imagem inversa de todo ponto de $\pi(\mathcal{C}(f))$ admite n pontos (incluindo suas multiplicidades).

Observação 3.6.2 *A multiplicidade de um ponto $(a,b) \in \mathcal{C}(f)$ é, por definição, a multiplicidade de b como raiz de $f(a,y) = 0$.*

Na notação acima, o inteiro n é chamado o **grau** da projeção $\pi : \mathcal{C}(f) \to \mathbb{C}$.

Proposição 3.6.3 *Um polinômio irredutível f, dado em (3.14), admite apenas um número finito de pontos críticos.*

De acordo com a Proposição 3.6.3, existe apenas um número finito de pontos críticos da função algébrica implícita $y = y(x)$ definida por f. Dessa forma, com exceção de um conjunto finito de pontos, a imagem inversa de todo ponto de $\mathbb{C}$ admite n pontos distintos.

Se y é uma solução da equação polinomial

$$f_0(x)y^n + f_1(x)y^{n-1} + \cdots + f_{n-1}(x)y + f_n(x) = 0,$$

onde $f_0 \neq 0$, $f_1, \cdots, f_n$ são polinômios em x e n é um inteiro positivo, então $y = f(x)$ é chamada uma **função algébrica de** x.

Veja por exemplo, que $y(x) = x^{1/2}$ é uma solução da equação $y^2 - x = 0$ e, portanto, é uma função algébrica de x.

Proposição 3.6.4 *[9] Sejam $f(x,y)$ como em (3.14) um polinômio irredutível e S seu conjunto de pontos singulares. Então para todo $x \in \mathbb{C} \cup \{\infty\} \backslash S$ existem n-raízes distintas $y_1(x), y_2(x), \ldots, y_n(x)$ da equação $f(x,y) = 0$.*

A Proposição 3.6.4 nos mostra que, se escolhermos n valores distintos $y_1, y_2, \ldots, y_n$, satisfazendo as suas hipoteses, podemos construir um sistema de n equações e n incógnitas utilizando a matriz de Vandermonde de $y_1, y_2, \ldots, y_n$. (Veja [9]).

Recordemos que uma **variedade topológica de dimensão** m é um espaço de Hausdorff X, conexo por arcos, tal que todo ponto de X admite uma vizinhança homeomorfa a um aberto do $\mathbb{R}^m$. Se $m = 2$, a variedade é dita uma **superfície topológica**. Uma

aplicação contínua $\pi : \widetilde{\mathrm{V}} \to \mathrm{V}$, entre variedades topológicas de dimensão m, é uma **aplicação de recobrimento (ou revestimento)** se todo $v \in \mathrm{V}$ admite uma vizinhança $U \subset \mathrm{V}$ tal que $\pi^{-1}(U)$ é a união disjunta de abertos $\widetilde{U}_i \subset \widetilde{\mathrm{V}}$ tais que $\pi|_{\widetilde{U}_i} : \widetilde{U}_i \to U$ é um homeomorfismo. (Veja Figura 3.14).

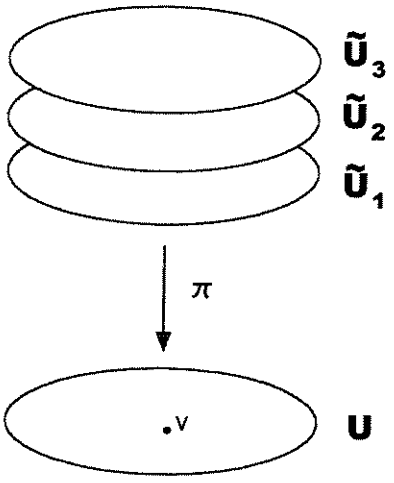


Figura 3.14: *Recobrimento*

Uma vizinhança U nas condições dadas acima será chamada **admissível.**

Note que uma aplicação de recobrimento $\pi : \widetilde{\mathrm{V}} \to \mathrm{V}$ é, em particular, um homeomorfismo local, isto é, dado um elemento $\widetilde{v} \in \widetilde{\mathrm{V}}$, existe $U \subset \mathrm{V}$, vizinhança admissível de $\pi(\widetilde{v})$ em V, tal que a restrição de π à componente conexa de $\pi^{-1}(U)$ contendo $\widetilde{v}$ é um homeomorfismo sobre sua imagem.

Definição 3.6.5 *Uma **aplicação de recobrimento** $\pi : \widetilde{\mathrm{V}} \to \mathrm{V}$ é chamada **finita** se, para todo $v \in \mathcal{V}$, $\pi^{-1}(v)$ é um conjunto finito de pontos. Neste caso, o número de pontos nas fibras $\pi^{-1}(v)$ fornece, à medida que v percorre* V, *uma aplicação* $\mathrm{V} \to \mathbb{Z}$ *que é localmente constante, mais precisamente constante em cada componente conexa de* V. *Se* V *é conexa, o inteiro n, imagem desta aplicação, é o **grau** do recobrimento. Neste caso, dizemos que $\pi : \widetilde{\mathrm{V}} \to \mathrm{V}$ é um **recobrimento** a n **folhas**.*

Dados um recobrimento $\pi : \widetilde{\mathrm{V}} \to \mathrm{V}$, um caminho (contínuo) $\gamma : [0,1] \to \mathrm{V}$ e um ponto $\widetilde{v} \in \widetilde{\mathrm{V}}$, um **levantamento** de γ **com ponto inicial** $\widetilde{v}$ é um caminho (contínuo) $\widetilde{\gamma} : [0,1] \to \widetilde{\mathrm{V}}$ tal que $\widetilde{\gamma}(0) = \widetilde{v}$ e tal que $\pi \circ \widetilde{\gamma} = \gamma$. Vejamos agora o seguinte resultado:

Lema 3.6.6 *[55] Seja $\pi : \widetilde{\mathrm{V}} \to \mathrm{V}$ um recobrimento. Para todo caminho γ em* V *e para todo ponto $\widetilde{v} \in \widetilde{\mathrm{V}}$ tal que $\pi(\widetilde{v}) = \widetilde{\gamma}(0)$, existe um levantamento de γ com ponto inicial $\widetilde{v}$.*

Demonstração. Como $[0,1]$ é compacto, existe n suficientemente grande tal que $\gamma[\frac{i-1}{n}, \frac{i}{n}] \subset U_i$ para alguma vizinhança admissível U_i, para todo $i \in \{1, 2, \ldots, n\}$. Chamaremos de $\widetilde{U}_1$ a componente conexa de $\pi^{-1}(U_1)$ contendo o ponto $\widetilde{v}$ dado; seja $\eta_1 : U_1 \to \widetilde{U}_1$

o homeomorfismo inverso de $\pi\mid_{\widetilde{U}_i}: \widetilde{U}_1 \to U_1$. Então, $\widetilde{\gamma}_1 = \eta_1 \circ \gamma\mid_{[0,1/n]}$ é um caminho iniciando em $\widetilde{v}$ tal que $\pi \circ \widetilde{\gamma}_1 = \gamma\mid_{[0,1/n]}$. Em outras palavras, $\widetilde{\gamma}_1$ é um levantamento do trecho $\gamma\mid_{[0,1/n]}$ de γ, com ponto inicial $\widetilde{v}$. Repetindo esse procedimento para o trecho $\gamma : [\frac{1}{n}, \frac{2}{n}] \to U_2$, obtemos o levantamento $\widetilde{\gamma}_2 : \eta_2 \circ \gamma\mid_{[1/n,2/n]}$ com ponto inicial $\widetilde{\gamma}_1(1/n) = \eta_1(\gamma(1/n)) = \eta_2(\gamma(1/n))$. Prosseguindo dessa forma, obtemos finalmente um levantamento de γ com ponto inicial $\widetilde{v}$ (veja Figura 3.15).

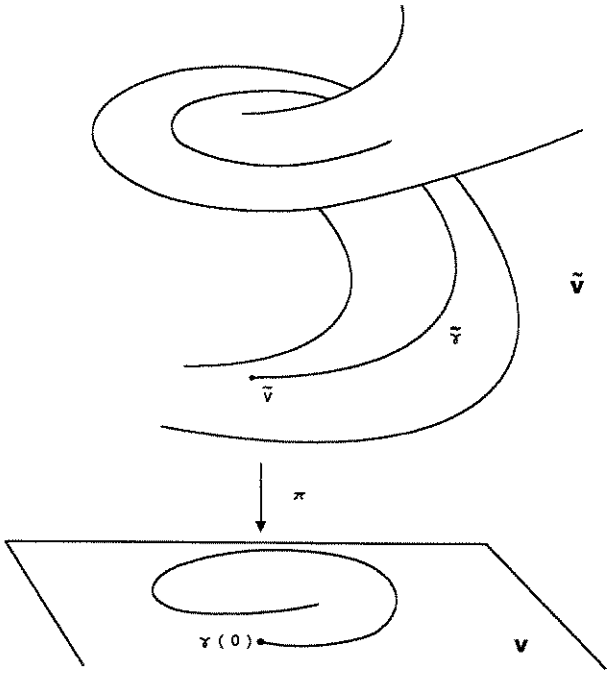


Figura 3.15: *Levantamento de* γ

■

Proposição 3.6.7 *[55] Sejam* $\mathcal{C}(f)$ *a superfície de Riemann associada a um polinômio irredutível* $f \in \mathbb{C}[X,Y]$ *e* $\pi : \mathcal{C}(f) \to \mathbb{C}$ *a projeção estrutural. Se* $c_1, c_2, \ldots, c_k$ *são os pontos críticos de* f*, a restrição*

$$\pi\Big|_{\mathcal{C}(f)\setminus\cup_{i=1}^{k}\pi^{-1}(c_i)} : \mathcal{C}(f)\setminus \cup_{i=1}^{k} \pi^{-1}(c_i) \to \mathbb{C}\setminus\{c_1, c_2, \ldots, c_k\}$$

é um recobrimento a $n = \deg_Y f$ *(grau de* f *em relação a variável* Y*) folhas.*

Sejam $\widetilde{\mathrm{V}}$ e V superfícies topológicas, exceto, possivelmente, em um conjunto discreto de pontos. Seja $\pi : \widetilde{\mathrm{V}} \to \mathrm{V}$ uma aplicação contínua. Suponhamos que existe um subconjunto $\mathrm{D} \subset \mathrm{V}$ discreto tal que a restrição $\pi\Big|_{\widetilde{\mathrm{V}}\setminus\pi^{-1}(\mathrm{D})} : \widetilde{\mathrm{V}}\setminus\pi^{-1}(\mathrm{D}) \to \mathrm{V}\setminus\mathrm{D}$ seja um recobrimento de grau n. Neste caso, dizemos que $\pi : \widetilde{\mathrm{V}} \to \mathrm{V}$ é um **recobrimento ramificado** de grau n.

Como conseqüência da Proposição 3.6.7, a projeção estrutural $\pi : \mathcal{C}(f) \to \mathbb{C}$ associada a um polinômio irredutível $f = f_0(x)y^n + \cdots + f_n(x)$ (com $f_0(x) \neq 0$ e $n \geq 1$) é um recobrimento ramificado de grau n.

Definição 3.6.8 *A* ***ordem de ramificação*** *de π no ponto (c,b) (ou de (c,b), a projeção π estando subentendida) é o inteiro não negativo $r-1$, onde r é o número de folhas do (único) ramo de f centrado em (c,b). Usaremos para isto a seguinte notação: $\mathcal{O}_\pi(c,b)$.*

Dizemos que (c,b) é um **ponto de ramificação** de π (ou de $\mathcal{C}(f)$, π estando subentendida) se a ordem de ramificação for maior ou igual a 1, isto é, se o ramo centrado em (c,b) apresenta pelo menos duas folhas.

O inteiro $\sum_{\substack{q\in\mathcal{C}(f)\\ q \text{ não-singular}}} \mathcal{O}_\pi(q)$ é chamado a **ordem de ramificação não-singular** de π.

Observação 3.6.9 *O que aparece, na literatura sobre o assunto, como índice de ramificação é o número de folhas do ramo. Usaremos a notação: $e_\pi(q)$. Assim, temos que $\mathcal{O}_\pi(q) = e_\pi(q) - 1$, de maneira que a ordem de ramificação não-singular de π também aparece como $\sum_{\substack{q\in\mathcal{C}(f)\\ q \text{ não-singular}}} (e_\pi(q)-1)$.*

Corolário 3.6.10 *[55] Se $(a,b) \in \mathcal{C}(f)$ é um ponto não-singular, tem-se que $\mathcal{O}_\pi((a,b)) = ord_{(a,b)}(X-a)$.*

Necessitamos agora, considerar a ordem de ramificação de $\pi : \mathcal{C}(f) \to \mathbb{C}$ num ponto singular de $\mathcal{C}(f)$, bem como entender o processo de "desingularização" de uma curva algébrica.

Para definir rigorosamente a ordem de ramificação em um ponto $(a,b) \in \mathcal{C}(f)$ (singular ou não), não é essencial resolver explicitamente as singularidades de $\mathcal{C}(f)$. Basta saber o número de folhas r_i em cada um dos ramos $x = a + t^{r_i}$, $y = \mu_i(t)$ de f em (a,b), definindo então $\mathcal{O}_\pi((a,b)) = \sum_i r_i$.

A resolução de singularidades de $\mathcal{C}(f)$ esclarece o conteúdo geométrico da projeção $\pi : \mathcal{C}(f) \to \mathbb{C}$, permitindo substituir π por uma outra "projeção" $\widetilde{\pi} : \widetilde{\mathcal{C}(f)} \to \mathbb{C}$ tal que $\widetilde{\mathcal{C}(f)}$ é uma superfície topológica genuína, isto é, sem pontos excepcionais. $\widetilde{\mathcal{C}(f)}$ é o modelo rigoroso que Riemann procurava.

O modelo de Riemann era ideal, desta forma não "cabendo" no espaço $\mathbb{R}^3$ sem auto-interseções. Assim, $\widetilde{\mathcal{C}(f)}$ não está em $\mathbb{R}^3$. Na melhor das hipóteses, $\widetilde{\mathcal{C}(f)} \subset \mathbb{C}^2 = \mathbb{R}^4$ (por exemplo, se f não tem pontos singulares). Em geral, necessita-se de mais dimensões, com isto $\mathbb{C}^2$ é, muitas vezes, também insuficiente.

Sabemos que, sob certos aspectos, é indispensável incluir o estudo do comportamento numa vizinhança de P_∞. Lembremos por exemplo que o resultado de que o número de zeros e pólos (incluindo as respectivas multiplicidades) de uma função racional em $\mathbb{C}$ coincidem, só é válido mediante a inclusão do ponto P_∞. Com isto, temos também que para o estudo da ramificação da projeção estrutural $\pi : \mathcal{C}(f) \to \mathbb{C}$, é importante considerar o ponto P_∞. Fazemos a seguinte pergunta: se compactificarmos $\mathbb{C}$ mediante à introdução de P_∞, então qual será o processo de compactificação de $\mathcal{C}(f)$ que devemos usar de modo que a compactificada $\overline{\mathcal{C}(f)}$ seja definida por equações algébricas? A resposta para isso é usar o **plano projetivo** $\mathbb{P}^2$. Como vimos anteriormente, os elementos de $\mathbb{P}^2$ são classes de equivalências de triplas $(a,b,c) \in \mathbb{C}^3\backslash\{(0,0,0)\}$ relativas à seguinte relação: $(a,b,c) \sim (a_1,b_1,c_1)$ se, e só se, existe $\lambda \in \mathbb{C}$, $\lambda \neq 0$, tal que $a_1 = \lambda a$, $b_1 = \lambda b$, $c_1 = \lambda c$, que representamos por $(a:b:c)$.

Lema 3.6.11 *[55]* $\mathbb{P}^2$ *é uma compactificação de* $\mathbb{C}^2$.

A seguir, $\mathbb{K}$ será um corpo algebricamente fechado com característica arbitrária. É bastante conhecido que os resultados e propriedades apresentadas para os casos do corpo de números complexos $\mathbb{C}$ é válido para um corpo algebricamente fechado $\mathbb{K}$.

Proposição 3.6.12 *[55] Seja* $\mathcal{X}$ *uma curva algébrica em* $\mathbb{P}^2$. *Então existe um polinômio homogêneo* $F \in \mathbb{K}[X, Y, Z]$, *sem fatores múltiplos, tal que:*

(i) F *se anula em todo ponto* $P \in \mathcal{X}$.

(ii) Se $G \in \mathbb{K}[X, Y, Z]$ *é um polinômio que se anula em todo ponto de* $\mathcal{X}$, *então* F *é fator de* G.

Além disso, F *é unicamente determinado (a menos de fatores constantes) pelas condições (i), (ii) e pela condição de não ter fatores múltiplos.*

Observação 3.6.13 *Uma interpretação pouco formal de resolver as singularidades de uma curva* $\mathcal{X} \subset \mathbb{P}^2$ *consiste em aplicar certas transformações admissíveis de* $\mathbb{P}^2$ *a* $\mathcal{X}$ *de modo que se obtenha uma curva sem pontos singulares. Tais transformações devem, o tanto quanto possível, preservar as propriedades da curva original* $\mathcal{X}$.

Observação 3.6.14 *Se* $G \in \mathbb{K}[X, Y, Z]$ *é homogêneo, denotamos por* $\pounds(G)$ *a curva projetiva cujos pontos são os zeros de* G.

Teorema 3.6.15 *[55] Toda curva projetiva* $\mathcal{X} \subset \mathbb{P}^2$ *admite um modelo projetivo não-singular.*

Portanto, se for dado um polinômio irredutível $f \in \mathbb{C}[x, y]$, então podemos obter um modelo de superfície de Riemann associado tomando um modelo não-singular projetivo $\widetilde{\mathcal{X}}$ do fecho projetivo $\mathcal{X} \subset \mathbb{P}^2$ de $\mathcal{X}_0 \subset \mathbb{C}^2$, onde $\mathcal{X}_0 = \pounds(f)$. Em relação a $\widetilde{\mathcal{X}}$ valem as seguintes propriedades:

1. $\widetilde{\mathcal{X}}$ não tem pontos singulares. Em outras palavras, os "ramos" em cada ponto de $\widetilde{\mathcal{X}}$ não somente apenas estão separados como também só existe um único "ramo" em cada um dos pontos de $\widetilde{\mathcal{X}}$. Do ponto de vista analítico, $\widetilde{\mathcal{X}}$ é definido como uma variedade analítica suave compacta de dimensão (complexa) 1;

2. A ordem de ramificação em um ponto $P \in \widetilde{\mathcal{X}}$ é o número de folhas do (único) ramo em P. A ordem total de ramificação (= ordem total de ramificação não-singular) é $\sum_{P \in \widetilde{\mathcal{X}}} \mathcal{O}_\pi(P)$.

Exemplo 3.6.16 *Seja* $f(x, y) = y^2 - x$. *Neste caso,* $\widetilde{\mathcal{X}} = \pounds(Y^2 - XZ)$, *visto que* $Y^2 - XZ$ *não tem singularidades.*

A aplicação π *é* $(x : z)$, *onde* $x = \widetilde{X}$ *e* $z = \widetilde{Z}$. *Vemos que* π *é a restrição da aplicação racional* $(X : Z)$ *de* $\mathbb{P}^2$ *em* $\mathbb{P}^1$, *que é uma projeção centrada no ponto* $(0 : 1 : 0)$ *da reta*

$z = 0$ no infinito. O grau de π é 2; dado um ponto $(\lambda : 0 : 1) \in \mathbb{P}^1$, $\lambda \neq 0$, os pontos em $\pi^{-1}((\lambda : 0 : 1))$ são as interseções da reta $X - \lambda Z$ com a cônica $Y^2 - XZ$. Explicitamente, $\pi^{-1}((\lambda : 0 : 1)) = \{(\lambda : \lambda : 1), (\lambda : -\lambda : 1)\}$ se $\lambda \neq 0$, enquanto que $\pi^{-1}((0 : 0 : 1)) = \{(0 : 0 : 1)\}$ (multiplicidade 2) e, analogamente, $\pi^{-1}((1 : 0 : 0)) = \{(1 : 0 : 0)\}$ (multiplicidade 2). Assim, a ordem total de ramificação de π é $1 + 1 = 2$.

Exemplo 3.6.17 *Seja $f(x, y) = y^2 - x(x^2 - 1)$. É facil verificar que o fecho projetivo $\mathcal{X} = \pounds(Y^2Z - X(X^2 - Z^2)) \subset \mathbb{P}^2$ é não-singular. Logo, $\widetilde{\mathcal{X}} = \mathcal{X}$.*

O gráfico real de $\mathcal{X}$ é constituído de dois pedaços, apesar de que $\mathcal{X}$, como superfície de Riemann (dimensão real 2), é constituída de um só pedaço irredutível, o que se conclui da irredutibilidade do polinômio $y^2 - x(x^2 - 1)$. A projeção $\pi : \widetilde{\mathcal{X}} \to \mathbb{P}^1$ é, novamente, a restrição a $\widetilde{\mathcal{X}}$ da projeção $(X : Z)$ centrada em $(0 : 1 : 0)$. As soluções de

$$\begin{cases} x = \lambda z \\ y^2 z - x(x^2 - z^2) = 0 \end{cases}$$

são, além de $(0 : 1 : 0)$, os pontos $(\lambda : \sqrt{\lambda(\lambda^2 - 1)} : 1)$ e $(\lambda : -\sqrt{\lambda(\lambda^2 - 1)} : 1)$. Logo, o grau de π é 2. Se $\lambda = 0$, os dois pontos acima coincidem, mostrando assim que $\pi^{-1}((0 : 0 : 0)) = \{(0 : 0 : 1)\}$ e que $(0 : 0 : 1)$ é um ponto de ramificação de ordem 1. Conclusões analogas ocorrerem para o caso $\lambda = \pm 1$. Finalmente, $\pi^{-1}((1 : 0 : 0)) = \{(0 : 1 : 0)\}$, o que se vê calculando a interseção $\pounds(Z) \cap \mathcal{X}$. Assim, π admite 4 pontos de ramificação, com ordem de ramificação 1 em cada um deles.

Se $\widetilde{\mathcal{X}} \subset \mathbb{P}^2$ é não-singular, o gênero coincide com o inteiro $\frac{1}{2}(d-1)(d-2)$, onde d é o grau de $\widetilde{\mathcal{X}}$. Os Exemplos 3.6.16 e 3.6.17 apresentam gênero 0 e 1, respectivamente. Se $\widetilde{\mathcal{X}}$ admite r pontos singulares e tais pontos são pontos duplos ordinários ou cuspidais de primeira espécie, o gênero de $\widetilde{\mathcal{X}}$ é dado por $\frac{1}{2}(d-1)(d-2) - r$.

Proposição 3.6.18 *[61] Toda superfície de Riemann é uma variedade real orientável bidimensional $\mathcal{C}^\infty$ conexa por caminhos. Toda superfície de Riemann compacta com g asas é difeomorfa ao toro com g furos (ou buracos), para algum único inteiro $g \geq 0$. Em particular, para $g = 0$ a superfície é difeomorfa a esfera S^2, para $g = 1$ é difeomorfa ao toro $T^2 = S^1 \times S^1$.(Veja a Figura 3.16).*

3.6.1 Curvas algébricas e superfícies de Riemann compactas

Nesta seção apresentamos algumas superfícies de Riemann compactas de interesse. Estas incluem a reta projetiva, plano projetivo e curvas planas suaves.

Teorema 3.6.19 *[38] Se $f(x, y)$ é um polinômio irredutível, então seu "lugar geométrico" de raízes $\mathcal{X}$ é conexo. Conseqüentemente se f é não-singular e irredutível, $\mathcal{X}$ é uma superfície de Riemann.*

O "lugar geométrico" das raízes de um polinômio irredutível $f(x, y)$ é chamado de uma curva plana afim irredutível.

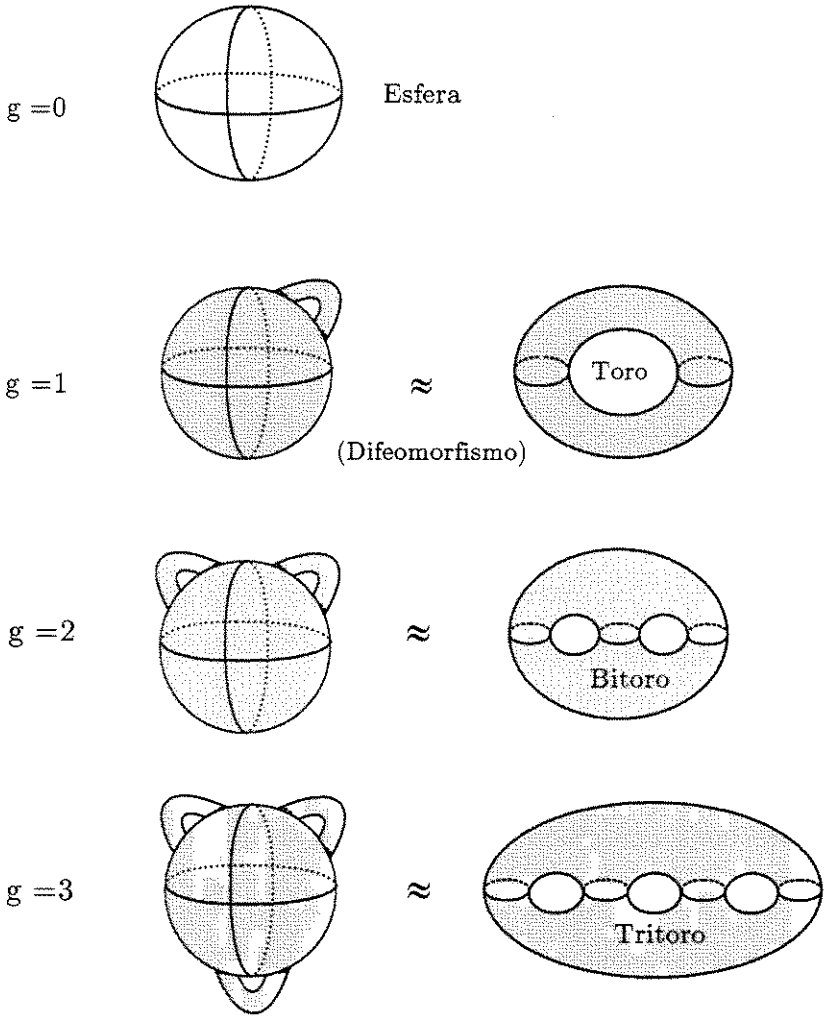


Figura 3.16: *Superfícies de Riemann Compactas*

A prova da conexidade de $\mathcal{X}$ se f é irredutível não é elementar, porém requer algumas das ferramentas de geometria algébrica, [52]. Admitindo a conexidade de $\mathcal{X}$ se f é irredutível, temos que: toda curva plana afim irredutível suave é uma superfície de Riemann.

As curvas mais estudadas e conhecidas dentre as curvas algébricas que geram supefícies de Riemann compactas são as curvas elípticas e as hiperelípticas, visto que elas tem aplicações em criptografia, teoria dos códigos, etc.

Exemplo 3.6.20 *Uma curva elíptica dada pelo polinômio* $f(x,y) = y^2 - (x-e_1)(x-e_2)(x-e_3)$ *tem gênero* $\mathrm{g} = 1$ *e é uma superfície de Riemann compacta, isto é, um toro, conforme mostra a Figura 3.17.*

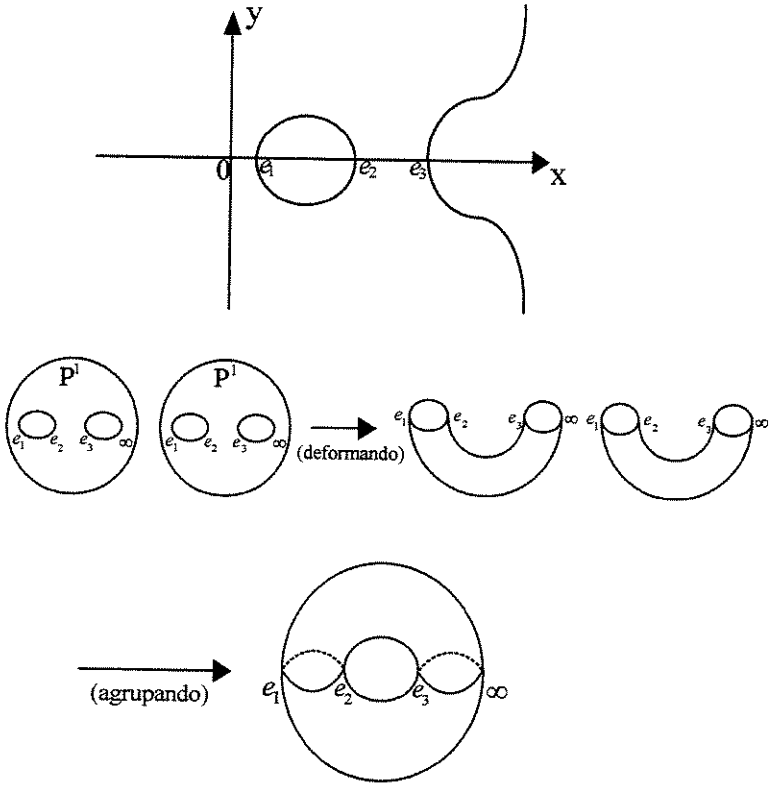


Figura 3.17: *Toro gerado por uma curva elíptica*

Exemplo 3.6.21 *Uma curva hiperelíptica*

$$y^2 = f(x), \qquad \deg f = 2\mathrm{g}+1,$$

tem gênero g *como uma superfície de Riemann. Para* $x \neq \alpha_1, \alpha_2, \ldots, \alpha_{2\mathrm{g}+1}$, $y^2 = f(x)$ *tem duas raízes distintas* $\pm\sqrt{f(x)}$. *A superfície de Riemann fechada é obtida juntando o ponto no infinito ao conjunto de todos os pontos* $(x, \sqrt{f(x)}), (x, -\sqrt{f(x)})$. *Isso pode ser visto na Figura 3.18.*

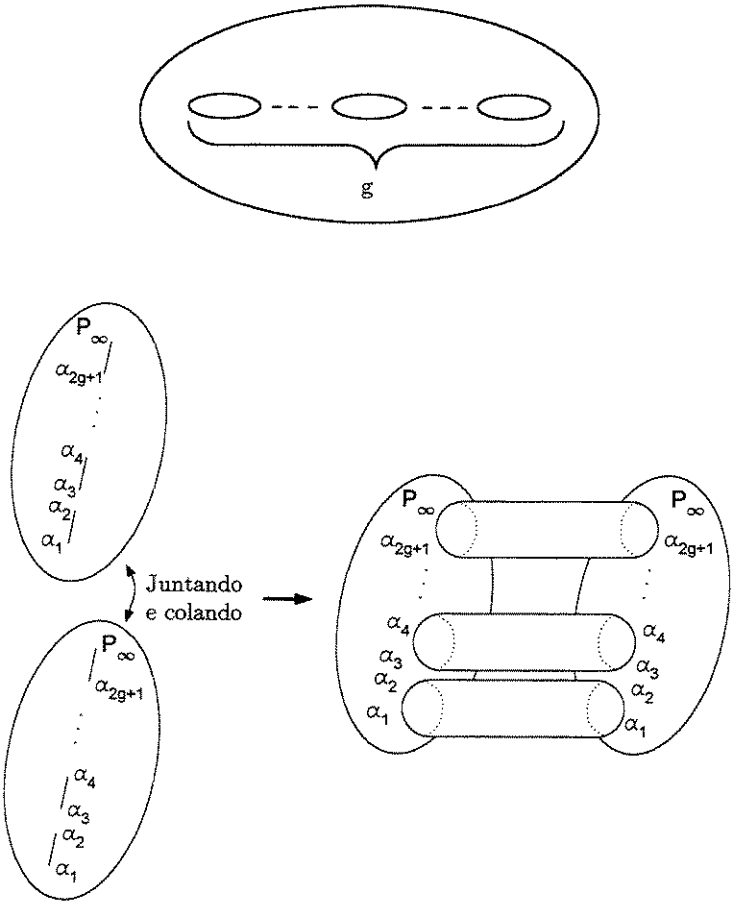


Figura 3.18: *Curva hiperelíptica gerando uma superfície de Riemann*

Se $f(x,y)$ é um polinômio irredutível, então os pontos no "lugar geométrico" das raízes de $\mathcal{X}$, onde f são formas singulares, é um conjunto finito. (Iste fato é nâo-trivial!). Se excluirmos estes pontos, então o subconjunto aberto resultante de $\mathcal{X}$ é uma superfície de Riemann. Isso é chamado a parte suave da curva plana afim $\mathcal{X}$ e, em geral, se f for um polinômio irredutível, a parte suave de seu lugar "geométrico" nulo é uma superfície de Riemann.

A reta projetiva $\mathbb{P}^1$ é o primeiro de uma série de exemplos que cercam as mais importantes e interessantes superfícies de Riemann compactas. Estas são superfícies mergulhadas no espaço projetivo.

Notamos aqui que o plano projetivo é compacto, pois pode ser coberto pelos três conjuntos compactos, isto é, os três conjuntos abertos

$$U_0 = \{[x:y:z] \mid x \neq 0\},\ U_1 = \{[x:y:z] \mid y \neq 0\} \text{ e } U_2 = \{[x:y:z] \mid z \neq 0\}.$$

Cada conjunto aberto U_i é homeomorfo ao plano afim $\mathbb{C}^2$.

Proposição 3.6.22 *[38] Seja $F(X,Y,Z)$ um polinômio homogêneo não-singular. Então a curva plana projetiva $\mathcal{X}$ que é seu lugar "geométrico" nulo em $\mathbb{P}^2$ é uma superfície de Riemann compacta. Além disso, para todo ponto de $\mathcal{X}$ pode-se tomar como uma coordenada local a razão das coordenadas homogêneas.*

Vimos anteriormente que $\mathcal{X}$ é uma superfície de Riemann, porém falta mostrar que a mesma é compacta. Na verdade, um subconjunto fechado de $\mathbb{P}^2$ é que é compacto. Tal superfície de Riemann é chamada uma curva plana projetiva suave, cujo grau é o grau do polinômio homogêneo definido.

Proposição 3.6.23 *[55] Um polinômio irredutível $f(x,y)$ admite apenas um número finito de pontos singulares.*

Definição 3.6.24 *Um ponto P em uma curva plana afim $\mathcal{X}$ definida por $f(x,y) = 0$ é chamado um nó da curva plana $\mathcal{X}$ se P for um ponto singular de $\mathcal{X}$, isto é, $f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$, mas a matriz Hessiana das segundas derivadas parciais*

$$\begin{pmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial y \partial x} & \frac{\partial^2 f}{\partial y^2} \end{pmatrix}$$

é não-singular em P, ou seja, se

$$\frac{\partial^2 f}{\partial x^2}(P)\frac{\partial^2 f}{\partial y^2}(P) \neq \left(\frac{\partial^2 f}{\partial x \partial y}(P)\right)^2.$$

Em termos dos coeficientes para f, esta condição significa que se expandirmos f em relação ao ponto $P = (x_0, y_0)$, o termo constante é zero (desde que $f(P) = 0$), os termos lineares são zero (desde que $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$), e os termos quadráticos são da forma

$$a(x-x_0)^2 + b(x-x_0)(y-y_0) + c(y-y_0)^2,$$

onde a equação quadrática homogênea $ax^2 + bxy + cy^2$ fatora-se em fatores lineares homogêneos distintos $l_1(x, y)l_2(x, y)$.

Se $f(P) = 0$ e uma das derivadas de f é não-nula em P, então $\mathcal{X}$ é localmente o gráfico de uma função, que, como está claro, é localmente igual a sua reta tangente. Note que a reta tangente em um ponto é exatamente os zeros da parte linear de f expandindo-se sobre esse ponto. Esse processo inteiro ocorre localmente para a singularidade em P. Pode ser executado igualmente bem para uma curva plana projetiva; afinal de contas, uma curva plana projetiva é localmente uma curva plana afim, e o conceito de um nó transfere-se imediatamente. Visto que uma curva plana projetiva, singular ou não, é certamente compacta (é um subconjunto fechado do plano projetivo que é compacto), o resultado de solucionar os nós de uma curva plana projetiva é uma superfície de Riemann compacta, se esta é conexa. Como em relação às curvas planas afins, a resolução é conexa se, e só se, o polinômio homogêneo que define a curva plana projetiva é irredutível. Isso resulta na seguinte proposição:

Proposição 3.6.25 *[38] Seja $F(X, Y, Z)$ um polinômio homogêneo irredutível de grau d, definindo o lugar "geométrico" das raízes por $\mathcal{X} \subset \mathbb{P}^2$. Assuma que em todos os pontos menos um número finito de pontos de $\mathcal{X}$, F é um polinômio não-singular, isto é, pelo menos uma de suas primeiras derivadas parciais é não-nula. Assuma além disso, que este número finito de pontos singulares são nós de $\mathcal{X}$. Então, a superfície de Riemann obtida pela solução destes nós de $\mathcal{X}$ é uma Superfície de Riemann compacta.*

Proposição 3.6.26 *[38] Seja $\mathcal{X}$ uma curva algébrica de gênero 0. Então $\mathcal{X}$ é isomorfa à esfera de Riemann $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\}$.*

Proposição 3.6.27 *[38] Toda curva algébrica de gênero um é isomorfa a uma curva cúbica plana projetiva suave.*

Proposição 3.6.28 *[38] Toda curva de gênero um é isomorfa ao toro complexo.*

Proposição 3.6.29 *[38] Toda curva algébrica de gênero dois é hiperelíptica.*

Teorema 3.6.30 (A trindade) *[42] As três seguintes categorias são equivalentes:*

I) Superfícies de Riemann Compactas;

II) Corpo de Funções Algébricas de uma variável;

III) Curvas projetivas irredutíveis não-singulares.

Corolário 3.6.31 *[42] Qualquer superfície de Riemann compacta é projetiva.*

Proposição 3.6.32 *[42] Uma superfície hiperelíptica $\mathcal{M}$ de gênero g (≥ 2) pode ser dada pela equação*

$$y^2 - (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_{2g+1}) = 0,$$

onde $\alpha_1, \ldots, \alpha_{2g+1}$ são números complexos mutuamente distintos, e vice-versa.

Proposição 3.6.33 (J.S. Milne) *Seja $\mathcal{X}$ uma curva algébrica afim não-singular sobre $\mathbb{C}$, então $\mathcal{X}(\mathbb{C})$ tem uma estrutura natural como uma superfície de Riemann.*

Demonstração. Seja P um ponto em $\mathcal{X}(\mathbb{C})$ e suponha que $\frac{\partial f}{\partial y}(P) \neq 0$. Então o teorema da função implícita mostra que a projeção $(x, y) \longmapsto x : \mathcal{X}(\mathbb{C}) \longrightarrow \mathbb{C}$ define um homeomorfismo de uma vizinhança aberta de P sobre uma vizinhança aberta de $x(P)$ em $\mathbb{C}$. Isto implica em ser uma vizinhança coordenada de P. ∎

Observação 3.6.34 *Observemos que se a curva $\mathcal{X}$ não é suave, quer dizer, é singular, para determinar seus pontos racionais é necessário considerar sua correspondente desingularização (modelo não singular de $\mathcal{X}$) $\widetilde{\mathcal{X}}$ (ver [18] Teorema 3, Seção 7.5). Por este motivo, para determinar o número de pontos racionais de $\mathcal{X}$ é necessário calcular nos seus pontos singulares o número de ramos que estas curvas apresentam em $\mathbb{K}$, .*

Exemplo 3.6.35 *Qualquer superfície de Riemann hiperelíptica é uma curva algébrica.*

Teorema 3.6.36 *[38] Toda superfície de Riemann compacta é uma curva algébrica.*

Teorema 3.6.37 *[9] A superfície de Riemann $\mathcal{M}$ associada ao polinômio irredutível $f(x, y)$ de grau n, em y, é compacta.*

Teorema 3.6.38 *[9] Seja $\widetilde{\mathcal{M}}$ uma superfície de Riemann compacta. Então existe um polinômio irredutível $f(x, y)$ tal que a superfície de Riemann associada é conformemente equivalente a $\widetilde{\mathcal{M}}$.*

Observação 3.6.39 *Uma variedade complexa 1-dimensional é usualmente chamada de **superfície de Riemann.** Assim, uma curva projetiva não-singular tem uma estrutura de superfície de Riemann. Reciprocamente, uma superfície de Riemann fechada admite a estrutura de uma curva projetiva não-singular. Para variedades projetivas não-singulares, certas propriedades analíticas e algébricas são em muitas formas equivalentes. Consequentemente, curvas algébricas sobre corpos finitos e superfícies de Riemann estão relacionadas.*

3.7 Apêndice 1

Introdução de Códigos Algébricos-Geométricos (AG)

Os **códigos de Goppa** são códigos algébrico-geométricos sobre um corpo finito $GF(q)$ que requerem para sua definição alguns conceitos prévios, como também notações específicas que passamos a expor agora.

Consideramos $\mathcal{X}$ uma curva algébrica sobre $GF(q)$ projetiva, não-singular (se não for, consideraremos seu modelo não-singular $\widetilde{\mathcal{X}}$, isto é, sua desingularização (veja [17] 7.5)) e absolutamente irredutível sobre $GF(q)$ (isto é, irredutìvel sobre $\overline{GF(q)}$), tal que seu gênero é g.

Definição 3.7.1 *Dizemos que D é um **divisor** da curva $\mathcal{X}$, se D é uma soma formal de pontos fechados de $\mathcal{X}$ com coeficientes inteiros nulos, com exceção de um número finito deles, isto é,$D = \sum_{P_i \in \mathfrak{C}} m_i P_i$, $m_i \in \mathbb{Z}$ e $m_i = 0$ para quase todo m_i.*

- Se $\forall i$, $m_i \geq 0$, então se diz que D é um **divisor efetivo.**
- Se chama grau de um divisor D, e se escreve $\mathrm{gr}(D)$, a soma de todos os coeficientes m_i que os definem, isto é, $\mathrm{gr}(D) = \sum m_i$.
- O suporte de um divisor D, que representamos por $\sup(D)$, é o conjunto dos pontos P_i que aparecem em sua expressão com $m_i \neq 0$, isto é,

$$\sup(D) = \{P_i \mid m_i \neq 0\}.$$

- Seja $\overline{GF(q)}(\mathcal{X})$ o corpo das funções racionais da curva $\mathcal{X}$ sobre $\overline{GF(q)}$. Se $P_i \in \mathcal{X}(\overline{GF(q)})$, então o anel local θ_{P_i} (as vezes denotado por $\theta_{P_i}(\mathcal{X})$) do ponto P_i na variedade $\mathcal{X}$ é o conjunto de funções racionais que são regulares em P_i, isto é, $\theta_{P_i}(\mathcal{X}) = \left\{ f/g \mid f, g \in \overline{GF(q)}[\mathcal{X}] \text{ e } g(P_i) \neq 0 \right\}$. O ideal maximal de θ_{P_i} é o conjunto $M_{p_i}(\mathcal{X}) = \{\gamma \in \theta_{P_i}(\mathcal{X}) \mid \gamma(P_i) = 0\}$ de funções em θ_{P_i} tal que são zeros em P_i. Seja t um elemento gerador de M_{p_i}, isto é, $M_{P_i}(\mathcal{X}) = (\mathrm{t})$. Podemos então, escrever cada elemento z de $\theta_{P_i}(\mathcal{X})$ de uma única maneira como $\mathrm{z} = u\mathrm{t}^m$, onde u é uma unidade e $m \in \mathbb{N}_0$. A função t é chamada de um parâmetro local ou parâmetro de uniformização de P_i. Se $m > 0$, então P_i é um zero de multiplicidade m de z. Escrevemos $m = ord_{P_i}(z) = v_{P_i}(z)$.

Definição 3.7.2 *[17][65][59] A aplicação $v_{P_i} : \theta_{P_i} \longrightarrow \mathbb{N}_0 \cup \{\infty\}$ é uma **valorização discreta**, se é sobrejetiva e satisfaz as seguintes propriedades:*

i) $v_{P_i}(f) = \infty$ *se, e somente se,* $f = 0$;

ii) $v_{P_i}(\lambda f) = v_{P_i}(f)$ *para todo* $\lambda \in \overline{GF(q)}$ *não-nulo;*

iii) $v_{P_i}(f+g) \geq \min\{v_{P_i}(f), v_{P_i}(g)\}$ *e a igualdade acontece quando* $v_{P_i}(f) \neq v_{P_i}(g)$;

iv) $v_{P_i}(fg) = v_{P_i}(f) + v_{P_i}(g)$;

v) *Se* $v_{P_i}(f) = v_{P_i}(g)$, *então existe um* λ *não-nulo tal que* $v_{P_i}(f - \lambda g) > v_{P_i}(g)$ *para todo* $f, g \in \theta_{P_i}$.

Se $v_{P_i}(z) = -m < 0$, então dizemos que z tem um **pólo de ordem** m em P_i. Se z é um elemento de $\overline{GF(q)}(\mathcal{X})$ com $v_{P_i}(z) = m$, então dizemos que z é um zero em P_i. Com esta colocação, se define **divisor** de uma função racional γ em $\mathcal{X}$, e se escreve $div(\gamma)$, como sendo

$$div(\gamma) = \sum_{P_i \in \mathcal{X}(\overline{GF(q)})} v_{P_i}(\gamma) P_i.$$

Definição 3.7.3 *[59] Seja* D *um divisor em uma curva* X. *Definimos o* ***espaço vetorial*** $\mathsf{L}(D)$ *sobre* $\overline{GF(q)}$ *por*

$$\mathsf{L}(D) = \{f \in \overline{GF(q)}(\mathcal{X})^* \mid (f) + D \succeq 0\} \cup \{0\}.$$

A ***dimensão de*** $\mathsf{L}(D)$ *sobre* $\overline{GF(q)}$ *é denotada por* $\dim(D)$.

Teorema 3.7.4 *[59] Seja* D *um divisor de uma curva* $\mathcal{X}$. *Então:*

i) $\dim(D) = 0$ *se* $\mathrm{gr}(D) < 0$;

ii) $\dim(D) \leq 1 + \mathrm{gr}(D)$.

No caso em que $\mathcal{X}$ é uma curva plana, as funções racionais, $\gamma = f/g$, verificam a igualdade

$$div(\gamma) = div(f) - div(g).$$

Definição 3.7.5 *[17] O grau do divisor de uma função racional* $\gamma \in \overline{GF(q)}(\mathcal{X})$ *é zero, isto é,* $\mathrm{gr}(\ div\ (\gamma)) = 0$, *visto que o número de zeros e o número de pólos de* γ *são iguais, contando com suas respectivas multiplicidades.*

Definição 3.7.6 *[17] Dada* $\gamma \in \overline{GF(q)}(\mathcal{X})$, *consideramos a forma diferencial* $\omega = \gamma dt$, *onde* t *é o parâmetro de uniformização em um ponto* P_i. *Por definição,* $v_{P_i}(\omega) = v_{P_i}(\gamma)$ *e* $div(\omega) = \sum_{P_i} v_{P_i}(\omega) P_i$. *Para cada forma diferencial* ω *existe uma única* $\gamma \in \overline{GF(q)}(\mathcal{X})$ *tal que* $\omega = \gamma dt$ *(ver [17], 8.4 Lema 3). O conjunto de todas as formas diferenciais (meromorfas) em* $\mathcal{X}$, *que representamos por* $\Omega_{\overline{GF(q)}}(\mathcal{X})$, *é um espaço vetorial sobre* $\overline{GF(q)}(\mathcal{X})$ *de dimensão 1, sendo que* $\{dt\}$ *é uma base de* $\Omega_{\overline{GF(q)}}(\mathcal{X})$.

Definição 3.7.7 *Seja* ω *uma diferencial e* $W = (\omega)$. *Então* W *é chamado um* ***divisor canônico***. *Agora, considere o espaço* $\mathsf{L}(W)$. *Este espaço de funções racionais pode ser traçado sobre um espaço isomorfo de formas diferenciais por* $f \longmapsto f\omega$.

Definição 3.7.8 *[59] Dado um divisor* D *e um divisor canônico* W *da curva* $\mathcal{X}$, *definimos os* $\overline{GF(q)}$*-espaços vetoriais*

$$\mathsf{L}(D) = \{\gamma \in \overline{GF(q)}(X) \mid div(\gamma) \geq -D\} \cup \{0\} \quad e$$
$$\Omega(D) = \{w \in \Omega_{\overline{GF(q)}}(X) \mid div(w) \geq D\} \cup \{0\}.$$

Tem-se que $\Omega(D) \simeq \mathsf{L}(W - D)$.

Teorema 3.7.9 (Teorema de Riemann-Roch) *[17] Seja $\mathcal{X}$ uma curva não-singular de gênero* g, *e W um divisor canônico de $\mathcal{X}$. É verificado, para cada divisor D de $\mathcal{X}$, que*

$$\dim \mathsf{L}(D) - \dim \mathsf{L}(W - D) = \mathrm{gr}(D) + 1 - \mathrm{g}.$$

Corolário 3.7.10 *[17] Para um divisor canônico W, temos que* $\mathrm{gr}(W) = 2\mathrm{g}-2$ *e* $\dim(W) = \mathrm{g}$.

Corolário 3.7.11 *[17] Seja D um divisor em uma curva projetiva suave de gênero* g *e seja* $\mathrm{gr}(D) > 2\mathrm{g} - 2$. *Então* $\dim(D) = \mathrm{gr}(D) - \mathrm{g} + 1$.

Trataremos, agora, de definir Código de Goppa correspondente a curva $\mathcal{X}$ através das definições e notações que acabamos de expressar.

Definição 3.7.12 *Seja $\mathcal{X}$ uma curva projetiva não-singular, de gênero* g *e absolutamente irredutível definida sobre o corpo $GF(q)$. Suponhamos que $\#\mathcal{X}(GF(q)) = r \geq n$, e consideramos os divisores racionais de $\mathcal{X}$: D e* G, *tais que:*

i) $D = P_1 + P_2 + \cdots + P_n$, *onde para* $\forall i = 1, \ldots, n$, $P_i \in \mathcal{X}(GF(q))$ *são todos distintos entre si.*

ii) G *é um divisor efetivo de $\mathcal{X}$ tal que* $\mathrm{sup}(\mathrm{G}) \cap \mathrm{sup}(D) = \varnothing$.

Definição 3.7.13 *[59] Um* ***código linear associado aos divisores*** *D e* G *para a curva $\mathcal{X}$, $\mathfrak{C}(D, \mathrm{G})$, de comprimento n sobre $GF(q)$ é a imagem da aplicação linear*

$$\begin{array}{rccl} \Phi: & \mathsf{L}(G) & \longrightarrow & (GF(q))^n \\ & \gamma & \longmapsto & \Phi(\gamma) = (\gamma(P_1), \ldots, \gamma(P_n)). \end{array}$$

Apresentamos agora, os principais resultados para os $[n, k, d]$-códigos $\mathfrak{C}$:

Teorema 3.7.14 *[59] O código $\mathfrak{C}(D, \mathrm{G})$ tem dimensão $k = \dim(\mathrm{G}) - \dim(\mathrm{G} - D)$ e distância mínima $d \geq n - \mathrm{gr}(\mathrm{G})$.*

Corolário 3.7.15 *[59] Suponha que o grau de* G *é estritamente menor que n. Então Φ é injetiva, consequentemente:*

a) $\mathfrak{C}(D, \mathrm{G})$ *é um $[n, k, d]$-código com*

$$d \geq n - \mathrm{gr}(\mathrm{G}) \quad e \quad k = \dim \mathrm{G} \geq \mathrm{gr}(\mathrm{G}) + 1 - \mathrm{g}$$

e $k + d \geq n + 1 - \mathrm{g}$.

b) Se $2\mathrm{g} - 2 < \mathrm{gr}(\mathrm{G}) < n$, *então* $k = \mathrm{gr}(\mathrm{G}) - \mathrm{g} + 1$.

c) Como $\mathfrak{C} = \mathrm{Im}(\Phi)$ *e se* $B = \{\xi_1, \ldots, \xi_k\}$ *é uma base de* $\mathsf{L}(\mathrm{G})$, *então a matriz associada a Φ, com respeito a B e a base canônica de $(GF(q))^n$, é dada por*

$$\begin{pmatrix} \xi_1(P_1) & \ldots & \xi_1(P_n) \\ \vdots & & \vdots \\ \xi_k(P_1) & \ldots & \xi_k(P_n) \end{pmatrix},$$

que é chamada de ***matriz geradora do código*** $\mathfrak{C}(D, \mathrm{G})$.

3.8 Apêndice 2

Conceitos de Topologia

Espaço Topológico é um conjunto X juntamente com uma coleção **T** de subconjuntos de X (chamados conjuntos abertos) com as seguintes propriedades:

(i) O conjunto vazio $\varnothing$ e X estão em **T**;

(ii) Qualquer interseção finita de conjuntos em **T** está também em **T**;

(iii) Uma união arbitrária de conjuntos em **T** está novamente em **T**.

Seja X um espaço topológico e $\mathbb{A} \subset$ X. Uma **topologia induzida em** $\mathbb{A}$ é uma coleção de conjuntos abertos da forma $U \cap \mathbb{A}$, onde U é um conjunto aberto de X.

Seja X um espaço topológico. O complementar de um conjunto aberto é chamado de **conjunto fechado**. Por exemplo, se $a, b \in \mathbb{R}$, então o conjunto $\{x \in \mathbb{R} : a \leq x \leq b\}$, é fechado.

Seja X um espaço topologico e $x \in$ X. Uma **vizinhança de** x é todo conjunto aberto que contém x.

Seja $\mathbb{A}$ um subconjunto de um espaço topológico X. Um ponto $x \in$ X é chamado de um **ponto aderente de** $\mathbb{A}$, se toda vizinhança de x contém um ponto de $\mathbb{A}$. O conjunto dos pontos aderentes de $\mathbb{A}$ é chamado o **fecho de** $\mathbb{A}$, o qual será denotado por $\overline{\mathbb{A}}$.

O fecho de um conjunto $\mathbb{A}$ é a interseção de todos os conjuntos fechados que contêm $\mathbb{A}$, isto é, o menor conjunto fechado que contém $\mathbb{A}$. O fecho de um conjunto fechado é ele mesmo.

Por exemplo, se $\mathbb{A} = \{x \in \mathbb{R}^n : \|x\| < 1\}$ é a bola aberta unitária em $\mathbb{R}^n$, então $\overline{\mathbb{A}}$ é a bola fechada $\{x \in \mathbb{R}^n : \|x\| \leq 1\}$.

Um subconjunto $\mathbb{A}$ de um espaço topológico X é chamado de **denso em** X se $\overline{\mathbb{A}} =$X.

Dizemos que um espaço topológico X é um **espaço de Hausdorff** (ou **espaço separado**) se, cada par de pontos distintos têm vizinhaças distintas; isto é, se $x, y \in$ X com $x \neq y$, então existem conjuntos abertos U_1 e U_2 de X com $x \in U_1$, $y \in U_2$ e $U_1 \cap U_2 = \varnothing$. X é denominado **segundo enumerável** se existe uma base enumerável para a sua topologia (veja Figura 3.19).

Por exemplo, um conjunto com a topologia discreta é Hausdorff.

O espaço *euclidiano* $\mathbb{R}^n$ com a sua topologia é um espaço *de* Hausdorff. Para, $x, y \in \mathbb{R}^n$, com $x \neq y$, a distância entre eles é positiva, isto é, $\|x - y\| > 0$. Então as bolas abertas em torno de x e y de ráio $\frac{1}{2}\|x - y\|$ não se interceptam. Usando o mesmo raciocínio, concluímos que qualquer *espaço métrico* é de Hausdorff.

Uma familia $\{V_\alpha\}_{\alpha \in I}$ de subconjuntos de um conjunto X é chamada uma **cobertura de** X se $\bigcup_{\alpha \in I} V_\alpha =$ X, isto é, se cada ponto de X pertence a pelo menos um V_α. Se, além disso, X é um espaço topológico, e cada V_α é um subconjunto aberto de X, então dizemos que $\{V_\alpha\}$ é uma **cobertura aberta** de X.

Um espaço topológico X é chamado de **compacto,** se $\{V_\alpha\}$ é qualquer cobertura aberta de X, então alguma sub-coleção finita de $\{V_\alpha\}$ já é uma cobertura de X; isto é,

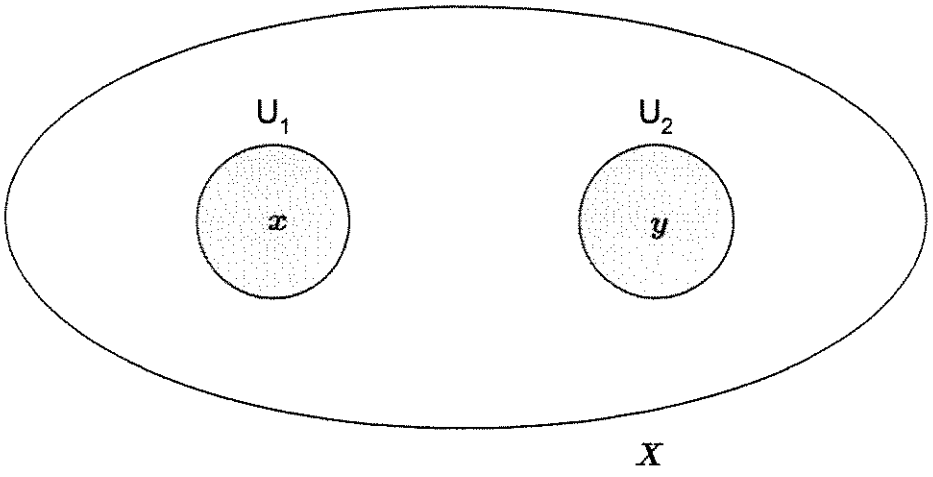


Figura 3.19: *Espaço de Hausdorff*

se $\{V_\alpha\}$ é qualquer cobertura aberta de X, então existe um número finito de elementos $\alpha_1,\alpha_2,\cdots,\alpha_n$ de I tal que $\bigcup_{1\leq j\leq n} V_{\alpha_j} = X$.

Um subconjunto $\mathbb{A}$ de um espaço topológico é chamado de **compacto** se ele é compacto na topologia induzida.

Observação 3.8.1 *Um subconjunto fechado de um espaço compacto é compacto.*

Observação 3.8.2 *Seja $a,b \in \mathbb{R}$ com $a \leq b$. Então o conjunto $\mathbb{A} = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ é compacto. Este fato é conhecido como o Teorema de Heine-Borel.*

Proposição 3.8.3 *[43] Um subconjunto compacto de um espaço de Hausdorff é fechado.*

Demonstração. Seja X um espaço de Hausdorff e $\mathbb{A}$ um subconjunto de X. Temos que mostrar que $X - \mathbb{A}$ é aberto. Para isso, é suficiente provar que todo ponto $x \in X - \mathbb{A}$ tem uma vizinhança que não intersecta $\mathbb{A}$. Seja $x \in X - \mathbb{A}$. Se $y \in \mathbb{A}$, podemos encontrar, desde que X é Hausdorff, uma vizinhança V_y de x e uma vizinhança U_y de y em **X**, tal que $V_y \cap U_y = \varnothing$. Se $U_y' = U_y \cap \mathbb{A}$, então $\{U_y'\}_{y\in\mathbb{A}}$ é uma cobertura aberta de $\mathbb{A}$, e como $\mathbb{A}$ é compacto, podemos achar $y_1, y_2, \cdots, y_n \in \mathbb{A}$, tal que $U_{y_1}' \cup U_{y_2}' \cup \cdots \cup U_{y_n}' = \mathbb{A}$. Então, $V = V_{y_1} \cap \cdots \cap V_{y_n}$ é um conjunto aberto contendo x, que não intersecta $\mathbb{A}$. ∎

Um espaço topológico X é chamado de **conexo** se ele não é a união de dois conjuntos abertos disjuntos não vazios. Um subespaço de um espaço topológico é chamado de **conexo** se ele é conexo na topologia induzida.

Um espaço topológico X é conexo se, e somente se, X não é a união de dois conjuntos fechados disjuntos não vazios. X é conexo se, e somente se, não existe subconjuntos de X os quais sejam aberto e fechado simultaneamente, exceto o próprio conjunto X e o conjunto vazio.

Uma **métrica** num conjunto M é uma função $d : M \times M \to \mathbb{R}$ que associa a cada par ordenado de elementos $x, y \in M$ um número real $d(x, y)$, chamado a **distância** de x a y,

de modo que sejam satisfeitas as seguintes condições para quaisquer $x, y, z \in \mathrm{M}$:

$d_1)$ $\mathrm{d}(x,x) = 0$; $d_3)$ $\mathrm{d}(x,y) = \mathrm{d}(y,z)$;
$d_2)$ *Se* $x \neq y$ *então* $\mathrm{d}(x,y) > 0$; $d_4)$ $\mathrm{d}(x,z) \leq \mathrm{d}(x,y) + \mathrm{d}(y,z)$.

Todo espaço métrico M pode ser considerado como um espaço topológico, no qual a família Υ é formada pelos subconjuntos abertos de M. Uma topologia Υ em X se diz **metrizável** quando existe uma métrica em X em relação à qual os abertos são os elementos de Υ.

Todo espaço topológico metrizável é um espaço de Hausdorff.

Sejam X e Y espaços topológicos. Um **homeomorfismo** de X em Y é uma bijeção contínua $\mathrm{f} : \mathrm{X} \to \mathrm{Y}$ cuja inversa $\mathrm{f}^{-1} : \mathrm{Y} \to \mathrm{X}$ também é contínua. Neste caso, diz-se que X e Y são homeomorfos.

Sejam X e Y espaços topológicos. Uma aplicação $\mathrm{f} : \mathrm{X} \to \mathrm{Y}$ chama-se um **homeomorfismo local** quando cada ponto $x \in \mathrm{X}$ está contido num aberto U tal que $\mathrm{V} = \mathrm{f}(U)$ é um aberto em Y e a restrição $\mathrm{f}|U$ é um homeomorfismo de U sobre V.

Sejam X e Y espaços topológicos. Diz-se que X e Y são **homeomorfos** quando existe uma aplicação diferenciável $\varphi : \mathrm{X} \to \mathrm{Y}$ cuja inversa $\varphi^{-1} : \mathrm{Y} \to \mathrm{X}$ também é diferenciável. A aplicação φ é chamada **difeomorfismo**. Dizemos que φ é um **difeomorfismo local** quando cada ponto $x \in \mathrm{X}$ está contido num aberto U tal que $\mathrm{V} = \varphi(U)$ é um aberto em Y e a restrição $\varphi|U$ é um **difeomorfismo** de U sobre V. Quando φ é uma aplicação de classe C^k dizemos que φ é um **difeomorfismo de classe** C^k.

A existência de um homeomorfismo local $\mathrm{f} : \mathrm{X} \to \mathrm{Y}$ faz com que X herde todas as propriedades topológicas locais de Y, como, conexidade local, compacidade local, etc. Se for sobrejetivo, então Y herda também as propriedades topológicas locais de X.

Um **caminho** é uma aplicação contínua $\mathrm{a} : J \to \mathrm{X}$, definido num intervalo compacto $J = [s_0, s_1]$. Um caminho se diz **fechado** quando $\mathrm{a}(s_0) = \mathrm{a}(s_1)$.

Sejam X uma variedade, U um subconjunto aberto de X. Definimos $\Gamma(U, O_{\mathrm{X}})$, ou simplesmente $\Gamma(U)$, como sendo o conjunto das fuções racionais em X que são definidas em cada ponto $P \in U$.

Sejam X e Y duas variedades. Um **morfismo** de X em Y é uma função $\psi : \mathrm{X} \longrightarrow \mathrm{Y}$ tal que:

(1) ψ é contínua;

(2) Para todo conjunto aberto U de Y, se $\mathrm{f} \in \Gamma(U, O_{\mathrm{Y}})$, então $\widetilde{\psi}(\mathrm{f}) = \mathrm{f} \circ \psi \in \Gamma(\psi^{-1}(U), O_{\mathrm{X}})$.

Um **isomorfismo** de X com Y é um morfismo ψ $1-1$ de X sobre Y tal que ψ^{-1} é um morfismo.

Uma **aplicação racional** $\psi : \mathrm{X} \longrightarrow \mathrm{Y}$ é uma classe de equivalência de pares $\langle U, \psi_U \rangle$, onde U é um subconjunto aberto não-vazio de X, ψ_U é um morfismo de U em Y, e onde $\langle U, \psi_U \rangle$ e $\langle V, \psi_{\mathrm{V}} \rangle$ são equivalentes se ψ_U e ψ_{V} em $U \cap \mathrm{V}$ são as mesmas.

Uma aplicação racional F de X em Y é dita ser **biracional** se existem dois conjuntos abertos $U \subset \mathrm{X}$, $\mathrm{V} \subset \mathrm{Y}$, e um isomorfismo $\mathrm{f} : U \longrightarrow \mathrm{V}$ que representa F. Dizemos que X e Y são biracionalmente equivalentes se existe uma aplicação biracional de X em Y. Uma

variedade é biracionalmente equivalente a qualquer subvariedade aberta de si mesma. $\mathcal{A}^n$ e $\mathbb{P}^n$ são biracionalmente equivalentes.

Proposição 3.8.4 *[18] Duas variedades são* ***biracionalmente equivalentes*** *se, e somente se, seus corpos de funções são isomorfos.*

Uma variedade é dita ser racional se ela é biracionalmente equivalente a $\mathcal{A}^n$ (ou $\mathbb{P}^n$) para algum n.

Capítulo 4

Decodificação de Códigos Alternantes Cíclicos

O nosso objetivo neste capítulo é apresentar uma estrutura geométrica de curvas algébricas, através de polinômios absolutamente irredutíveis, aos processos de localização e de determinação da magnitude dos erros dos algoritmos de decodificação de códigos alternantes cíclicos sobre corpos finitos. Os códigos alternantes podem ser decodificados através de qualquer uma das técnicas de decodificação utilizadas para os códigos BCH. Todavia, existem bons algoritmos para decodificação de códigos BCH e Reed-Solomon, porém específicos para estas duas classes. A estrutura geométrica introduzida se aplica no processo de decodificação da classe dos códigos alternantes através do grupo das unidades independentemente da estrutura algébrica em consideração. Neste contexto, incorporaremos, ao algoritmo de Berlekamp-Massey (BM) e ao algoritmo de Peterson-Gorenstein-Zierler (PGZ), uma estrutura geométrica de curvas algébricas na caracterização do processo de localização dos erros. Mais exatamente, descreveremos os passos para o algoritmo de decodificação dos códigos alternantes sobre corpos finitos, apresentados no Capítulo 2. Na Seção 4.1, apresentaremos o algoritmo de Berlekamp-Massey e, em seguida, aplicaremos um procedimento desenvolvido por Forney para a determinação da magnitude dos erros.

Na Seção 4.2, apresentaremos o algoritmo de Berlekamp-Massey Ampliado. Este algoritmo difere do original pelo acréscimo de novos passos com o intuito de localizar e de determinar a magnitude dos erros através dos pontos racionais da curva construída através do polinômio (Chave1) ou do polinômio (Chave2). A função da incorporação destes passos na decodificação de códigos tradicionais (BCH, Reed-Solomon, Goppa, etc.) sobre corpos finitos é de estabelecer uma relação entre a estrutura algébrica existente e a estrutura geométrica de curvas algébricas, via a construção de polinômios absolutamente irredutíveis apresentada no Capítulo 3. Dessa forma, teremos uma estrutura geométrica associada ao algoritmo. Observamos que este algoritmo não será alterado nos seus fundamentos e, portanto, a complexidade permanecerá praticamente inalterada.

Na Seção 4.3, apresentaremos uma proposta de decodifição baseada no algoritmo de Peterson-Gorenstein-Zierler, [7], na qual os erros serão localizados por meio dos pontos racionais da curva construída através do polinômio (Chave1) ou do polinômio (Chave2) e, por meio destes, também determinar a magnitude dos erros. Este algoritmo, como no caso da Seção 4.2, também não será alterado nos seus fundamentos e, portanto, sua

complexidade permanecerá praticamente inalterada.

4.1 Algoritmo de Berlekamp-Massey

Nesta seção abordaremos o problema da decodificação por máxima verossimilhança de códigos lineares, considerando a métrica de Hamming, isto é, dada uma palavra recebida r, o decodificador decodifica-a, na métrica de Hamming, como sendo a palavra-código v que está mais próxima a r.

Suponha que uma palavra código $v(x) = v_0 + v_1x + \cdots + v_{n-1}x^{n-1}$ seja transmitida e que os erros introduzidos pelo canal de comunicação resultem no seguinte vetor recebido

$$r(x) = r_0 + r_1x + \cdots + r_{n-1}x^{n-1}.$$

Seja $e(x)$ o padrão de erro. Então,

$$r(x) = v(x) + e(x). \tag{4.1}$$

Para efeito de simplificação, consideraremos nesta seção apenas os códigos BCH no sentido estrito, ou seja, caso em que $l = 1$ na definição do código BCH. Assim, a matriz verificação de paridade será

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \dots & (\alpha^2)^{n-1} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \alpha^{\delta-1} & (\alpha^{\delta-1})^2 & \dots & (\alpha^{\delta-1})^{n-1} \end{bmatrix}.$$

O procedimento usual no processo de decodificação é iniciar com a computação da síndrome, a partir do vetor recebido $r(x)$. A i-ésima síndrome é dada por

$$S_i = r_0 + r_1\alpha^i + r_2\alpha^{2i} + \ldots + r_{n-1}\alpha^{(n-1)i} = r(\alpha^i) \tag{4.2}$$

para $1 \leq i \leq \delta - 1$. Observe que as componentes do vetor síndrome $\overline{S}$ são elementos do corpo $GF(q^m)$. As componentes S_i podem ser obtidas dividindo-se $r(x)$ por $m_i(x)$, o polinômio minimal de α^i, ou seja:

$$r(x) = q_i(x)m_i(x) + p_i(x),$$

onde $\partial p_i < \partial m_i$. Como $m_i(\alpha^i) = 0$, temos

$$S_i = r(\alpha^i) = p_i(\alpha^i).$$

Portanto, a componente S_i do vetor $\overline{S}$ é obtida avaliando-se $p_i(x)$ em $x = \alpha^i$.

Como $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$ são raízes da palavra-código $v(x)$, isto é, $v(\alpha^i) = 0$, para $1 \leq i \leq \delta - 1$, então segue de (4.1) e (4.2) que

$$S_i = e(\alpha^i), \tag{4.3}$$

para $1 \leq i \leq \delta - 1$. Desta última relação podemos afirmar que o vetor síndrome $\overline{S}$ depende unicamente do padrão de erro ocorrido $\overline{e}$. Suponha agora que o padrão de erro contenha ν erros nas localizações $x^{j_1}, x^{j_2}, \cdots, x^{j_\nu}$ e com magnitudes $Z_1, Z_2, \cdots, Z_\nu$, respectivamente, isto é,

$$e(x) = Z_1 x^{j_1} + Z_2 x^{j_2} + \ldots + Z_\nu x^{j_\nu}, \tag{4.4}$$

onde $0 \leq j_1 < j_2 < \cdots < j_\nu \leq n-1$. Das igualdades (4.3) e (4.4) obtemos o seguinte conjunto de equações

$$\begin{aligned} S_1 &= Z_1\alpha^{j_1} + Z_2\alpha^{j_2} + \ldots + Z_\nu\alpha^{j_\nu} \\ S_2 &= Z_1\left(\alpha^{j_1}\right)^2 + Z_2\left(\alpha^{j_2}\right)^2 + \ldots + Z_\nu\left(\alpha^{j_\nu}\right)^2 \\ &\vdots \quad\quad \vdots \\ S_{\delta-1} &= Z_1\left(\alpha^{j_1}\right)^{\delta-1} + Z_2\left(\alpha^{j_2}\right)^{\delta-1} + \ldots + Z_\nu\left(\alpha^{j_\nu}\right)^{\delta-1}, \end{aligned} \tag{4.5}$$

onde $\alpha^{j_1}, \alpha^{j_2}, \cdots, \alpha^{j_\nu}$ e $Z_1, Z_2, \cdots, Z_\nu$ são incógnitas. Qualquer método de resolução destas equações é um algoritmo de decodificação para os códigos BCH. Uma vez que $\alpha^{j_1}, \alpha^{j_2}, \cdots, \alpha^{j_\nu}$ tenham sido encontrados, as potências $j_1, j_2, \cdots, j_\nu$ especificam as localizações dos erros. As correspondentes magnitudes são dadas por $Z_1, Z_2, \cdots, Z_\nu$. Em geral, as equações em (4.5) têm q^k soluções (o número de padrões de erro correspondentes a uma dada síndrome). Cada solução conduz a um padrão de erro diferente. Se o número de erros for menor ou igual a $t = \lfloor (\delta - 1)/2 \rfloor$, onde δ é a distância de projeto, então a solução que produz o padrão de erro com o menor número de erros é a solução correta.

Por conveniência, definimos

$$Y_i = \alpha^{j_i},$$

onde $1 \leq i \leq \nu$. Esses elementos Y_i são chamados de números de localização de erro, visto que eles trazem informação a respeito da localização dos erros. Então, as equações de (4.5) podem ser expressas na forma

$$S_j = \sum_{i=1}^{\nu} Z_i Y_i^j, \tag{4.6}$$

onde $1 \leq j \leq \delta - 1$ e ν representa o número de erros que ocorreram.

Iremos resolver primeiramente o problema da localização dos erros para depois resolvermos o problema da determinação das magnitudes dos mesmos. Observe que, no caso dos códigos lineares binários, a localização dos erros já implica necessariamente a determinação das magnitudes dos mesmos.

Sejam os valores $\sigma_1, \sigma_2, \ldots, \sigma_\nu$ definidos através da equação

$$\sigma(Y) = (Y - Y_1)(Y - Y_2)\ldots(Y - Y_\nu) = Y^\nu + \sigma_1 Y^{\nu-1} + \ldots + \sigma_{\nu-1}Y + \sigma_\nu. \tag{4.7}$$

Esses valores são conhecidos como as funções simétricas elementares dos Y_i e o polinômio de grau ν, (4.7), é conhecido como o **polinômio localizador de erros**. Multiplicando ambos os lados da equação (4.7) por $Z_i Y_i^j$ e, depois, substituindo Y_i, $1 \leq i \leq \nu$, em Y, tem-se como resultado o seguinte conjunto de equações

$$Z_i Y_i^{j+\nu} + Z_i Y_i^{j+\nu-1}\sigma_1 + \ldots + Z_i Y_i^{j+1}\sigma_{\nu-1} + Z_i Y_i^j \sigma_\nu = 0.$$

Somando-as para $1 \leq i \leq \nu$ e substituindo-as pelas equações em (4.6), resulta que

$$S_{j+\nu} + S_{j+\nu-1}\sigma_1 + S_{j+\nu-2}\sigma_2 + \ldots + S_{j+1}\sigma_{\nu-1} + S_j\sigma_\nu = 0. \tag{4.8}$$

Mas todos os S_j são conhecidos se $1 \leq j \leq \delta - 1 - \nu$. Portanto, o cálculo dos σ_i a partir do vetor síndrome é feito resolvendo-se o sistema linear (4.8) de modo que ν tenha o menor valor possível. Isto é requerido pois estaremos assumindo que o vetor erro que ocorre é aquele que possui o menor peso de Hamming possível, isto é, o número de equações em (4.8) é maximizado. Por construção, sabemos que sempre existe uma solução para (4.8). O conjunto de equações lineares (4.8) relaciona as síndromes com os coeficientes de $\sigma(Y)$. O algoritmo que será apresentado a seguir é muito eficiente em aplicações práticas.

4.1.1 Descrição dos passos do Algoritmo de Berlekamp-Massey

Em vista dos fatos relacionados acima, Seção 4.1, deduzimos que o procedimento eficiente de decodificação de códigos alternantes compreende os seguintes passos:

Passo 1: Cálculo do vetor síndrome $\overline{S} = (S_1, S_2, \cdots, S_{\delta-1})$, a partir do vetor recebido $\overline{r}$;

Passo 2: Cálculo das funções simétricas elementares $\sigma_1, \sigma_2, \cdots, \sigma_\nu$, a partir do vetor $\overline{S}$;

Passo 3: Cálculo dos números de localização de erro $Y_1, Y_2, \cdots, Y_\nu$, a partir dos σ_i's;

Passo 4: Cálculo das magnitudes dos erros Z_i, a partir dos Y_i's e $\overline{S}$.

A seguir, analisaremos detalhadamente cada um dos quatro passos acima.
Passo 1: *Cálculo do vetor síndrome.*

$$\overline{S} = \overline{r} \cdot H^T.$$

Passo 2: *Cálculo das funções simétricas elementares.*

A questão analisada aqui será determinar a solução do sistema linear (4.8), nas incógnitas $\sigma_i's$, $1 \leq i \leq \nu$, de tal maneira que o padrão de erro ν seja mínimo, dado que as componentes de um vetor síndrome $S_1, S_2, \cdots, S_{\delta-1}$ foram estabelecidas pelo decodificador. O algoritmo conhecido mais eficiente para resolver este sistema é o **Algoritmo de Berlekamp-Massey**, o qual passaremos a descrever.

Este algoritmo é interativo, no sentido de que, no n-ésimo passo, o decodificador procura determinar um conjunto de l_n valores $\sigma_i^{(n)}$, tal que as $n - l_n$ equações (conhecidas como somas de potências)

$$\begin{array}{rcl} S_n\sigma_0^{(n)} + S_{n-1}\sigma_1^{(n)} + \ldots + S_{n-l_n}\sigma_{l_n}^{(n)} & = & 0 \\ S_{n-1}\sigma_0^{(n)} + S_{n-2}\sigma_1^{(n)} + \ldots + S_{n-l_n-1}\sigma_{l_n}^{(n)} & = & 0 \\ \vdots & & \vdots \\ S_{l_n+1}\sigma_0^{(n)} + S_{l_n}\sigma_1^{(n)} + \ldots + S_1\sigma_{l_n}^{(n)} & = & 0 \end{array} \tag{4.9}$$

sejam satisfeitas, com o menor l_n possível, onde $\sigma_0^{(n)} = 1$. Este conjunto de valores $\sigma^{(n)}$ é mais comumente escrito na seguinte forma polinomial

$$\sigma^{(n)}(Y) = \sigma_0^{(n)} + \sigma_1^{(n)}Y + \ldots + \sigma_{l_n}^{(n)}Y^{l_n}.$$

Este polinômio tem grau menor ou igual a l_n e representa a solução do n-ésimo estágio.

Agora, suponha que no n-ésimo estágio o decodificador tenha determinado $\sigma^{(n)}(Y)$, com l_n mínimo, tal que o sistema (4.8) seja satisfeito. No $(n+1)$-ésimo estágio, o decodificador procura encontrar o polinômio $\sigma^{(n+1)}(Y)$ de menor grau, tal que as equações

$$\sum_{i=0}^{l_{n+1}} S_{j-1}\sigma_i^{(n+1)} = 0, \quad l_{n+1}+1 \leq j \leq n+1$$

sejam satisfeitas. A n-ésima **discrepância** será denotada por d_n e é definida por

$$d_n = S_{n+1}\sigma_0^{(n)} + S_n\sigma_1^{(n)} + \ldots + S_{n+1-l_n}\sigma_{l_n}^{(n)}.$$

A seguir, apresentaremos dois lemas que serão importantes na obtenção do algoritmo de Berlekamp-Massey. Estes lemas estão diretamente relacionados com a determinação de $\sigma^{(n+1)}(Y)$, não necessariamente com o menor valor de l_{n+1} possível, a partir de $\sigma^{(n)}(Y)$.

Lema 4.1.1 *[45] Suponha que $\sigma^{(n)}(Y)$ seja um polinômio solução minimal para as n primeiras somas de potências, isto é, existe um l_n mínimo que satisfaz às equações (4.9), e suponha ainda que a próxima discrepância $d_n \neq 0$. Seja*

$$\sigma^{(m)}(Y) = 1 + \sigma_1^{(m)}Y + \ldots + \sigma_{l_m}^{(m)}Y^{l_m}$$

um polinômio solução para as m primeiras somas de potências, com $1 \leq m < n$ e tal que $d_m \neq 0$. Então o polinômio

$$\sigma^{(n+1)}(Y) = \sigma^{(n)}(Y) - d_n d_m^{-1} Y^{n-m}\sigma^{(m)}(Y)$$

é uma solução para as $n+1$ primeiras somas de potências. Mais ainda,

$$l_{n+1} = \max\{l_n, l_m + n - m\}.$$

Lema 4.1.2 *[45] Sejam $\sigma^{(n)}(Y)$, l_n e $d_n \neq 0$ como definidos no Lema 4.1.1. Suponha que $\sigma^{(n+1)}(Y)$ seja um polinômio solução das equações (4.9), satisfazendo $n+1-l_{n+1}$ equações e que*

$$\sigma^{(n+1)}(Y) = \sigma^{(n)}(Y) - aY^{n-m}\sigma^{(m)}(Y),$$

onde $a \neq 0$ e $\sigma_0^{(m)} = 1$. Então o polinômio $\sigma^{(m)}(Y)$ é uma solução para as $m - l_m$ primeiras equações de (4.9) cuja próxima discrepância d_m satisfaz $d_m = d_n a^{-1}$ e $l_m = l_{n+1} - (n-m)$.

Como conseqüência dos Lemas 4.1.1 e 4.1.2, temos o seguinte teorema.

Teorema 4.1.3 *[45]Seja $\sigma^{(n)}(Y)$ uma solução minimal no n-ésimo estágio e $\sigma^{(m)}(Y)$ uma das soluções minimais anteriores, $1 \leq m < n$, tal que $d_m \neq 0$ e $m - l_m$ tenha o máximo valor. Então uma solução minimal no estágio $n+1$ é $\sigma^{(n+1)}(Y)$, onde*

(*i*) *se* $d_n = 0$, *então*

$$\sigma^{(n+1)}(Y) = \sigma^{(n)}(Y) \quad e \quad l_{n+1} = l_n; \tag{4.10}$$

(*ii*) *se* $d_n \neq 0$, *então*

$$\sigma^{(n+1)}(Y) = \sigma^{(n)}(Y) - d_n d_m^{-1} Y^{n-m} \sigma^{(m)}(Y) \quad e \quad l_{n+1} = \max\{l_n, l_m + n - m\}. \tag{4.11}$$

Iremos agora descrever o algoritmo da solução do problema original, isto é, solução das equações (4.8). As suas entradas são as componentes do vetor síndrome $\overline{S}$. O algoritmo produzirá como saída um conjunto de valores σ_i, $1 \leq i \leq \nu$, tais que as equações em (4.8) sejam satisfeitas com o mínimo valor de ν possível.

Algoritmo de Berlekamp-Massey (BM)

Iniciamos preenchendo os dados iniciais como mostra a seguinte tabela de valores

n	$\sigma^{(n)}(Y)$	d_n	l_n	$n - l_n$
-1	1	1	0	-1
0	1	S_1	0	0
1				
2				
$\vdots$				
$\delta - 1$				

Tabela 4.1: *Passos iniciais do algoritmo de Berlekamp-Massey*

Em seguida, adotamos os seguinte procedimentos:

(1) $n \longleftarrow 0$;

(2) se $d_n = 0$, então $\sigma^{(n+1)}(Y)$ e l_{n+1} são dados por (4.10). Vá para (5);

(3) se $d_n \neq 0$, então encontramos um $m \leq n - 1$, tal que $d_m \neq 0$. Assim, $\sigma^{(n+1)}(Y)$ e l_{n+1} são dados por (4.11);

(4) se $n < \delta - 2$, então

$$d_{n+1} = S_{n+2} + S_{n+1}\sigma_1^{(n+1)} + \cdots + S_{n+2-l_{n+1}}\sigma_{l_{n+1}}^{(n+1)};$$

(5) $n \longleftarrow n + 1$; se $n < \delta - 1$ vá para (2); caso contrário, $\sigma(Y)$ será o polinômio localizador de erro procurado.

A resposta procurada será dada pelo polinômio $\sigma^{(\delta-1)}$, cujos coeficientes formam uma solução para o sistema de equações (4.8).

Passo 3: *Cálculo do número de localização de erros.*

Determinados os valores $\sigma_1, \sigma_2, \cdots, \sigma_\nu$ que satisfazem às equações (4.8), Passo 2, estamos agora aptos a encontrar as raízes do polinômio $\rho(Y)$ de grau ν dado pela equação (4.7), isto é, pelo polinômio

$$\rho(Y) = Y^v \sigma(1/Y) = Y^\nu + \sigma_1 Y^{\nu-1} + \cdots + \sigma_{\nu-1} Y + \sigma_\nu,$$

onde $\rho(Y)$ é chamado de **polinômio recíproco** de $\sigma(Y)$. Como o número de elementos de $GF(q^m)$ é finito, basta então encontrarmos as raízes de $\rho(Y) = 0$. Dessa forma, teremos as localizações dos erros. Tal procedimento é conhecido como **busca de Chien**. Tal busca consiste em se testar primeiramente se α^{n-1} é uma raiz de $\rho(Y)$. Em caso afirmativo, então o dígito r_{n-1} está incorreto. De forma análoga, as outras potências menores de α vão sendo testadas (se α^{n-l} for uma raiz, então o dígito r_{n-l} está incorreto, onde $1 \leq l \leq n$), até que ν delas sejam determinadas como sendo as raízes de $\rho(Y)$.

Uma maneira rápida de se avaliar o polinômio $\rho(Y)$ em $Y = Y_0$ é através da **regra de Horn**, isto é,

$$\rho(Y_0) = ((((Y_0 + \sigma_1)Y_0 + \sigma_2)Y_0 + \sigma_3)Y_0 + \ldots + \sigma_{\nu-1})Y_0 + \sigma_\nu.$$

Passo 4: *Cálculo das magnitudes dos erros.*

Para completar a decodificação, descreveremos um método para a determinação das magnitudes dos erros Z_i, $1 \leq i \leq \nu$. Inicialmente, mostraremos que estas magnitudes ficam univocamente determinadas uma vez que os Y_i, $1 \leq i \leq \nu$, são conhecidos, isto é, que os números de localização de erros calculados no passo anterior são conhecidos.

Para encontrarmos o vetor $\overline{Z}$, aplicaremos o procedimento proposto por Forney, [16]. Tal procedimento requer o conhecimento dos números de localização de erros $Y_1, Y_2, \cdots, Y_\nu$ e das suas funções simétricas elementares $\sigma_1, \sigma_2, \cdots, \sigma_\nu$, calculados nos dois passos anteriores.

Primeiramente, defina as funções simétricas elementares σ_{jl} dos números de localização de erros $Y_1, Y_2, \ldots, Y_{j-1}, Y_{j+1}, \ldots, Y_\nu$, através da relação

$$\prod_{i \neq j}(Y - Y_i) = \sum_{l=0}^{\nu-1} \sigma_{jl} Y^{\nu-1-l}. \tag{4.12}$$

Da equação (4.7), temos que

$$\prod_{i=1}^{\nu}(Y - Y_i) = \sum_{l=0}^{\nu} \sigma_i Y^{\nu-i}, \tag{4.13}$$

onde σ_0 e $\sigma_{j,0}$ são iguais a 1, a unidade de $GF(q^m)$. A partir de (4.12) e (4.13), obtemos

$$(Y - Y_i) \sum_{l=0}^{\nu-1} \sigma_{jl} Y^{\nu-1-l} = \sum_{l=0}^{\nu} \sigma_i Y^{\nu-i}.$$

Conseqüentemente,

$$\sum_{l=0}^{\nu-1} \sigma_{jl} Y^{\nu-l} - \sum_{l=0}^{\nu-1} \sigma_{jl} Y_j Y^{\nu-1-l} = \sum_{l=0}^{\nu} \sigma_i Y^{\nu-i}. \tag{4.14}$$

Da igualdade (4.14), concluímos que os coeficientes σ_{jl} podem ser obtidos, recursivamente, a partir dos Y_i's e σ_i's (já conhecidos), através da relação

$$\sigma_{ji} = \sigma_i + Y_j \sigma_{j,i-1} \tag{4.15}$$

onde $0 \leq i \leq \nu - 1$ e $\sigma_0 = \sigma_{j,0} = 1$. Denotando a magnitude de cada erro por Z_j, temos que

$$\sum_{l=0}^{\nu-1} \sigma_{jl} S_{\nu-l} = \sum_{l=0}^{\nu-1} \sigma_{jl} \sum_{i=1}^{\nu} Z_i Y_i^{\nu-l} = \sum_{i=1}^{\nu} Z_i Y_i \sum_{l=0}^{\nu-1} \sigma_{jl} Y_i^{\nu-1-l}. \tag{4.16}$$

Mas por (4.12), a igualdade 4.16 resulta em

$$\sum_{l=0}^{\nu-1} \sigma_{jl} S_{\nu-l} = \sum_{i=1}^{\nu} Z_i Y_i \prod_{m \neq j} (Y_i - Y_m) = Z_j Y_j \prod_{m \neq j} (Y_j - Y_m), \tag{4.17}$$

onde a última igualdade segue do fato de que o somatório em questão só não se anula se $i = j$. Pela equação (4.17) podemos concluir que

$$\sum_{l=0}^{\nu-1} \sigma_{jl} S_{\nu-l} = Z_j \sum_{l=0}^{\nu-1} \sigma_{jl} {X_j}^{\nu-l}.$$

Daí segue que cada Z_j, $1 \leq j \leq \nu$, é dado pela expressão

$$Z_j = \frac{\sum_{l=0}^{\nu-1} \sigma_{jl} S_{\nu-l}}{\sum_{l=0}^{\nu-1} \sigma_{jl} {X_j}^{\nu-l}}. \tag{4.18}$$

Com isto terminamos o quarto passo do processo de decodificação dos códigos alternantes que é a determinação das magnitudes dos erros Y_j, $1 \leq j \leq \nu$, através da equação (4.18).

Iremos agora ilustrar com exemplos a aplicação destes procedimentos.

Exemplo 4.1.4 *Seja $C(n, \eta)$ o código BCH sobre $GF(16)$ gerado pelo polinômio $g(x) = x^8 + x^7 + x^6 + x^4 + 1$ e com seu polinômio dual $h(x) = x^7 + x^6 + x^4 + 1$. Seja $GF(16)$ o corpo de Galois dado por $\alpha^4 + \alpha + 1 = 0$, isto é, $GF(16) \cong \frac{GF(2)}{<x^4+x+1>}$. As raízes de $g(x)$ são $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9$ e α^{12}. Como somente quatro das raízes possuem potências consecutivas, então $d_{\min}(C) \geq 5$. Por outro lado, o peso do polinômio gerador é 5; assim, a distância mínima do código é exatamente 5 e, por isso, a capacidade de correção de erros é de 2 erros aleatórios. A matriz verificação de paridade para este código é*

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha^{14} & \alpha & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^9 & \alpha^{11} & \alpha^{13} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha & \alpha^5 & \alpha^9 & \alpha^{13} & \alpha^2 & \alpha^6 & \alpha^{10} & \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^{11} \end{bmatrix}.$$

Supondo que o vetor todo nulo $c = (000000000000000)$ seja transmitido através do canal e que o vetor recebido seja $\overline{r} = (00000\alpha^3 00000\alpha^8 0000)$. Aplicando os procedimentos de decodificação do algoritmo de Berlekamp-Massey, temos:

1. ***Cálculo do vetor síndrome:*** *$S_i = r(\alpha^i)$, $1 \leq i \leq 4$, onde $r(x)$ é o polinômio recebido. Assim, o vetor síndrome S é dado por*

$$\overline{S} = \overline{r} \cdot H^T = \begin{pmatrix} \alpha^5 & \alpha^6 & \alpha^5 & \alpha^{11} \end{pmatrix};$$

2. ***Cálculo das funções simétricas elementares:*** *A partir da Tabela (4.1) continuamos com o preenchimento dos dados, usando o algoritmo de Berlekamp-Massey, obtendo a Tabela 4.2. Assim, o polinômio localizador de erros é dado por*

n	$\sigma^{(n)}(Y)$	d_n	l_n	$n - l_n$
-1	1	1	0	-1
0	1	α^5	0	0
1	$1+\alpha^5 Y$	α^7	1	0
2	$1+\alpha Y$	α^{13}	1	1
3	$1+\alpha^{11}Y + \alpha^{11}Y^2$	α^3	2	1
4	$1+\alpha^3 Y + \alpha Y^2$	0		

Tabela 4.2: *Algoritmo de BM aplicado em* $\overline{r} = (00000\alpha^3 00000\alpha^8 0000)$

$$\sigma(Y) = 1 + \alpha^3 Y + \alpha Y^2,$$

o que significa que o padrão de erro introduzido pelo canal contém dois erros. Além disso, $\sigma_1 = \alpha^3$ e $\sigma_2 = \alpha$;

3. ***Cálculo dos números de localização de erros:*** *Resolvemos a equação polinomial*

$$\rho(Y) = Y^2\sigma(1/Y) = Y^2 + \alpha^3 Y + \alpha = 0,$$

determinando, assim, as raízes do ***polinômio recíproco*** *de $\sigma(Y)$, $Y_1 = \alpha^5$ e $Y_2 = \alpha^{11}$, as quais podem ser determinadas por inspeção direta em $GF(16)$. Desse modo, podemos afirmar que os dois erros ocorreram nas posições Y^5 e Y^{11}.*

4. ***Cálculo das magnitudes dos erros:*** *Este cálculo é realizado através das equações (4.15) e (4.18). Pela equação (4.15), temos que*

$$\begin{aligned} &\sigma_{10} = 1, && \sigma_{20} = 1, \\ &\sigma_{11} = \sigma_1 + Y_1\sigma_{10} = \alpha^3 + \alpha^5 \cdot 1 = \alpha^{11}, && \sigma_{21} = \sigma_1 + Y_2\sigma_{20} = \alpha^3 + \alpha^{11} \cdot 1 = \alpha^5, \\ &\sigma_{12} = \sigma_2 + Y_1\sigma_{11} = \alpha + \alpha^5 \cdot \alpha^{11} = 0, && \sigma_{22} = \sigma_2 + Y_2\sigma_{21} = \alpha + \alpha^{11} \cdot \alpha^5 = 0. \end{aligned}$$

Agora, usando a equação (4.18), obtemos as magnitudes dos dois erros, $Z_1 = \alpha^3$ e $Z_2 = \alpha^8$.

Exemplo 4.1.5 *Seja $C(15, 5)$ o código RS sobre $GF(16)$ gerado pelo polinômio $g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)$. As raízes de $g(x)$ são $\alpha, \alpha^2, \alpha^3, \alpha^4$, e, consequentemente,*

$d_{\min}(C) \geq 5$. *Logo, a distância mínima do código é exatamente* 5, *uma vez que* $g(x)$ *é formado por* 5 *mônomios. A matriz verificação de paridade para este código é*

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha^{14} & \alpha & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^9 & \alpha^{11} & \alpha^{13} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha & \alpha^5 & \alpha^9 & \alpha^{13} & \alpha^2 & \alpha^6 & \alpha^{10} & \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^{11} \end{bmatrix}.$$

Supondo que o vetor todo nulo $c = (000000000000000)$ *seja transmitido através do canal e que o vetor recebido seja* $\overline{r} = (000\alpha000\alpha^{11}0000000)$. *Aplicando os procedimentos de decodificação do algoritmo de Berlekamp-Massey, temos:*

1. *Vetor síndrome:* $\overline{S} = \overline{r} \cdot H^T = \begin{pmatrix} \alpha^7 & \alpha^6 & \alpha^4 & \alpha^{10} \end{pmatrix}$;

2. *Funções simétricas elementares: para este caso, o algoritmo de Berlekamp-Massey nos fornece a Tabela 4.3. Desse modo,* $\sigma(Y) = 1 + \alpha^4 Y + \alpha^{10} Y^2$ *será o polinômio*

n	$\sigma^{(n)}(Y)$	d_n	l_n	$n - l_n$
-1	1	1	0	-1
0	1	α^7	0	0
1	$1+\alpha^7 Y$	α^8	1	0
2	$1+\alpha^{14} Y$	α^8	1	1
3	$1+\alpha^3 Y + \alpha^7 Y^2$	1	2	1
4	$1+\alpha^4 Y + \alpha^{10} Y^2$	0	2	2

Tabela 4.3: *Algoritmo de BM aplicado em* $\overline{r} = (000\alpha000\alpha^{11}0000000)$

localizador de erros, o que significa que o padrão de erro introduzido pelo canal contém dois erros e, além disso, $\sigma_1 = \alpha^4$ *e* $\sigma_2 = \alpha^{10}$;

3. *Números de localização de erros: Resolvendo a equação*

$$\rho(Y) = Y^2 \sigma(1/Y) = Y^2 + \alpha^4 Y + \alpha^{10} = 0,$$

obtemos as raízes do ***polinômio recíproco*** *de* $\sigma(Y)$, $Y_1 = \alpha^3$ *e* $Y_2 = \alpha^7$, *obtidas por inspeção direta em* $GF(16)$, *concluindo portanto que ocorreram erros nas posições* Y^3 *e* Y^7;

4. *Magnitudes dos erros: Da equação (4.15), segue que*

$$\begin{aligned} &\sigma_{10} = 1, && \sigma_{20} = 1, \\ &\sigma_{11} = \sigma_1 + Y_1\sigma_{10} = \alpha^4 + \alpha^3 \cdot 1 = \alpha^7, && \sigma_{21} = \sigma_1 + Y_2\sigma_{20} = \alpha^4 + \alpha^7 \cdot 1 = \alpha^3, \\ &\sigma_{12} = \sigma_2 + Y_1\sigma_{11} = \alpha^{10} + \alpha^3 \cdot \alpha^7 = 0, && \sigma_{22} = \sigma_2 + Y_2\sigma_{21} = \alpha^{10} + \alpha^7 \cdot \alpha^3 = 0. \end{aligned}$$

Por outro lado, a equação (4.18) nos dá

$$Z_1 = \frac{\sigma_{10} S_2 + \sigma_{11} S_1}{\sigma_{10} Y_1^2 + Y_1 \sigma_{11}} = \frac{1 \cdot \alpha^6 + \alpha^7 \cdot \alpha^7}{1 \cdot \alpha^6 + \alpha^3 \cdot \alpha^7} = \frac{\alpha^6 + \alpha^{14}}{\alpha^6 + \alpha^{10}} = \alpha$$

$$Z_2 = \frac{\sigma_{20} S_2 + \sigma_{21} S_1}{\sigma_{20} Y_2^2 + Y_2 \sigma_{21}} = \frac{1 \cdot \alpha^6 + \alpha^3 \cdot \alpha^7}{1 \cdot \alpha^{14} + \alpha^7 \cdot \alpha^3} = \frac{\alpha^6 + \alpha^{10}}{\alpha^{14} + \alpha^{10}} = \alpha^{11}.$$

Portanto, as magnitudes dos dois erros são: $Z_1 = \alpha$ *e* $Z_2 = \alpha^{11}$.

Exemplo 4.1.6 *Considere um código RS* $(15, 7)$ *(capaz de corrigir até três erros) definido sobre* $GF(16)$, *gerado pelo polinômio* $g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)$. *O seu polinômio dual é* $h(x) = (x+\alpha^7)(x+\alpha^8)(x+\alpha^9)(x+\alpha^{10})(x+\alpha^{11})(x+\alpha^{12})(x+\alpha^{13})(x+\alpha^{14})(x+1)$. *As raízes de* $g(x)$ *são* $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$ *e* α^6, *consequentemente* $d_{\min}(C) \geq 7$. *A matriz verificação de paridade para este código é dada por*

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{14} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{14} \\ 1 & \alpha^3 & (\alpha^3)^2 & \cdots & (\alpha^3)^{14} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^6 & (\alpha^6)^2 & \cdots & (\alpha^6)^{14} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha^{14} & \alpha & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^9 & \alpha^{11} & \alpha^{13} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha & \alpha^5 & \alpha^9 & \alpha^{13} & \alpha^2 & \alpha^6 & \alpha^{10} & \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^{11} \\ 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} \\ 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \alpha^9 & 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \alpha^9 & 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \alpha^9 \end{bmatrix}$$

Assuma que o vetor todo nulo $\overline{v} = (000000000000000)$ *seja transmitido através do canal e que o vetor recebido seja* $\overline{r} = (000\alpha^7 00\alpha^3 00000\alpha^4 00)$. *De modo análogo ao Exemplo 3.5.2, obtemos:*

1. *Vetor síndrome:* $\overline{S} = \overline{r} \cdot H^T = \begin{pmatrix} \alpha^{12} & 1 & \alpha^{14} & \alpha^{10} & 0 & \alpha^{12} \end{pmatrix}$;

2. *Funções simétricas elementares: neste caso, o algoritmo de Berlekamp-Massey nos dá a Tabela 4.4. Portanto,* $\sigma(Y) = 1+\alpha^7 Y+\alpha^4 Y^2+\alpha^6 Y^3$ *é o polinômio localizador*

n	$\sigma^{(n)}(Y)$	d_n	l_n	$n - l_n$
-1	1	1	0	-1
0	1	α^{12}	0	0
1	$1+\alpha^{12}Y$	α^7	1	0
2	$1+\alpha^3 Y$	1	1	1
3	$1+\alpha^3 Y+\alpha^3 Y^2$	α^7	2	1
4	$1+\alpha^4 Y+\alpha^{12} Y^2$	α^{10}	2	2
5	$1+\alpha^7 Y+\alpha^4 Y^2+\alpha^6 Y^3$	0	3	2
6	$1+\alpha^7 Y+\alpha^4 Y^2+\alpha^6 Y^3$	-	-	-

Tabela 4.4: *Algoritmo de BM aplicado em* $\overline{r} = (000\alpha^7 00\alpha^3 00000\alpha^4 00)$

de erros, o que significa que o padrão de erro introduzido pelo canal contém três erros. Mais ainda, $\sigma_1 = \alpha^7$, $\sigma_2 = \alpha^4$ *e* $\sigma_3 = \alpha^6$;

3. *Números de localização de erro: resolvendo a equação polinomial*

$$\rho(Y) = Y^3 + \alpha^7 Y^2 + \alpha^4 Y + \alpha^6 = 0,$$

determinamos as raízes do ***polinômio recíproco*** *de* $\sigma(Y)$, $Y_1 = \alpha^3$, $Y_2 = \alpha^6$ *e* $Y_3 = \alpha^{12}$, *as quais podem ser encontradas por inspeção direta em* $GF(16)$. *Assim, podemos afirmar que os três erros ocorreram nas posições* Y^3, Y^6 *e* Y^{12}.

4. *Magnitudes dos erros: Pela equação (4.15) temos que*

$$\begin{array}{lll} \sigma_{10} = 1, & \sigma_{20} = 1, & \sigma_{30} = 1, \\ \sigma_{11} = \alpha^4, & \sigma_{21} = \alpha^{10}, & \sigma_{31} = \alpha^2, \\ \sigma_{12} = \alpha^3, & \sigma_{22} = 1, & \sigma_{32} = \alpha^9. \end{array}$$

Agora, usando a equação (4.18), obtemos as magnitudes dos três erros: $Z_1 = \alpha^7$, $Z_2 = \alpha^3$ *e* $Z_3 = \alpha^4$.

4.2 Algoritmo de Berlekamp-Massey Ampliado

Com o objetivo de ampliar a capacidade do processo da localização e da determinação da magnitude dos erros no sistema de decodificação, realizados pelo algoritmo de Berlekamp-Massey, substituiremos a terceira etapa desse algoritmo por três novas etapas sem que, com isso, ocorra uma alteração significativa na complexidade de decodificação. Esta incorporação corresponderá à implementação de uma estrutura geométrica, através das curvas algébricas não-singulares (ou seus modelos suaves), definidas através de polinômios absolutamente irredutíveis, conforme as condições estabelecidas na Definição 3.2.5 e Proposição 3.2.8. Isto no contexto do corpo de números complexos é equivalente à caracterização das superfícies de Riemann associadas.

O resultado desse procedimento será denominado de **algoritmo de Berlekamp-Massey ampliado**, cujas etapas constam dos seguintes passos:

Passo 1: Cálculo do vetor síndrome $\overline{S} = (S_1, S_2, \cdots, S_{\delta-1})$, a partir do vetor recebido $\overline{r}$;

Passo 2: Cálculo das funções simétricas elementares $\sigma_1, \sigma_2, \cdots, \sigma_\nu$, a partir do vetor $\overline{S}$;

Passo 3: Obtenção do polinômio $f(x, y)$ estabelecido na Definição 3.2.5 ou na Proposição 3.2.8, através de S_1 e dos σ_i's.

Passo 4: Cálculo dos números de localização de erros $Y_1, Y_2, \cdots, Y_\nu$, a partir dos pontos racionais do polinômio homogêneo $F(X, Y, Z)$ de $f(x, y)$;

Passo 5: Identificação do tipo de curva algébrica gerada pelo polinômio $f(x, y)$, isto é, se $f(x, y)$ é singular ou não-singular e consequentemente determinar o gênero da curva algébrica associada;

Passo 6: Cálculo das magnitudes dos erros Z_i's, a partir dos pontos racionais que identificam a localização dos erros do polinômio $F(X, Y, Z)$, isto é, utilizando as síndromes S_i's e os Y_i's.

A seguir, analisaremos detalhadamente cada um dos seis passos acima.

Passo 1: *Cálculo do vetor síndrome.*

$$\overline{S} = \overline{r} \cdot H^T.$$

Passo 2: *Cálculo das funções simétricas elementares.*

Este passo é o mesmo do algoritmo de Berlekamp-Massey.

Passo 3: *Obtenção do polinômio (Chave1) (ou polinômio Chave2), através de S_1 e dos σ_i's.*

Determinados os valores dos σ_i's, $1 \leq i \leq \nu$, Passo 2, obtemos o polinômio de grau v, estabelecido na Definição 3.2.5 (ou Proposição 3.2.8), substituindo os a_i's pelos σ_i's e b por S_1.

Passo 4: *Cálculo dos números de localização dos erros.*

Para determinarmos os números de localização dos erros, necessitamos encontrar todos os pontos racionais da curva gerada pelo polinômio homogêneo $F(X, Y, Z)$ de $f(x, y)$, isto é, as raízes do polinômio F sobre o corpo $GF(q)$. Como o número de elementos de $GF(q)$ é finito, basta então determinar os pontos racionais do polinômio F utilizando o algoritmo de Gaétan, veja Apêndice 4.4. Como $F(X, Y, 1) = f(x, y)$ e $f(x = S_1, y) = \rho(Y)$, onde $\rho(Y)$ é o polinômio recíproco do polinômio determinado na saída do algoritmo de BM, então somente os pontos racionais onde $X = S_1$ e $Z = 1$ são de nosso interesse. Com isso, determinamos as correspondentes localizações de erros na coordenada Y, as quais são dadas pelos pontos $P_i = (S_1, Y_i, 1)$, onde $1 \leq i \leq \nu$ (veja Figura 4.1). Portanto, os Y_i's selecionados, além de serem ordenadas dos pontos racionais do polinômio, também correspondem aos números de localização de erros. Lembramos que a existência da condição $Y_i = \alpha^i$, implica a ocorrência de um erro na posição $i + 1$ da palavra-código.

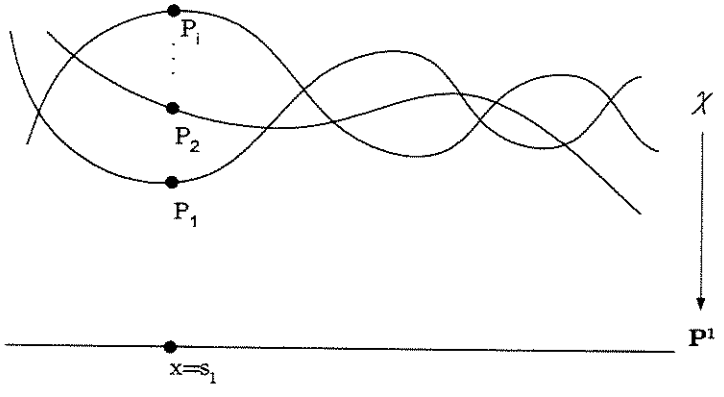


Figura 4.1: *Localização por pontos racionais*

Passo 5: *Identificação do tipo da curva algébrica associada ao polinômio determinado no Passo 3 quanto a singularidade e obtenção do seu gênero.*

Neste passo, devemos levar em consideração os seguintes fatos:

1. Se $f(x,y)$ é um polinômio absolutamente irredutível, isto é, irredutível no fecho, então o "lugar geométrico" das raízes $\mathcal{X}$ é conexo. Como o subconjunto fechado irredutível X do espaço $\mathcal{A}^n$ é uma variedade algébrica afim. Conseqüentemente, o conjunto de zeros de $\mathcal{X}$ do polinômio F é irredutível e, portanto, é uma variedade afim. Para $n = 3$ a variedade V(F) é uma superfície, [58].

2. No caso de a curva $\mathcal{X}$ gerada por $f(x,y)$ ser síngular, é necessário considerar sua correspondente desingularização (modelo não-singular da curva $\mathcal{X}$) $\widetilde{\mathcal{X}}$ (veja Teoremas 3.3.10 e 3.3.11, Subseção 3.3.4), que, na verdade, consiste em eliminar os pontos singulares, que, pela Proposição 3.6.23, são finitos. Desse modo, $\widetilde{\mathcal{X}}$ também gera uma superfície.

Consequentemente, se o polinômio é absolutamente irredutível sobre $GF(q)$, isto é, irredutível sobre o fecho algébrico de $GF(q)$, então, a curva abstrata $\mathcal{X}$ como definida aqui é um espaço topológico completo, que é de fato compacto. Sobre o copro de números complexos $\mathbb{C}$ a curva abstrata $\mathcal{X}$ é simplesmente uma superfície de Riemann, [39]. Além do gênero, parâmetro caracterizador da superfície, o grau do polinômio em y corresponde à quantidade de folhas que cobre esta superfície. No caso da decodificação, o grau de y corresponde à quantidade de erros que ocorreram na decodificação, isso se for olhado no contexto do corpo de números complexos.

Se a curva for não-singular, então o gênero é dado pela expressão (3.9). Caso contrário, é dado pela expressão (3.8).

Passo 6: *Cálculo das magnitudes dos erros Z_i's, a partir dos pontos racionais.*

A obtenção das magnitudes Z_j, $1 \leq j \leq \nu$, é o último passo do processo de decodificação dos códigos alternantes. Os Z_i's também serão determinados através das coordenadas dos pontos racionais P_i's. Assim, as magnitudes dos erros são obtidas diretamente do polinômio $f(x,y)$. Pela Proposição 3.6.4, temos que sempre existem v-raízes distintas $y_1(x), y_2(x), \ldots, y_v(x)$ para a equação $f(x,y) = 0$. Como utilizamos as localizações dos erros Y_i's, as quais são distintas, então temos, pelo Teorema 4.2.1, que a matriz de *Vandermonde* é não-singular e que o sistema (4.20) abaixo tem solução única.

Teorema 4.2.1 *[5]A matriz de Vandermonde, definida na forma*

$$\mathsf{V} = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ Y_1 & Y_2 & \ldots & Y_\mu \\ Y_1^2 & Y_2^2 & \ldots & Y_\mu^2 \\ \vdots & \vdots & & \vdots \\ Y_1^{\mu-1} & Y_2^{\mu-1} & \ldots & Y_\mu^{\mu-1} \end{bmatrix}, \tag{4.19}$$

tem determinante não-nulo se, e somente se, todos os Y_i para $i = 1, \ldots, \mu$ são distintos.

Demonstração. Suponhamos que $Y_i = Y_j$, para todo $i \neq j$. Assim, as colunas Y_i e Y_j de V são iguais, condição esta que implica em $\det \mathsf{V} = 0$. Isso é uma contradição, pois, por hipótese, $\det \mathsf{V} \neq 0$. Para mostrar a recíproca, usaremos de indução sobre μ. Se $\mu = 1$, segue que $\mathsf{V} = [1]$ e, portanto, $\det \mathsf{V} \neq 0$. Suponhamos, que o teorema é verdadeiro para

a matriz de Vandermonde $\mu-1 \times \mu-1$. Consideremos $y = Y_1$ e $\det \mathsf{V}$ uma função em y, ou seja,

$$\det(\mathsf{V}) = D(y) = \begin{bmatrix} 1 & y & y^2 & \dots & y^{\mu-1} \\ 1 & Y_2 & Y_2^2 & \dots & Y_2^{\mu-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & Y_\mu & Y_\mu^2 & \dots & Y_\mu^{\mu-1} \end{bmatrix}.$$

Logo, desenvolvendo em forma de determinantes, temos,

$$D(y) = \begin{vmatrix} Y_2 & Y_2^2 & \cdots & Y_2^{\mu-1} \\ \vdots & \vdots & \cdots & \vdots \\ Y_\mu & Y_\mu^2 & \cdots & Y_\mu^{\mu-1} \end{vmatrix} + y \begin{vmatrix} 1 & Y_2^2 & \cdots & Y_2^{\mu-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & Y_\mu^2 & \cdots & Y_\mu^{\mu-1} \end{vmatrix} + \cdots + y^{\mu-1} \begin{vmatrix} 1 & Y_2 & \cdots & Y_2^{\mu-2} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & Y_\mu & \cdots & Y_\mu^{\mu-2} \end{vmatrix},$$

o qual pode ser escrito como

$$D(y) = d_{\mu-1}y^{\mu-1} + \cdots + d_1 y + d_0.$$

Como $d_{\mu-1}$ é um determinante de uma matriz de Vandermonde $\mu-1 \times \mu-1$, segue, pela hipótese de indução, que $d_{\mu-1} \neq 0$. Logo, $D(y)$ é um polinômio de grau $\mu-1$ e tem no máximo $\mu-1$ raízes, pois estamos trabalhando sobre um corpo. Agora, se $y = Y_i$, $i = 2, \cdots, \mu$, segue que $D(Y_i) = 0$, pois temos duas linhas iguais na matriz, e portanto Y_i, $i = 2, \cdots, \mu$, são todas raízes de $D(y)$. Mas, por hipótese, os $Y_i's$, $i = 1, \cdots, \mu-1$, são todos distintos e, assim, o polinômio $D(y)$ pode ser fatorado como

$$D(y) = d_{\mu-1}\left[\prod_{i=2}^{\mu}(y - Y_i)\right].$$

Desse modo, o determinante da matriz original de Vandermonde é

$$D(Y_1) = d_{\mu-1}\left[\prod_{i=2}^{\mu}(Y_1 - Y_i)\right].$$

Como $d_{\mu-1} \neq 0$ e $Y_1 \neq Y_i$, $i = 2, \cdots, \mu$, segue que o determinante da matriz de Vandermonde $\mu \times \mu$ é não-nulo e, por indução, o teorema é verdadeiro para todo μ. ∎

Observe que as ν primeiras equações de (4.6), as quais relacionam as componentes do vetor síndrome com os Y_i's e Z_i's, podem ser escritas na forma de sistema, isto é,

$$\overline{Y}.\overline{Z}^T = \overline{S}^T \Longrightarrow \begin{bmatrix} Y_1 & Y_2 & \dots & Y_\nu \\ Y_1^2 & Y_2^2 & \dots & Y_\nu^2 \\ \vdots & \vdots & & \vdots \\ Y_1^\nu & Y_2^\nu & \dots & Y_\nu^\nu \end{bmatrix} \begin{bmatrix} Z_1 \\ Z_2 \\ \vdots \\ Z_\nu \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_\nu \end{bmatrix}. \tag{4.20}$$

Os ν valores $y_1, y_2, \dots, y_\nu$ são distintos e consequentemente o sistema com ν equações e ν incógnitas, e, cuja matriz $\overline{Y}$ é a matriz de Vandermonde de $y_1, y_2, \dots, y_\nu$ que é não-singular (conforme Teorema 4.2.1). Então, o sistema (4.20) é não-singular e pode ser resolvido facilmente em termos das incógnitas Z_i's, se invertermos a matriz $\overline{Y}$ em (4.20). Logo, o vetor das magnitudes $\overline{Z} = (Z_1, Z_2, \cdots, Z_\nu)$ fica univocamente determinado.

Terminaremos esta seção com três exemplos que ilustram a aplicação desse procedimento de decodificação dos códigos alternantes.

Exemplo 4.2.2 *Seja $A(\overline{\alpha}, y)$ o código alternante sobre $GF(16)$, com $\overline{\alpha} = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14})$, $y = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14})$ e $r = 4$. Consequentemente $d_{\min}(C) \geq r + 1 = 5$. A matriz verificação de paridade para este código é dada por*

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{14} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^{14})^2 \\ 1 & \alpha^3 & (\alpha^2)^3 & \cdots & (\alpha^{14})^3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \alpha & 0 & \cdots & 0 \\ 0 & 0 & \alpha^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha^{14} \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha^{14} & \alpha & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^9 & \alpha^{11} & \alpha^{13} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha & \alpha^5 & \alpha^9 & \alpha^{13} & \alpha^2 & \alpha^6 & \alpha^{10} & \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^{11} \end{bmatrix}.$$

Supondo que o vetor todo nulo $\overline{c} = (000000000000000)$ seja transmitido através do canal e que o vetor recebido seja $\overline{r} = (000\alpha000\alpha^{11}0000000)$. Aplicando os procedimentos de decodificação do algoritmo de Berlekamp-Massey ampliado, temos:

1. *Cálculo do vetor síndrome: $S_i = r(\alpha^i)$, $1 \leq i \leq 4$, onde $r(x)$ é o polinômio recebido. Assim, o vetor síndrome S é dado por*

$$\overline{S} = \overline{r} \cdot H^T = \begin{pmatrix} \alpha^7 & \alpha^6 & \alpha^4 & \alpha^{10} \end{pmatrix};$$

2. *Cálculo das funções simétricas elementares: a partir da tabela (4.1) continuamos com o preenchimento dos dados, usando o algoritmo de Berlekamp-Massey, obtendo a Tabela 4.5. Portanto, o polinômio localizador de erros é dado por*

n	$\sigma^{(n)}(Y)$	d_n	l_n	$n - l_n$
-1	1	1	0	-1
0	1	α^7	0	0
1	$1+\alpha^7 Y$	α^8	1	0
2	$1+\alpha^{14} Y$	α^8	1	1
3	$1+\alpha^3 Y + \alpha^7 Y^2$	1	2	1
4	$1+\alpha^4 Y + \alpha^{10} Y^2$	0	2	2

Tabela 4.5: *Algoritmo de BM para* $\overline{r} = (000\alpha000\alpha^{11}0000000)$

$$\sigma(Y) = 1 + \alpha^4 Y + \alpha^{10} Y^2,$$

o que significa que o padrão de erro introduzido pelo canal contém dois erros e que $\sigma_1 = \alpha^4$ e $\sigma_2 = \alpha^{10}$;

3. *Obtenção do polinômio (Chave1) estabelecido na Definição 3.2.5 ou polinômio (Chave2) da Proposição 3.2.8, através de* S_1 *e dos* σ_i*'s. Como ocorreram dois erros e* $\sigma_1 \neq 0$*, então, segue da Proposição 3.2.8 que o polinômio associado é*

$$f(x,y) = y^2 + (x + \sigma_1 + S_1)y + (x + \sigma_1 + S_1)(x + \frac{\sigma_2}{\sigma_1} + S_1).$$

Como $\sigma_1 = \alpha^4$, $\sigma_2 = \alpha^{10}$ *e* $S_1 = \alpha^7$, *então*

$$f(x,y) = y^2 + xy + \alpha^3 y + x^2 + \alpha^{12}x + \alpha^{13};$$

4. *Cálculo dos números de localização dos erros: Inicialmente, realizamos a homogeneização do polinômio* $f(x,y)$*, Definição 3.3.7, e depois determinamos os pontos racionais do polinômio homogêneo* $F(X,Y,Z) = 0$*, utilizando o algoritmo de Gaétan, veja Apêndice 4.4. Desse modo, obtemos os seguintes pontos racionais:* $(\alpha^6, \alpha^6, 1)$, $(\alpha^{12}, \alpha^6, 1)$, $(\alpha^{13}, 1, 1)$, $(\alpha^4, 1, 1)$, $(\alpha^7, \alpha^3, 1)$, $(\alpha^{13}, \alpha^2, 1)$, $(\alpha^{12}, \alpha^7, 1)$, $(\alpha^5, \alpha^2, 1)$, $(\alpha^4, \alpha^9, 1)$, $(\alpha^{10}, \alpha^{12}, 1)$, $(\alpha^6, \alpha^3, 1)$, $(\alpha^7, \alpha^7, 1)$, $(\alpha^5, \alpha^9, 1)$, $(\alpha^{10}, 0, 1)$, $(\alpha^3, 0, 1)$, $(\alpha^{10}, 1, 0)$, $(\alpha^5, 1, 0)$. *Observando os pontos onde* $X = S_1 = \alpha^7$ *e* $Z = 1$*, isto é,* $F(S_1, Y, 1) = 0$*, temos onde ocorreram os erros. Os pontos racionais satisfazendo* $X = S_1 = \alpha^7$ *e* $Z = 1$ *são* $P_1 = (\alpha^7, \alpha^3, 1)$ *e* $P_2 = (\alpha^7, \alpha^7, 1)$ [1]*. Portanto, os erros ocorreram em* $Y_1 = \alpha^3$ *e* $Y_2 = \alpha^7$ *e consequentemente na quarta e oitava posições da palavra-código.*

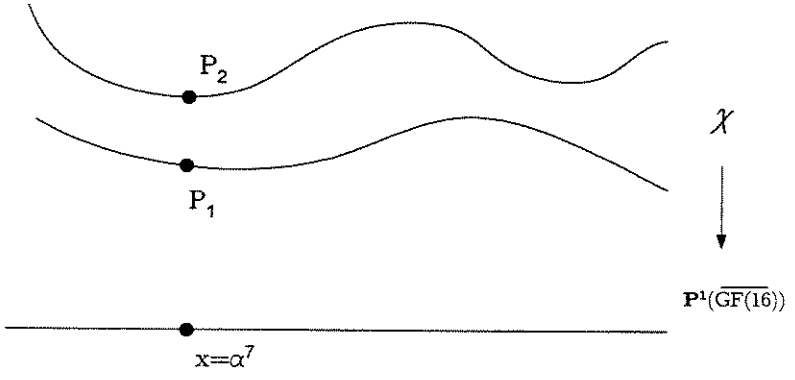


Figura 4.2: *Localização de* P_1 *e* P_2 *na curva* $\mathcal{X}$

5. *Singularidade e gênero da curva algébrica associada: A curva sobre* $\overline{GF(16)}$ *gerada por* $f(x,y) = 0$ *é não-singular, consequentemente o gênero da curva é dado pela equação (3.9), portanto é* 0;

6. *Cálculo das magnitudes dos erros: Usando o fato de que os pontos racionais* $P_1 = (\alpha^7, \alpha^3, 1)$ *e* $P_2 = (\alpha^7, \alpha^7, 1)$*, indicam as localizações dos erros* Y_1, Y_2*, que são distintas por hipótese, então devemos encontrar as magnitudes* $Z_i \in GF(16)$, $i = 1, 2$ *resolvendo o sistema (4.20) invertendo a matriz* $\overline{Y}$*. Portanto, as magnitudes dos erros são* $Z_1 = \alpha$ *e* $Z_2 = \alpha^{11}$.

[1] Para cada ponto em $\mathbb{P}^1$ há dois pontos na curva $\mathcal{X}$.

Exemplo 4.2.3 *Usando os dados do código RS* $(15,7)$ *do Exemplo 4.1.6, temos que o vetor síndrome* S *é dado por*

$$\overline{S} = \begin{pmatrix} \alpha^{12} & 1 & \alpha^{14} & \alpha^{10} & 0 & \alpha^{12} \end{pmatrix}$$

e as funções simétricas elementares são $\sigma_1 = \alpha^7$, $\sigma_2 = \alpha^4$ *e* $\sigma_3 = \alpha^6$. *Como ocorreram três erros e*

$$\frac{\sigma_t}{\sigma_j} - S_1^2 = \frac{\alpha^6}{\alpha^7} - (\alpha^{12})^2 = \alpha^{14} - \alpha^9 = \alpha^4 \quad e \quad -(S_1 - \sigma_1)^2 = -(\alpha^{12} - \alpha^7)^2 = -(\alpha^2)^2 = \alpha^4,$$

então, pela Definição 3.2.5, temos $f_1(x) = x + \sigma_1 - S_1 = x + \alpha^7 - \alpha^{12} = (x + \alpha^2)$ *e* $\rho = 1$, *logo*

$$\begin{aligned} g_2(x) &= x + \tfrac{\sigma_2}{\sigma_1} - S_1 = x + \alpha^{12} - \alpha^{12} = x; \\ g_3(x) &= x^2 + x - S_1 + \tfrac{\sigma_3}{\sigma_1} - S_1^2 = x^2 + x - \alpha^{12} + \alpha^{14} - \alpha^9 = x^2 + x + \alpha^6, \end{aligned}$$

portanto, o polinômio procurado é

$$f(x,y) = y^3 + (x + \alpha^2)y^2 + x(x + \alpha^2)y + (x + \alpha^2)(x^2 + x + \alpha^6).$$

Homogeneizando o polinômio $f(x,y)$, *obtemos*

$$F(X,Y,Z) = Y^3 + (X + \alpha^2 Z)Y^2 + X(X + \alpha^2 Z)Y + (X + \alpha^2 Z)(X^2 + XZ + \alpha^6 Z^2).$$

Os pontos racionais do polinômio homogêneo $F(X,Y,Z) = 0$ *são:* $(\alpha^{10}, \alpha^{13}, 1)$, $(\alpha^{11}, \alpha^5, 1)$, $(\alpha^{13}, \alpha^{14}, 1)$, $(\alpha^{13}, \alpha^6, 1)$, $(\alpha^{12}, \alpha^3, 1)$, $(\alpha^9, \alpha^3, 1)$, $(\alpha^8, \alpha^5, 1)$, $(\alpha^5, \alpha^{11}, 1)$, $(\alpha^3, \alpha^3, 1)$, $(\alpha^3, \alpha, 1)$, $(\alpha^{12}, \alpha^6, 1)$, $(\alpha^{12}, \alpha^{12}, 1)$, $(\alpha^{14}, \alpha^{10}, 1)$, $(\alpha^7, \alpha^6, 1)$, $(\alpha^3, \alpha^5, 1)$, $(\alpha^2, 0, 1)$, $(1, 1, 0)$ *e* $(0, 1, 1)$. *Observando os pontos onde* $X = S_1 = \alpha^{12}$ *e* $Z = 1$, *identificamos onde ocorreram os erros. Os pontos racionais satisfazendo* $X = S_1 = \alpha^{12}$ *e* $Z = 1$ *são* $(\alpha^{12}, \alpha^3, 1)$, $(\alpha^{12}, \alpha^6, 1)$ *e* $(\alpha^{12}, \alpha^{12}, 1)$. *Portanto,* $Y_1 = \alpha^3$, $Y_2 = \alpha^6$ *e* $Y_3 = \alpha^{12}$, *logo os erros ocorreram na quarta, na sétima e na décima terceira posição do vetor recebido. A curva sobre* $\overline{GF(16)}$ *gerada por* $f(x,y) = 0$ *é não-singular, consequentemente, o gênero da curva é dado pela equação (3.9), portanto o gênero da curva é* 1. *Usando o fato de que os pontos racionais* $P_1 = (\alpha^{12}, \alpha^3, 1)$, $P_2 = (\alpha^{12}, \alpha^6, 1)$ *e* $P_3 = (\alpha^{12}, \alpha^{12}, 1)$, *indicam as localizações dos erros* Y_1, Y_2, Y_3 *que são distintas por hipótese, então devemos encontrar as magnitudes* $Z_i \in GF(16)$, $i = 1, 2, 3$ *resolvendo o sistema (4.20) invertendo a matriz* $\overline{Y}$. *Portanto, as magnitudes dos erros são* $Z_1 = \alpha^7$, $Z_2 = \alpha^3$ *e* $Z_3 = \alpha^4$.

Exemplo 4.2.4 *Seja* C *o código RS sobre* $GF(8)$ *gerado pelo polinômio* $g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4)$. $GF(8) \cong \frac{GF(2)}{<x^3 + x + 1>}$. *As raízes de* $g(x)$ *são* $\alpha, \alpha^2, \alpha^3, \alpha^4$, *e consequentemente* $d_{\min}(C) \geq 5$. *Como o código RS é MDS, a distância mínima é exatamente* 5. *A matriz verificação de paridade para este código é*

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{bmatrix}.$$

Supondo que o vetor todo nulo $\overline{c} = (0000000)$ *seja transmitido através do canal e que o vetor recebido seja* $\overline{r} = (\alpha 00\alpha^2 000)$. *Aplicando o procedimento de decodificação descrito acima temos:*

O vetor síndrome S *é*

$$\overline{S} = \overline{r} \cdot H^T = \begin{pmatrix} \alpha^6 & 0 & \alpha^2 & 1 \end{pmatrix}.$$

Cálculando as funções simétricas elementares temos: $\sigma_1 = \alpha$ *e* $\sigma_2 = \alpha^3$.

Como ocorreram dois erros e $\sigma_1 \neq 0$, *então, pela Proposição 3.2.8, temos*

$$f(x,y) = y^2 + (x+\alpha^5)y + (x+\alpha^5)(x+1).$$

O polinômio homogêneo de $f(x,y)$ *é* $F(X,Y,Z) = Y^2 + XY + \alpha^5 YZ + X^2 + \alpha^4 XZ + \alpha^5 Z^2$. *Fazendo* $F(X,Y,Z) = 0$, *temos que seus pontos racionais são:* $(\alpha^6,1,1)$, $(\alpha^6,\alpha^3,1)$, $(\alpha,1,1)$, $(\alpha,\alpha^2,1)$, $(1,\alpha^4,1)$, $(0,\alpha^3,1)$, $(0,\alpha^2,1)$, $(1,0,1)$, $(\alpha^5,0,1)$. *Observando os pontos onde* $X = S_1 = \alpha^6$ *e* $Z = 1$, *temos onde ocorreram os erros. Os pontos racionais satisfazendo* $X = S_1 = \alpha^6$ *e* $Z = 1$ *são* $(\alpha^6,1,1)$ *e* $(\alpha^6,\alpha^3,1)$. *Portanto, os erros ocorreram na primeira e na quarta posição do vetor recebido.*

A curva sobre $GF(8)$ *gerada por* $f(x,y) = 0$ *é não-singular, consequentemente, o gênero da curva é dado pela equação (3.9), portanto o gênero da curva é* 0.

Cálculo das magnitudes dos erros: Como os pontos racionais $P_1 = (\alpha^6,1,1)$ *e* $P_2 = (\alpha^6,\alpha^3,1)$, *indicam as localizações dos erros* Y_1, Y_2, *que são distintas por hipótese, então devemos encontrar as magnitudes* $Z_i \in GF(8)$, $i = 1,2$, *resolvendo o sistema (4.20). Portanto, as magnitudes dos erros são* $Z_1 = \alpha$ *e* $Z_2 = \alpha^2$.

Observe que esta curva é maximal, pois atende ao limitante da Definição 3.4.2.

Exemplo 4.2.5 *Seja* C *o código de Srivastava generalizado sobre* $GF(32)$, *com* $z_i = 1$, *para todo* i, $s = 1$, $m = 5$, $t = 4$, $w = 0$ *e* $\alpha_1 = \alpha^{31} = 1$, $\alpha_2 = \alpha^{30}$, $\alpha_3 = \alpha^{29}$, $\ldots$, $\alpha_{31} = \alpha$. *Assim, a distância mínima é* $d_{\min}(C) \geq st + 1 = 5$. *Logo, a matriz verificação de paridade para este código é*

$$H = \begin{bmatrix} \frac{1}{1-0} & \frac{1}{\alpha^{30}-0} & \frac{1}{\alpha^{29}-0} & \frac{1}{\alpha^{28}-0} & \cdots & \frac{1}{\alpha^2-0} & \frac{1}{\alpha-0} \\ \frac{1}{(1-0)^2} & \frac{1}{(\alpha^{30}-0)^2} & \frac{1}{(\alpha^{29}-0)^2} & \frac{1}{(\alpha^{28}-0)^2} & \cdots & \frac{1}{(\alpha^2-0)^2} & \frac{1}{(\alpha-0)^2} \\ \frac{1}{(1-0)^3} & \frac{1}{(\alpha^{30}-0)^3} & \frac{1}{(\alpha^{29}-0)^3} & \frac{1}{(\alpha^{28}-0)^3} & \cdots & \frac{1}{(\alpha^2-0)^3} & \frac{1}{(\alpha-0)^3} \\ \frac{1}{(1-0)^4} & \frac{1}{(\alpha^{30}-0)^4} & \frac{1}{(\alpha^{29}-0)^4} & \frac{1}{(\alpha^{28}-0)^4} & \cdots & \frac{1}{(\alpha^2-0)^4} & \frac{1}{(\alpha-0)^4} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \cdots & \alpha^{29} & \alpha^{30} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \cdots & \alpha^{27} & \alpha^{29} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \cdots & \alpha^{25} & \alpha^{28} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha & \cdots & \alpha^{23} & \alpha^{27} \end{bmatrix}$$

Supondo que o vetor todo nulo $\overline{c} = (0000000000\ldots00000)$ *seja transmitido através do canal e que o vetor recebido seja* $\overline{r} = (0\alpha^5 0000\ldots0\alpha 0)$. *Aplicando os procedimentos de decodificação do algoritmo de Berlekamp-Massey ampliado, temos:*

O vetor síndrome S *é*

$$\overline{S} = \overline{r} \cdot H^T = \begin{pmatrix} \alpha^{21} & \alpha & \alpha^9 & \alpha^2 \end{pmatrix}.$$

Cálculando as funções simétricas elementares temos: $\sigma_1 = \alpha^{27}$ *e* $\sigma_2 = \alpha^{30}$.

Como ocorreram dois erros e $\sigma_1 \neq 0$, *então, pela Proposição 3.2.8, temos*

$$f(x,y) = y^2 + (x+\alpha^{17})y + (x+\alpha^{17})(x+\alpha^4).$$

O polinômio homogêneo de $f(x,y)$ *é* $F(X,Y,Z) = Y^2 + XY + \alpha^{17}YZ + X^2 + \alpha^{18}XZ + \alpha^{21}Z^2$. *Fazendo* $F(X,Y,Z) = 0$, *temos que seus pontos racionais são:* $(\alpha^4, \alpha^{18}, 1)$, $(\alpha^5, \alpha^6, 1)$, $(\alpha^5, \alpha^{13}, 1)$, $(\alpha^6, \alpha^{15}, 1)$, $(\alpha^6, \alpha^{19}, 1)$, $(\alpha^9, \alpha^{13}, 1)$, $(\alpha^9, \alpha^{22}, 1)$, $(\alpha^{10}, \alpha^{12}, 1)$, $(\alpha^{10}, \alpha^{20}, 1)$, $(\alpha^{11}, \alpha^8, 1)$, $(\alpha^{11}, \alpha^{25}, 1)$, $(\alpha^{13}, \alpha^{12}, 1)$, $(\alpha^{13}, 1, 1)$, $(\alpha^{14}, \alpha^{25}, 1)$, $(\alpha^{14}, \alpha^{26}, 1)$, $(\alpha^{20}, \alpha^{22}, 1)$, $(\alpha^{21}, \alpha, 1)$, $(\alpha^{21}, \alpha^{29}, 1)$, $(\alpha^{23}, \alpha^9, 1)$, $(\alpha^{23}, \alpha^{19}, 1)$, $(\alpha^{24}, \alpha^{20}, 1)$, $(\alpha^{24}, 1, 1)$, $(\alpha^{25}, \alpha, 1)$, $(\alpha^{25}, \alpha^3, 1)$, $(\alpha^{28}, \alpha^9, 1)$, $(\alpha^{28}, \alpha^{15}, 1)$, $(\alpha^{29}, \alpha^8, 1)$, $(\alpha^{29}, \alpha^{26}, 1)$, $(\alpha^{30}, \alpha^3, 1)$, $(\alpha^{30}, \alpha^{29}, 1)$, $(1, 0, \alpha^{14})$, $(1, 0, \alpha^{27})$. *Observando os pontos onde* $X = S_1 = \alpha^{21}$ *e* $Z = 1$, *temos onde ocorreram os erros. Os pontos racionais satisfazendo* $X = S_1 = \alpha^{21}$ *e* $Z = 1$ *são* $(\alpha^{21}, \alpha, 1)$ *e* $(\alpha^{21}, \alpha^{29}, 1)$. *Portanto, os erros ocorreram na segunda e na trigésima posição do vetor recebido.*

A curva sobre $\overline{GF(32)}$ *gerada por* $f(x,y) = 0$ *é não-singular, consequentemente, o gênero da curva é dado pela equação (3.9), portanto o gênero da curva é* 0.

Cálculo das magnitudes dos erros: Como os pontos racionais $P_1 = (\alpha^{21}, \alpha, 1)$ *e* $P_2 = (\alpha^{21}, \alpha^{29}, 1)$, *indicam as localizações dos erros* Y_1, Y_2, *que são distintas por hipótese, então devemos encontrar as magnitudes* $Z_i \in GF(32)$, $i = 1, 2$, *resolvendo o sistema (4.20). Portanto, as magnitudes dos erros são* $Z_1 = \alpha^5$ *e* $Z_2 = \alpha$.

Observe que esta curva é maximal, pois atende ao limitante da Definição 3.4.2.

4.3 Algoritmo de Peterson-Gorenstein-Zierler Ampliado

De modo análogo aos procedimentos adotados na obtenção do algoritmo de Berlekamp-Massey ampliado, iremos propor um algoritmo de decodificação, a partir do algoritmo de Peterson-Gorenstein-Zierler, [7]. A função básica deste algoritmo é determinar, usando as propriedades dos sistemas lineares (4.8), as funções simétricas elementares. Os implementos dos passos que iremos introduzir visam a localização dos erros através dos pontos racionais da curva algébrica associada ao polinômio (Chave1) ou polinômio (Chave2) e, para os códigos alternantes definidos no Capítulo 2, a identificação da primeira síndrome.

As equações (4.8) podem ser escritas na seguinte forma matricial

$$\begin{bmatrix} S_1 & S_2 & \cdots & S_\mu \\ S_2 & S_3 & \cdots & S_{\mu+1} \\ \vdots & \vdots & & \vdots \\ S_{\delta-\mu-1} & S_{\delta-\mu} & \cdots & S_{\delta-2} \end{bmatrix} \begin{bmatrix} \sigma_\mu \\ \sigma_{\mu-1} \\ \vdots \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} -S_{\mu+1} \\ -S_{\mu+2} \\ \vdots \\ -S_{\delta-1} \end{bmatrix}. \tag{4.21}$$

Mostraremos, no Teorema 4.3.1, que a matriz associada ao sistema (4.21) é não-singular, quando existirem ν erros na recepção do vetor transmitido.

O teorema a seguir nos fornece a condição para a determinação dos ν erros ocorridos na recepção do vetor transmitido.

Teorema 4.3.1 *[5] A matriz de síndromes*

$$M = \begin{bmatrix} S_1 & S_2 & \cdots & S_\mu \\ S_2 & S_3 & \cdots & S_{\mu+1} \\ \vdots & \vdots & & \vdots \\ S_\mu & S_{\mu+1} & \cdots & S_{2\mu-1} \end{bmatrix} \tag{4.22}$$

é não-singular se μ é igual a ν, o número de erros que realmente ocorreram. A matriz é singular se μ é maior do que ν.

Demonstração. Seja $Y_\mu = 0$ para $\mu > \nu$. Seja a matriz (4.19) com elementos $V_{ij} = Y_j^{i-1}$, e seja D a matriz diagonal

$$D = \begin{bmatrix} Z_1Y_1 & 0 & \ldots & 0 \\ 0 & Z_2Y_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & Z_\mu Y_\mu \end{bmatrix}$$

com elementos $D_{ij} = Z_iY_i\delta_{ij}$, onde $\delta = 1$ se $i = j$ e zero caso contrário. Então a matriz produto VDV^T tem elementos

$$\left(VDV^T\right)_{ij} = \sum_{i=1}^{\mu} Y_l^{i-1} \sum_{k=1}^{\mu} Z_lY_l\delta_{lk}Y_k^{j-1} = \sum_{i=1}^{\mu} Y_l^{i-1}Z_lY_lY_l^{j-1} = \sum_{i=1l}^{\mu} Z_lY_l^{i+j-1},$$

que são iguais ao ij-ésimo elemento da matriz M e, portanto, $M = VDV^T$. Assim, o determinante de M satisfaz

$$\det M = \det V \det D \det V \det M = (\det V)^2(\det D).$$

Se μ é maior que ν, então $\det D = 0$ e portanto, $\det(M) = 0$; consequentemente, M é singular. Se μ é igual a ν, então $\det D \neq 0$. Além disso, a matriz (4.19) tem determinante não-nulo se as colunas são diferentes e não-nulas, no qual é verdadeiro se μ é igual a ν. Portanto, $\det M \neq 0$. Isso completa a demonstração do teorema. ∎

De acordo com o Teorema 4.3.1, para calcular os valores correto dos erros ν's, primeiro fixamos $\nu = t$ e calculamos o determinante da matriz (4.22). Se for não-nulo, este é o valor correto de ν. Caso contrário, se o determinante for zero, reduzimos o valor de ν por 1 e repetimos o procedimento. Continuamos com esse procedimento, até que um determinante não-nulo seja obtido. Assim, a quantidade de erros que ocorreram na palavra recebida é então conhecida. Em seguida, invertemos a matriz (4.22) e calculamos os σ_i's. Após isto, determinaremos o polinômio (Chavel) ou polinômio (Chave2) como objetivo de obtenção dos pontos racionais do polinômio homogêneo de $f(x, y)$.

Algoritmo de Peterson-Gorenstein-Zierler

Em vista aos fatos relacionados acima, deduzimos que o procedimento de decodificação de códigos alternantes compreende os seguintes passos:

(1) $\mu \longleftarrow \lfloor (\delta - 1)/2 \rfloor$ 0;

(2) se $\det M \neq 0$, então a solução do sistema (4.21) é encontrada, portanto fim. Caso contrário vá para (3);

(3) $\mu \longleftarrow \mu - 1$; vá para (2).

O número de erros é dado por $\nu = \mu$ e a solução $(\sigma_1, \sigma_2, \ldots, \sigma_\nu)$ de (4.21) é encontrada multiplicando-se a matriz M^{-1} por $(-S_{\mu+1}, -S_{\mu+2}, \ldots, -S_{2\mu})^T$.

Em virtude dos comentários acima, a decodificação de códigos alternantes pode ser realizada com os seguintes procedimentos, que será denominado de **algoritmo de Peterson-Gorenstein-Zierler ampliado**, cujas etapas constam dos seguintes passos:

Passo 1: Cálculo do vetor síndrome $\overline{S} = (S_1, S_2, \cdots, S_{\delta-1})$, a partir do vetor recebido $\overline{r}$;

Passo 2: Identificação da condição de singularidade da matriz (4.22);

Passo 3: Cálculo das funções simétricas elementares $\sigma_1, \sigma_2, \cdots, \sigma_\nu$ através do sistema (4.21);

Passo 4: Obtenção do polinômio (Chave1) ou polinômio (Chave2), através de S_1 e dos σ_i's.

Passo 5: Cálculo dos números de localização de erros $Y_1, Y_2, \cdots, Y_\nu$, a partir dos pontos racionais do polinômio homogêneo $F(X, Y, Z)$ de $f(x, y)$;

Passo 6: Identificação do tipo de curva algébrica gerada pelo polinômio $f(x, y)$, isto é, se $f(x, y)$ é singular ou não-singular e consequentemente determinar o gênero da curva algébrica;

Passo 7: Cálculo das magnitudes dos erros Z_i's a partir dos pontos racionais que identificam a localização dos erros do polinômio $F(X, Y, Z)$.

A seguir, analisaremos detalhadamente cada um dos sete passos acima.

Passo 1: *Cálculo do vetor síndrome.*

$$\overline{S} = \overline{r} \cdot H^T.$$

Passo 2: *Identificação da condição de singularidade da matriz (4.22).*

Determinamos a matriz (4.22) e verificamos se é não-singular, caso contrário, reduzimos o valor de ν por 1 e repetimos o procedimento até que um determinante não-nulo seja obtido;

Passo 3: *Cálculo das funções simétricas elementares.*

Usamos o Passo 3 *e* determinamos a solução do sistema linear (4.21) nas incógnitas $\sigma_i's$, $1 \leq i \leq \nu$, tal que ν seja mínimo, usando o fato de que a matriz M é não-singular.

Feito isso, passamos a analisar o quarto passo que determina o polinômio (*Chave*1) ou polinômio (*Chave*2).

Passo 4: *Obtenção do polinômio (Chave1) ou polinômio (Chave2), através de* S_1 *e dos* σ_i*'s.*

Este passo é idêntico ao Passo 3 do algoritmo de Berlekamp-Massey Ampliado.

Passo 5: *Cálculo dos números de localização dos erros.*

Este passo é idêntico ao Passo 4 do algoritmo de Berlekamp-Massey Ampliado.

Passo 6: *Identificação quanto a condição de singularidade da curva gerada pelo polinômio* $f(x, y)$.

Determinamos se a curva algébrica associada ao polinômio obtido no Passo 4 é singular ou não-singular e determinamos seu gênero. Este passo é idêntico ao Passo 5 do algoritmo de Berlekamp-Massey Ampliado.

Passo 7: *Cálculo das magnitudes dos erros* Z_i's, *a partir dos pontos racionais.*

Este passo é idêntico ao Passo 6 do algoritmo de Berlekamp-Massey Ampliado.

Para ilustrar a aplicação dos procedimentos de decodificação descritos acima, apresentaremos alguns exemplos.

Exemplo 4.3.2 *Como exemplo do procedimento de decodificação, considere um código* $BCH(15, 5)$ *(capaz de corrigir até três erros) definido sobre* $GF(16)$ *gerado pelo polinômio* $g(x) = x^{10}+x^8+x^5+x^4+x^2+x+1$. *Seja* $GF(16)$ *o corpo de Galois tal que* $\alpha^4+\alpha+1 = 0$. *Temos que* $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ *são raízes de* $g(x)$, *portanto* $d_{\min}(C) \geq 7$. *A matriz verificação de paridade para este código é*

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha^{14} & \alpha & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^9 & \alpha^{11} & \alpha^{13} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha & \alpha^5 & \alpha^9 & \alpha^{13} & \alpha^2 & \alpha^6 & \alpha^{10} & \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^{11} \\ 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} \\ 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \alpha^9 & 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \alpha^9 & 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \alpha^9 \end{bmatrix}.$$

Assuma que a palavra toda nula $\overline{c} = (000000000000000)$ *seja transmitida através do canal e que o vetor recebido seja* $\overline{r} = (001000010000000)$. *Agora, seguiremos os passos do algoritmo de decodificação.*

1. *Cálculo do vetor síndrome* $\overline{S}$*: a* i*-ésima síndrome* $S_i = r(\alpha^i)$, $1 \leq i \leq 6$, *onde* $r(x)$ *é o polinômio recebido. Portanto,*

$$\overline{S} = \overline{r}H^T = \begin{pmatrix} \alpha^{12} & \alpha^9 & 0 & \alpha^3 & \alpha^0 & 0 \end{pmatrix}.$$

2. *Identificação da condição de singularidade da matriz (4.22). Neste passo, iniciamos com* $\nu = 3$ *e verificaremos se a matriz*

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} \alpha^{12} & \alpha^9 & 0 \\ \alpha^9 & 0 & \alpha^3 \\ 0 & \alpha^3 & 1 \end{bmatrix}$$

é não-singular. Como o determinante de M é nulo, então consideramos agora $\nu = 2$ e verificamos se M é não-singular. Assim,

$$M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = \begin{bmatrix} \alpha^{12} & \alpha^9 \\ \alpha^9 & 0 \end{bmatrix}.$$

Como $\det M = \alpha^3$ *é não-nulo, então ocorreram dois erros.*

3. *Cálculo das funções simétricas elementares: resolvendo o sistema (4.21), temos que,* $\sigma_1 = \alpha^{12}$ *e* $\sigma_2 = \alpha^9$.

4. *Obtenção do polinômio (Chave1) ou polinômio (Chave2): como* $\sigma_1 \neq 0$ *e* $\sigma_2 = \sigma_1^2$, *então utilizamos o polinômio (Chave2) para determinar o polinômio* $f(x, y)$. *Assim, temos que*

$$f_1(x) = x + \sigma_1 - S_1 = x + \alpha^{12} - \alpha^{12} = x \quad e$$
$$g(x) = \sigma_1(x - S_1 + \sigma_1) = \alpha^{12}(x - \alpha^{12} + \alpha^{12}) = \alpha^{12}x.$$

Logo, $f(x, y) = y^2 + xy + \alpha^{12}x$.

5. *Cálculo dos números de localização de erros: os pontos racionais do polinômio homogêneo* $F(X, Y, Z) = 0$ *são:* $(\alpha^7, \alpha^8, 1)$, $(\alpha^2, \alpha^{10}, 1)$, $(\alpha^7, \alpha^{11}, 1)$, $(\alpha^{11}, \alpha^5, 1)$, $(\alpha^{10}, \alpha^{13}, 1)$, $(\alpha^2, \alpha^4, 1)$, $(\alpha^4, \alpha, 1)$, $(\alpha^{12}, \alpha^2, 1)$, $(\alpha^{12}, \alpha^7, 1)$, $(\alpha^{11}, \alpha^3, 1)$, $(\alpha^8, \alpha^{14}, 1)$, $(\alpha^{10}, \alpha^9, 1)$, $(\alpha^8, \alpha^6, 1)$, $(\alpha^4, 1, 1)$, $(1, 1, 0)$, $(1, 0, 0)$, $(0, 0, 1)$. *Esta curva é maximal. Observando os pontos onde* $X = s_1$ *e* $Z = 1$, *identificamos a posição dos erros. Os pontos racionais onde ocorreram os erros foram* $(\alpha^{12}, \alpha^2, 1)$ *e* $(\alpha^{12}, \alpha^7, 1)$. *Portanto, os erros ocorreram na terceira e na oitava componente.*

6. *Identificação da condição de singularidade da curva algébrica gerada pelo polinômio* $f(x, y)$: *a curva sobre* $\overline{GF(16)}$ *gerada por* $f(x, y) = 0$ *é não-singular de gênero* 0.

7. *Cálculo das magnitudes dos erros* Z_i*'s, a partir dos pontos racionais: Como o código é binário, os erros são de magnitudes* 1 *e, conseqüentemente, o erro é dado por* $\overline{e} = (0010000010000000)$.

Exemplo 4.3.3 *Considere o código de Goppa* $C(L, g)$, *onde* $L = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}$ *e* $d = 5$, *assim* $g(x) = x^{d-1} = x^4$ *e* $t = 2$. *Logo, a matriz verificação de paridade do código de Goppa (2.11), é dada por*

$$H = \begin{bmatrix} 1 & \alpha^{11} & \alpha^7 & \alpha^3 & \alpha^{14} & \alpha^{10} & \alpha^6 & \alpha^2 & \alpha^{13} & \alpha^9 & \alpha^5 & \alpha & \alpha^{12} & \alpha^8 & \alpha^4 \\ 1 & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & 1 & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & 1 & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 \\ 1 & \alpha^{13} & \alpha^{11} & \alpha^9 & \alpha^7 & \alpha^5 & \alpha^3 & \alpha & \alpha^{14} & \alpha^{12} & \alpha^{10} & \alpha^8 & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^{14} & \alpha^{13} & \alpha^{12} & \alpha^{11} & \alpha^{10} & \alpha^9 & \alpha^8 & \alpha^7 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{bmatrix}.$$

Assuma que a palavra toda nula $\overline{c} = (000000000000000)$ *seja transmitida através do canal e que o vetor recebido seja* $\overline{r} = (0000\alpha^3 00\alpha^5 0000000)$. *Aplicando os procedimentos de decodificação do algoritmo de Peterson-Gorenstein-Zierler ampliado, temos:*

Cálculando o vetor síndrome, temos

$$\underline{S} = \underline{r}H^T = \begin{pmatrix} \alpha^{12} & \alpha^8 & \alpha^7 & \alpha^2 \end{pmatrix}.$$

Determinar a matriz (4.22) e verificar se é não-singular. Neste passo, iniciamos com $\nu = 2$ *e verificaremos se a matriz*

$$M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = \begin{bmatrix} \alpha^{12} & \alpha^8 \\ \alpha^8 & \alpha^7 \end{bmatrix}.$$

é não-singular. Como o determinante de M *é não-nulo, isto é,*

$$\det M = \det \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = \det \begin{bmatrix} \alpha^{12} & \alpha^8 \\ \alpha^8 & \alpha^7 \end{bmatrix} = 1,$$

então ocorreram dois erros.

Resolvendo o sistema (4.21), temos que $\sigma_1 = \alpha^3$ *e* $\sigma_2 = \alpha^{11}$.

Como $\sigma_1 \neq 0$ *e* $\sigma_2 \neq \sigma_1^2$, *então utilizando o polinômio (Chave2) para determinar o polinômio* $f(x, y)$, *temos que*

$$f_1(x) = x + \sigma_1 - S_1 = x + \alpha^3 - \alpha^{12} = x + \alpha^{10} \quad e$$
$$g(x) = (x + \sigma_1 - S_1)(x + \sigma_2/\sigma_1 - S_1) = (x + \alpha^{10})(x + \alpha^9).$$

Logo, $f(x, y) = y^2 + (x + \alpha^{10})y + (x + \alpha^{10})(x + \alpha^9)$.

Os pontos racionais do polinômio homogêneo de $f(x, y)$ *são:* $(\alpha, \alpha, 1)$, $(\alpha, \alpha^{10}, 1)$, $(\alpha^3, \alpha^3, 1)$, $(\alpha^3, \alpha^{10}, 1)$, $(\alpha^9, \alpha^{13}, 1)$, $(\alpha^{12}, \alpha^4, 1)$, $(\alpha^{12}, \alpha^7, 1)$, $(\alpha^{13}, \alpha, 1)$, $(\alpha^{13}, \alpha^3, 1)$, $(\alpha^{14}, \alpha^7, 1)$, $(\alpha^{14}, \alpha^8, 1)$, $(1, \alpha^4, 1)$, $(1, \alpha^8, 1)$, $(\alpha^5, 1, 0)$, $(1, 0, \alpha^5)$, $(1, 0, \alpha^6)$, $(\alpha^{10}, 1, 0)$. *Esta curva é uma curva maximal. Observando os pontos onde* $X = S_1$ *e* $Z = 1$, *temos onde ocorreram os erros. Os pontos racionais que ocorreram os erros foram* $(\alpha^{12}, \alpha^4, 1)$ *e* $(\alpha^{12}, \alpha^7, 1)$. *Portanto, os erros ocorreram na quinta e na oitava componente do vetor recebido.*

A curva sobre $\overline{GF(16)}$ *gerada por* $f(x, y) = 0$ *é não-singular de gênero* 0.

Como os pontos racionais $P_1 = (\alpha^7, \alpha^3, 1)$ *e* $P_2 = (\alpha^7, \alpha^7, 1)$, *indicam as localizações dos erros* Y_1, Y_2, *que são distintas por hipótese, então devemos encontrar as magnitudes* $Z_i \in GF(16)$, $i = 1, 2$, *resolvendo o sistema (4.20) invertendo a matriz* $\overline{Y}$. *Portanto, as magnitudes dos erros são* $Z_1 = \alpha^3$ *e* $Z_2 = \alpha^5$.

4.4 Apêndice

Algoritmo Para Pontos Singulares e Pontos Racionais

Os algoritmos que apresentaremos a seguir são baseados nos algoritmos de Gaétan e Dominique, [26].

Seja $\mathcal{X}$ uma curva plana projetiva definida sobre $GF(q)$ com equação $F(X,Y,Z)=0$.

Algoritmo para determinar pontos singulares

Sejam F_X, F_Y e F_Z, respectivamente, as derivadas de F com respeito as variáveis X, Y e Z. Então

$$(a:b:c)\in\mathcal{X} \text{ é singular } \iff \begin{cases} F(a,b,c)=0 \\ F_X(a,b,c)=0 \\ F_Y(a,b,c)=0 \\ F_Z(a,b,c)=0 \\ (a,b,c)\neq(0,0,0). \end{cases} \qquad \text{(Sing)}$$

Para resolver o sistema (Sing), adotaremos os seguintes passos, utilizando o pacote do Sistema Maple7:

```
with(algcurves): (pacote que trabalha com curvas algébricas no Maple);
 m:; n: (números naturais);
p: (número primo);
alias(alpha=RootOf(x^m+x+n-1)): (gera o corpo de Galois p^m);
f1: (Polinômio nas variáveis x e y, isto é, f1(x,y));
F1:=homogeneous(f1,x,y,z) mod p; (Polinômio homogêneo de f1(x,y));
F1x:=diff(F1,x)mod p;
F1y:=diff(F1,y)mod p;
F1z:=diff(F1,z)mod p;
 for i from 1 by 1 to m^n - 1 do
    for j from 1 by 1 to m^n - 1 do
      if (simplify(subs({x=alpha^i,y=alpha^j,z=1},F1))mod p)=0 and
        (simplify(subs({x=alpha^i,y=alpha^j,z=1},F1x))mod p)=0 and
        (simplify(subs({x=alpha^i,y=alpha^j,z=1},F1y))mod p)=0
      then print(alpha^i,alpha^j,1) end if; od;
      if (simplify(subs({x=alpha^j,y=1,z=0},F1))mod p)=0 and
        (simplify(subs({x=alpha^j,y=1,z=0},F1x))mod p)=0 and
        (simplify(subs({x=alpha^j,y=1,z=0},F1z))mod p)=0
      then print(alpha^j,1,0) end if;
      if (simplify(subs({x=alpha^j,y=0,z=1},F1))mod p)=0 and
        (simplify(subs({x=alpha^j,y=0,z=1},F1x))mod p)=0 and
        (simplify(subs({x=alpha^j,y=0,z=1},F1y))mod p)=0
      then print(alpha^j,0,1) end if;
      if (simplify(subs({x=0,y=alpha^j,z=1},F1))mod p)=0 and
```

```
    (simplify(subs({x=0,y=alpha^j,z=1},F1x))mod p)=0 and
    (simplify(subs({x=0,y=alpha^j,z=1},F1y))mod p)=0
 then print(0,alpha^j,1) end if; od;
if (simplify(subs({x=1,y=0,z=0},F1))mod p)=0 and
    (simplify(subs({x=1,y=0,z=0},F1y))mod p)=0 and
    (simplify(subs({x=1,y=0,z=0},F1z))mod p)=0
 then print(1,0,0) end if;
if (simplify(subs({x=0,y=0,z=1},F1))mod p)=0 and
    (simplify(subs({x=0,y=0,z=1},F1x))mod p)=0 and
    (simplify(subs({x=0,y=0,z=1},F1y))mod p)=0
 then print(0,0,1) end if;
if (simplify(subs({x=0,y=1,z=0},F1))mod p)=0 and
    (simplify(subs({x=0,y=1,z=0},F1x))mod p)=0 and
    (simplify(subs({x=0,y=1,z=0},F1z))mod p)=0
 then print(0,1,0) end if;
```

Algoritmo para determinar pontos racionais

Para encontrar os pontos racionais de uma curva algébrica sobre corpos finitos, usaremos a mesma idéia do algoritmo anterior.

Então,

$$(a:b:c) \in \mathcal{X} \text{ é racional sobre } GF(q) \Longleftrightarrow \begin{cases} F(a,b,c)=0 \\ a^q - a = 0 \\ b^q - b = 0 \\ c^q - c = 0 \\ (a,b,c) \neq (0,0,0). \end{cases} \quad \text{(Rac)}$$

Para resolver o sistema (Rac), adotaremos os seguintes passos utilizando também o pacote do Sistema Maple7:

```
with(algcurves): (pacote que trabalha com curvas algébricas no Maple);
    m: n: (números naturais);
    p: (número primo);
    alias(alpha=RootOf(x^m+x+n-1)): (gerando o corpo de Galois p^m);
    f1: (Polinômio nas variáveis x e y, isto é, f1(x,y));
    F1:=homogeneous(f1,x,y,z) mod p; (Polinômio homogêneo de f1(x,y));
    soma:=0;
    for i from 1 by 1 to m^n - 1 do
       for j from 1 by 1 to m^n - 1 do
        if (simplify(subs({x=alpha^i,y=alpha^j,z=1},F1))mod p)=0
        then soma:=soma+1: print(alpha^i,alpha^j,1) end if;
        od;
        if (simplify(subs({x=alpha^j,y=1,z=0},F1))mod p)=0
        then soma:=soma+1:print(alpha^j,1,0) end if;
```

```
 if (simplify(subs({x=1,y=0,z=alpha^j},F1))mod p)=0
 then soma:=soma+1:print(1,0,alpha^j) end if;
 if (simplify(subs({x=0,y=alpha^j,z=1},F1))mod p)=0
 then soma:=soma+1:print(0,alpha^j,1) end if;
 od;
if (simplify(subs({x=1,y=0,z=0},F1))mod p)=0
 then soma:=soma+1:print(1,0,0) end if;
if (simplify(subs({y=1,x=0,z=0},F1))mod p)=0
 then soma:=soma+1:print(0,1,0) end if;
if (simplify(subs({z=1,x=0,y=0},F1))mod p)=0
 then soma:=soma+1:print(0,0,1) end if;
 od;soma;
```

Capítulo 5

Conclusões

Nossa proposta, neste trabalho, foi estabelecer uma relação entre curvas algébricas, através de polinômios absolutamente irredutíveis, e o processo de decodificação dos códigos alternantes. A principal motivação foi a construção de polinômios absolutamente irredutíveis $f(x, y)$ sobre corpos finitos, que, por sua vez, geram curvas algébricas associadas diretamente ao processo de decodificação dos códigos alternantes. Desta forma, a estrutura geométrica do problema em foco teve como ponto de partida a busca dessa estrutura utilizando a relação entre o polinômio irredutível $f(x, y)$, dado por

$$f(x, y) = f_0(x)y^n + f_1(x)y^{n-1} + \cdots + f_n(x)$$

gerador de uma superfície de Riemann compacta e a saída do algoritmo de Berlekamp-Massey (BM), isto é, a determinação de um polinômio de duas variáveis (x, y), tal que para um determinado valor $x = x_0$ tivessemos o polinômio

$$f(x_0, y) = y^n + \sigma_1 y^{n-1} + \cdots + \sigma_n$$

como a saída do algorítmo de BM, ou equivalentemente, a superfície de erros.

Além disso, mostramos alguns exemplos de curvas com muitos pontos racionais derivados desta construção que são bastante utilizados na construção de códigos algébrico-geométricos (AG). Corpos de funções algébricas ou, equivalentemente, curvas algébricas, proporcionam uma ferramenta útil para a Teoria da Codificação e outros ramos da Teoria da Informação, como por exemplos, os códigos algébrico-geométricos e os códigos traço. Nestas aplicações, o número de pontos racionais de um corpo de função desempenha um papel crucial na construção de códigos AG, como mostrado no Exemplo 3.5.12. Tal código foi construído a partir de uma das curvas algébricas apresentadas na Seção 3.5.

Os objetivos deste trabalho estiveram fundamentados no processo de codificação e decodificação através das estruturas geométricas associadas aos códigos lineares. Ao longo do desenvolvimento desta reflexão, foram adotados os seguintes procedimentos, com seus respectivos resultados:

No Capítulo 2, foi apresentada uma investigação detalhada das principais subclasses dos códigos alternantes e suas generalizações. Também foram apresentadas diversas propriedades existentes entre essas subclasses, principalmente a relação entre a forma das matrizes geradora e verificação de paridade dessas subclasses, e, a partir disso, mostramos

vários exemplos dessas relações existentes. Apresentamos também, a relação de equivalência entre as formas das matrizes verificação de paridade do Código Clássico de Goppa.

No Capítulo 3, foi introduzida uma proposta de construção de polinômios absolutamente irredutíveis, que é muito importante no contexto da geometria algébrica e da Teoria da Codificação. No âmbito dessa discussão, introduzimos as principais curvas algébricas utilizadas para construir Códigos Algébrico-Geométricos, isto é, curvas maximais. Com base nisso, foram apresentados vários exemplos de curvas geradas por essa construção que possuem muitos pontos racionais. Observamos, ainda, que os polinômios (Chave1) e (Chave2) apresentados na Seção 3.2 podem ser representados da seguinte forma $f(x,y) = x^n + y^n + g(x,y)$, onde o grau de $g(x,y)$ é menor ou igual a n.

No Capítulo 4, foram introduzidos, nos algoritmos de Berlekamp-Massey e de Peterson-Gorenstein-Zierler, novos passos, com o objetivo de estabelecer, no processo de decodificação dos códigos alternantes, uma relação entre a estrutura algébrica existente e a estrutura geométrica através de curvas algébricas, que é obtida via construção de polinômios absolutamente irredutíveis apresentada no Capítulo 3. Os pontos racionais que estão diretamente relacionados na localização dos erros são pontos não-singulares da curva algébrica associada, e estes são utilizados através da matriz de Vandermonde para determinar as magnitudes dos erros. Por outro lado, os polinômios que determinam as localizações dos erros podem também ser utilizados para gerar curvas maximais, indicando, assim, que existe uma relação entre os códigos alternantes e os códigos algébrico-geométricos (a natureza dessa relação poderá ser investigada em trabalhos futuros). Dessa forma, introduzimos uma importante estrutura geométrica no contexto de decodificação de códigos alternantes cíclicos – este processo pode ser utilizado em qualquer um dos algoritmos de decodificação dessa classe de códigos.

Em síntese, e para reiterar as principais contribuições deste trabalho, destacamos a construção de polinômios absolutamente irredutíveis sobre corpos finitos; a incorporação de uma estrutura geométrica, até então inédita, aos algoritmos de Berlekamp-Massey e de Peterson-Gorestein-Zierler. A estrutura geométrica introduzida se aplica ao processo de decodificação da classe dos códigos alternantes através do grupo das unidades independentemente da estrutura algébrica em consideração. Finalmente, é importante mencionar a relevância de se utilizar conceitos e resultados (ou teorias) de base matemática para a solução de questões na área de Engenharia.

5.1 Proposta para Futuros Trabalhos

Durante o desenvolvimento deste trabalho, foram identificados vários tópicos de interesse tanto no contexto da Matemática quanto no contexto da Engenharia, especificamente no que diz respeito às curvas algébricas e aos processos de codificação e decodificação, respectivamente, os quais ficam como perspectivas abertas para futuras pesquisas. Dentre eles, podemos citar os seguintes:

- A determinação das condições, sobre o polinômio absolutamente irredutível (Chave1), para que as curvas algébricas geradas sejam não-singulares.

- O estabelecimento de condições para que as curvas geradas pelos polinômios (Chave1) e (Chave2) apresentados na Seção 3.2, sejam maximais.
- A determinação das relações existentes entre as curvas geradas pelos polinômios (Chave1) e (Chave2) apresentados na Seção 3.2 e as curvas mais conhecidas, isto é, curvas hermitianas, curvas de Klein, etc.
- A construção e identificação de Códigos Algébrico-Geométricos e Códigos Traço, a partir da proposta de construção de polinômios absolutamente irredutíveis.
- A determinação do tipo de relação existente entre os códigos alternantes e os códigos algébrico-geométricos no processo de decodificação e no processo de codificação, respectivamente.
- A determinação de condições a partir da proposta de construção de polinômios absolutamente irredutíveis afim de que essa proposta seja ampliada para a decodificação de códigos AG.
- Estabelecer uma estrutura geométrica no processo de decodificação dos códigos de bloco lineares sobre anéis finitos a partir do trabalho [3] utilizando polinômios absolutamente irredutíveis.

Referências Bibliográficas

[1] S. S. Abhyankar, "Desingularization of plane curves," *American Mathematical Society Proceedings of Symposia in Pure Mathematics*, Vol. 40 - Parte 1, pp.1-45, 1983.

[2] S. S. Abhyankar, *Algebraic Geometry for Scientists and Engineers*, Mathematical Surveys and Monographs, American Mathematical Society, Vol. 35, 1990.

[3] Antonio A. de Andrade, "Uma contribuição à construção e decodificação de códigos de blocos lineares sobre anéis finitos". *Tese de Doutorado, FEEC – UNICAMP*, Dez. 1996.

[4] C. L. Bajaj, C. M. Hoffmann, R. E. Lynch and J. E. H. Hopcroft, "Tracing surface intersections," *Computer Aided Geometric Design*, No. 5, North-Holland, pp.285-307, 1988.

[5] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

[6] E. R. Berlekamp, "Goppa Codes," *IEEE Trans. Inform. Theory*, Vol. IT-19, pp. 590-592, September, 1973.

[7] R. E. Brahut, *Theory and Practice of Error Control Codes*, Reading, MA: Addison-Wesley, 1983.

[8] R. T. Chien and M. D. Choy, "Algebraic generalization of BCH-Goppa-Hergert codes", *IEEE Trans. Inform. Theory*, Vol. IT-21, No. 1, pp. 70-79, 1975.

[9] Celso J. Costa, *Funções Elípticas, Algébricas e Superfícies Mínimas*. 18º Colóquio Brasileiro de Matemática, Impa, Rio de Janeiro, 1991.

[10] D. A. Cox and B. Sturmfels, Eds. *Applications of Computational Algebraic Geometry*. American Mathematical Society, 1997.

[11] P. Delsarte, "On subfield subcodes of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 21, pp. 575-576, 1975.

[12] Y. Driencourt, "Some properties of elliptic codes over a field of characteristic 2," *In Proc. AAAECC-3*, Grenoble 1985, Lect. Notes Comp. Sc. vol. 229, pp.185-193, 1986.

[13] P. Elias, "List decoding for noisy channels," *Technical Report 335*, Research Laboratory of Electronics, MIT, 1957.

[14] Gui-Liang Feng, and T. R. N. Rao, "Decoding of algebraic-geometric codes up to the designed minimum distance,"*IEEE Trans. Inform. Theory*, vol. 39, No. 1, pp.37-45, jan. 1993.

[15] Gui-Liang Feng, and T. R. N. Rao, "A simple Approach for Construction of Algebraic-Geometric Codes from Affine Plane Curves,"*IEEE Trans. Inform. Theory*, vol. 40, No. 4, julho 1994.

[16] G. D. Forney Jr., "On decoding BCH codes", *IEEE Trans. Inform. Theory*, Vol. IT-11, pp. 549-557, October 1965.

[17] Willian Fulton, *Algebraic Curves: an Introduction to Algebraic Geometry*, Benjamin, New York, 1969.

[18] W. Fulton, *Curvas Algebraicas*. Ed. Reverte, S. A., 1971.

[19] A. Garcia and H. Stichtenoth, "Algebraic function fields over finite fields with many rational places," *IEEE Trans. Inform. Theory*, Vol. 41, No.6, pp. 1548-1563, November 1995.

[20] A. Garcia and H. Stichtenoth, "Asymptotically good towers of function fields over finite fields," C. R. Acad. Sci. Paris 322 I, pp. 1067-1070, 1996.

[21] V. D. Goppa, "A new class of linear correcting codes," *Prob. Peredachi Informatsii*, vol. 6, No. 3, pp. 24-30, July-September, 1970.

[22] V. D. Goppa, "Rational representation of codes and (L, g)-codes," *Prob. Peredachi Informatsii*, vol. 7, No. 3, pp. 41-49, July-September, 1971.

[23] V. D. Goppa, "Codes associated with divisors," *Prob. Peredachi Informatsii*, vol. 13, pp. 33-39, 1977.

[24] V. D. Goppa, "Codes on algebraic curves". *Sov. Math. Dokl.* vol. 24, pp.75-91, 1981.

[25] V. D. Goppa, "Algebraic-geometric codes,"*Math. USSR Izvestiya 3*, vol. 21, pp. 75-91, 1983.

[26] Gaétan Haché and D. Le Brigand, "Effective construction of algebraic geometry codes,"*IEEE Trans. Inform. Theory*, vol. 41, pp. 1615-1628, Nov. 1995.

[27] H. J. Helgert, "Srivastava codes", *IEEE Trans. Inform. Theory*, vol. 18, pp. 292-297, 1972.

[28] H. J. Helgert, "Noncyclic generalizations of BCH and Srivastava codes", *Information and Control*, Vol 21, pp. 280-290, (1972).

[29] H. J. Helgert, "Alternant codes,"*Information and Control*, Vol 26, pp. 369-380, (1974).

[30] H. J. Helgert, "Binary primitive alternant codes,"*Information and Control*, Vol 27, pp. 101-108, (1975).

[31] H. J. Helgert, "Alternant codes," Talk given at *Information Theory Workshop, Lenox, Mass., June* 1975.

[32] Y. Ihara, "Some remarks on the number of rational points of algebraic curves over finite fields,"*J. Fac. Sci. Tokyo,* Vol. 28, pp.721-724, 1981.

[33] C. D. Jensen, "Fast decoding of codes from algebraic geometry," *IEEE Trans. Inform. Theory*, vol. 40, pp. 223-230, Jan 1994.

[34] J. Justesen, K. J. Larsen, A. Havemose, H. E. Jensen and T. Høholdt, "Construction and decoding of a class of algebraic geometric codes," *IEEE Trans. Inform. Theory*, vol. 35, pp. 811-821, July 1989.

[35] R. Kötter, "A fast parallel Berlekamp-Massey type algorithm for Hermitian codes,"*In Proc. Algebraic and Combinatorial Coding Theory, ACCT94, pp.125-128 (Novgorod, Russia, Sept. 1994).*

[36] R. Kötter, "A fast parallel implementation of a Berlekamp-Massey algorithm for algebraic-geometric codes,"*IEEE Trans. Inform. Theory, vol. 44, No. 4, julho 1998.*

[37] D. M. Mandelbaum, "A method for decoding of generalized Goppa codes," *IEEE Trans. Inform. Theory*, vol. 23, pp. 137-140, 1977.

[38] Rick Miranda, *Algebraic Curves and Riemann Surfaces*, American Mathematical Society, Vol. 5, 1997.

[39] Carlos J. Moreno, *Algebraic Curves over Finite Fields*, Cambridge Tracts in Mathematics, Vol. 97, USA, 1991.

[40] T. Muir (1904-1923), *The Theory of Determinants*, Vols. I-IV, Dover, New York.

[41] T. Muir e W. H. Metzler (1930), *A Treatise on the Theory of Determinants*, privately published, Albany, New York.

[42] Makoto Namba, *Geometry of Projective Algebraic Curves*, Monographs and textbooks in pure and applied mathematics, v. 88, New York, 1984.

[43] M. S. Narasimhan, R. R. Simha, Raghavan Narasimhan and C. S. Seshadri, *Riemann Surfaces*, School of Mathematics, Tata Institute of Fundamental Research, Bombay 5, India, 1963.

[44] Mª. Cruz Rodríguez Palánquez, *Aritmética de Curvas Cuasihermitícas*, Universidad Complutense de Madrid, julio 1996.

[45] W. W. Peterson and E. J. Weldon, Jr., *Error Correcting Codes*, 2nd. ed., MIT Press, Cambridge, Mass., 1972.

[46] S. C. Porter, *Decoding codes arising from Goppa's construction on algebraic curves*, Ph.D. dissertation, Yale Univ., New Haven, CT, Dec. 1988.

[47] Oliver Pretzel, *Codes and Algebraic Curves*, Oxford Lecture Series in Mathematics and its Applications, N°. 8, Oxford, 1998.

[48] S. Sakata, "Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array,"*J. Symb. Comput.*, Vol. 5, pp.321-337, 1988.

[49] S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen and T. Høholt, "Fast decoding of AG-codes up to the designed minimum distance,"*IEEE Trans. Inform. Theory*, vol. 41, pp. 1672-1677, Nov. 1992.

[50] J. P. Serre, "Sur le nombre de points rationnels d'une courbe alge'brique sur un cops fini,"*C.R.Sci. Paris* 296, Serie I , pp.397-402, 1993.

[51] J. P. Serre, *Rational points on curves over finite fields*, Notes of lectures at Harvard University 1985.

[52] I. R. Shafarevich, *Basic Algebraic Geometry*, Springer-Verlag, Berlin, 1977.

[53] N. A. Shekhunova, S. V. Bezzateev, and E. T. Mironchikov, "A subclass of binary Goppa codes", *Translated from Problemy Peredachi Informatsii*, vol. 25, No. 3, pp. 98-102, July-September, 1989.

[54] M. A. Shokrollahi and H. Wasserman, "List decoding of algebraic-geometric codes,"*IEEE Trans. Inform. Theory*, Vol. 45, pp.432-437, Mar. 1999.

[55] Aron Simis, *Introdução às funções algébricas e funções abelianas*, 10° Coloquio Brasileiro de Matemática, Poços de Caldas, 1975.

[56] A. N. Skorobogatov and S. G. Vlădut. "On the decoding of algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 36, 5, pp. 1051-1060, Sept. 1990.

[57] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.

[58] Serguei A. Stepanov, *Arithmetic of Algebraic Curves*, Monographs in Contemporary Mathematics, Consultants Bureau, New York, 1994.

[59] Henning Stichtenoth, *Algebraic Function Fields and Codes*, Universitext, Springer-Verlag, Berlin Heidelberg, New York, 1993.

[60] Y. Sugiyama, M. Kasahara, S. Hirawawa and T. Namekawa, "A method for solving key equation for decoding Goppa codes," *Information and Control*, Vol 27, pp. 87-99, (1975).

[61] M. A. Tsfasman and S. G. Vlădut, *Algebraic-Geometric Codes*, Mathematics and Its Applications. Kluwer Academic Publishers. Soviet Series. Vol. 58, 1991.

[62] M. A. Tsfasman, S. G. Vlădut and T. Zing, "Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound,"*Math. Nachr.*, Vol. 104, pp. 13-28, 1982.

[63] K. T. Tzeng and K. Zimmermann, "On extending Goppa codes to cyclic codes,"*IEEE Trans. Inform. Theory*, Vol. IT-21, No. 6, pp. 712-716, November, 1975.

[64] Kenji Ueno, *An Introduction to Algebraic Geometry*, Translations of Mathematical Monographs, Vol. 166, American Mathematical Society, 1997.

[65] J. H. van Lint and G. van der Geer, *Introduction to coding theory and algebraic geometry.* DMV Seminar, 12. Birkhãuser Verlag, Basel, 1988.

[66] J. M. Wozencraft, "List decoding,"*Quarterly Progress Report, Research Laboratory of Electronics*, MIT 48, pp.90-95, 1958.

[67] M. K. Yasuo Sugiyama, Shigeichi Hirasawa and Toshihiko Namekawa, "Further results on Goppa codes and their applications to constructing efficient binary codes,"*IEEE Trans. Inform. Theory*, Vol. IT-22, No. 5, pp. 518-526, September, 1976.

Índice Remissivo