Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Departamento de Engenharia Elétrica
Programa de Pós-Graduação em Engenharia Elétrica

Códigos de Hermite Generalizados: algoritmos de decodificação de lista e aplicações

Taciana Araújo de Souza

Campina Grande - PB, Brasil
Outubro - 2019

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Centro de Engenharia Elétrica e Informática
Programa de Pós-Graduação em Engenharia Elétrica

Códigos de Hermite Generalizados: algoritmos de decodificação de lista e aplicações

Taciana Araújo de Souza

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande como parte dos requisitos necessários para obtenção do grau de Doutor em Ciências, no domínio da Engenharia Elétrica.

Área de Concentração: Processamento da Informação.
Linha de Pesquisa: Eletrônica e Telecomunicações.

Prof. Francisco Marcos de Assis, DSc.
Prof. Leocarlos Bezerra da Silva Lima, DSc.
Orientadores

Campina Grande - PB
Outubro - 2019

S729c Souza, Taciana Araújo de.

Códigos de hermite generalizados: algoritmos de decodificação de lista e aplicações / Taciana Araújo de Souza. – Campina Grande, 2019.

88 f. : il. color.

Tese (Doutorado em Engenharia Elétrica e Informática) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática, 2019.

"Orientação: Prof. Dr. Francisco Marcos de Assis, Prof. Dr. Leocarlos Bezerra da Silva Lima".

Referências.

1. Códigos Algébrico-geométricos Multiponto. 2. Curva Hermitiana Generalizada. 3. Decodificação de Lista. 4. Salto em Frequência. 5. DCMA. 6. Redes de Rádio por Pacotes. I. Assis, Francisco Marcos de. II. Lima, Leocarlos Bezerra da Silva. III. Título.

CDU 519.725:621.3.049.77(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

"CÓDIGOS DE HERMITE GENERALIZADOS: ALGORITMOS DE DECODIFICAÇÃO DE LISTA E APLICAÇÕES"

TACIANA ARAÚJO DE SOUZA

TESE APROVADA EM 18/10/2019

FRANCISCO MARCOS DE ASSIS, Dr., UFCG
Orientador(a)

LEOCARLOS BEZERRA DA SILVA LIMA, D.Sc., UFCG
Orientador(a)

FERNANDO EDUARDO TORRES ORIHUELA, Dr., UNICAMP
Examinador(a)

RICARDO MENEZES CAMPELLO DE SOUSA, Ph.D., UFPE
Examinador(a)

WASHINGTON LUIZ ARAÚJO NEVES, Ph.D., UFCG
Examinador(a)

BRUNO BARBOSA ALBERT, D.Sc., UFCG
Examinador(a)

CAMPINA GRANDE - PB

Aos meus pais, Maria do Socorro e Gabriel.

Agradecimentos

Agradeço a Deus pela vida e aos meus pais, por todo o amor recebido, o que me permitiu acreditar ser capaz de chegar até aqui. Aos amigos do IQuanta, pela amizade e pelo conhecimento compartilhado durante os anos do doutorado. Em especial ao amigo Vinícius, por me incentivar e acompanhar desde o início, e à Milena, pela amizade sincera que me fez suportar a distância da família. Agradeço especialmente às amigas Suzete e Silvana, que foram minhas maiores referências durante a minha formação acadêmica e cuja amizade é um presente divino. Aos anjos-amigos Eva Campos, Baldoino Sonildo e Kíssia Carvalho, sem os quais não conseguiria seguir em frente no momento mais difícil. Ao Instituto Federal da Paraíba, instituição na qual cursei parte da minha formação acadêmica e onde trabalho atualmente. Em especial, agradeço ao reitor prof. Nicácio Lopes e à Lucrécia, diretora do Campus Cajazeiras, por todo o apoio que tornou viável a conclusão desta tese. Agradeço à toda minha família, que soube compreender minha ausência necessária em muitos momentos durante essa pesquisa. Aos meus queridos irmãos, em especial à Alessandra, por tudo o que partilhamos até aqui. Aos meus orientadores, Prof. Francisco Marcos de Assis e Prof. Leocarlos B. S. Lima, por aceitarem o desafio de me guiar nesta pesquisa e por todo o conhecimento compartilhado. Serei eternamente grata aos dois por tornarem possível realizar este sonho. Agradeço em especial aos membros da banca pelas valiosas contribuições. Agradeço ao CNPQ e ao IFPB pelo apoio financeiro e aos funcionários da Copele, em especial à Ângela e Pedro, pela seriedade e competência com que atuam no serviço público.

"O conhecimento serve para encantar as pessoas,
não para humilhá-las."
(Mário Sérgio Cortella)

Resumo

Códigos algébrico-geométricos (AG) são construídos a partir de divisores de uma curva algébrica, os quais podem ter suporte em um único ponto ou em vários pontos, neste caso, são chamados de multiponto. Os códigos AG de um ponto foram amplamente estudados, assim como diversos algoritmos de decodificação e aplicações. O problema da decodificação de lista foi investigado ao longo desta pesquisa para códigos AG multiponto, visto que tais algoritmos exibem melhor desempenho mesmo quando se deseja listas "com apenas uma palavra código", ou seja, em comparação com algoritmos de decodificação única, que são menos flexíveis. Nesse sentido, a principal contribuição desta tese consiste num algoritmo de decodificação de lista, que é baseado no algoritmo de decodificação única proposto por Drake [1] para códigos AG multiponto. Nesta pesquisa foram investigados códigos AG multipontos obtidos a partir de uma generalização da curva Hermitiana, que permite construir sequências de códigos com bons parâmetros. Tais códigos são comparados com os códigos de Hermite e códigos Reed-Solomon para aplicações em sistemas de comunicação que utilizam de salto em frequência para acesso múltiplo por divisão de código. Os códigos Hermitianos generalizados permitem atingir um número de usuários maior do que utilizando códigos Reed-Solomon ou códigos de Hermite sem aumentar o alfabeto (corpo finito). Além disso, são apresentados resultados comparativos entre esses códigos utilizando a probabilidade de erro de pacote para sistemas de transmissões de redes de rádio por pacote, considerando o canal AWGN e canais com interferência de banda parcial.

Palavras-Chave: Códigos algébrico-geométricos multiponto, curva Hermitiana generalizada, decodificação de lista, salto em frequência, CDMA, redes de rádio por pacotes.

Abstract

Algebraic-geometric (AG) codes are constructed from divisors of an algebraic curve, which can be supported in a single point or in several points, in this case, they are called multipoint. One-point AG codes have been extensively studied, as have various decoding algorithms and applications. The list decoding problem has been investigated this research for multipoint AG codes, as such algorithms present better performance even when desiring "single-word"lists, ie, compared to unique decoding algorithms, which are less flexible. In this sense, the main contribution of this thesis is a list decoding algorithm, which is based on the unique decoding algorithm proposed by Drake [1] for multipoint AG codes. In this research we investigated multipoint AG codes obtained from a generalization of the Hermitian curve, which allows the construction of code sequences with good parameters. Such codes are compared to Hermite codes and Reed-Solomon codes for communication system that use frequency hopping for code division multiple access. Generalized Hermitian codes allow to reach a larger number of users than using Reed-Solomon codes or Hermite codes without increasing the alphabet (finite body). In addition, comparative results are presented between these codes using packet error probability for packet radio network transmission systems, considering the AWGN channel and channels with partial band interference.

Key words: Algebraic-geometric multipoint codes, generalized Hermitian curve, list decoding, frequency-hopping, CDMA, packet radio network.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Símbolos

$\mathbb{F}$ – Corpo finito com q elementos
K – Corpo arbitrário
F – Fecho algébrico de $\mathbb{F}_q$
$\mathbb{A}^n$ – Espaço afim n-dimensional sobre K, cujos vetores são denotados por $(x_1, x_2, \cdots, x_n)$
$\mathbb{P}^n$ – Espaço projetivo n-dimensional sobre K, cujos vetores são denotados por $(x_0, x_1, x_2, \cdots, x_n)$
$\mathbb{P}^1$ – Linha projetiva
$\mathcal{X}$ – Curva projetiva suave absolutamente irredutível sobre $\mathbb{F}_q$
$\mathbb{F}_q(\mathcal{X})$ – Corpo de funções da curva $\mathcal{X}$
$\mathcal{C}$ – Código linear
$\mathcal{R}$ – Taxa de código
δ – Distância mínima relativa
g – Gênero da curva
N – Número de pontos da curva
n – Comprimento do código linear
d – Distância mínima do código
k – Dimensão do código
Q – Ponto no infinito
η – Taxa de colisões entre duas sequências de um código
U – Número de máximo de usuários em um sistema de comunicação
K –Número de pares fonte-usuários em um sistema de comunicação
U_{RS} – Número máximo de usuários em sistemas utilizando códigos RS
U_H – Número máximo de usuários em sistemas utilizando códigos de Hermite
U_{HG} – Número máximo de usuários em sistemas utilizando códigos Hermitianos generalizados
L_{RS} – Número de palavras-código RS num pacote
L_H – Número de palavras-código de Hermite num pacote
P_e – Probabilidade de erro

Lista de Siglas

RS – Reed-Solomon
AG – Algébrico-geométrico
FKS – F. K. Schmidt
FH – *Frequency-Hopping*
CDMA – *Code Division Multiple Access*
AWGN – *Additive white Gaussian noise*
BCH – Bose - Chaudhuri - Hocquenghem
BMS – Berlekamp-Massey-Sakata
FHSS – *Frequency-Hopping Spread Spectrum*
DSSS – *Direct Sequence Spread Spectrum*
HG – Curva Hermitiana generalizada

CAPÍTULO 1

Introdução

A comunicação digital envolve implicitamente a informação transmitida de um ponto a outro por uma sucessão de processos, tais como: a geração de um sinal de uma mensagem; a descrição desse sinal de mensagem por meio de símbolos elétricos, auditivos ou visuais; a codificação desses símbolos em uma forma apropriada à transmissão por um meio físico; a transmissão desses símbolos até o destino; a decodificação; reprodução dos símbolos originais e recriação do sinal de mensagem original, com uma degradação da qualidade [2].

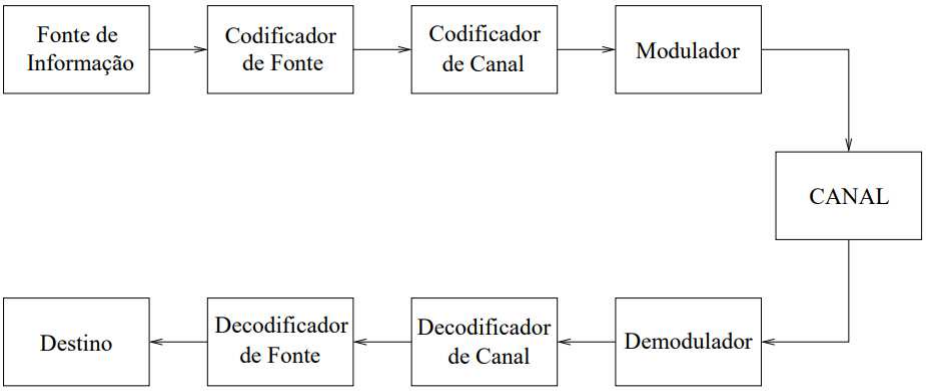

Figura 1.1 – Elementos de sistema de um comunicação digital

A Figura 1.1 ilustra um modelo de um sistema de comunicação digital. Os códigos corretores de erros são introduzidos pelo codificador de canal através da inserção de redundâncias controladas ao sinal com objetivo de diminuir a taxa de erro por bit e, assim, garantir a confiabilidade na transmissão e/ou armazenamento de informações [3]. Esses códigos podem ser classificados em códigos de bloco e códigos convolucionais. Essa classificação é baseada na presença ou não de memória nos codificadores, assim, os códigos de bloco são ditos sem memória e os códigos convolucionais são ditos com memória, pois um determinado bit codificado depende de um ou mais bits de informação anteriores combinados linearmente. Dentre os códigos de bloco, destacam-se os códigos lineares.

Seja $\mathbb{F}$ um corpo finito com q elementos. Um código de bloco de comprimento n é dito

código linear $\mathcal{C} \subset \mathbb{F}^n$, denotado por (n, k), quando $\mathcal{C}$ for subespaço de dimensão k de $\mathbb{F}^n$. A taxa de informação de um código de bloco, ou simplesmente, taxa do código, é dada por $\mathcal{R} = \frac{k}{n}$, em que k é o número de símbolos de informação na entrada do codificador e n o comprimento da palavra código. Este parâmetro é importante para análise do desempenho, pois a taxa do código determina o quanto de informação é possível transmitir por uso do canal. Em 1948, Shannon [4] mostrou que dado um canal ruidoso com capacidade C e informações transmitidas a uma taxa $\mathcal{R}$, se $\mathcal{R} < C$, então existe uma técnica de codificação que permite fazer com que a probabilidade de erro no receptor seja arbitrariamente pequena. Diante disso, uma questão relevante sobre códigos corretores de erros é qual é o maior comprimento que um código pode ter e sua relação com a capacidade de correção de erros. A resposta envolve um outro parâmetro chamado *distância mínima* d.

A distância de Hamming entre duas palavras de um código $\mathcal{C}$ corresponde ao número de coordenadas nas quais as palavras diferem entre si. Desse modo, a *distância mínima* d consiste na menor distância de Hamming entre duas palavras quaisquer do código. A capacidade de correção de erros de um código está relacionada ao número de palavras códigos de $\mathcal{C}$ e à distância mínima do código. Dado um código $\mathcal{C} \in \mathbb{F}^n$ ao aumentar a dimensão de $\mathcal{C}$ obtém-se um número maior de palavras código, contudo, isso naturalmente diminui a distância mínima do código, o que diminui a capacidade de correção de erros. Desse modo, códigos corretores de erros são ditos *bons códigos* quando tem o comprimento n tão grande quanto possível, mantendo finitas e não nulas a taxa de informação $\mathcal{R}$ e a distância mínima relativa $\delta = d/n$. Portanto, não comprometem a taxa de transmissão em detrimento da capacidade de correção de erros, ou vice versa, quando $n \to \infty$.

Considere $A_q(n, d)$ a cardinalidade de um código de bloco, com comprimento de bloco n e distância mínima d. A função taxa de informação assintótica, que relaciona a taxa de informação $\mathcal{R}$ e a distância mínima relativa δ de um código quando n tende para infinito, é definida por

$$\mathcal{R}(\delta) = \lim_{n\to\infty} \frac{\log_q A_q(n, \delta \cdot n)}{n}.$$

Teorema 1 *(Limite de Gilbert-Varshamov) [5] Considere* $0 \leq \delta \leq \frac{q-1}{q}$*, então*

$$\mathcal{R}(\delta) \geq 1 - H_q(\delta),$$

em que H_q *é a função entropia definida por*

$$H_q(x) = \begin{cases} 0, & x = 0 \\ x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x), & 0 < x < \frac{q-1}{q}. \end{cases}$$

Desse modo, se um código corretor de erros $\mathcal{C}$ excede de modo não trivial este limite, isto é, $R(\delta) > 0$ e $\delta > 0$, então o código é considerado um código assintoticamente bom. Nesse sentido, na década de 1970, o matemático russo V. D. Goppa propôs os primeiros códigos

algébrico-geométricos (AG), os quais excedem este limite [6].

Anteriormente, na década de 1960, foram propostos os códigos de Reed-Solomon (RS) [7], capazes de corrigir múltiplos erros e que apresentam diversas vantagens com relação a outros códigos e, por isso, vêm sendo utilizados em diversas aplicações práticas em sistemas de comunicações e armazenamento digital. Contudo, em um código RS o comprimento da palavra código n está limitado pela ordem de $\mathbb{F}$, isto é, utilizando-se um corpo finito com q elementos, o código RS não poderá ter o comprimento maior do que q [8]. Os códigos AG, por sua vez, podem ser construídos avaliando funções racionais sobre os pontos racionais de uma curva projetiva e o comprimento da palavra código depende do número de pontos racionais da curva, que pode ser bem maior do que a ordem do corpo finito sobre o qual está descrita a curva.

Como consequência imediata dos resultados da teoria da informação apresentados por Shannon [4], sabe-se que, quanto maior o comprimento, melhor será o desempenho do código e, portanto, os códigos AG são uma excelente alternativa aos códigos RS. Nesse sentido, tais códigos são objeto dessa pesquisa de doutorado, mais especificamente, códigos Hermitianos generalizados multipontos.

1.1 – Formulação do Problema

Um código AG pode ser construído com base em um divisor G com suporte em um único ponto racional, chamado código AG de um ponto, ou com base em um divisor G que tem suporte sobre m pontos racionais ($m \geq 2$). Os códigos AG de um ponto foram amplamente estudados, incluindo a determinação dos seus parâmetros, bem como o desenvolvimento de diversos algoritmos de decodificação, incluindo os algoritmos de decodificação de lista. Contudo, é possível obter códigos AG multiponto com parâmetros melhores do que os códigos AG de um ponto comparáveis na mesma curva [1, 9].

Em 2016, Hu e Zhao [9] apresentaram códigos AG multiponto a partir de uma generalização da curva Hermitiana introduzida por Bassa *et al.* [10], fornecendo uma fórmula pra encontrar a base do espaço Riemann-Roch de uma série de divisores e uma fórmula explícita para determinar os códigos duais. Esta curva tem um número de pontos racionais superior aos códigos de Hermite e aos códigos RS e, portanto, pode ser usada em aplicações que necessitam de códigos com o comprimento maior.

A utilização prática de qualquer tecnologia nova depende da sua viabilidade de implementação. Com relação aos códigos corretores de erros é fundamental que possam ser implementados algoritmos de decodificação eficientes, isto é, que sejam capazes de decodificar com probabilidade de erro pequena e baixa complexidade computacional.

O processo de decodificação consiste em determinar uma estimativa da palavra código, c, a partir da palavra recebida, v, corrigindo os possíveis erros introduzidos pelo canal. Uma das abordagens possíveis para a decodificação é a recuperação do erro procurando a palavra código que tem a maior probabilidade de ter sido transmitida. Esta tarefa é chamada de *decodificação*

de máxima verossimilhança e este problema equivale a encontrar a palavra código mais próxima de v com relação a uma medida de distância definida a priori. Portanto, geralmente, utiliza-se um decodificador de distância mínima. Neste decodificador, dada uma palavra recebida v, é selecionada uma única palavra código c que satisfaz $d(c, v) < \frac{d}{2}$ se tal palavra c existe e, caso contrário, uma falha é declarada [11]. Este processo caracteriza a chamada *decodificação única*, visto que obtém-se uma única palavra código na saída do decodificador.

A decodificação única impõe restrições ao decodificador para que seja considerada apenas a palavra mais próxima da palavra enviada. Contudo, na década de 1950, de modo independente, Elias [12] e Wozencraft [13] propuseram que ao invés de uma única palavra na saída do decodificador, poderia se obter uma lista de palavras código que estão dentro de uma certa distância de Hamming do vetor recebido. A decodificação da lista permite a recuperação de erros além do limite de $\frac{d}{2}$ e, portanto, permite uma correção de erros significativa mesmo na presença de uma grande quantidade de ruído.

Sudan [14] apresentou um algoritmo de decodificação de lista para códigos Reed-Solomon que foi generalizado por Shokrollahi e Wasserman [15] para códigos AG. Posteriormente, Guruswami [16] apresentou uma investigação detalhada da decodificação da lista e demonstrou seu potencial, viabilidade e importância como um conceito combinatório e algorítmico. Contudo, foram abordados apenas os códigos AG de um ponto.

Em 2009, Drake [1] propôs dois algoritmos de decodificação única pra códigos AG multiponto que utiliza em uma das etapas um algoritmo de decodiificação de lista, mas a saída do algoritmo é sempre uma única palavra código. Nesse sentido, uma das contribuições da tese consiste num algoritmo de decodificação de lista para códigos AG multiponto baseado neste algoritmo.

De modo geral, em ambos os algoritmos, dada uma palavra recebida v de um código AG multiponto, a decodificação é feita a partir da imersão desse código em um subcódigo de um código de um ponto. E, para fazer esta imersão, é necessário encontrar uma função que induz um isomorfismo entre códigos AG multipontos. Portanto, uma das contribuições da tese consiste em generalizar o método apresentado por Drake [17] para encontrar esta função para os códigos Hermitianos generalizados multiponto.

Outra contribuição desta tese é a análise da aplicação desses códigos em sistemas de comunicação que utilizam salto em frequência (*Frequency-Hopping*). Os códigos Reed-Solomon são comumente utilizados em sistemas de acesso múltiplo que utilizam salto em frequência para modulação por divisão de código, os sistemas FH-CDMA (*Frequency-Hopping Code Division Multiple Access*). Contudo, o número de usuários no sistema é limitado pelo tamanho do corpo finito sobre o qual o código é construído [18]. Os códigos de Hermite foram investigados anteriormente para aplicações que utilizam salto em frequência porque permitem aumentar o comprimento da palavra código sem aumentar o corpo finito [18, 19].

Nesse sentido, propomos a utilização da curva Hermitiana generalizada [10], que fornece códigos com comprimento maiores do que a curva de Hermite. Para a análise do desempenho

desta curva foi considerada a taxa de colisões entre as sequências de um código, que pode ser vista como a probabilidade de duas sequências terem o mesmo símbolo na mesma posição. Observa-se que esta taxa cresce lentamente com relação à curva Hermitiana generalizada, enquanto o número de usuários no sistema cresce de forma rápida. Portanto, a curva apresenta-se como uma boa alternativa para esta aplicação.

Além disso, observa-se que em redes de rádio por pacote utilizando salto em frequência o uso dos códigos de Hermite também melhora o desempenho do sistema, reduzindo a probabilidade de erro por pacote [19]. Portanto, investigamos o desempenho dos códigos Hermitianos generalizados multiponto nesta aplicação para canais AWGN e canais com interferencia de banda parcial.

1.2 – Contribuições da Tese

- Algoritmo de decodificação de lista baseado no algoritmo de decodificação única proposto por Drake [17];
- Generalização do método para encontrar a isometria entre códigos Hermitianos generalizados multiponto;
- Aplicação do algoritmo de interpolação proposto por Lee e O'Sullivan para a curva F. K. Schmidt (FKS);
- Análise do desempenho dos códigos Hermitianos generalizados multiponto para aplicações que utilizam salto em frequência, tais como: sistemas de comunicação de múltiplo acesso (FH-CDMA) e em redes de rádio por pacotes.

1.3 – Organização da Tese

Este documento está organizado em seis capítulos. No Capítulo 2 são apresentados os códigos Hermitianos generalizados multipontos propostos por Hu e Zhao [9]. No Capítulo 3 são apresentados algoritmos de decodificação de lista para códigos AG, além dos algoritmos de decodificação única baseado em listas propostos por Drake [1]. No Capítulo 4 são apresentados os resultados obtidos nesta pesquisa relacionados à decodificação de lista para códigos AG multiponto. No Capítulo 5 são apresentados os resultados da análise de desempenho dos códigos Hermitianos generalizados aplicados em sistemas de comunicação de acesso múltiplo e em redes de rádio por pacotes. No Capítulo 6 são apresentadas as considerações finais. Em seguida, constam as referências bibliográficas, e, por fim, os apêndices: o apêndice A, contendo a lista de publicações; o apêndice B, que apresenta uma breve descrição de conceitos matemáticos relevantes para esta pesquisa; o apêndice C, contendo uma breve introdução aos

códigos corretores de erros e, no apêndice D são apresentados os algoritmos em Macaulay2 e SageMath utilizados ao longo dessa pesquisa.

CAPÍTULO 2

Códigos Hermitianos Generalizados Multiponto

Na década de 1970, Goppa [20] apresentou uma nova forma de construir códigos lineares a partir de corpos de funções algébricas. Esta construção também pode ser feita em termos de curvas algébricas e a chave nas construções de Goppa reside no fato de que pode-se obter informação sobre os parâmetros do código em termos da informação do corpo de funções em que o mesmo foi construído (número de lugares, gênero). O método de Goppa é uma generalização dos códigos de Reed-Solomon, conforme será mostrado na seção 2.1.

Dentre os códigos AG destacam-se os códigos de Hermite, que foram amplamente estudados por serem considerados fáceis de descrever, codificar e decodificar [9]. Tais códigos são construídos sobre pontos racionais da curva de Hermite, a qual possui várias generalizações, dentre elas a curva de F. K. Schmidt [21] e a generalização introduzida por Bassa *et al.* [10]. Ambas foram investigadas ao longo dessa pesquisa e permitem construir códigos multipontos com parâmetros melhores do que códigos de um ponto comparável na mesma curva [22], os quais são descritos neste capítulo.

Os códigos AG podem ser construídos de duas formas distintas: construção por funções, em que o código é obtido avaliando funções racionais em um conjunto de pontos distintos de uma curva ou construção por diferenciais, em que o código consiste no resíduo de diferenciais em um conjunto de pontos distintos de uma curva [23]. Neste capítulo é apresentada a construção por funções dos códigos AG, para maiores detalhes consultar o Apêndice B ou [21, 23].

Inicialmente, vejamos a descrição geométrica dos códigos Reed-Solomon, que são um caso particular dos códigos AG, em que a curva é a linha projetiva $\mathbb{P}^1$.

2.1 – Códigos Reed-Solomon

Uma função racional em $\mathbb{P}^1$ é um quociente $\frac{a(x,y)}{b(x,y)}$, em que $a(x,y)$ e $b(x,y)$ são polinômios de mesmo grau. Um ponto em $\mathbb{P}^1$ é chamado um pólo de uma função racional $\frac{a(x,y)}{b(x,y)}$ se $b(x,y)$

é zero neste ponto (e $a(x, y)$ não é nulo).

Definição 1 *(Descrição Geométrica dos códigos Reed-Solomon) Seja o ponto $Q = (1, 0)$, definimos o espaço vetorial $\mathcal{L}$ de todas as funções racionais $\frac{a(x,y)}{b(x,y)}$, em que $a(x, y)$ e $b(x, y)$ tem coeficientes em $\mathbb{F}_q$, de modo que essas funções não têm pólos, exceto possivelmente em Q de ordem no máximo $k - 1$.*

Os pontos racionais em $\mathbb{P}^1$ são Q e os pontos $P_i = (\alpha_i, 1)$, em que $\alpha_i \in \mathbb{F}_q$. Sejam $P_1, P_2, \cdots, P_n$ pontos diferentes de Q. Então, o código Reed-Solomon pode ser definido por

$$\mathcal{C} := \{(f(P_1), f(P_2), \cdots, f(P_n)); f \in \mathcal{L}\}; \tag{2.1}$$

com $n \leq q$ e distância mínima $d = n - k + 1$.

Exemplo 1 *Considere a linha projetiva $\mathbb{P}^1$ sobre $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. Note que o ponto $Q = (x, y) = (1, 0)$ é o ponto no infinito sobre $\mathbb{P}^1$. Os pontos racionais em $\mathbb{P}^1$ são Q e $P_i = (\alpha_i, 1)$, com $\alpha_i \in \mathbb{F}_4$. Seja $Y = x/y$ uma função racional e considere o espaço vetorial $\mathcal{L} = \langle 1, Y, Y^2 \rangle$. Portanto, a matriz geradora do código é obtida avaliando as funções $f_1 = 1, f_2 = Y, f_3 = Y^2$ nos pontos P_i. A matriz geradora do código Reed-Solomon $\mathcal{C}(4, 3)$ sobre $\mathbb{F}_4$ é*

$$M = \begin{pmatrix} f_1(P_1) & f_1(P_2) & f_1(P_3) & f_1(P_4) \\ f_2(P_1) & f_2(P_2) & f_2(P_3) & f_2(P_4) \\ f_3(P_1) & f_3(P_2) & f_3(P_3) & f_3(P_4) \end{pmatrix}.$$

Avaliando as funções f_j nos pontos $P_1 = (0, 1), P_2 = (1, 1), P_3 = (\alpha, 1)$ e $P_4 = (\alpha^2, 1)$ temos

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

2.2 – Códigos Algébrico-Geométricos

A fim de compreender a construção dos códigos sobre curvas algébricas é necessário definir alguns conceitos da Geometria Algébrica, tais como divisores de uma curva e espaço de Riemann-Roch. Nesta seção introduzimos alguns desses conceitos importantes e para maiores detalhes consulte o Apêndice C ou [8, 21].

Uma forma elegante de manipular um conjunto de pontos de uma curva algébrica é dada pelo conceito de divisor de uma curva $\mathcal{X}$ [5].

Definição 2 *(Divisores) Seja $\mathcal{X}$ uma curva projetiva sobre $\mathbb{F}_q$.*

- *Um divisor D é uma soma formal (um conjunto de pontos dispostos em forma de uma soma ponderada) $D = \sum_{P \in \mathcal{X}} n_P P$, com $n_P \in \mathbb{Z}$ e $n_P = 0$, $\forall P \in \mathcal{X}$, exceto para um número finito de pontos P;*
- *Um divisor é chamado efetivo se todos os valores de n_P são não-negativos ($D \succ 0$);*
- *O grau do divisor D é $deg(D) = \sum n_P$.*

Definição 3 *Seja G um divisor em uma curva $\mathcal{X}$. O espaço de Riemann-Roch associado ao divisor G é definido por:*

$$\mathcal{L}(G) := \{f \in \mathbb{F}_q(\mathcal{X})^* : (f) + G \succ 0\} \cup \{0\}, \tag{2.2}$$

em que $G = \sum_i n_i P_i - \sum_j m_j Q_j$, com $n_i, m_j > 0$, então $\mathcal{L}(G)$ consiste da função nula e das funções no corpo de funções $\mathbb{F}_q(\mathcal{X})$ que têm zeros de multiplicidade pelo menos m_j em Q_j e não tem pólos exceto possivelmente nos pontos P_i, com ordem no máximo n_i em P_i. Denotamos $l(G)$ a dimensão de $\mathcal{L}(G)$.

Nesta pesquisa restringimos nosso estudo às curvas não-singulares e, neste caso, o gênero da curva pode ser definido pelo teorema a seguir.

Teorema 2 *Se $\mathcal{X} \in \mathbb{P}^n$ é uma curva plana projetiva não-singular de grau d, então o gênero da curva $\mathcal{X}$ é dado por*

$$g = \frac{1}{2}(d-1)(d-2) \tag{2.3}$$

Um resultado importante da geometria algébrica é o Teorema de Riemann-Roch, que permite calcular a dimensão de um espaço de Riemann-Roch $\mathcal{L}(G)$. No estudo dos códigos AG, consideraremos o caso do Corolário 1, quando $deg(G) > 2g - 2$ conforme veremos a seguir. Para maiores detalhes quanto ao Teorema de Riemann-Roch e à definição de divisor canônico consulte [21].

Teorema 3 *(Riemann-Roch) Seja G um divisor em uma curva plana projetiva não-singular de gênero g, então para algum divisor canônico W [21]*

$$l(G) - l(W - G) = deg(G) - g + 1. \tag{2.4}$$

Corolário 1 *Se $deg(G) > 2g - 2$, então*

$$l(G) = deg(G) - g + 1. \tag{2.5}$$

Seja $\mathcal{X}$ uma curva projetiva não-singular sobre $\mathbb{F}_q$ de gênero g, em que q é um número primo ou uma potência de um número primo. Sejam $P_1, P_2, \cdots, P_n$ pontos racionais e D o divisor $P_1 + P_2 + \cdots + P_n$. Além disso, G é algum divisor cujo suporte é disjunto de D e

$$2g - 2 < deg(G) < n. \tag{2.6}$$

Definição 4 *O código algébrico-geométrico $\mathcal{C}(D,G)$ de comprimento n sobre $\mathbb{F}_q$ é a imagem do mapeamento $ev : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n$ definido por:*

$$ev(f) := (f(P_1), f(P_2), \cdots, f(P_n)). \tag{2.7}$$

*Se o código $\mathcal{C}(D,G)$ é um código algébrico-geométrico tal que G é uma combinação linear de m pontos distintos, então chamamos $\mathcal{C}(D,G)$ de código m-ponto. Se $m > 1$, dizemos que o código $\mathcal{C}(D,G)$ é dito um código **multiponto**.*

O código $\mathcal{C}(D,G)$ tem parâmetros $[n,k,d]$, em que:

- *n é o comprimento da palavra código;*
- *$k = l(G)$ é a dimensão do código;*
- *$d \geq n - deg(G)$ é a distância mínima do código.*

A construção do código dual do código $\mathcal{C}(D,G)$, denotado por $\mathcal{C}^*(D,G)$ é feita por diferenciais e não será detalhada aqui, para maiores detalhes consultar [21, 23].

Exemplo 2 *Seja $\mathcal{X}$ a curva $x^3 + y^3 + z^3 = 0$ sobre $\mathbb{F}_4$. Seja $G = 2Q$ um divisor, em que $Q = (0,1,1)$, então $\mathcal{L}(G) = \mathcal{L}(2Q) = \{f \in \mathbb{F}_q(\mathcal{X})^* : (f) + 2Q \succ 0\} \cup \{0\}$.*

Logo, f tem pólos de ordem no máximo 2 em Q. Tome $n = 8$, então D é a soma dos pontos racionais restantes. Na Tabela 2.1 são apresentados os pontos racionais desta curva.

Tabela 2.1 – Pontos racionais da curva $\mathcal{X}$ no espaço projetivo $\mathbb{P}^2$ sobre $\mathbb{F}_4$, com $\alpha^2 = \alpha + 1$.

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	Q
x	1	1	1	1	1	1	0	0	0
y	0	0	0	α^2	α	1	α^2	α	1
z	α^2	α	1	0	0	0	1	1	1

A matriz geradora de um código AG é construída de modo que cada linha i corresponde ao valor de uma função da base ϕ_i calculada em todos os pontos racionais, em que o valor desta função em cada ponto P_j constitui o valor na coluna j.

Exemplo 3 *(Matriz geradora do código) Considerando o Exemplo 2 a dimensão de $\mathcal{L}(2Q)$ é igual a 2 e, a função constante $\phi_1 = 1$ e a função $\phi_2 = \frac{x}{y+z}$ formam uma base de $\mathcal{L}(2Q)$ sobre $\mathbb{F}$, portanto, a matriz geradora do código será:*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha & \alpha^2 & 1 & \alpha & \alpha^2 & 1 & 0 & 0 \end{pmatrix}. \tag{2.8}$$

A construção de códigos AG está intimamente ligada ao conceito de lacunas e anti-lacunas de Weierstrass. Dado um ponto racional P de uma curva algébrica $\mathcal{X}$ de gênero g. Seja u um inteiro não negativo e considere divisores de um ponto, isto é, $G = uP$.

Definição 5 *(Lacunas) Um inteiro não negativo u é dito uma lacuna ("gap") de um ponto P de uma curva $\mathcal{X}$, se $l(uP) = l((u-1)P)$.*

Definição 6 *(Anti-lacuna) Um inteiro positivo u é dito ser uma anti-lacuna ("nongap") de um ponto P de uma curva $\mathcal{X}$, se $l(uP) \neq l((u-1)P)$, ou seja, se, e somente se, existe uma função racional $f \in \mathcal{L}(uP)$, tal que $v_Q(f) = -u$ (possui pólos em P).*

O teorema a seguir mostra que o número de lacunas de um ponto racional P de uma curva $\mathcal{X}$ é igual ao gênero da curva. Além disso, as anti-lacunas de um ponto P formam um semigrupo numérico com a operação de adição, chamado semigrupo de Weierstrass, definido a seguir.

Teorema 4 *(Teorema das lacunas de Weierstrass) Sejam $\mathcal{X}$ uma curva de gênero g e P um ponto racional. Então existem exatamente g lacunas $i_1 < \cdots < i_g$ de P. Além disso, $i_1 = 1$ e $i_g \leq 2g - 1$.*

Definição 7 *(Semigrupo de Weierstrass) Seja $\mathcal{X}$ uma curva projetiva suave de gênero $g \geq 1$ sobre o corpo $\mathbb{F}_q$ e $\mathbb{F}_q(\mathcal{X})$ o corpo das funções racionais de $\mathcal{X}$. Seja P um ponto racional da curva e $\mathbb{N}_0$ o conjunto dos número inteiros não negativos. O conjunto*

$$H(P) := \{u \in \mathbb{N}_0; \exists\ f \in\ \mathbb{F}_q(\mathcal{X}) \text{ com } (f)_\infty = uP\}. \tag{2.9}$$

em que $(f)_\infty$ denota o divisor de pólos de f, é um semigrupo numérico, chamado semigrupo de Weierstrass de $\mathcal{X}$ em P. O conjunto $\mathbb{N}_0 \backslash H(P)$ é chamado de lacunas de Weierstrass de P e sua cardinalidade é g.

Dada uma curva algébrica $\mathcal{X}$ e um ponto racional P da curva, os códigos AG de um ponto podem ser construídos a partir do conhecimento do semigrupo de Weierstrass associado ao ponto P, o qual contém todos os valores u para os quais podemos definir um divisor do tipo $G = uP$, que definem códigos de um ponto. Além disso, é possível determinar o semigrupo de Weierstrass para mais de um ponto, os quais serão abordados nesta pesquisa apenas para a construção de códigos Hermitianos generalizados multiponto conforme apresentado por Hu e Zhao [9]. Na seção seguinte, antes de introduzir tais códigos, são apresentados os códigos de Hermite e FKS de um ponto.

2.2.1 – Curva de Hermite

A classe de curvas algébricas de Hermite são amplamente utilizadas na construção de códigos corretores de erros devido aos bons parâmetros de comprimento e distância mínima

relativa, como também à simplicidade da estrutura do espaço de funções definido por esta classe de curvas [5].

Seja $\mathbb{F}_q = \mathbb{F}_{r^2}$, em que r é uma potência de primo. $\mathbb{F}_q(\mathcal{X})$ é o corpo de funções de Hermite, em que a curva de Hermite no espaço projetivo $\mathbb{P}^2$ sobre $\mathbb{F}_q$ é dada por

$$\mathcal{X} : x^{r+1} + y^{r+1} + z^{r+1} = 0. \tag{2.10}$$

A versão da curva de Hermite no espaço afim $\mathbb{A}^2$ sobre $\mathbb{F}_q$ é dada pela equação

$$\mathcal{X} : x^{r+1} + y^{r+1} + 1 = 0. \tag{2.11}$$

A curva de Hermite pode ser reescrita de uma forma mais conveniente como [21]:

$$\mathcal{X} : y^r + y = x^{r+1}. \tag{2.12}$$

A curva de Hermite é não-singular(suave) irredutível, e possui as seguintes propriedades:

- $N = r^3 + 1$ é o número de pontos racionais, sendo um deles o ponto no infinito Q.
- $g = \frac{q-r}{2}$ é o gênero da curva.
- $v_Q(x) = -r$ e $v_Q(y) = -(r+1)$ correspondem a valorização discreta de x e y, respectivamente, no ponto Q.
- Para um divisor de um ponto $G = uQ$ a base do espaço de Riemann-Roch associado a G é $\mathcal{L}(G) = \{x^i y^j | 0 \leq i, 0 \leq j \leq r-1, 0 \leq ir + j(r+1) \leq u\}$.
- $H(Q) = \langle r, r+1 \rangle$ é o semigrupo de Weierstrass para o ponto no infinito Q.

O código de Hermite pode ser definido por $\mathcal{C}_H := \mathcal{C}(D, G)$ sobre a curva $\mathcal{X}$ com gênero g sobre $\mathbb{F}_{r^2}$, dada por 2.12 tal que $2g - 2 < deg(G) < n$ tem os seguintes parâmetros:

- $n = r^3 = q\sqrt{q}$,
- $k = deg(G) - g + 1$,
- $d = r^3 - deg(G)$.

Os códigos de Hermite de um ponto $\mathcal{C}(D, uQ)$, para algum $u \in H(Q)$ tal que $2g-2 < u < n$, têm o código dual $\mathcal{C}^*(D, uQ) = \mathcal{C}(D, (r^3 + r^2 - r - 2 - u)Q)$ [5].

Exemplo 4 *Seja $r = 2$ e $q = r^2 = 4$. Considere a curva de Hermite definida por $x^3 = y^2 + y$ sobre $\mathbb{F}_4 = \{0, \alpha, \alpha^2, \alpha^3\}$ e $n = r^3 = 8$. Escolhendo $u = 4$, o espaço linear $L(4Q) = \langle 1, x, y, x^2 \rangle$. O código de Hermite é um código $[8, 4, 4]$ sobre $\mathbb{F}_4$. Os pontos racionais da curva $\mathcal{X}$ são mostrados na Tabela 2.2.*

Tabela 2.2 – Pontos racionais da curva $\mathcal{X}$ no espaço afim $\mathbb{A}^2$ sobre $\mathbb{F}_4$, com $\alpha^2 = \alpha + 1$.

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	Q
x	0	1	1	α	α	α^2	α^2	α	0
y	0	α	α^2	α	α^2	1	α^2	α^2	1

A matriz geradora do código é:

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & 1 & \alpha^2 & \alpha^2 \\ 0 & 1 & 1 & \alpha^2 & \alpha^2 & \alpha & \alpha & \alpha^2 \end{pmatrix}. \tag{2.13}$$

Nas próximas seções são apresentadas duas curvas que são consideradas generalizações da curva de Hermite e foram utilizadas ao longo dessa pesquisa. Veremos que a curva de Hermite pode ser vista como um caso particular dessas curvas.

2.2.2 – Curva F. K. Schmidt

Seja $\mathbb{F}_q$ um corpo finito com $q = r^2$ elementos, em que r é uma potência de um inteiro primo. Seja $\mathcal{X}$ sobre a curva FKS definida pela equação [21]

$$\mathcal{X} : y^r + y = x^p, \tag{2.14}$$

em que $p|(r+1)$, ou seja, p é um divisor de $r+1$. Note que se $p = r+1$, então $\mathcal{X}$ é uma curva de Hermite.

A curva de FKS possui as seguintes propriedades [21]:

- $N = r(1 + (r-1)p) + 1$ é o número de pontos racionais, sendo um deles o ponto no infinito Q.
- $g = \frac{1}{2}(r-1)(p-1)$ é o gênero da curva.
- $v_Q(x) = -r$ e $v_Q(y) = -p$.
- Para um divisor de um ponto $G = uQ$ a base do espaço de Riemann-Roch associado a G é $\mathcal{L}(G) = \{x^i y^j | 0 \leq j \leq r-1, 0 \leq i, ir + jp \leq u\}$.
- $H(Q) = \langle r, p \rangle$ é o semigrupo de Weierstrass para o ponto no infinito Q.

O código FKS de um ponto definido por $\mathcal{C}_{FKS} := \mathcal{C}(D, G)$ sobre a curva FKS tal que $p|(r+1)$ sobre $\mathbb{F}_{r^2}$. Sejam $D = P_1 + \cdots + P_n$ e $G = uQ$, com P_i um ponto racional e $n = N - 1$. Considerando $2g - 2 < deg(G) < n$, o código FKS tem os seguintes parâmetros:

- $n = r(1 + (r-1)p)$,

- $k = deg(G) - g + 1$,
- $d = r(1 + (r - 1)p) - deg(G)$.

Exemplo 5 *Seja $\mathbb{F}_q$ um corpo finito com $q = r^2 = 9$ elementos em que $r = 3$ e $p = 2$. A curva FKS sobre $\mathbb{F}_9$ é dada por*

$$x^2 - y^3 - y = 0.$$

O código $\mathcal{C}_{FKS}(D, G)$ sobre $\mathbb{F}_9$, com $G = uQ$ e D um divisor contendo os demais pontos racionais da curva, tem parâmetros $[15, 7, 8]$. Seja $u = 7$, então a base do espaço linear $\mathcal{L}(G)$ é dada por $\mathcal{L}(7Q) = \langle 1, x, y, x^2, xy, y^2, xy^2 \rangle$.

Exemplo 6 *Considere a curva FKS sobre $\mathbb{F}_9$ como no exemplo anterior, com $r = 3$ e $p = r + 1 = 4$, isto é, a curva de Hermite sobre $\mathbb{F}_9$ dada por*

$$x^4 - y^3 - y = 0.$$

Observe que se $u = 16$, teremos um código $\mathcal{C}_{FKS}(D, 16Q)$ com os parâmetros $[27, 14, 11]$.

2.2.3 – Curvas Hermitianas Generalizadas

Na década de 80, Tsfasman *et al.* [6] apresentaram uma sequência de códigos de Goppa construída a partir de uma sequência de corpos de funções definidos sobre um corpo finito, chamada torre de corpos de funções. Observe que é possível determinar se uma torre de corpos fornece uma boa sequência de códigos corretores de erros utilizando um parâmetro assintótico, chamado de limite da torre, definido a partir do gênero e do número de lugares racionais de cada corpo de funções que forma a torre. Torres com limite positivo, conhecidas como torres assintoticamente boas, podem medir a precisão dos parâmetros relativos de códigos lineares, na medida em que melhoram a cota de Gilbert-Varshamov [24].

Nesse sentido, Bassa *et al.* [25] mostraram como obter torres de corpos de funções sobre corpos finitos não-primos, construindo algumas torres recursivas com muitos pontos racionais. A partir dessa construção, Hu e Zhao [9] obtiveram códigos AG multiponto que atingem novos parâmetros, em que a curva utilizada é considerada uma generalização da curva Hermitiana. É importante observar que esta curva é apenas uma das várias generalizações da curva Hermitiana [10, 21, 26].

Nesta seção é apresentada a curva Hermitiana generalizada utilizada nesta pesquisa, para qual é possível construir códigos com o comprimento maior do que os códigos FKS (ou Hermite), o que as torna interessantes em diversas aplicações, por exemplo, onde é desejável aumentar o comprimento do código sem aumentar a ordem do corpo finito utilizado.

Antes de introduzir os códigos Hermitianos generalizados, vejamos algumas definições e limites que permitem analisar o comportamento assintótico do número de pontos racionais em

curvas algébricas com relação ao gênero. A análise desses limites permite identificar torres de corpos de funções capazes de produzir uma boa sequência de códigos corretores de erros.

Seja $\mathbb{F}_q$ um corpo finito, então o corpo de funções $F/\mathbb{F}_q$ (ou equivalentemente, uma curva algébrica), com $\mathbb{F}_q$ algebricamente fechado em F, tem um número finito de lugares (pontos) racionais, que será denotado aqui por $N(F)$ e o gênero denotado por $g(F)$ [21].

O limite superior Hasse-Weil afirma que

$$N(F) \leq 1 + q + 2g(F)\sqrt{q}.$$

Este limite foi melhorado por Serre [27] substituindo $2\sqrt{q}$ por $\lfloor 2\sqrt{q} \rfloor$.

Ihara [28] foi o primeiro a perceber que o limite superior de Hasse-Weil se torna fraco quando o gênero $g(F)$ é grande em relação à q, isto é, que este limite só pode ser atingido se $g(F) \leq \frac{q-\sqrt{q}}{2}$. Nesse sentido, Ihara [28] introduziu um limite para analisar o comportamento assintótico das torres de funções, o qual é definido a seguir.

Definição 8 *Para um inteiro $g(F) \geq 0$, seja o número real*

$$N_q(g) := max\{N(F)|F \textit{ é um corpo de funções sobre } \mathbb{F}_q \textit{ de gênero } g(F)\},$$

então

$$A(q) := \lim_{g(F)\to\infty} sup \frac{N_q(g)}{g(F)} \tag{2.15}$$

é chamado de constante de Ihara.

O limite de Hasse-Weil afirma que $A(q) \leq 2\sqrt{q}$ e Ihara mostrou que $A(q) < \sqrt{2q}$. Além disso, o limite de Drinfeld-Vlădut afirma que $A(q) \leq \sqrt{q} - 1$, para qualquer potência de primo q.

Se q é um quadrado, $q = l^2$ para algum l, usando a teoria das curvas modulares, Ihara mostrou que $A(q) = \sqrt{q} - 1$. Além disso, Tsfasman-Vladut-Zink usaram este fato para provar a existência de códigos lineares longos com parâmetros relativos acima do limite de Gilbert-Varshamov para $l \geq 7$.

Definição 9 *(Torres de corpos de funções) Seja K um corpo arbitrário. Uma sequência $(F^{(1)}/K, F^{(2)}/K, \cdots)$ de corpos de funções é chamada uma torre se $F^{(i)} \subset F^{(i+1)}$ para todo $i \in \mathbb{Z}_+^*$ [21].*

Definição 10 *Dada uma torre $\mathcal{F} = (F^{(1)}/\mathbb{F}_q, F^{(2)}/\mathbb{F}_q, \cdots)$, $N^{(i)} = N(F^{(i)})$ e $g^{(i)} = g(F^{(i)})$ (gênero de $F^{(i)}/\mathbb{F}_q$). O limite da torre $\lambda(\mathcal{F})$ é definido como*

$$\lambda(\mathcal{F}) = \lim_{i\to\infty} \frac{N^{(i)}}{g^{(i)}}.$$

Pela definição 8 temos que $0 \leq \lambda(\mathcal{F}) \leq A(q)$.

Definição 11 *Uma torre de corpos de funções* $\mathcal{F} = (F^{(1)}/\mathbb{F}_q, F^{(2)}/\mathbb{F}_q, \cdots)$ *é dita assintoticamente boa se;*

- $\lim_{i\to\infty} g^{(i)} = \infty$,
- $\lim_{i\to\infty} inf\left(\frac{N^{(i)}}{g^{(i)}}\right) = k > 0$,

isto é, o número de pontos racionais cresce de uma forma mais rápida que o gênero da curva, com uma razão k.

Logo, pode-se observar que em torres assintoticamente boas o número de pontos racionais cresce de forma rápida em relação ao gênero, o qual explode para o infinito à medida que se aumenta o nível da torre. Portanto, tais torres são capazes de produzir sequências de bons códigos, tais como os códigos Hermitianos generalizados apresentados na seção seguinte.

2.3 – Códigos Hermitianos Generalizados Multiponto

Ao longo desta pesquisa foram investigadas duas generalizações da curva de Hermite, as curvas FKS [21] e a curva Hermitiana generalizada introduzida por Bassa *et al.* [10]. Mais especificamente, neste último caso, foram considerados os códigos multiponto apresentados por Hu e Zhao [9]. Tais curvas são definidas a seguir.

Nesta seção, considere r um número primo ou uma potência de um número primo e F_{r^c} o corpo finito de ordem r^c e a, b primos relativos tais que $a+b = c$. Seja $\mathcal{X}$ uma curva Hermitiana generalizada [9, 10] dada por

$$\mathcal{X} : \frac{y^{r^a}}{x} + \frac{y^{r^{a+1}}}{x^r} + \cdots + \frac{y^{r^{c-1}}}{x^{r^{b-1}}} + \frac{y}{x^{r^b}} + \cdots + \frac{y^{r^{a-1}}}{x^{r^{c-1}}} = 1 \tag{2.16}$$

Observe que substituindo xy por z para $c = 2$ e $a = b = 1$ na curva 2.16 temos exatamente a curva de Hermite sobre $\mathbb{F}_{r^2}$.

$$\frac{y^r}{x} + \frac{y^{r^0}}{x^r} = 1 \Rightarrow x^{r-1}y^r + y = x^r \Rightarrow x^r y^r + xy = x^{r+1} \Rightarrow z^r + z = x^{r+1}. \tag{2.17}$$

As torres de curvas construídas a partir da Equação 2.16 são ótimas no sentido de que elas alcançam assintoticamente o limite de Drinfeld-Vlãdut. Portanto, nesta tese, consideramos os códigos multiponto apresentados por Hu e Zhao [9] para a Equação 2.16 com parâmetros $c = 3$, $a = 1$ e $b = 2$. Com esses parâmetros a curva Hermitiana generalizada $\mathcal{X}$ sobre $\mathbb{F}_{r^3}$ é definida por

$$\mathcal{X} : \frac{y^{r^2}}{x^r} + \frac{y}{x^{r^2}} + \frac{y^r}{x} = 1, \tag{2.18}$$

em que $g = \frac{r^4-3r^2+2}{2}$ é o gênero da curva $\mathcal{X}$.

Considere os divisores D, V, Q e P, definidos a seguir.

- $D := \sum_{\alpha,\beta} D_{\alpha,\beta}$, em que $D_{\alpha,\beta} := (x = \alpha, y = \beta)$ com $\alpha, \beta \in \mathbb{F}_{r^3}^*$ satisfazendo a Equação 2.18;
- $V := (x = 0, y = \infty)$, o divisor consistindo de todos os pontos no infinito no eixo y, que podem ser escritos como $V = \sum_{\mu} V_{\mu}$, em que $V_{\mu} := (x = 0, y = \infty, x^r y^{r+1} = \mu)$ representa um ponto racional em V e $\mu^{r-1} = -1$ quando r é par;
- $Q := (x = \infty, y = \infty)$, que contém um único lugar racional apenas no caso em que r é ímpar;
- $P := (x = 0, y = 0)$, é a origem.

Os divisores D, V, Q e P contém todos os pontos racionais da curva 2.18, em que

- $div(x) = P + (r+1)V - rQ$ e $div(y) = r^2P - rV - Q$;
- $deg(P) = 1$, $deg(Q) = r$, e $deg(V) = r - 1$.

Hu e Zhao [9] apresentaram como um dos principais resultados uma base do espaço de Riemann-Roch para códigos Hermitianos generalizados utilizando o teorema de Pick, dada pela seguinte proposição.

Proposição 1 *(Proposição 3 [9]) Seja $G = uQ+sP+tV$, os elementos $x^i y^j$ com $(i,j) \in \Omega_{u,s,t}$ formam uma base de $\mathcal{L}(G)$, em que*

$$\Omega_{u,s,t} := \{(i,j) | -t \leq (r+1)i - rj < r^3 + r^2 + r - t, -i - r^2 j \leq s, ri + j \leq u\}. \quad (2.19)$$

Seja $\mathcal{C}_{u,s} := \mathcal{C}_{u,s,0}$ o código $\mathcal{C}_{u,s,t}$ com $t = 0$. Hu e Zhao [9] mostraram que $\mathcal{C}_{u,s,t}$ é equivalente a um código $\mathcal{C}_{u',s'}$, para $u', s' \in \mathbb{Z}$. Portanto, nesta tese restringimos o estudo dos códigos AG multiponto $\mathcal{C}_{u,s,t}$ para os códigos $\mathcal{C}_{HG} := \mathcal{C}(D, uQ + sP)$. Além disso, consideramos os códigos $\mathcal{C}_{HG}$ tais que $2g - 2 < deg(uQ + sP) < n$ com parâmetros:

- $n = r^5 - r^2$;
- $k = ur + s - \frac{r^4 - 3r^2}{2}$;
- $d = r^5 - r^2 - ur - s$.

Semigrupo de Weierstrass

Os códigos $\mathcal{C}_{u,s}$, com $u, s \in \mathbb{Z}$ não são necessariamente distintos para diferentes índices u e s. Por conveniência, Hu e Zhao [9] restringiram os índices para um conjunto específico, cujos códigos produzidos serão diferentes. Para um u fixado, o semigrupo de Weiertrass associado a u é definido por

$$H_u = \{s \in \mathbb{Z} | \mathcal{L}(uQ + sP) \neq \mathcal{L}(uQ + (s-1)P)\}. \tag{2.20}$$

Considere o subconjunto H_u^* do semigrupo de Weiertrass H_u para o qual existe um código $\mathcal{C}_{u,s}$ de comprimento n, definido por

$$H_u^* = \{s \in \mathbb{Z} | \mathcal{C}_{u,s} \neq \mathcal{C}_{u,(s-1)}\}. \tag{2.21}$$

Seja $H_u^* = \{s_1^* < s_2^* < \cdots < s_n^*\}$. Então, $dim(\mathcal{C}_{u,s_i^*}) = i$. Note que $H_u^* \subseteq H_u$ e

$$H_u^* \cap \{s | ur + s < n\} = H_u \cap \{s | ur + s < n\}. \tag{2.22}$$

Além disso, seja $s \in \mathbb{Z}$ tal que $ur + s \geq n$, $s \in H_u^* \Leftrightarrow s \in H_u^{\perp}$. Portanto, a parte restante de H_u^* pode ser calculada a partir de $H_u^{\perp}$, que é definido por

$$H_u^{\perp} := \begin{cases} r^5 + r^4 - r^3 - r^2 - 2r + 1 - H_{r^2-1-u}, \text{ para } 0 \leq u \leq r^2 - 1, \\ r^5 + r^4 - 2r^3 - 2r^2 - 3r + 1 - H_{2r^2+r-u}, \text{ para } r^2 \leq u \leq r^2 + r. \end{cases} \tag{2.23}$$

Exemplo 7 *Seja $\mathcal{C}_{u,s}$ sobre $\mathbb{F}_8$. Desse modo, $r = 2$ e $c = 3$. A curva Hermitiana generalizada sobre $\mathbb{F}_8$ é dada por*

$$\mathcal{X} := \frac{y^2}{x} + \frac{y^4}{x^2} + \frac{y}{x^4} = 1.$$

Fixando $u = 4$ e $s = 8$, então $G = 4Q + 8P$ e a base do espaço de Riemann-Roch é dada por

$$\mathcal{L}(G) = \langle xy, x^2, x, 1, x^2y^{-1}, xy^{-1}, y^{-1}, x^3y^{-2}, x^2y^{-2}, xy^{-2}, y^{-2} \rangle.$$

O gênero da curva $\mathcal{X}$ é $g = 3$ e os parâmetros do código são $[28, 8, 14]$.

No capítulo 5 são apresentados resultados comparativos entre os códigos Reed-Solomon, os códigos de Hermite e Hermite generalizado, apresentados neste capítulo, para aplicações em sistemas de comunicações. Além disso, considerando o problema da decodificação de canal para códigos AG multiponto, restringimos nosso estudo à decodificação de lista, que será detalhada no próximo capítulo.

CAPÍTULO 3

Decodificação de lista para códigos AG

O problema da decodificação para um código corretor de erro consiste em determinar a palavra-código correta que foi enviada pelo canal de comunicação. Dada uma palavra recebida, quando o algoritmo de decodificação restringe a busca pela palavra à uma distância de Hamming da palavra recebida menor que a metade da distância mínima do código, isso garante que a decodificação será única. Contudo, é possível resolver o problema da decodificação considerando uma vizinhança maior da palavra recebida, ampliando essa busca para uma lista de palavras-código ao invés de uma única palavra. Elias [12] e Wozencraft [13] mostraram que a decodificação de lista torna possível uma correção de erros significativa mesmo na presença de uma grande quantidade de ruído. Neste capítulo são detalhados alguns algoritmos de decodificação de lista para códigos AG, incluindo um algoritmo de fatoração utilizado a fim de determinar a lista de palavras-código numa vizinhança da palavra recebida.

3.1 – Revisão bibliográfica

Em 1989, Justesen *et al.* [29] apresentaram a construção de uma classe de códigos derivados de curvas algébricas planas e um algoritmo de decodificação que consiste em uma generalização do algoritmo de Peterson [3] para decodificação de códigos BCH [30, 31].

O primeiro algoritmo que representou um avanço importante para a utilização dos códigos AG foi proposto por Justesen *et al.* [29]. Além deste, diversos algoritmos eficientes já foram implementados tais como os apresentados em [32–40].

Em 1990, Skorobogatov e Vlãdut [41] apresentaram uma generalização do algoritmo de Justesen *et al.* [29] para curvas arbitrárias. O algoritmo proposto ficou conhecido como *algoritmo básico* e é capaz de corrigir até $\lfloor \frac{d-g-1}{2} \rfloor$ erros ocorridos na palavra recebida, em que g é o gênero da curva usada na geração do código e d a distância mínima do código. No mesmo ano, Sakata [42] apresentou uma generalizaçãoo código em várias variáveis do clássico algoritmo de Berlekamp-Massey [3], que passou a ser conhecida como algoritmo BMS.

Em 1992, Porter *et al.* [38] apresentaram um algoritmo baseado na solução da equação

chave. Em 1993, Feng e Rao [37] apresentaram um algoritmo que utiliza um esquema de decisão por maioria para determinar as síndromes desconhecidas da palavra recebida.

Os decodificadores citados anteriormente são chamados algoritmos de decodificação única, ou seja, a saída do decodificador fornece uma única palavra-código. Contudo, na década de 1950, de modo independente, Elias [12] e Wozencraft [13] propuseram que ao invés de uma única palavra na saída do decodificador, podemos obter uma lista de palavras-código que estão dentro de uma certa distância de Hamming do vetor recebido. E, mesmo quando o decodificador é limitado a produzir um número relativamente pequeno de respostas, a decodificação da lista permite a recuperação de erros além do limite de $\lfloor \frac{d-1}{2} \rfloor$.

O objetivo original de Elias [12] na formulação da decodificação de lista consistia em provar os limites superior e inferior para a probabilidade de erro de decodificação sob máxima verossimilhança para um decodificar no canal binário simétrico. Em particular, Elias [12] mostrou que, quando é permitido que a saída do decodificador seja uma pequena lista de palavras de código candidatos e um erro de decodificação é declarado apenas quando a palavra de código original não está na lista de saída, a probabilidade de erro de média de todos os códigos é quase tão boa quanto a do melhor código, e, de fato, quase todos os códigos são quase tão bons como o melhor código.

Em 1997, Sudan [14] apresentou um algoritmo de decodificação de lista para códigos Reed-Solomon. Em 1999, Shokrollahi e Wasserman [15] apresentaram uma generalização do algoritmo de Sudan [14] para códigos AG. Este algoritmo é baseado em um esquema contendo dois passos fundamentais: a interpolação e a fatoração de polinômios sobre corpos finitos. Em seguida, utilizando uma abordagem similar, Guruswami e Sudan [43] melhoraram o algoritmo proposto por Sudan [14] para resolver o problema de decodificação da lista para outros códigos algébricos, incluindo códigos alternantes e códigos AG. No caso de códigos AG (n, k, d) sobre $\mathbb{F}_q$, o algoritmo proposto é capaz de corrigir até $e < n - \sqrt{n(n-d)}$ erros, melhorando o limite anteriormente conhecido de $n - \sqrt{2n(n-d)} - g + 1$ erros (g é o gênero da curva).

O passo de interpolação foi melhorado por Høholdt e Nielsen [44]. Sakata [45] também forneceu uma melhoria de interpolação usando uma abordagem de base de Gröbner e algoritmo Berlekamp-Massey-Sakata. Kötter e Vardy [46] utilizaram uma abordagem semelhante a Guruswami e Sudan [43] para a decodificação por decisão suave de códigos Reed-Solomon e códigos AG.

Em 2001, em sua tese, Guruswami [16] apresentou uma investigação detalhada da decodificação da lista e demonstrou seu potencial, viabilidade e importância como um conceito combinatório e algorítmico. Nessa tese foram demonstrados vários resultados combinatórios que contribuem para a compreensão do potencial e dos limites da decodificação da lista, e sua relação com parâmetros mais clássicos, como a taxa e a distância mínima. Em 2006, Guruswami [47] apresentou alguns resultados algorítmicos centrais da decodificação de lista, que culminaram com a obtenção da "capacidade de decodificação da lista".

O primeiro passo da decodificação de lista para códigos AG, a interpolação, obtém um

polinômio em uma variável sobre um corpo de funções em várias variáveis, cuja fatoração é um problema que envolve um grande número de operações algébricas. Nesse sentido, na busca por algoritmos eficientes para executar a fatoração, em 2000, Roth e Ruckenstein [48] apresentaram um procedimento eficiente para decodificação de lista de códigos Reed-Solomon, no qual a etapa da fatoração utiliza um algoritmo de reconstrução para determinar as raízes de polinômios em uma variável sobre anéis polinomiais. A fim de generalizar este algoritmo para códigos AG, Wu e Siegel [49] estenderam o algoritmo rápido de Roth e Ruckenstein [48] para encontrar raízes de polinômios em uma variável sobre um corpo de funções.

Em 2002, O'Keeffe e Fitzpatrick [50] apresentaram um algoritmo de base de Gröbner geral que foi aplicado para resolver interpolação em problemas na decodificação dos códigos Reed-Solomon e, posteriormente, em [51] para códigos AG de um ponto.

A etapa da interpolação na decodificação de lista de códigos AG pode ser vista como o problema de encontrar o polinómio mínimo de um ideal com relação a uma determinada ordem monomial. Com base nesse fato, em 2008, a fim de resolver o problema da decodificação de lista para códigos de Reed-Solomon, Lee e O'Sullivan [52] apresentaram um algoritmo com base na teoria de bases de Gröbner de módulos e, em 2009, generalizaram o algoritmo para códigos de Hermite de um ponto [53].

Os diversos algoritmos de decodificação de lista citados foram desenvolvidos para códigos de um ponto. No entanto, demonstrou-se que códigos AG multiponto podem ter melhores parâmetros do que os códigos de um ponto [9]. Com relação à decodificação de códigos multiponto, em 2009, Drake [1], utilizando a decodificação de lista, apresentou um algoritmo de decodificação única baseado no fato de que todos os códigos multiponto são subcódigos de códigos de um ponto. Fujisawa e Sakata [54, 55] apresentaram um método rápido de decodificação de códigos AG multiponto que também considera o fato de que podem ser incorporados a subcódigos de um ponto e que esses códigos podem ser decodificados por uma variação do algoritmo BMS original chamado algoritmo BMS vetorial.

Em 2012, Matsumoto et al [56] apresentaram uma generalização do algoritmo de decodificação única para códigos AG de um ponto sobre as curvas Miura-Kamiya proposto por Lee, Bras-Amorós e O'Sullivan [57] para códigos AG de um ponto. E, além disso estenderam o algoritmo de decodificação única para a decodificação de lista de códigos AG de um ponto.

3.2 – Decodificação de lista para códigos AG

Esta tese tem como um dos objetivos contribuir para a decodificação de lista de códigos AG multiponto, para isto iniciou-se o estudo a partir de dois métodos de decodificação de lista pra códigos AG. Primeiramente, será enunciado o método de Wasserman-Shokrolahi [15] e, em seguida, o método proposto por Lee e O'Sullivan para códigos de Hermite, o qual foi adaptado para a curva de F. K. Schmidt [21] e para a curva hermitiana generalizada [10].

De modo geral, os algoritmos de decodificação de lista consistem de dois passos básicos: a

interpolação, na qual o objetivo é encontrar um polinômio interpolador que depende da palavra recebida e das características do código, e a fatoração, na qual o objetivo é encontrar as raízes do polinômio obtido no primeiro passo.

Neste capítulo são descritos os algoritmos de Shokrollahi- Wasserman [15] e Lee-O'Sullivan [53], este último foi implementado utilizando os softwares Macaulay2 e SageMath para utilização nesta pesquisa.

Definição 12 *Um código linear $\mathcal{C}$ de comprimento n sobre $\mathbb{F}_q$ é chamado (e,l)-decodificável se toda esfera de Hamming de raio e em $\mathbb{F}_q^n$ contém no máximo l palavras-código.*

Exemplo 8 *Observe que todo código linear $\mathcal{C}(n,k,d)$ é $(\lfloor (d-1)/2 \rfloor, 1)$-decodificável.*

3.2.1 – Algoritmo de Wasserman-Shokrollahi

Seja $\mathcal{X}$ uma curva absolutamente irredutível sobre $\mathbb{F}_q$ de gênero g e K denota neste capítulo o corpo de funções da curva.

Teorema 5 *[15] Seja $\mathcal{C} := \mathcal{C}(D,G)$ um código AG, com grau de G igual a u, comprimento n e dimensão k sobre uma curva algébrica sobre $\mathbb{F}_q$ de gênero g. Então, para algum inteiro positivo l, $\mathcal{C}$ é $(n-\beta-1,l)$-decodificável, em que $\beta := \lceil (n+1)/(l+1) + lu/2 + g - 1 \rceil$ e $u := k+g-1$.*

Corolário 2 *Seja $u := k+g-1$ e $\beta := \lceil \sqrt{2un} + g - 1 \rceil$. Então $\mathcal{C}$ é $(n-\beta-1, \lceil \sqrt{2n/u} \rceil)$-decodificável.*

Seja F um divisor de grau $\beta - lu$ que deve ser definido de modo que tenha suporte disjunto de D. Seja $f \in \mathcal{L}(G)$ e seja $c = (f(P_1), \cdots, f(P_n))$ a imagem do mapeamento ev.

Suponha que $v = (v_1, \cdots, v_n) \in {\mathbb{F}_q}^n$ é tal que c e v coincidem em pelo menos $\beta + 1$ coordenadas. O algoritmo a seguir calcula uma lista com no máximo l palavras-código, uma das quais deve ser c.

O algoritmo de decodificação de lista segue os seguintes passos:

Passo 1: (INTERPOLAÇÃO) Encontrar um polinômio não nulo

$$H(T) := a_l T^l + \cdots + a_1 T + a_0 \in K[T]$$

em que $a_j \in \mathcal{L}(F + (b-j)G)$, de modo que $H(P_i, v_i) := \sum_{j=0}^{b} a_j(P_i) v_i^j$ é zero para $i = 1, \cdots, n$.

Passo 2: (FATORAÇÃO) Encontrar as raízes ρ de $H(T)$ em K.

Para cada ρ calcule $c_\rho := (\rho(P_1), \cdots, \rho(P_n))$. Se c_ρ não está definida ou se a distância entre c_ρ e v é maior que $n - \beta - 1$, descarte c_ρ.

Exemplo 9 *Considere a curva de Hermite definida no plano projetivo sobre* $\mathbb{F}_{64}$ *por*

$$\mathcal{X} : X^9 + Y^8Z + YZ^8 = 0,$$

com gênero $g = 28$ *e* 513 *pontos racionais.*

A curva tem $Q, P_1, \cdots, P_{512}$ *pontos racionais. Sejam os divisores* $D = P_1 + \cdots + P_{512}$ *e* $G = uQ = 44Q$.
Fixando $b = 2$ *e um divisor* F *de modo que* $deg(F) = \beta - bu$. *Pelo Teorema 5,* $\beta = 242$ *e, além disso, o código é* $(n - \beta - 1, b)$*-decodificável. Logo,* $deg(F) = 242 - 2 \cdot 44 = 154$.
Portanto, o código $\mathcal{C}(D, G)$ *corrige* $n - \beta - 1 = 512 - 242 - 1 = 269$ *erros e produz uma lista com duas palavras código.*

Sabendo que a distância mínima do código é $d = n - u = 512 - 44 = 468$*, então o limite de correção única de erros é* $\lfloor (d-1)/2 \rfloor = \lfloor (468-1)/2 \rfloor = 233$.
Portanto, o código é $(269, 2)$*-decodificável.*

A etapa de interpolação da decodificação de lista de códigos AG pode ser vista como o problema de encontrar o polinômio mínimo de um ideal com relação a uma certa ordem monomial. Nesse sentido, em 2008, Lee e O'Sullivan [52] apresentaram um algoritmo de decodificação de lista para códigos de Hermite de um ponto com base na teoria de bases de Gröbner de módulos, o qual será apresentado na próxima seção. Além disso, no capítulo 4, é apresentada uma adaptação deste algoritmo pra a curva FKS, que consiste de uma generalização da curva de Hermite [21].

3.2.2 – Algoritmo de Lee-O'Sullivan

Dado um código AG $\mathcal{C}(D, G)$, em que $D = P_1 + \cdots + P_n$, e $G = uQ$, em que $Q = P_\infty$, considera-se um conjunto de geradores de um módulo induzido a partir do ideal para $P_1, P_2, \cdots, P_n$ e converte-se os geradores para uma base de Gröbner do módulo, na qual o polinômio mínimo é encontrado.

Considere $\mathbb{F}$ um corpo finito com $q = r^2$ elementos. Seja $\mathcal{X}$ uma curva plana de Hermite definida pelo polinômio absolutamente irredutível $X^{r+1} - Y^r - Y$ sobre $\mathbb{F}$. O anel de coordenadas de $\mathcal{X}$ é o domínio de integridade

$$R = \mathbb{F}[x, y]/\langle X^{r+1} - Y^r - Y \rangle.$$

O corpo de funções de $\mathcal{X}$ é o corpo de frações K de R e, x e y as classes residuais de X e Y em R, respectivamente. Assim, $x^{r+1} - y^r - y = 0$ e $R = \mathbb{F}[x, y]$.

Seja k a dimensão do código $\mathcal{C}_u$. Para codificar, fixe uma base de $\mathcal{L}(uQ)$, dizemos $\{\varphi_1, \varphi_2, \cdots, \varphi_k\}$. Seja $\omega = (\omega_1, \cdots, \omega_n) \in \mathbb{F}^k$ uma mensagem a ser codificada em uma palavra código

$$c = ev(\mu),$$

em que $\mu = \sum_{i=1}^{k} \omega_i \varphi_i$. Chamamos μ de função mensagem correspondente à palavra código c.

Defina, para $0 \leq i \leq n$,

$$H_i = -\frac{(X^{r^2} - X)(Y^r + Y - \beta_i^r - \beta_i)}{(X - \alpha_i)(Y - \beta_i)} \in \mathbb{F}[X, Y]$$

e seja h_i a classe residual de H_i em R. Para $v = (v_1, \cdots, v_n) \in \mathbb{F}^n$, definimos

$$h_v = \sum_{i=1}^{n} v_i h_i.$$

Considere $f = \psi_a z^a + \cdots + \psi_1 z + \psi_0 \in R[z]$, com $\psi_i \in R$, o u-grau ponderado de f é definido por

$$deg_u(f) = max_{0 \leq i \leq a}(-v_Q(\psi_i) + ui)$$

Suponha que alguma palavra código de C_u foi enviada através de um canal ruidoso. Seja v o vetor recebido. Fixamos um inteiro m, chamado de parâmetro de multiplicidade. Defina

$$I_{v,m} = \langle z - h_v, \eta \rangle^m$$

um ideal de $R[z]$, com $\eta = x^{r^2} - x$.

Teorema 6 *[53] Suponha que $f \in I_{v,m}$ é não nulo. Seja $w = deg_u(f)$. Se $c = ev(\mu)$ é uma palavra código de C_u satisfazendo $d(v, c) < n - w/m$, então $f(\mu) = 0$.*

O primeiro passo da decodificação de lista dos códigos de Hermite é construir um polinômio f não nulo do ideal $I_{v,m}$. O segundo passo é encontrar as raízes de f sobre R, que resulta em uma lista de funções mensagens correspondentes às palavras-código. Para maximizar a probabilidade da lista incluir a função mensagem original para a palavra enviada, f deve ser escolhido tal que o u-grau ponderado de f seja minimizado, de acordo com o Teorema 6.

Definimos os monômios de $R[z]$ como sendo o conjunto

$$\Omega = \{x^i y^j z^k | 0 \leq i, 0 \leq j \leq r - 1, 0 \leq k\}$$

Observe que todo elemento de $R[z]$ pode ser escrito como uma única combinação linear dos monômios de $R[z]$ sobre $\mathbb{F}$ e, além disso,

$$deg_u(x^i y^j z^k) = ri + (r + 1)j + uk.$$

Para dois monômios $x^{i_1} y^{j_1} z^{k_1}$ e $x^{i_2} y^{j_2} z^{k_2}$ em Ω, definimos

$$x^{i_1} y^{j_1} z^{k_1} >_u x^{i_2} y^{j_2} z^{k_2},$$

se $deg_u(x^{i_1}y^{j_1}z^{k_1}) > deg_u(x^{i_2}y^{j_2}z^{k_2})$ ou $k_1 > k_2$. Desse modo, $>_u$ define uma ordem total em Ω e o termo líder de f é definido da forma usual. Para $f \in R[z]$, z-deg(f) é o grau de f como um polinômio em z sobre R.

O polinômio interpolador $H(z)$ é o único, a menos de uma constante múltipla, elemento de $I_{v,m}$ com o menor termo líder com relação à $>_u$. Portanto, é um elemento de $I_{v,m}$ com o menor u-grau ponderado e, além disso, tem o menor z-grau entre esses elementos. Portanto, podemos dizer que o H-polinômio é uma escolha ótima para o passo da interpolação da decodificação de lista, e que o objetivo do passo da interpolação é encontrar o H-polinômio eficientemente [53]. Observe que é possível limitar o tamanho da lista, a fim de estimar a capacidade de correção de erros da lista.

Seja l um inteiro positivo tal que $z - deg(H) \leq l$. Denominamos l o tamanho da lista. Seja

$$R[z]_l = \{f \in R[z] | z - deg(f) \leq l\}.$$

Observe que $R[z]_l$ é um módulo livre sobre R com uma base $\{1, z, \cdots, z^l\}$. Definindo o ideal

$$I_{v,m,l} = I_{v,m} \cap R[z]_l,$$

claramente $I_{v,m,l}$ é um submódulo de $R[z]_l$ sobre R.

Proposição 2 *$I_{v,m,l}$, como um módulo sobre R, tem um conjunto de geradores consistindo de G_i, $0 \leq i \leq l$, em que*

$$G_i = \begin{cases} (z - h_v)^i \eta^{m-i}, 0 \leq i \leq m, \\ z^{i-m}(z - h_v)^m, m \leq i. \end{cases}$$

Note que o anel $R = \mathbb{F}[x, y]$ por sua vez é um módulo livre sobre $\mathbb{F}[x]$, com uma base $\{1, y, \cdots, y^{r-1}\}$. Assim, $R[z]_l$ pode ser visto como um módulo livre sobre $\mathbb{F}[x]$ com uma base livre $\{y^j z^i | 0 \leq l, 0 \leq j \leq r - 1\}$. Os elementos de $\Omega \cap R[z]_l$ são chamados monômios de $R[z]_l$. Além disso, $I_{v,m,l}$ é visto como um submódulo do módulo livre $R[z]_l$ sobre $\mathbb{F}[x]$. Um conjunto de geradores para $I_{v,m,l}$, como um módulo sobre $\mathbb{F}[x]$, é

$$\{y^j G_i | 0 \leq i \leq l, 0 \leq j \leq r - 1\}$$

É imediato que o H-polinômio de $I_{v,m}$ é também o elemento de $I_{v,m,l}$ com o menor termo líder com relação a $>_u$. Como uma consequência da definição de bases de Gröbner, H ocorre como o menor elemento em qualquer base de Gröbner do módulo $I_{v,m,l}$ sobre $\mathbb{F}[x]$ com relação à $>_u$. Ao contrário do cálculo de bases de Gröbner de ideais, verifica-se que o cálculo de uma base de Gröbner do módulo $I_{v,m,l}$ sobre $\mathbb{F}[x]$ pode ser feito de forma mais eficiente [53].

O algoritmo de interpolação para códigos de Hermite apresentado em [53], para o módulo livre $R[z]_l$ sobre $\mathbb{F}[x]$ e o conjunto de geradores $y^j G_i$ do submódulo $I_{v,m,l}$ de $R[z]_l$ é apresentado em seguida.

Seja $T = \{(i,j)|0 \leq i \leq l, 0 \leq j \leq r-1\}$, ordenado lexicograficamente. Então, $\{y^j z^i|(i,j) \in T\}$ é uma base para $R[z]_l$ como um $\mathbb{F}[x]$-módulo. O índice de $f \in R[z]_l$ é o maior valor de $(i,j) \in T$ tal que o coeficiente de $y^j x^i$ é não nulo. Seja $ind(\cdot)$ o par ordenado contendo os expoentes (i,j) dos elementos $y^j G_i$, ou seja, $ind(y^j G_i) = (i,j)$. O peso de um elemento da base $y^j z^i$ é $ui + (r+1)j$. Assim, se o termo líder, com relação à $>_u$, de $f \in R[z]_l$ é $x^k y^j z^i$, então $ind(lt(f)) = (i,j)$.

Algoritmo I

O algoritmo encontra o elemento de $I_{v,m,l}$ com o menor termo líder.

Seja $g_{(i,j)} = \sum_{(i',j') \in T} a_{(i,j),(i',j')} y^{j'} z^{i'}$ para $(i,j) \in T$ durante a execução do algoritmo.

Inicialmente, fixe $g_{(i,j)} \leftarrow y^j G_i$ para $(i,j) \in T$.

I-1. Fixe $r \leftarrow (0,0)$.

I-2. Tome o sucessor de t. Se $t \in T$, então prossiga. Caso contrário, vá para o passo I-6.

I-3. Faça $s \leftarrow ind(lt(g_t))$. Se $s = t$, então volte ao passo I-2.

I-4. Seja $d \leftarrow deg(a_{t,s}) - deg(a_{s,s})$ e $c \leftarrow lc(a_{t,s}) lc(a_{s,s})^{-1}$.

I-5. (a) Se $d \geq 0$, então faça

$$g_t \leftarrow g_t - c x^d g_s$$

(b) Se $d < 0$, então, armazene g_s em uma variável temporária,

$$g_s \leftarrow g_t$$

$$g_t \leftarrow x^{-d} g_t - c g_s$$

Volte para o passo I-3.

I-6. Saída $g_{(i,j)}$ com o menor termo líder, e termina o algoritmo.

A idéia do algoritmo é atualizar o conjunto de geradores até $ind(lt(g_t)) = t$, para todo $t \in T$, nesse momento o conjunto atualizado de geradores é uma base de Gröbner de $I_{v,m,l}$.

Exemplo 10 *Seja $q = 2$. Considere a curva de Hermite definida por $X^3 + Y^2 + Y = 0$ sobre $\mathbb{F}_4 = \{0, \alpha, \alpha^2, \alpha^3\}$ e $n = 8$. Escolhendo $u = 4$, o espaço linear $\mathcal{L}(4Q) = \langle 1, x, y, x^2 \rangle$. O código de Hermite será um código $[8,4,4]$ sobre $\mathbb{F}_4$. A mensagem a ser enviada é $\omega = (\alpha^2, \alpha^2, 0, \alpha^2)$, e a palavra código será:*

$$ev(\mu) = (\alpha^2, \alpha^2, \alpha^2, \alpha^2, 0, 0, 0, 0),$$

em que $\mu = \alpha^2 + \alpha^2 x + \alpha^2 x^2$.

Suponha que $v = (\alpha^2, 0, 0, \alpha^2, 0, 0, 0, 0)$. Seja $m = 2$ o parâmetro de multiplicidade e $\eta = x^4 + x$. Isto significa que $z\text{-}grau(H) = 2$. Assim, tomamos $l = 2$ como o tamanho da lista. Seja $R = \mathbb{F}_4[x,y]$ com $y^2 = y + x^3$ um módulo sobre $\mathbb{F}_4[x]$. O ideal

$I_{v,2,2} = \langle G_0, yG_0, G_1, yG_1, G_2, yG_2 \rangle$ *é dado por*

$$I_{v,2,2} = \langle z + h_v, \eta \rangle^2 = \langle \eta^2, \eta z + \eta h_v, z^2 + {h_v}^2 \rangle = \langle G_0, G_1, G_3 \rangle,$$

em que $h_v = \alpha^2 x^2 y + \alpha x^3 + \alpha^2 xy + x^2 + \alpha^2 y + x + \alpha^2$.

Inicialização do Algoritmo I:

$g_{(0,0)} = (x^8 + x^2)$

$g_{(0,1)} = (x^8 + x^2)y$

$g_{(1,0)} = (x^4 + x)z + (\alpha^2 x^6 + \alpha^2 x^5 + \alpha^2 x^4 + \alpha^2 x^3 + \alpha^2 x^2 + \alpha^2 x)y + (\alpha x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + \alpha^2 x)$

$g_{(1,1)} = (x^4 + x)yz + (\alpha x^7 + \alpha x^6 + \alpha x^5 + \alpha x^4 + \alpha x^3 + \alpha x^2)y + (\alpha^2 x^9 + \alpha^2 x^8 + \alpha^2 x^7 + \alpha^2 x^6 + \alpha^2 x^5 + \alpha^2 x^4)$

$g_{(2,0)} = z^2 + (\alpha x^4 + \alpha x^2 + \alpha)y + (\alpha x^7 + \alpha^2 x^6 + \alpha x^5 + x^4 + \alpha x^3 + x^2 + \alpha)$

$g_{(2,1)} = yz^2 + (\alpha x^7 + \alpha^2 x^6 + \alpha x^5 + \alpha^2 x^4 + \alpha x^3 + \alpha^2 x^2)y + (\alpha x^7 + \alpha x^5 + \alpha x^3)$

Aplicando o Algoritmo I para a palavra recebida v *e o ideal* $I_{v,2,2}$ *o* H*-polinômio encontrado é*

$$H(z) = (x^2 + x)z^2 + (\alpha^2 x^4 + \alpha^2 x)z.$$

Este polinômio pode ser fatorado como

$$H(z) = (x^2 + x)z(z + \alpha^2 x^2 + \alpha^2 x + \alpha^2).$$

Portanto, as raízes de H *são:* $z = 0$ *e* $z = \alpha^2 x^2 + \alpha^2 x + \alpha^2$. *Esta última foi a mensagem enviada.*

Em 2013, o algoritmo proposto por Lee e O'Sullivan [52] para códigos de Hermite de um ponto foi generalizado para outros códigos AG de um ponto por Matsumoto *et al.* [58]. Nesse sentido, considerando que a curva de Hermite é um caso particular da curva F. K. Schmidt (FKS), mostraremos no próximo capítulo que o algoritmo de Lee e O'Sullivan [53] pode ser estendido para a curva FKS.

3.2.3 – Algoritmo de interpolação polinomial genérico

O algoritmo de interpolação apresentado na seção anterior, para códigos de Hermite, foi estendido por Lax [59] para códigos AG de um ponto sobre uma curva $\mathcal{X}$. Além disso, foi proposto um algoritmo de interpolação polinomial genérico baseado na substituição da n-upla $v = (v_1, \cdots, v_n)$ por uma n-upla de variáveis $v_0 = (v_{01}, \cdots, v_{0n})$.

Seja $\mathcal{X}$ uma curva suave projetiva absolutamente irredutível sobre $\mathbb{F}_q$ de gênero g. Sejam P um ponto racional da curva e $\mathcal{C}(D, uP)$ um código AG de um ponto. Então, a curva $\mathcal{X}_0 = \mathcal{X} - \{P\}$ é uma variedade afim $V_{\mathbf{F}}(J)$ para um ideal $J \subseteq \mathbb{F}_q[X_1, \cdots, X_s]$.

Fixe $A = \mathbb{F}_q[X1, \cdots, X_s]$ e $R = A/J$ denota o anel de coordenadas de $\mathcal{X}_0$. Seja $J \subseteq I$ tal que I é um ideal de A tal que $V_F(I) = \{P_1, \cdots, P_n\} = Supp(D)$. Se $D = P_1 + \cdots + P_n$, então $I = J$.

Considere $R_q = A/I_q$, em que

$$I_q = I + \langle X_1^q - X_1, X_2^q - X_2, \cdots, X_s^q - X_s \rangle.$$

Sejam $P_i = (a_{i1}, a_{i2}, \cdots, a_{is})$ e os ideais maximais de A correspondentes denotados por $M_i = \langle X_1 - a_{i1}, X_2 - a_{i2}, \cdots, X_s - a_{is} \rangle$, com $i = 1, 2, \cdots, n$. Segue-se que

$$R_q \cong \oplus_{i=1}^{n} A/M_i.$$

O mapeamento $ev : R_q \rightarrow \mathbb{A}^n$ é um isomorfismo entre espaços vetoriais tal que $f \rightarrow (f(P_1), f(P_2), \cdots, f(P_n))$. Deste modo, o espaço vetorial $\mathcal{L}(uP)$ pode ser identificado como um $\mathbb{F}_q$ - subespaço vetorial $\mathcal{L}$ de R_q e o código $\mathcal{C}(D, uP)$ é a imagem do mapeamento ev. Deste modo, dizemos que o código $\mathcal{C}(D, uP)$ é visto como um código de uma variedade afim.

De modo análogo ao Algoritmo I, primeiramente, é necessário fixar os polinômios $H_i \in A$ tais que $Hi(P_j) = \delta_{i,j}$, ou seja, $H_i(P_i) = 1$ e $H_i(P_j) = 0$, para $i \neq j$. Para isso, defina

$$H_i(X_1, \cdots, X_s) = \prod_{j=1}^{s} [1 - (X_j - a_{ij})^{q-1}].$$

Seja h_i a classe residual de H_i em R, para $i = 1, 2, \cdots, n$. Dada uma palavra recebida $v = (v_1, \cdots, v_n)$, definimos

$$H_v = \sum_{i=1}^{n} v_i H_i$$

e h_v a classe residual de H_v em R.

Fixe $P_{iv} = (a_{i1}, \cdots, a_{in}, v_i)$ e $M_{iv} = \langle X_1 - a_{i1}, X_2 - a_{i2}, \cdots, X_s - a_{is}, Z - v_i \rangle$ os ideais maximais em $A[Z]$ correspondentes a P_{iv}, para $i = 1, 2, \cdots, n$.

Proposição 3 $I_q + \langle Z - H_v \rangle = \cap_{i=1}^{n} M_{iv}$.

Sejam $x_1, x_2, \cdots, x_s$ as classes residuais de $X_1, X_2, \cdots, X_s$ em R. O ideal maximal M_{iv} em $A[Z]$ corresponde ao ideal maximal $\overline{M}_{iv} = \langle x_1 - a_{i1}, x_2 - a_{i2}, \cdots, x_s - a_{is} \rangle$ em $R[Z]$.

De modo análogo ao que foi apresentado por Lee e O'Sullivan [53] para a curva de Hermite, Lax [52] define o ideal

$$\overline{I}_{m,v} = ((I/J)R[Z] + \langle x_1^q - x_1, x_2^q - x_2, \cdots, x_s^q - x_s, Z - h_v \rangle)^m.$$

Corolário 3 *Para um m inteiro positivo,*

$$\overline{I}_{m,v} = \cap_{i=1}^{n} \overline{M}_{iv}.$$

Para limitar o tamanho da lista contendo no máximo l palavras código, deve-se considerar o grau do polinômio interpolador em Z no máximo l. Além disso, considere que o polinômio interpolador pode ser visto como um elemento em um R-módulo livre $R[Z]_l = \oplus_{j=0}^{l} RZ^j$, em vez de visualizar o polinômio de interpolação como um elemento em $R[Z]$. Assim, é possível usar bases de Gröbner para módulos ao invés de bases de Gröbner para ideais e encontrar o polinômio interpolador como sendo o polinômio de menor grau na base.

Assuma que $m \geq l$. É possível determinar um ideal $\overline{I}_{m,v,l} = \overline{I}_{m,v} \cap R_l[Z]$. E considerando $\overline{I}_{m,v,l}$ como um R-módulo pode-se determinar uma base de Gröbner e o polinômio interpolador correspondente.

Teorema 7 *Considere $H(Z) \in \overline{I}_{m,v}$ com grau positivo em Z. Seja $\mu = deg_u(H(Z))$ e $c = ev(\varphi)$ uma palavra código de $\mathcal{C}(D, uP)$ tal que a distância de Hamming $d(c, v)$ satisfaz $d < n - (\mu/m)$. Então, φ é uma raiz de $H(Z)$, isto é, $H(\varphi) = 0$.*

De modo geral, pode-se sintetizar o algoritmo proposto por Lax [59] para códigos AG conforme apresentamos a seguir. O algoritmo proposto busca encontrar o polinômio $H(Z)$ com menor grau, com relação à ordem $<_u$, cujas raízes formam uma lista de palavras que estão em um raio de decodificação de lista dado.

Algoritmo II

Seja $\mathcal{C}(D, uP)$ código AG de um ponto com parâmetros $[n, k, d]$ e $v = (v_1, \cdots, v_n)$ uma palavra recebida:

II-1. Fixe o tamanho desejado da lista l;

II-2. Calcule a multiplicidade como sendo um inteiro positivo m, tal que $m > \frac{lu}{n-d}$;

II-3. Calcule h_v;

II-4. Fixe o ideal $\overline{I}_{m,v} = ((I/J)R[Z] + \langle x_1^q - x_1, x_2^q - x_2, \cdots, x_s^q - x_s, Z - h_v\rangle)^m$;

II-5. Calcule o ideal $\overline{I}_{m,v,l} = \overline{I}_{m,v} \cap R_l[Z]$.

II-6. Calcule uma base de Gröbner B do ideal $\overline{I}_{m,v,l}$;

II-7. Determinar o polinômio de menor grau com relação à ordenação monomial $>_u$ e este será o polinômio interpolador $H(Z)$.

De modo mais geral, este algoritmo pode ser visto de uma forma genérica, em que v é considerada uma palavra recebida genérica $v_0 = (v_{01}, \cdots, v_{0n})$.

3.3 – Algoritmo de fatoração

A etapa da fatoração nos algoritmos de decodificação pode ser executada a partir de algoritmos de fatoração de polinômios, produzindo uma lista de raízes desse polinômio, que corresponde à lista de palavras-código a uma determinada distância da palavra-código que foi enviada. Contudo, pode-se observar que a palavra enviada foi construída como uma combinação

linear de uma base de um espaço de funções para códigos AG (incluindo Reed-Solomon) e, portanto, o decodificador tem conhecimento dessa base de funções. Portanto, é possível restringir a busca dessas raízes sob essa base do espaço de funções. Desse modo, em geral, obtém-se uma lista menor do que numa busca utilizando algoritmos de fatoração tradicionais.

Nesse sentido, Roth e Ruckenstein [48] propuseram uma implementação eficiente da lista de decodificação dos códigos Reed-Solomon. Estendendo este algoritmo, Wu e Siegel [49] apresentaram um algoritmo eficiente para encontrar as raízes de polinômios univariados sobre corpos de funções e, assim, tem-se um algoritmo de decodificação de lista eficiente para códigos AG, o qual será detalhado nesta seção.

Inicialmente, considere o exemplo para códigos Reed-Solomon, que ilustra a ideia do algoritmo.

Exemplo 11 *Considere um código Reed-Solomon como no Exemplo 1. Seja* $H(T) = T^2 + (Y^2 + Y + 1)T + (Y^3 + Y)$ *um polinômio interpolador sobre* $\mathbb{F}_4$*. Então, uma das raízes de* $H(T)$ *será uma palavra código na base* $\mathcal{L} = \langle 1, Y, Y^2 \rangle$*.*

Considerando que as raízes do polinômio $H(T)$ *são do tipo* $f = f_0 + f_1Y + f_2Y^2$*, então* $H(f_0 + f_1Y + f_2Y^2) = 0$*.*

Observe que o coeficiente líder de $H(f_2Y^2)$ *é igual ao coeficiente líder de* $H(f_0 + f_1Y + f_2Y^2))$ *e, portanto, será igual a zero. Logo,*

$$f_2^2 + f_2 = 0 \Rightarrow \alpha_1 \in \{0, 1\}$$

em que α_1 *é uma raiz do polinômio na variável* f_2*.*

Para alguma raiz α_1 *defina:*

$$H_1(T) := H(T)$$

e

$$H_2(T) = H_1(T + \alpha_1 Y^2).$$

Note que

$$H_2(f_0 + f_1Y) = 0.$$

Logo, o coeficiente líder de $H_2(f_1Y)$ *é igual a zero.*
Para a raiz $\alpha_1 = 0$*, obtemos a equação polinomial* $f_1 + 1 = 0 \Rightarrow f_1 = 1$*. Para a raiz* $\alpha_1 = 1$*, obtemos* $f_1 = 0$*.*

Para alguma raiz α_2 *de* f_1*, defina:*

$$H_3(T) = H_2(T + \alpha_2 Y) \Rightarrow H_3(f_0) = 0.$$

Assim, o coeficiente líder de $H_3(f_0)$ *é igual a zero.*
Para $\alpha_2 = 1$*, encontramos* $f_0 = 0$*.*
Para $\alpha_2 = 0$*, encontramos* $f_0 = 1$*.*

Desse modo, as raízes de $H(T)$ são $f = Y$ e $f = Y^2 + 1$.

O algoritmo de fatoração proposto por Wu e Siegel [49] generaliza esta ideia para códigos AG de um ponto $\mathcal{C}(D, \rho P)$, conforme veremos a seguir.

Seja $H(T)$ um polinômio com raízes em $\mathcal{L}(\rho P) = \langle \varphi_1, \cdots, \varphi_k \rangle$. Então,

$$f = f_1\varphi_1 + \cdots + f_k\varphi_k$$

é uma raiz de $H(T)$ se, e somente se,

$$H(f_1\varphi_1 + \cdots + f_k\varphi_k) = 0.$$

Seja ρ_i a ordem da função φ_i em P, então $\varphi_1^{i_1} \cdots \varphi_k^{i_k}$ tem um pólo de ordem $i_1\rho_1 + \cdots + i_k\rho_k$ em P.

Considere a ordenação lexicográfica graduada ponderada de modo que o monômio $\varphi_1^{i_1}\varphi_2^{i_2} \cdots \varphi_k^{i_k}$, reduzido módulo a curva, tem o grau definido por

$$deg(\varphi_1^{i_1}\varphi_2^{i_2} \cdots \varphi_k^{i_k}) = i_1\rho_1 + i_2\rho_2 + \cdots + i_k\rho_k.$$

Observe que o termo com maior grau ponderado é chamado termo líder e seu coeficiente é o coeficiente líder. Além disso, note que o termo líder será o termo que tem a menor valorização discreta ord_P.

De modo análogo ao exemplo do código Reed-Solomon, o coeficiente líder de $H(f_1\varphi_1 + \cdots + f_k\varphi_k) = 0$ deve ser zero. Portanto, o sistema de equações polinômiais sobre $\mathbb{F}_q$ com incógnitas $f_1, f_2, \cdots, f_k$, é

$$\begin{cases} a_1(f_1, \cdots, f_k) = 0, \\ \vdots \\ a_t(f_1, \cdots, f_k) = 0. \end{cases} \tag{3.1}$$

As raízes f_i do sistema acima formam as raízes do polinômio $H(T)$. Portanto, usando a ideia do Exemplo 1 as raízes de $H(T)$ que pertencem ao espaço $\mathcal{L}(\rho P)$ podem ser encontradas utilizando o algoritmo *Root-Finding*, que descrevemos a seguir de modo breve. Para maiores detalhes sobre o Algoritmo *Root-Finding* consultar [49].

Observe que os coeficientes do polinômio $H(T)$ são funções racionais h_j que vamos denotar por $h_j(X)$ e $H(T)$ será denotado por $H(X;T)$ ao longo do algoritmo.

Algoritmo III - *Root-Finding*

III-1 Encontrar uma função racional ϕ tal que

$$ord_P(\phi) = min\{ord_P(\widehat{G}(X))|j = 0, 1, \cdots, s\}$$

III-2 $\widetilde{G}(X;T) \leftarrow \frac{1}{\phi}\widehat{G}(X;T)$;

III-3 Calcule o polinômio não-nulo $\widetilde{G}(P,T) \in \mathbb{F}_q[T]$;

III-4 Encontre as raízes γ de $\widetilde{G}(P,T) = 0$;

III-5 Para cada raiz distinta γ de $\widetilde{G}(P,T) = 0$ faça $g[i] = \gamma$.

III-6 Se $i = k$, então **saída =** $g[k, \cdots, 1] = [f_1, \cdots, f_k]$; Caso contrário, faça

- $G(X;T) \leftarrow \widetilde{G}(X;T+\gamma)$.
- $\widehat{G}(X;T) \leftarrow G(X; \frac{\varphi_{k-i}}{\varphi_{k-i+1}}T)$.

III-7 *Root-Finding* ($\widehat{G}(X;T)$, k, $i+1$).

Exemplo 12 *Considere a quártica de Klein sobre* $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^6\}$ *definida pela seguinte equação projetiva:*

$$\mathcal{X} : X^3Y + Y^3Z + Z^3X = 0. \tag{3.2}$$

A curva $\mathcal{X}$ *tem* 24 *pontos racionais. Seja* $Q = (0:1:0)$ *e considere um código AG de um ponto* $\mathcal{C}(D,G)$*, com* $G = 7Q$ *e* $D = P_1 + \cdots + P_{23}$*. Sejam* $x = \frac{X}{Z}$ *e* $y = \frac{Y}{Z}$*. A função racional* x *tem um pólo de ordem* 2 *em* Q *e* y *tem um pólo de ordem* 3 *em* Q*, isto é,*

$$ord_Q(x) = -2$$

$$ord_Q(y) = -3$$

Seja o polinômio $H(T) = T^2 + (\alpha^3xy + x^2y)T + \alpha^3x^3y^2$ *cujas raízes que fazem parte do código* $\mathcal{C}(D, 7Q)$ *pertencem ao espaço* $\langle 1, y, xy, y^2, x^2y\rangle$.

Aplicando o Algoritmo Root-Finding temos

O tamanho da base é $k = 5$ *e inicialmente,* $i = 1$.

$$\widehat{G}_1(X;T) = H(X;\varphi_5 T) = H(X;x^2yT)$$

$$\widehat{G}_1(X;T) = x^4y^2T^2 + (x^4y^2 + \alpha^3x^3y^2)T + \alpha^3x^3y^2$$

Note que $\phi_1 = x^4y^2$

$$\widetilde{G}_1(X;T) = \frac{1}{\phi_1}\widehat{G}_1(X;T) = T^2 + (1 + \frac{\alpha^3}{x})T + \frac{\alpha^3}{x}$$

Para calcular $\widetilde{G}_1(Q;T)$ *devemos observar que se* $ord_Q(f) > 0$*, então* f *se anula no ponto* Q.

$$ord_Q(\frac{\alpha^3}{x}) = ord_Q(\alpha^3) - ord_Q(x) = 0 - (-2) = 2 > 0$$

$$\widetilde{G}_1(Q;T) = T^2 + T$$

Logo, as raízes desse polinômio são $\gamma \in \{0, 1\}$.

Tomemos o primeiro caminho a partir da raiz $\gamma = 1 \Rightarrow g[1] = \gamma = 1$.

Como $i = 1 \neq k$*, então o algoritmo segue até que* $i = 5$*, e a saída será* $[f_1, f_2, f_3, f_4, f_5] = [0, 0, 0, 0, 1]$.

Portanto, uma das raízes do polinômio $H(T)$ *será*

$$f = 0 \cdot 1 + 0 \cdot y + 0 \cdot xy + 0 \cdot y^2 + 1 \cdot x^2y \Rightarrow f = x^2y$$

De modo análogo, seguindo desde o passo 1, a partir da raiz $\gamma = 0$ *teremos* $[f_1, f_2, f_3, f_4, f_5] = [0, 0, \alpha^3, 0, 0]$ *e*

$$f = \alpha^3 xy.$$

Portanto, a fatoração do polinômio $H(T)$ *é dada por:*

$$H(T) = (T + x^2y)(T + \alpha^3 xy).$$

Observe que este algoritmo faz uma busca pelas raízes de $H(T)$ que pertencem ao espaço $\mathcal{L}(G)$. Contudo, se devido ao processo de interpolação na decodificação de lista, o polinômio interpolador tiver raízes em outro espaço de funções, este algoritmo mostra-se eficiente por reduzir o número de raízes possíveis, pois são encontram-se apenas as que poderiam ser produzidas pelo espaço $\mathcal{L}(G)$. Desse modo, o algoritmo proposto por Wu e Siegel [49] é chamado um algoritmo eficiente para decodificação de lista de códigos AG de um ponto.

Nesta tese, propõe-se o uso deste algoritmo na fatoração na decodificação de lista para a adaptação do algoritmo proposto por Drake [1], que usa a decodificação de lista para determinar uma única palavra código, produzindo um algoritmo de decodificação única via listas. Os algoritmos propostos por Drake [1] são apresentados na próxima seção.

3.4 – Decodificação via lista para códigos AG multipontos

Os algoritmos apresentados até o momento foram descritos para códigos de um ponto. Contudo, os códigos multiponto podem apresentar parâmetros melhores e, por isso, despertam grande interesse [9]. Com relação à decodificação única, em 2014, Sakata e Fujisawa [55] propuseram um algoritmo rápido de decodificação para códigos AG multiponto.

Com relação à decodificação de lista, embora o algoritmo proposto por Wasserman e Shokrollahi [15] possa ser aplicado para códigos multiponto, visto que, na definição do código $\mathcal{C}(D, G)$ é exigido apenas que o divisor G seja disjunto de D, o algoritmo se aplica apenas para códigos com baixas taxas [1]. A fim de eliminar essa restrição, Guruswami e Sudan [43] consideraram uma singularidade para códigos de um ponto.

Em sua tese, Drake [1] apresentou vários resultados relevantes para a decodificação de códigos AG, dentre eles melhorou o limite no tamanho da lista de saída do algoritmo de

Guruswami e Sudan [43] para códigos AG de um ponto, diminuindo o grau do polinômio interpolador e, consequentemente, o número de palavras código da lista.

Além disso, Drake [1] mostrou que é possível construir um decodificador via listas para códigos multiponto, isto é, um algoritmo de decodificação única que utiliza a decodificação de lista. Os algoritmos propostos por Drake [1] consideram que um código AG multiponto pode ser isométrico a um subcódigo de um código de um ponto, satisfazendo algumas condições apresentadas no lema a seguir.

Lema 1 *[1] Seja $\mathcal{X}$ uma curva projetiva não-singular sobre $\mathbb{F}_q$. Dado um código multiponto $\mathcal{C}(D,G)$ em $\mathcal{X}$, $\mathcal{C}(D,G)$ é isométrico ao subcódigo de um ponto $\mathcal{C}(D,uP)$ em $\mathcal{X}$ para algum ponto racional P no suporte de G.*

3.4.1 – Algoritmo IV - Drake

Seja $\mathcal{C} := \mathcal{C}(D, a_1Q_1 - \sum_{i=2}^{m} a_iQ_i)$ um código m-ponto sobre um corpo finito ${\mathbb{F}_q}^n$ em que $D := P_1 + P_2 + \cdots + P_n$. Suponha que v seja a palavra recebida que tem no máximo $\lfloor \frac{d-1}{2} \rfloor$ erros.

Entrada: $a_1, a_2, \cdots, a_m$, v, parâmetro $t := n - \lfloor \frac{d-1}{2} \rfloor$.

Premissa: $t^2 > a_1 n$.

Seja $\Omega := \{f \in L(a_1P : d(ev(f), v) \leq n - t\}$.

Inicialização: Fixe os parâmetros:

$$r := \lfloor \frac{2gt + a_1n + \sqrt{(2gt + a_1n)^2 - 4(g^2-1)(t^2 - a_1n)}}{2(t^2 - a_1n)} \rfloor + 1$$

e

$$s := \lfloor \frac{rt - 1 - g}{a_1} \rfloor.$$

Passo 1 (**Interpolação**) Encontrar o polinômio não nulo $H(T) \in K(T)$, em que K denota o corpo de funções asssociado a $\mathcal{X}$, satisfazendo

1. $H(f) \in \mathcal{L}((rt-1)Q_1)$ para todo $f \in \mathcal{L}(a_1Q_1)$ e

2. $v_{P_i}(H(h)) \geq r$ para cada $i \in \{1, \cdots, n\}$ com $H(P_i) = v_i$.

em que $H(P_i) := \{n' \in \mathbb{N}; \exists f \in \mathbb{F}_q(X)$ com $(f)_\infty = n'P_i\}$ é o semigrupo numérico de Weierstrass de X em P_i.

Passo 2 (**Fatoração**) Encontrar as raízes $h \in \mathcal{L}(a_1Q_1)$ do polinômio H. Para cada h, se $h(P_i) = v_i$ para pelo menos t valores de i, então adicionamos h para Ω. Desta forma, encontra-se todas as funções h que possivelmente dão origem à palavra código em $\mathcal{C}' := \mathcal{C}(D, a_1Q_1)$ até a distância $\lfloor \frac{d-1}{2} \rfloor$ de v.

Passo 3 (**Verificar zeros**) Calcular a ordem de h em Q_i para cada h encontrado no passo 2 até encontrar uma função h tal que $v_{Q_i}(h) \geq -a_i$ para todo i, $2 \leq i \leq m$.

Passo 4 Decodificar w como $((h(P_1), \cdots, h(P_n))$.

Passo 5 Saída: $((h(P_1), \cdots, h(P_n))$, a única palavra código em $\mathcal{C}$ tal que $d(ev(h), v) \leq \lfloor \frac{d-1}{2} \rfloor$.

Além desse algoritmo, Drake [1] apresentou uma modificação em que um código multiponto é incorporado em vários códigos de um ponto e o polinômio de interpolação é obtido como o maior divisor comum dos polinômios obtidos em casa imersão.

3.4.2 – Algoritmo V - Drake

Seja $\mathcal{C} := (D, \sum_{i=1}^{m} a_i Q_i)$ um código m-ponto sobre $\mathbb{F}_q$ em que $D := P_1 + \cdots + P_n$. Suponha que $v \in {\mathbb{F}_q}^n$ seja a palavra recebida que tem no máximo $\lfloor \frac{d-1}{2} \rfloor$ erros.

Entrada: $a_1, a_2, \cdots, a_m$, v, parâmetro $t := n - \frac{d-1}{2}$.

Passo 0: Escolha um subconjunto não vazio $J \subseteq \{1, \cdots, m\}$. Para cada $j \in J$, encontre um código de um ponto $\mathcal{C}_j := \mathcal{C}(D, (a_i - b_{jj})Q_j)$ tal que

$$\mathcal{C} \cong \mathcal{C}(D, (a_j - b_{jj})Q_j - \sum_{1 \leq i \leq m; i \neq j} (b_{ij} - a_i)Q_i) \subseteq C_j$$

é a incorporação induzida pela função racional f_j com $v_{Q_i}(f_j) = b_{ij}$ para todo $1 \leq i \leq m$, $b_{ij} \geq a_i$ para todo $i \neq j$, $b_{jj} < a_j$, e $t^2 > (a_j - b_{jj})n$.

Passo 1: Fixe os parâmetros: Para cada $\mathcal{C}_j$, fixe os parâmetros conforme o passo 1 do Algoritmo.

Passo 2: (Interpolação) Para cada $\mathcal{C}_j$, encontre o polinômio interpolador não nulo $H_j(T) \in K[T]$ como no passo 2. Seja

$$H(T) := gcd\{H_j(T) : j \in J\}$$

em que $H_j(T) = H_j(f_j T)$.

Passo 3: (Fatoração) Encontrar todas as raízes do polinômio $H(T)$ como no passo da fatoração padrão. Desta forma, encontramos todas as funções $h \in \mathcal{L}(\sum_{i=1}^{m} a_i Q_i)$ que possivelmente geram todas as palavras código que estão à distância $\lfloor \frac{d-1}{2} \rfloor$ de v.

Passo 4: (Verificando os zeros) Calcule a ordem de h em Q_i para cada h encontrada no passo 3 até encontrar um em que $v_{Q_i}(h) \geq -a_i$ para todo $i \notin J$.

Passo 5: Decodifique w como $(h(P_1), \cdots, h(P_n))$.

Saída:$((h(P_1), \cdots, h(P_n))$, que é a única palavra código em $\mathcal{C}$ tal que $d(ev(h), v) \leq \lfloor \frac{d-1}{2}$.

É importante notar que neste algoritmo, no passo em que utiliza a decodificação de lista, Drake [1] utiliza o algoritmo de Guruswami e Sudan [43], contudo, poderia ser substituído por qualquer outro algoritmo de decodificação de lista de códigos AG de um ponto, sem nenhum prejuízo. Drake [1] demonstrou que este algoritmo fornece um decodificador de distância

mínima.

Observe que os dois algoritmos propostos por Drake [1] fornecem a decodificação única de códigos multipontos. Em sua tese, Drake [1] melhorou o limite no número de palavras-código produzidas pelo algoritmo de decodificação de lista e propôs que seja investigado o tamanho médio da lista produzida, visto que o algoritmo de decodificação para códigos multiponto exige que verifiquemos a lista de palavras-chave de saída no supercódigo.

Outra questão relevante investigada nesta tese está relacionada à isometria entre o código multiponto e um subcódigo de um código de um ponto, considerando que é necessário determinar uma função que fornece esta isometria entre os códigos e que não está definida a melhor forma de escolher esta função. Além disso, o Algoritmo 3.4.2, utiliza o máximo divisor comum para substituir as múltiplas funções obtidas, contudo, Drake [1] propõe determinar uma única "melhor"função para esta substituição, o que ainda está em aberto.

Durante esta pesquisa algumas dessas questões elencadas por Drake [1] foram investigadas e alguns resultados são apresentadas no próximo capítulo. Algumas aplicações dos códigos AG multiponto no Capítulo 5.

CAPÍTULO 4

Resultados

Neste capítulo são apresentados os principais resultados obtidos ao longo desta pesquisa relativos à decodificação de lista para os códigos FKS e para códigos Hermitianos generalizados multiponto.

Durante o desenvolvimento dessa pesquisa, os algoritmos utilizados foram implementados utilizando Macaulay2 e Sagemath. No próximo capítulo são apresentados os resultados relativos às aplicações dos códigos Hermitianos generalizados multipontos.

4.1 – Algoritmo de interpolação para a curva FKS

Conforme foi apresentado no Capítulo 2, a curva FKS é uma das generalizações da curva de Hermite e, durante esta pesquisa, foi a primeira generalização a ser investigada.

Observe que a decodificação de lista pode ser dividida em dois passos fundamentais: a interpolação e a fatoração. Nesse sentido, investigamos como adaptar para os códigos FKS o algoritmo de interpolação proposto por Lee e O'Sullivan [53] para códigos de Hermite, o qual é baseado em bases de Gröbner sobre módulos.

Observamos que para adaptar este algoritmo para a curva FKS é necessário alterar alguns parâmetros. Seja $\mathbb{F}$ um corpo finito com r^2 elementos e $\mathcal{X} \subset \mathbb{A}^2$ uma curva plana definida pelo polinômio absolutamente irredutível $X^p - Y^r - Y$ sobre $\mathbb{F}$, com $p|(r+1)$. O anel de coordenadas de $\mathcal{X}$ é

$$R = \mathbb{F}[X, Y]/\langle X^p - Y^r - Y \rangle.$$

Sejam x e y as classes residuais de X e Y, respectivamente. Assim,

$$x^p - y^r - y = 0 \text{ e } R = F[x, y].$$

Seja $\Omega = \{x^i y^j z^k | 0 \leq i, 0 \leq j \leq r-1, 0 \leq k\}$ o conjunto de monômios de $R[z]$. Define-se

o grau de u ponderado para os monômios $x^i y^j z^k$ da seguinte forma

$$deg_u(x^i y^j z^k) = ri + pj + uk.$$

De modo análogo ao algoritmo de interpolação proposto para a curva de Hermite [53] é possível encontrar o polinômio interpolador, que deve ser o elemento da base de $I_{v,m}$ com o menor termo líder com relação à ordem $>_u$.

É importante observar que uma condição importante para a eficiência do algoritmo é que a ordem total $>_u$ definida em $R = \mathbb{F}[x, y]$, também deve determinar uma ordem monomial total no módulo livre $R[z]_l$ sobre $\mathbb{F}[x]$, para a curva de Hermite. Contudo, ao aplicarmos o Algoritmo I para o caso $p < r + 1$ da curva de FKS, se tomarmos $R[z]_l$ como um módulo sobre $\mathbb{F}[x]$, a ordenação total não será mantida no $\mathbb{F}[x]$-módulo, visto que para a curva de FKS o peso de y é igual a r, tal que $r < p$, em que p é o peso de x. Desse modo, y tem o peso maior do que x. Portanto, para preservar a ordenação monomial $>_u$ devemos aplicar o Algoritmo I considerando $R[z]_l$ como um módulo livre sobre $\mathbb{F}[y]$.

Note que o anel $R = \mathbb{F}[x, y]$ pode ser visto como um módulo livre sobre $\mathbb{F}[y]$ com uma base $\{1, x, \cdots, x^{p-1}\}$. Assim, $R[z]_l$ é um módulo livre sobre $\mathbb{F}[y]$ com uma base $\{x^j z^i | 0 \leq i \leq l; 0 \leq j \leq p - 1\}$.

Na construção do ideal $I_{v,m,l}$ definimos $\eta = y^{r^2} - y$, e o conjunto dos geradores de $I_{v,m,l}$ como um módulo sobre $\mathbb{F}[y]$ será

$$\{x^j G_i | 0 \leq i \leq l; 0 \leq j \leq p - 1\}.$$

Seja $T = \{(i, j) | 0 \leq i \leq l, 0 \leq j \leq r - 1\}$, ordenado lexicograficamente. Então, $\{y^j z^i | (i, j) \in T\}$ é uma base para $R[z]_l$ como um $\mathbb{F}[x]$-módulo. O índice de $f \in R[z]_l$ é o maior valor de $(i, j) \in T$ tal que o coeficiente de $y^j x^i$ é não nulo. Note que $ind(y^j G_i) = (i, j)$. O peso de um elemento da base $y^j z^i$ é $ui + (r + 1)j$. Assim, se o termo líder, com relação à $>_u$, de $f \in R[z]_l$ é $x^k y^j z^i$, então $ind(lt(f)) = (i, j)$.

O algoritmo a seguir encontra o elemento de $I_{v,m,l}$ com o menor termo líder para a curva FKS com $p < r + 1$.Observe que o caso $p = r + 1$ corresponde exatamente à curva de Hermite.

Algoritmo de interpolação para curva FKS

Seja $g_{(i,j)} = \sum_{(i',j') \in T} a_{(i,j),(i',j')} x^{j'} z^{i'}$ para $(i, j) \in T$ durante a execução do algoritmo.
Inicialmente, fixe $g_{(i,j)} \leftarrow x^j G_i$ para $(i, j) \in T$.

Passo 1. Fixe $t \leftarrow (0, 0)$.

Passo 2. Tome o sucessor de t. Se $t \in T$, então prossiga. Caso contrário, vá para o **Passo 6**.

Passo 3. Faça $s \leftarrow ind(lt(g_t))$. Se $s = t$, então volte ao **Passo 2**.

Passo 4. Tome $d \leftarrow deg(a_{t,s}) - deg(a_{s,s})$ e $c \leftarrow lc(a_{t,s}) lc(a_{s,s})^{-1}$.

Passo 5. (a) Se $d \geq 0$, então faça

$$g_t \leftarrow g_t - cx^d g_s$$

(b) Se $d < 0$, então, armazene g_s em uma variável temporária,

$$g_s \leftarrow g_t$$

$$g_t \leftarrow x^{-d} g_t - c g_s$$

Volte para o **Passo 3**.

Passo 6. Saída $g_{(i,j)}$ com o menor termo líder, e termina o algoritmo.

A idéia do algoritmo é atualizar o conjunto de geradores até $ind(lt(g_t)) = t$, para todo $t \in T$, nesse momento o conjunto atualizado de geradores é uma base de Gröbner de $I_{v,m,l}$.

Exemplo 13 *Seja $\mathbb{F}$ um corpo finito com q elementos, em que $q = r^2$, $r = 3$ e considere $p = 2$. Considere os seguintes parâmetros $u = 7$, $l = 2$ e a multiplicidade $m = 2$. A curva FKS sobre $\mathbb{F}_9$ é dada por*

$$x^2 - y^3 - y = 0$$

Seja $\mathbb{F} = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$. A base do espaço linear $\mathcal{L}(uQ) = \langle 1, x, y, x^2, xy, y^2, xy^2 \rangle$.

Seja ω a mensagem, ev a palavra código, e o erro e v a mensagem recebida dada por

$\omega = [0, 0, 0, 0, 0, 1, 0]$.

$ev = [0, 2, 2, 1, \alpha + 1, -\alpha - 1, 1, \alpha + 1, -\alpha - 1, 1, -\alpha - 1, \alpha + 1, 1, -\alpha - 1, \alpha + 1]$.

Considere o seguinte vetor com dois erros: $e = [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]$.

$v = [1, 2, 2, 1, \alpha + 1, -\alpha - 1, 1, \alpha + 1, -\alpha - 1, 1, -\alpha - 1, \alpha + 1, 1, -\alpha - 1, \alpha - 1]$.

O polinômio interpolador é

$$H(z) = (\alpha y^5 + xy^3 + \alpha y^4 + (-\alpha + 1)xy^2 + (a - 1)y^3 - \alpha xy$$
$$+\alpha y^2 - y)z^2 + (-y^9 + \alpha y^7 + xy^5 + \alpha y^6 + (-\alpha + 1)xy^4$$
$$+(\alpha - 1)y^5 - \alpha xy^3 + \alpha y^4 - y^3 + y)z + y^{11} + \alpha y^9$$
$$+xy^7 + \alpha y^8 + (-\alpha + 1)xy^6 + (\alpha - 1)y^7 - \alpha xy^5 + \alpha y^6 - y^5 - y^3$$

O polinômio fatorado é

$$H(z) = [y^2 - z][(-\alpha y^5 - xy^3 - \alpha y^4 + (\alpha - 1)xy^2 + (-\alpha + 1)y^3$$
$$+\alpha xy - \alpha y^2 + y)z + y^9 + \alpha y^7 + xy^5 + \alpha y^6$$
$$+(-\alpha + 1)xy^4 + (\alpha - 1)y^5 - \alpha xy^3 + \alpha y^4 - y^3 - y].$$

Portanto, $z = y^2$ é uma das raízes e é a palavra código enviada.

4.2 – Isometria entre códigos multiponto

Os algoritmos de decodificação via listas propostos por Drake [1] fornecem uma decodificação única para códigos AG multiponto utilizando a decodificação de lista. Contudo, para implementar esses algoritmos é necessário fazer uma imersão de um código AG multiponto em um código de um ponto, sobre o qual é aplicado o algoritmo de decodificação de lista. Em seguida, é realizada uma verificação para encontrar qual das palavras da lista estão contidas no código AG multiponto.

Observe que, se o código multiponto for do tipo $\mathcal{C}(D, a_1Q_1 - \sum_{i=2}^{m} a_iQ_i)$, em que $a_i \geq 0$, sabe-se que $\mathcal{L}(a_1Q_1 - \sum_{i=2}^{m} a_iQ_i) \subset \mathcal{L}(a_1Q_1)$, ou seja, é fácil ver que o código multiponto é um subcódigo do código de um ponto $\mathcal{L}(a_1Q_1)$. Contudo, se o código multiponto for do tipo $\mathcal{L}(\sum_{i=1}^{m} a_iQ_i)$, em que $a_i \geq 0$, é necessário encontrar um isomorfismo entre este código e um subcódigo de um código de um ponto.

A fim de determinar uma isometria entre dois códigos $\mathcal{C}(D, G)$ e $\mathcal{C}'(D, G')$ é necessário encontrar uma função que induz o isomorfismo entre os espaços $\mathcal{L}(G)$ e $\mathcal{L}(G')$.

Suponha $G = a_1Q_1 + a_2Q_2 + \cdots + a_mQ_m$ e $G = b_1Q_1 - (b_2Q_2 + \cdots + b_mQ_m)$, com $a_i, b_i \geq 0$, divisores sobre a curva $\mathcal{X}$. Observe que é possível definir um isomorfismo entre $\mathcal{L}(G)$ e $\mathcal{L}(G')$ de modo que $\mathcal{L}(G') \subset \mathcal{L}(b_1Q_1)$.

Em sua tese, Drake [1] ressalta que seria interessante determinar uma maneira ótima de encontrar a função que induz esse isomorfismo e em [17] mostra uma forma exaustiva de busca para esta função.

De acordo com Drake [17], dada uma função h no espaço $\mathcal{L}(G)$, é possível encontrar uma função $f \in \mathbb{F}_q(\mathcal{X})$ tal que $fh \in \mathcal{L}(G')$ reescrevendo G da seguinte forma:

$$G = G_+ - G_-,$$

em que $G_+, G_- \geq 0$.

Em seguida, incremente o valor de $\lambda \in \mathbb{Z}^+$ até que o espaço $l(\lambda degG_+P - \lambda G_+) \neq 0$, isto é, até que exista pelo menos uma função não constante em $\mathcal{L}(\lambda degG_+P - \lambda G_+)$. De fato, uma função qualquer contida nesse espaço induz um isomorfismo entre $\mathcal{L}(G)$ e $\mathcal{L}((\lambda degG_+)P + G - \lambda G_+)$, em que $\mathcal{L}((\lambda degG_+)P + G - \lambda G_+) \subset \mathcal{L}((\lambda degG_+)P)$.

De fato, esse procedimento fornece uma maneira de encontrar esta função para códigos cujo divisor G contém apenas lugares de grau 1. Contudo, durante esta pesquisa, quando consideramos códigos Hermitianos generalizados multiponto propostos por Hu e Zhao [9] sobre $\mathbb{F}_{r^3}$, observa-se que o divisor Q tem grau r e a forma para encontrar a função f proposta por Drake [17] não se aplica diretamente para um divisor contendo lugares de grau > 1.

Nesta seção generalizamos esta forma proposta por Drake [17] para determinar esta função

e, como exemplo, aplicamos para os códigos Hermitianos generalizados [9] quando temos um divisor G contendo pontos de grau > 1. A fim de ilustrar estes fatos apresentamos dois exemplos a seguir.

Exemplo 14 *Considere a curva Hermitiana generalizada sobre $\mathbb{F}_{r^3}$ e um código multiponto $\mathcal{C}(D, uQ + sP)$. Suponha que $u, s \in \mathbb{Z}_+$, e seja $G = G_+ - G_- \Rightarrow G = G_+ = uQ + sP$.*

De acordo com a demonstração do Lema 1 em [17], definindo um divisor da seguinte forma $G_+ - (degG_+)Q$, deveríamos obter um divisor de grau zero, isto é,

$$deg(G_+ - (degG_+)Q) = 0.$$

Contudo, observamos que isso só ocorre se $degQ = 1$.

Observe que quando $degQ = r$, o grau de G será

$$degG = u(degQ) + s(degP) = ur + s.$$

Note que

$$deg(G_+ - (degG_+)Q) = degG_+ - (ur+s)degQ = (ur+s) - (ur+s)r = (ur+s)(1-r) = 0$$

Porém, isso é um absurdo já que $r > 1$, pois r é uma potência de primo.

Portanto, este método para determinar a função f que se baseia na demonstração do Lema 1 [17] não pode ser aplicada de forma direta para obter um isomorfismo entre códigos multipontos propostos por Hu e Zhao [9]. Verificamos que é necessário considerar o $degQ$, conforme é apresentado a seguir.

Considere um código Hermitiano generalizado multiponto $\mathcal{C}(D, uQ + sP)$ como descrito no capítulo 2. Desse modo, $G = uQ + sP$, em que $degQ = r$ e $degP = 1$. Seja $G = G_+ - G_-$, tal que $G = G_+ = uQ + sP$.

Suponha que $u, s \in \mathbb{Z}_+$. Como $\mathbb{F}_q$ é um corpo finito, então a classe dos divisores de grau zero é finita. Portanto, existe uma função f cujo divisor tem grau zero

$$deg((degQ)G_+ - (degG_+)Q) = 0,$$

ou seja, (f) pode ser escrito como

$$(f) = \lambda((degQ)G_+ - (degG_+)Q)$$

para algum $\lambda \in \mathbb{Z}_+$.

Observe que

$$deg((degQ)G_+ - (degG_+)Q) = (degQ)(degG_+) - (degG_+)(degQ) = r(ur+s) - (ur+s)r = 0.$$

Logo,

$$f \in \mathcal{L}(\lambda((degG_+)Q - (degQ)G_+)),$$

para algum $\lambda \in \mathbb{Z}_+$.

Desse modo, dada uma função $h \in \mathcal{L}(G)$, temos

$$fh \in \mathcal{L}(\lambda((degG_+)Q - (degQ)G_+) + G) = \mathcal{L}(\lambda(degG_+)Q - (\lambda degQ - 1)G_+ - G_-).$$

Portanto, $\mathcal{L}(G)$ e $\mathcal{L}(\lambda(degG_+)Q - (\lambda degQ - 1)G_+ - G_-)$ são isomorfos.

Além disso, $\mathcal{L}(\lambda(degG_+)Q - (\lambda degQ - 1)G_+ - G_-) \subset \mathcal{L}(\lambda(degG_+)Q$. Observe que se $degQ = 1$, este resultado é reduzido ao caso apresentado no Lema 1 em [17].

Exemplo 15 *Considere um código Hermitiano generalizado multiponto* $(C)(D, 5Q + 3P)$ *sobre* $\mathbb{F}_{r^3}$*, com* $r = 2$*, isto é, um código sobre* $\mathbb{F}_8$*. Considere* $\lambda = 7$ *e existe uma função* $f \in \mathcal{L}(21Q - 42P)$ *que define um isomorfismo entre* $\mathcal{L}(5Q + 3P)$ *e* $\mathcal{L}(26Q - 39P)$*.*

Seja $f = x^6y^9 \in \mathcal{L}(21Q - 42P)$*, observe que*

$$\mathcal{L}(5Q + 3P) = \langle x^2y, xy, x^2, x, 1, x^3y^{-1}, x^2y^{-1}, xy^{-1}\rangle,$$

e, multiplicando cada função $h \in \mathcal{L}(5Q + 3P)$ *por* f *temos:*

$$\mathcal{L}(26Q - 39P) = \langle x^8y^{10}, x^7y^{10}, x^8y^9, x^7y^9, x^6y^9, x^9y^8, x^8y^8, x^7y^8\rangle.$$

4.3 – Algoritmo de decodificação via lista para códigos AG multiponto

O algoritmo de decodificação proposto por Drake [1] utiliza o algoritmo de decodificação de lista Guruswami-Sudan para obter uma lista que contém a palavra enviada. Em seguida, verifica dentre as palavras da lista qual delas está a uma distância da palavra recebida menor que a metade da distância mínima do código e pertence ao código multiponto.

Considere, por exemplo, um código AG de dois pontos do tipo $\mathcal{C}(D, aQ_1 - bQ_2)$, com $a, b \in \mathbb{Z}_+^*$, com parâmetros $[n, k, d]$. Este código é um subcódigo do código de um ponto $\mathcal{C}(D, aQ_1)$, sobre o qual é aplicado o algoritmo de interpolação. Em seguida, verifica-se quais palavras da lista estão a uma distância $d' \leq \frac{d-1}{2}$. Por fim, verifica-se quais palavras tem zeros de ordem pelo menos b em Q_2. Desse modo obtém-se apenas uma palavra código que pertence a $\mathcal{C}(D, aQ_1 - bQ_2)$.

Nesta seção apresentamos uma adaptação deste algoritmo. Inicialmente, observa-se que o algoritmo de interpolação pode ser substituído por outros algoritmos de decodificação de lista e consideramos nesta tese o algoritmo proposto por Lee e O'Sullivan [53] que utiliza bases de Gröbner para encontrar o polinômio interpolador.

Observe que o algoritmo de interpolação proposto por Lee e O'Sullivan [52] é aplicado aos códigos de Hermite de um ponto, o qual foi generalizado para a curva FKS nesta tese. Além disso, Lax [59] mostrou que ele pode ser aplicado de modo mais geral para códigos AG de um ponto. Este algoritmo foi utilizado para a interpolação nesta tese pela eficiência de implementação, utilizando bases de Gröbner para obter o polinômio interpolador.

Na próxima seção é apresentada uma adaptação do algoritmo de decodificação via listas proposto por [1]. A ideia geral é substituir os passos 3 e 4 do algoritmo por um único passo, visto que a fatoração utilizando o algoritmo *Root-Finding* permite identificar diretamente a palavra-código que pertence ao código multiponto, comparando as bases dos espaços de Riemann-Roch.

Algoritmo de decodificação de lista

Entrada: Seja $\mathcal{C}(D, \sum_{i=1}^{m} a_i Q_i)$, com $a_i \in \mathbb{Z}$ com parâmetros $[n, k, d]$.
Inicialização:

- Se $a_j > 0$, para algum j, e $a_i \leq 0$, $\forall j \neq i$, então $\mathcal{C}(D, \sum_{i=1}^{m} a_i Q_i) \subset \mathcal{C}(D, a_j Q_j)$. Neste caso, $\mathcal{C}(D, G') = \mathcal{C}(D, \sum_{i=1}^{m} a_i Q_i)$.

- Caso contrário, encontre uma isometria entre o código $\mathcal{C}(D, \sum_{i=1}^{m} a_i Q_i)$ e um subcódigo $\mathcal{C}(D, G')$ de um código de um ponto $\mathcal{C}(D, a_j Q_j)$, de modo que $\mathcal{C}(D, G') \subset \mathcal{C}(D, a_j Q_j)$.

Passo 1: Aplique um algoritmo para obter um polinômio interpolador $H(z)$ no código de um ponto $\mathcal{C}(D, a_j Q_j)$.

Passo 2: Aplique o algoritmo de fatoração *Root-Finding* considerando a base do código multiponto $\mathcal{C}(D, G')$ e obtenha uma lista com L funções, que correspondem às raízes do polinômio $H(z)$.

Saída:

- Se $L = 1$ então, a única função h na lista corresponde exatamente à palavra código que foi enviada, que será $(h(P_1), h(P_2), \cdots, h(P_n))$.

- Caso contrário, tem-se uma lista de L palavras que pertencem ao código multiponto.

Destacamos que para aplicar o Algoritmo *Root Finding* para a fatoração sobre a base do código multiponto $\mathcal{C}(D, G)$ a ordenação monomial é um fator importante. Observa-se que para um código AG um ponto, ou seja, $G = uQ$, usando a ordenação lexicográfica ponderada, os pesos das variáveis coincidem com as valorizações das funções x,y e z no ponto Q.

Ao longo da pesquisa diversas ordenações monomiais foram testadas para códigos multiponto. De modo geral, buscou-se definir a ordenação lexicográfica ponderada para um espaço de funções gerado por um divisor multiponto G de modo análogo ao que é apresentado por Wu e Siegel [49], isto é, utilizando as valorizações das funções x,y e z em todos os pontos de G.

Contudo, apenas com a realização da imersão do código multiponto em um código de um ponto foi possível executar o Algoritmo *Root-Finding* considerando a ordenação obtida com relação ao código de um ponto. Portanto, os monômios pertencentes à base do código multiponto devem ser odenados conforme a ordenação da base do código de um ponto.

Exemplo 16 *Considere $\mathcal{X}$ a curva Hermitiana generalizada sobre $\mathbb{F}_8$, em que $r = 2$. Observe que o espaço $\mathcal{L}(5Q - 2P) = \langle x^2y, x^2, xy\rangle$ está contido em $\mathcal{L}(5Q) = \langle x^2y, x^2, xy, x, 1\rangle$.*

Observou-se durante a execução do Algoritmo Root-Finding a busca pelos coeficientes das funções da base do código $\mathcal{L}(5Q - 2P)$ deve seguir uma ordenação monomial baseada na valorização do ponto Q, pois esta base está contida em $\mathcal{L}(5Q)$. Seja $v_Q(x) = -r^2 = -4$ e $v_Q(y) = -r = -2$, observe que

$$v_Q(x^2y) = 2 \cdot v_Q(x) + v_Q(y) = -8 - 2 = -10,$$

$$v_Q(x^2) = 2 \cdot v_Q(x) = -8,$$

$$v_Q(xy) = v_Q(x) + v_Q(y) = -4 - 2 = -6,$$

$$v_Q(x) = -4,$$

$$v_Q(1) = 0.$$

Portanto, a base do espaço de Riemann-Roch $\mathcal{L}(5Q)$ deve ser colocada no algoritmo da seguinte forma $[\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5] = [x^2y, x^2, xy, x, 1]$, com as respectivas valorizações no ponto Q $[-10, -8, -6, -4, 0]$.

No exemplo 17 mostra que o Passo 2 do Algoritmo de decodificação de lista proposto consiste em fatorar o polinômio interpolador, obtido no Passo 1, através da busca dos coefifientes das funções da base do código multiponto.

Exemplo 17 *Considere o código multiponto conforme o exemplo 16 e $h \in \mathcal{L}(5Q - 2P)$. Note que*

$$h = a_0x^2y + a_1x^2 + a_2xy$$

pode ser reescrita na base de $\mathcal{L}(5Q)$ como

$$h = a_0x^2y + a_1x^2 + a_2xy + a_3x + a_4,$$

em que $a_3 = a_4 = 0$. Portanto, se h é raiz de um polinômio interpolador $H(z)$, obtido sobre o código de um ponto associado ao espaço $\mathcal{L}(5Q)$, e sabe-se que a palavra-código enviada

pertence ao espaço $\mathcal{L}(5Q-2P)$, a busca na fatoração pode ser restrita à base desse espaço. Desse modo, observa-se que o passo 3 do Algoritmo III [1] não é necessário quando se utiliza o algoritmo Root-Finding sobre a base de $\mathcal{L}(5Q-2P)$. Assim, pode-se obter diretamente a palavra que pertence ao código multiponto.

Exemplo 18 *Seja $\mathcal{X}$ uma curva Hermitiana generalizada sobre $\mathbb{F}_8$. Considere o código multiponto $\mathcal{C}(D, 5Q-P)$ com parâmetros $[28, 4, 20]$. Observe que $\mathcal{L}(5Q-P) \subset \mathcal{L}(5Q)$.*

Usando a decodificação proposta por Drake [1] podemos aplicar um algoritmo de decodificação de lista sobre $\mathcal{L}(5Q)$. Considere o algoritmo de interpolação [59] e teremos:

Seja $w = [1,0,0,1]$ a mensagem a ser enviada e a base do espaço $\mathcal{L}(5Q-P) = \langle x^2y, x^2, xy, x\rangle$, então a mensagem enviada na base do espaço será $c = x^2y + x$.

A palavra código é $ev = [0, \alpha, \alpha^2, \alpha^2+\alpha, \alpha^2+\alpha, \alpha^2+1, \alpha^2, \alpha^2+\alpha+1, \alpha, \alpha^2+\alpha+1, 0, \alpha^2+1, a, \alpha+1, \alpha^2+\alpha+1, \alpha^2+\alpha, 0, \alpha^2+\alpha+1, \alpha^2, \alpha+1, \alpha^2, \alpha, \alpha^2+1, \alpha+1, 0, \alpha+1, \alpha^2+\alpha, \alpha^2+1]$.

Introduzindo um único erro na posição 23 *da mensagem obter a palavra recebida*

$v = [0, \alpha, \alpha^2, \alpha^2+\alpha, \alpha^2+\alpha, \alpha^2+1, \alpha^2, \alpha^2+\alpha+1, \alpha, \alpha^2+\alpha+1, 0, \alpha^2+1, \alpha, \alpha+1, \alpha^2+\alpha+1, \alpha^2+\alpha, 0, \alpha^2+\alpha+1, \alpha^2, \alpha+1, \alpha^2, \alpha, \alpha^2, \alpha+1, 0, \alpha+1, \alpha^2+\alpha, \alpha^2+1]$.

A partir da palavra recebida, aplicando o algoritmo de interpolação obtemos:

$$Hv = (\alpha^2+\alpha+1)xy^7+(\alpha^2)x^8y^3+x^6y^4+(\alpha+1)x^2y^6+(\alpha^2)x^5y^4+xy^6+(\alpha^2)x^{10}y+(\alpha)x^8y^2$$

$$+(\alpha^2+1)x^4y^4+(\alpha^2+\alpha+1)x^2y^5+x^9y+x^7y^2+(\alpha^2+\alpha)x^5y^3+(\alpha^2)xy^5+(\alpha^2+\alpha)x^{10}+$$

$$(\alpha^2)x^6y^2+(\alpha)x^4y^3+x^7y+(\alpha+1)x^4y^2+(\alpha)y^4+(\alpha)x^5y+x^3y^2+xy^3+(\alpha^2+\alpha)x^4y+$$

$$(\alpha^2+\alpha)x^2y^2+(\alpha^2)x^3y+(\alpha)xy^2+(\alpha^2+1)x^2y+(\alpha+1)xy,$$

e o ideal $I = \langle x^3y^2+x^2y^4+y-x^4\rangle + \langle x^8-x, y^8-y, z-Hv\rangle^m$. Assumindo $m=3$, satisfazendo a condição $\delta < n - \frac{\mu}{m}$, temos o seguinte polinômio interpolador:

$$H(z) = x^2y^3z^2+(\alpha^2)x^4y^3z+(\alpha^2+\alpha)x^6y^3+y^2z^3+(\alpha^2)x^7y^2+(\alpha^2)x^5y^3+(\alpha^2)x^2y^2z^2+$$

$$(\alpha^2+\alpha)x^4y^2z+x^8y+x^4y^3+x^3yz^2+xy^2z^2+(\alpha^2)yz^3+(\alpha^2+\alpha)x^5y^2+(\alpha^2+\alpha)x^2yz^2+x^6z+$$

$$x^2y^2z+xz^3+(\alpha^2)x^8+(\alpha^2+1)x^4y^2+(\alpha^2)xyz^2+(\alpha^2+\alpha)z^3+x^7+x^5y+x^3y^2+x^2z^2+$$

$$(\alpha^2+1)x^2yz+(\alpha)x^4y+(\alpha^2+\alpha)xz^2+x^3z+(\alpha^2+1)x^3y+(\alpha^2+\alpha)x^2z+x^4+(\alpha^2+\alpha)x^3.$$

Aplicando o algoritmo de fatoração Root-Finding com relação à base do código multiponto $\mathcal{C}(D, 5Q-P)$ obtém-se uma única palavra código, que corresponde à mensagem enviada $z = x^2y + x$ e um fator irredutível de grau 2.

Observe que ao realizar a fatoração do polinômio interpolador considerando a base do código multiponto, o passo 3 do algoritmo proposto por Drake [1] é eliminado. Além disso,

se a busca pela função h não for restrita à um raio dentro da metade da distância mínima do código, pode-se obter uma lista de L funções, ao invés de uma única palavra, pois é esta restrição que torna os algoritmos apresentados por Drake [1] algoritmos de decodificação única. Como trabalho futuro, pode-se investigar melhor a relação entre o tamanho da lista obtida fatorando sobre o código de ponto conforme proposto por Drake [1] e o tamanho da lista obtida fatorando sobre o código multiponto, conforme proposto nesta tese.

Durante o desenvolvimento da pesquisa surgiram dificuldades de implementação utilizando o software Macaulay2, devido à limitação do software quanto à depuração dos erros. Portanto, buscou-se outro software gratuito de código aberto, o SageMath, que utiliza uma linguagem baseada em Python e consiste em uma alternativa viável de código aberto para Magma, Maple, Mathematica e Matlab.

No capítulo seguinte são apresentadas algumas aplicações dos códigos Hermitianos generalizados multiponto.

CAPÍTULO 5

Aplicações

Os códigos AG fornecem sequências de código assintoticamente boas com parâmetros melhores do que o limite de Gilbert-Varshamov em uma certa faixa da taxa e para alfabetos suficientemente grandes [60, 61]. Além disso, tais códigos são fáceis de descrever, codificar e decodificar. Os parâmetros de um código AG são estritamente dependentes da curva escolhida na construção. Nesta tese, os códigos Hermitianos generalizados são utilizados para aplicações em sistemas que usam espalhamento espectral com salto em frequência. Os códigos de Hermite foram amplamente investigados e apresentaram um bom desempenho em diversas aplicações [62], incluindo a geração de sequências para salto em frequência. Considerando que os códigos Hermitianos generalizados apresentados nesta tese são uma classe dos códigos AG que contém os códigos de Hermite, apresentaremos o desempenho desses códigos para esta aplicação em comparação com os códigos RS e códigos de Hermite.

Códigos Hermitianos generalizados multiponto podem atingir parâmetros melhores do que os códigos de Hermite, visto que a curva generalizada tem um número de pontos maior do que a curva de Hermite [9]. Nesta pesquisa, investigamos o desempenho desses códigos usando a probabilidade de erro de pacote para canais AWGN e para canais com interferência de banda parcial. Além disso, resultados analíticos e experimentais sobre o número de usuários nos sistemas FH-CDMA e a taxa de colisões entre sequências são apresentados para mostrar que tais códigos têm vantagens sobre os códigos RS e os códigos de Hermite.

Existem duas principais técnicas de espalhamento espectral: espectro de dispersão por saltos em frequência (*Frequency-Hopping Spread Spectrum* - FHSS) e espectro de dispersão por sequência direta (*Direct Sequence Spread Spectrum* - DSSS). Apresentamos a seguir o desempenho de códigos Hermitianos generalizados multiponto para gerar padrões de saltos em frequência (FH) para redes de rádio de pacotes [19] e sistemas de múltiplo acesso por divisão por código (CDMA) [63], nos quais vários usuários compartilham uma certa largura de banda, com uma certa probabilidade de erro.

Um sistema FH-CDMA pode ser considerado como um esquema de transmissão de pacotes, em que o tempo é dividido em intervalos de comprimento iguais ao tempo que leva para

transmitir um pacote (mais um tempo de guarda) e cada pacote pode ser considerado uma única palavra código [63]. O desempenho desse tipo de sistema pode ser medido usando a taxa de transferência do canal de múltiplo acesso, que é o número médio de transmissões de pacote bem sucedidas por unidade de tempo. Aumentar esta taxa significa aumentar o número de usuários que transmitem e maximiza simultaneamente a transmissão de informações confiáveis. Assis e Alencar [63] mostraram que usando códigos de Hermite, em vez de códigos RS, é possível obter um melhor desempenho para aplicações que não requerem transmissão em tempo real.

Macdonald e Pursley [19] mostraram que os códigos de Hermite também são uma alternativa atraente aos códigos RS para uso em redes de rádio por pacotes com espalhamento espectral por saltos em frequência. Os resultados analíticos para a probabilidade de erro de pacote para transmissões usando salto em frequência comprovam a vantagem dos códigos de Hermite para o canal de ruído branco gaussiano aditivo (AWGN) e para os canais de interferência de banda parcial. Em geral, à medida que a taxa do código diminui ou o tamanho do alfabeto do símbolo aumenta, o desempenho relativo dos códigos Hermitianos melhora em relação aos códigos RS.

A fim de apresentar de forma clara a análise de desempenho dos códigos Hermitianos generalizados para estas aplicações, que é baseada em outros trabalhos que comparam códigos RS e de Hermite [18, 19, 63], a notação utilizada neste capítulo é apresentada ao longo do texto de forma análoga aos trabalhos citados sempre que possível.

5.1 – Sistemas de Salto em Frequência

Técnicas de espalhamento espectral têm diversas aplicações, tais como sistemas de posicionamento global (GPS), redes locais sem fio (WLAN), interconexão celular e múltiplo acesso por divisão de código (CDMA), que permite que vários usuários acessem o sistema de comunicação simultaneamente [64].

Um sistema CDMA usa a modulação por espalhamento de espectro enquanto transmite sinais de múltiplos usuários na mesma banda de frequência ao mesmo tempo. Todos os sinais usam todo o espectro alocado, mas as sequências de propagação ou os padrões de salto de frequência diferem [63]. Sistemas CDMA são resistentes à interferência e à interceptação, tornando-os a escolha da maioria das redes de comunicação móvel [65].

Salto em frequência é uma técnica de espalhamento espectral que envolve o particionamento da banda de frequência alocada, chamada banda de salto, em um grande número de sub-bandas menores. A transmissão é realizada em rajadas curtas em uma sub-banda por vez, pulando de sub-banda para sub-banda de uma forma pseudo-aleatória [64]. Esta técnica é amplamente aplicada em sistemas de comunicação e várias pesquisas foram desenvolvidas para melhorar o desempenho de esquemas de salto em frequência [66–71].

O desempenho dos códigos Hermitianos generalizados multiponto é apresentado usando a probabilidade de colisões entre duas sequências geradas por um código. Além disso, as medidas de região alcançável e taxa de transferência para sistemas FH-CDMA serão usadas.

Considerando que esses sistemas podem ser vistos como um esquema de transmissão em pacotes, em que cada pacote é visto como uma palavra código, são apresentados neste capítulo os resultados da probabilidade de erro de pacote para alguns tipos de canais de transmissão. Esta análise foi apresentada por Macdonald e Pursley [19] para redes de rádio por pacotes para códigos de Hermite e códigos RS. A descrição dos sistemas, os tipos de canais e as medidas de desempenho utilizadas nesta pesquisa são apresentadas nas próximas seções.

5.2 – Sistemas FH-CDMA

Considere o esquema FH-CDMA representado na Figura 5.1. De modo análogo ao que foi apresentado por Assis [18], apresentamos o seguinte procedimento para gerar padrões de saltos em frequência utilizando códigos Hermitianos generalizados multiponto.

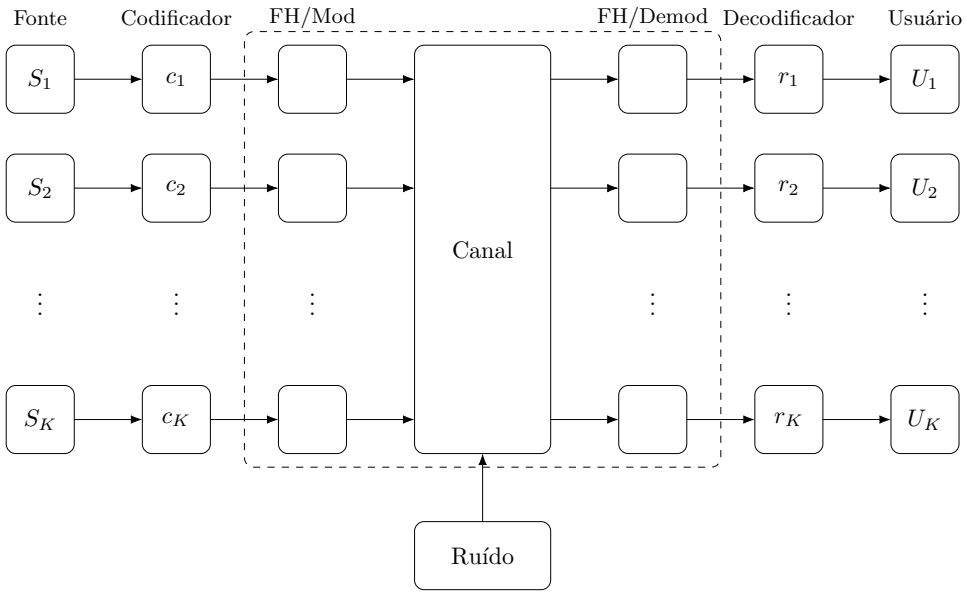

Figura 5.1 – Sistema de comunicação FH-CDMA.

Considere um código multiponto Hermitiano generalizado $\mathcal{C}_{HG}(D, uQ+sP)$ sobre $\mathbb{F}_q$, com $D = P_1 + \cdots + P_n$. para cada função $h \in \mathcal{L}(uQ + sP)$ o padrão de salto em frequência é gerado pelo seguinte procedimento:

I. Uma regra $S(\cdot)$ é definida para o mapeamento dos elementos do corpo em frequências;

II. Cada frequência é dada por $f_j(h) = S(h(P_i))$, para $j = 1, 2, \cdots, q$ e $i = 1, 2, ..., n$, em que $f_j(h)$ é a j-ésima frequência, mapeada pela função h.

Dizemos que existe uma colisão entre duas sequências de um código linear $\mathcal{C}(n, k, d)$, $c = (c_1, c_2, \cdots, c_n)$ e $c' = (c'_1, c'_2, \cdots, c'_n)$, quando elas coincidem em alguma posição, ou seja, $c_i = c'_i$, para algum i. Observe que o número máximo de colisões entre quaisquer duas

sequências geradas por um código com distância mínima d e comprimento n é dado por $n-d$. Portanto, a probabilidade de colisões entre quaisquer duas sequências do código $\mathcal{C}$ pode ser estimada pela razão entre o número máximo de colisões possíveis e o comprimento dessas sequências, que será denotada por η, e definida por $\eta = (n-d)/n = 1 - d/n$.

Para um código RS e um código de Hermite sobre $\mathbb{F}_q$, a probabilidade de colisões é dada, respectivamente, por [18]

$$\eta_{RS} = \frac{1}{2} - \frac{1}{2\sqrt{q}} - \frac{1}{q} \simeq \frac{1}{2}, \tag{5.1}$$

e

$$\eta_H = \frac{1}{\sqrt{q}} - \frac{1}{q} - \frac{1}{q\sqrt{q}} \simeq \frac{1}{\sqrt{q}}. \tag{5.2}$$

Seja $\mathcal{C}_{HG} := \mathcal{C}(D, uQ + sP)$ um código Hermitiano generalizado multiponto $\mathbb{F}_{r^3}$ com parâmetros (n_{HG}, k_{HG}, d_{HG}). A probabilidade de colisões é dada por

$$\eta_{HG} = 1 - \frac{d_{HG}}{n_{HG}} = \frac{r^4 - 3r + 1}{r^5 - r^2} \simeq \frac{1}{r} = \frac{1}{\sqrt[3]{q}}. \tag{5.3}$$

Observe que há um pequeno aumento na probabilidade de colisões para códigos Hermitianos generalizados, ou seja, $\eta_{HG} > \eta_H$. Contudo, o seu desempenho deve considerar o número máximo de usuários no sistema e, neste caso, o número de usuários em sistemas utilizando códigos Hermitianos generalizados cresce mais rapidamente do que a probabilidade de colisões.

Considere que o número máximo de usuários no sistema FH-CDMA é dado por $U = q^k$ para um código $\mathcal{C}(n,k,d)$ sobre $\mathbb{F}_q$. Observe que para códigos RS, este número será limitado pelo número de elementos do corpo finito, pois $k < n = q$ [18].

Uma das vantagens do uso de códigos AG é a possibilidade de aumentar o número de usuários em sistemas FH-CDMA sem aumentar o alfabeto utilizado para gerar os padrões de salto, ou seja, sem aumentar o corpo finito utilizado para construir o código. Observe que aumentando o comprimento do código é possível aumentar sua dimensão e, consequentemente, o número máximo de usuários do sistema.

Para um dado alfabeto M, que pode ser mapeado em q frequências, os códigos Hermitianos generalizados mostram um aumento significativo no número de usuários, mantendo uma boa probabilidade de colisões η entre as sequências, o que significa que a probabilidade de um usuário escolher o mesmo padrão de salto em frequência usando códigos Hermitianos generalizados permanece próxima da probabilidade de um usuário escolher o mesmo padrão de salto em frequência usando códigos de Hermite ou códigos RS.

Assis e Alencar [63] mostraram que os códigos de Hermite apresentam um desempenho melhor nos sistemas FH-CDMA em relação aos códigos RS. Para comparar os códigos de Hermite $\mathcal{C}_H$ e os códigos Hermitianos generalizados $\mathcal{C}_{HG}$, devemos usar o mesmo alfabeto $\mathbb{F}_q$. Portanto, observe que para códigos de Hermite devemos ter $\mathbb{F}_{\tilde{r}^2}$ e para os códigos Hermitianos

generalizados devemos ter $\mathbb{F}_{r^3}$, de modo que $q = \overline{r}^2 = r^3$, para $\overline{r}$ e r potências de primo. Isto implica que o número máximo de usuários utilizando tais códigos é dado, respectivamente, por

$$U_H = q^{\frac{\overline{r}-\sqrt{\overline{r}}}{2}} \tag{5.4}$$

e

$$U_{HG} = q^{k_{HG}} = q^{ur+s-\frac{r^4-3r}{2}}. \tag{5.5}$$

Substituindo os valores $\overline{r} = \sqrt{q}$ e $r = \sqrt[3]{q}$ nas Equações 5.5 e 5.4 temos

$$U_H = q^{\frac{\sqrt{q}-\sqrt[4]{q}}{2}} \simeq q^{q^{1/2}} \tag{5.6}$$

e

$$U_{HG} = q^{\frac{\sqrt[3]{q^4}-3\sqrt[3]{q}}{2}} \simeq q^{q^{4/3}}. \tag{5.7}$$

Observe que $U_{HG} > U_H$. Portanto, conforme pode-se observar nas tabelas 5.2 e 5.3, o número máximo de usuários permitido em um sistema FH-CDMA usando códigos Hermitianos generalizados está bem acima do número máximo de usuários em sistemas com códigos de Hermite.

As tabelas 5.1 e 5.2 mostram que uma das vantagens de usar códigos de Hermite em vez de códigos RS é a possibilidade de aumentar o número de usuários sem aumentar o alfabeto M (corpo finito). No Exemplo 19, pode-se observar que os sistemas FH-CDMA usando códigos de Hermite possuem uma probabilidade de colisões menor do que os sistemas que usam os códigos RS.

Exemplo 19 *Considere dois sistemas com o mesmo número de usuários, um utilizando um código RS $\mathcal{C}_{RS}$ com dimensão k_{RS} e outro utilizando um código de Hermite $\mathcal{C}_H(D, uP)$ com dimensão $k_H = u - g + 1$. De acordo com o que foi mostrado por Assis [18], devemos ter $k_{RS} = u - g + 1$. Sejam os códigos RS e Hermite definidos sobre $\mathbb{F}_{16}$. A curva de Hermite é definida por $\mathcal{X} := y^4 + y = x^5$. Observe que $\eta_{RS} = \frac{1}{2} - \frac{\sqrt{q}}{2q} - \frac{1}{q} \approx 0.31$ e $\eta_H = \frac{1}{\sqrt{q}} - \frac{1}{q} - \frac{1}{q\sqrt{q}} \approx 0.17$. Portanto, o código de Hermite apresenta uma taxa de colisão menor do que os códigos RS, isso significa um melhor desempenho para gerar sequências nos sistemas FH-CDMA.*

Os exemplos 20 e 21 mostram dois códigos Hermitianos generalizados para os quais é possível observar o desempenho comparado aos códigos RS, que são comumente usados para salto de frequência.

Exemplo 20 *Seja $\mathcal{C}_{RS}(8, 3)$ um código RS estendido com $n_{RS} = 8$ e $d_{RS} = 6$. Observe que gerando sequências para sistemas FH-CDMA usando este código, podemos ter no máximo $U_{RS} = 8^3 = 512$ usuários e a probabilidade de colisões $\eta_{RS} = 0.25$. O código Hermitiano generalizado $\mathcal{C}_{HG} = \mathcal{C}(D, 5Q - P)$ sobre $\mathbb{F}_8$ com parâmetros $(28, 6, 18)$ fornece um sistema*

com o número máximo de usuários $U_{HG} = 8^6 = 262144$ *para* $\eta_{HG} = 0.36$*. Embora a probabilidade de colisões obtida para códigos RS seja ligeiramente inferior à taxa obtida pelo código Hermitiano generalizado, observe que o número máximo de usuários permitido pelo sistema usando este último é bem maior do que num sistema usando o código RS. Portanto, isso indica que tais códigos podem ser uma alternativa melhor do que os códigos RS para sistemas FH-CDMA.*

Exemplo 21 *Considere o código de um ponto Hermitiano generalizado* $\mathcal{C}_{HG} = \mathcal{C}(D, 4Q)$ *sobre* $\mathbb{F}_8$ *com parâmetros* $(30, 4, 22)$*. Observe que a probabilidade de colisões* $\eta_{HG} = 1 - \frac{d}{n} = 0.26$ *se aproxima da mesma probabilidade obtida pelo código RS do Exemplo 20, mas o número de usuários é* $U_{HG} = 8^4 = 4096$*, que é muito maior do que quando o código RS é usado.*

Tabela 5.1 – Códigos Hermitianos Generalizados Multiponto $\mathcal{C}_{u,s}$ com taxa $1/2$ sobre $\mathbb{F}_{r^3}$.

r	$q = r^3$	$n = (r^3 - 1)r^2$	k	$U = q^k$	η
2	8	28	14	8^{14}	0.50
3	27	234	117	27^{117}	0.33
4	64	1008	504	64^{504}	0.25
5	125	3100	1550	125^{1550}	0.20
7	343	16758	8379	343^{8379}	0.14
8	512	32704	16352	512^{16352}	0.13
9	729	58968	29484	729^{29484}	0.11
12	1728	248688	124344	1728^{124344}	0.08
16	4096	1048320	524160	4096^{524160}	0.06

Tabela 5.2 – Códigos de Hermite $\mathcal{C}_H(D, uP)$ com taxa $1/2$ sobre $\mathbb{F}_{\overline{r}^2}$.

$\overline{r}$	$q = \overline{r}^2$	$n = \overline{r}^3$	k	$U = q^k$	η
2	4	8	4	4^4	0.50
3	9	27	13	9^{13}	0.33
4	16	64	32	16^{32}	0.25
5	25	125	62	25^{62}	0.20
7	49	343	171	49^{171}	0.14
8	64	512	256	64^{256}	0.13
9	81	729	364	81^{364}	0.11
12	144	1728	864	144^{864}	0.08
16	256	4096	2048	256^{2048}	0.06
64	4096	262144	131072	4096^{131072}	0.02

Além da análise da probabilidade de colisões entre duas sequências, pode-se considerar a probabilidade de erro quando ocorre uma colisão para comparar o desempenho dos códigos.

Tabela 5.3 – Códigos Reed-Solomon $\mathcal{C}_{RS}$ com taxa $1/2$ sobre $\mathbb{F}_q$.

q	$n = q$	k	$U = q^k$	η
8	8	4	8^4	0.50
27	27	13	27^{13}	0.33
64	64	32	64^{32}	0.25
125	125	62	125^{62}	0.20
343	343	172	343^{172}	0.14
512	512	256	512^{256}	0.13
729	729	364	729^{364}	0.11
1728	1728	864	1728^{864}	0.08
4096	4096	2048	4096^{2048}	0.06

Considere o esquema de múltiplo acesso com K pares de fonte-usuário conforme a Figura 5.1, em que cada par fonte-usuário tem um padrão de salto em frequência único. Os padrões de salto são modelados como independentes, distribuídos de forma idêntica no conjunto de intervalos de frequência q. Os dados (M-ários) de cada fonte são codificados por codificadores idênticos. Cada par fonte-usuário K corresponde a um canal discreto sem memória. Quando a informação secundária não está disponível, o canal é modelado como um canal simétrico sem memória M-ário com probabilidade de erro $\frac{P_{h,K}(M-1)}{M}$, em que a probabilidade $P_{h,K}$ de um dos outros $K-1$ usuários pular para a mesma frequência. Isto implica que, se ocorrer uma colisão, o demodulador terá a mesma probabilidade de escolher qualquer um dos símbolos transmitidos.

Dado que há q faixas de frequência disponíveis e que todos os padrões de salto são independentes, a probabilidade $P_{h,K}$ é dada por [72]

$$P_{h,K} = 1 - (1 - p_h)^{-1}, \tag{5.8}$$

em que

$$p_h = \begin{cases} \frac{2}{q} - \frac{1}{q^2}, & \text{assíncrono,} \\ \frac{1}{q}, & \text{síncrono,} \end{cases} \tag{5.9}$$

é a probabilidade de outro usuário pular (por alguma parte do tempo de permanência) para a mesma frequência. Supõe-se que sempre que dois ou mais usuários ocupem o mesmo intervalo de frequência ao mesmo tempo, a probabilidade de erro é $(M-1)/M$, ou seja, o demodulador tem a mesma probabilidade de escolher qualquer um dos M diferentes símbolos [63, 73]. Nesta tese, apenas o caso assíncrono é considerado, do mesmo modo que foi feito por Assis [63].

Uma medida útil para projetar sistemas adaptativos é a dada pela relação entre o número de usuários e a taxa do código, chamada de região alcançável, pois esses sistemas ajustam a taxa do código de acordo com o tráfego de canal [63]. Para probabilidade fixa P_e', uma generalização da aproximação para a região alcançável pode ser obtida pela relação [73]

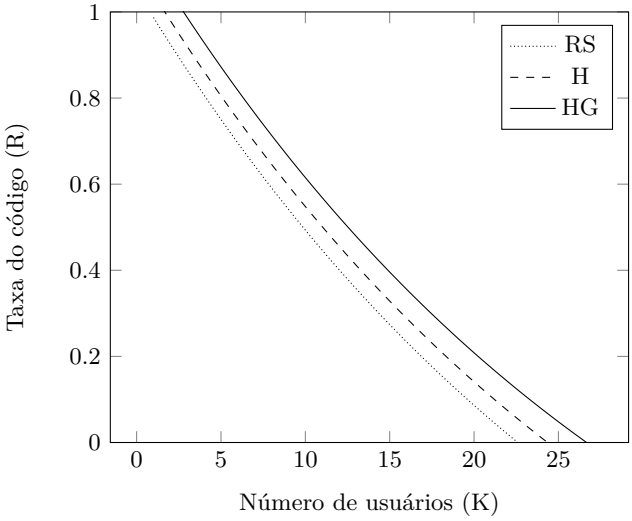

Figura 5.2 – Região alcançável para códigos sobre $\mathbb{F}_{64}$ com $\mathcal{R} = 1/2$ e $P_e \leq 10^{-3}$.

$$K \leq 1 + \frac{ln(\frac{1-g/n+R'}{2})}{ln(1-p_h)}, \tag{5.10}$$

em que

$$R' = \frac{\frac{q}{q-1}R - \frac{1}{q-1}(1+2\sigma^2) + \frac{q\sigma}{q-1}\sqrt{2(1-R^2)+4\sigma^2}}{1+2\sigma^2} \tag{5.11}$$

com $\sigma = \frac{\Phi^{-1}(1-P'_e)}{\sqrt{2n}}$ e $\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{\frac{-t^2}{2}}dt$.

Para códigos Hermitianos generalizados, n e k são maiores do que para o código de Hermite. Observe que, para grandes n e q, R' se aproxima de R. A figura 5.2 mostra os resultados da região alcançável para o código Hermitiano generalizado em comparação com o código de Hermite e o código RS para $M = 64$. Observa-se que o código Hermitiano generalizado apresenta um melhor desempenho, pois para um mesmo número de usuários, atinge uma taxa do código maior.

O desempenho dos sistemas FH-CDMA também pode ser medido usando a taxa de transferência do canal de múltiplo acesso. A figura 5.3 mostra os resultados da taxa de transferência para os códigos RS, códigos de Hermite e códigos Hermitianos generalizados com taxa $1/2$ e $q = 64$. Estes resultados mostram que os códigos Hermitianos generalizados e os códigos de Hermite têm vantagens sobre os códigos RS. A taxa de transferência normalizada para grandes valores de n e k é dada por [63, 73]

$$W(K,R,q) = \begin{cases} \frac{RK}{q}, & K < 1 + \frac{ln(\frac{1-g/n+R'}{2})}{ln(1-p_h)}, \\ \frac{RK}{2q}, & K = 1 + \frac{ln(\frac{1-g/n+R'}{2})}{ln(1-p_h)}, \\ 0, & K > 1 + \frac{ln(\frac{1-g/n+R'}{2})}{ln(1-p_h)}. \end{cases} \tag{5.12}$$

Na próxima seção é apresentada a comparação dos códigos RS, códigos de Hermite e códigos Hermitianos generalizados para sistemas de redes de rádio por pacote.

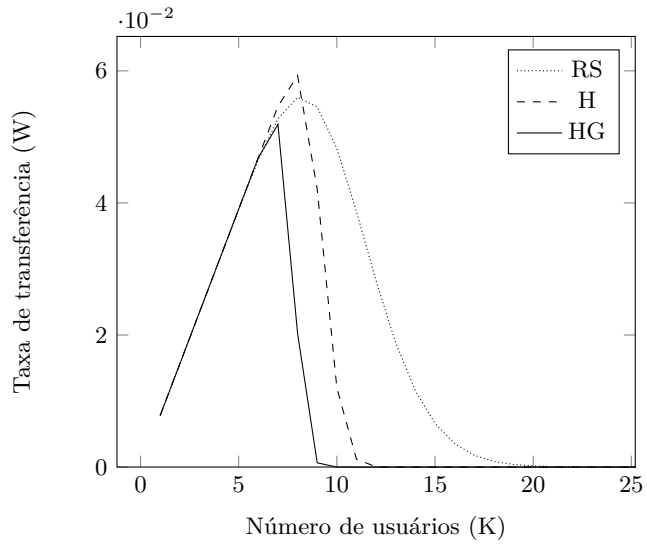

Figura 5.3 – Taxa de transferência normalizada para códigos sobre $\mathbb{F}_{64}$ com $\mathcal{R} = 1/2$.

5.3 – Redes de rádio de pacotes com salto em frequência

Nos esquemas de transmissão em pacotes que usam códigos para gerar padrões de salto em frequência, cada pacote pode ser considerado como uma única palavra código [19, 63]. No entanto, para comparações de desempenho com base na probabilidade de erro do pacote, o tamanho do pacote deve ser o mesmo para todos os códigos. Nesta tese, consideramos que para o código Hermitiano generalizado existe uma palavra código por pacote, para o código RS existem L_{RS} palavras código por pacote e para o código de Hermite existem L_H palavras código por pacote.

Considere o alfabeto do código com M símbolos tais que $M = 2^z$, onde $z = 6i$ com $i \in \mathbb{Z}_+^*$. Em todos os canais considerados a seguir, o padrão de salto é modelado como uma sequência de variáveis aleatórias independentes distribuídas uniformemente sobre o conjunto de frequências permitidas e os padrões de salto para diferentes transmissões são independentes [19].

5.3.1 – Canal AWGN

Para um canal com ruído gaussiano branco aditivo (*Additive white Gaussian noise* - AWGN), consideramos a decodificação somente de erros e dizemos que um erro de pacote ocorre se pelo menos uma palavra recebida não for decodificada. Note que para um pacote com L palavras-código, os erros em diferentes palavras-código são independentes, então a probabilidade de erro de pacote pode ser obtida facilmente a partir da probabilidade de erro da palavra-código.

A probabilidade de erro de pacote para um sistema de salto em frequência de um código $\mathcal{C}(n, k, d)$ com capacidade de decodificação e correção somente de erros de t é dada por

$$P_e = 1 - \sum_{i=0}^{t} \left(\begin{array}{c} n \\ i \end{array} \right) p^i (1-p)^{n-i}, \tag{5.13}$$

em que p denota a probabilidade de erro quiescente, isto é, a probabilidade de erro para os símbolos M-ários que são transmitidos em faixas de frequência nos quais há apenas o ruído térmico. Os símbolos M-ários são compostos por sequências de $m = log_2 M$ símbolos binários e p é dado por

$$p = 1 - (1 - p_0)^m, \tag{5.14}$$

em que p_0 denota a probabilidade de erro de símbolos binários [19].

5.3.2 – Canal com interferência de banda parcial catastrófica

Para canais com interferência de banda parcial catastrófica, o ruído térmico está presente em cada faixa de frequência, mas a interferência é apenas em uma fração ρ das faixas de frequência [19]. Seja p a probabilidade de erro quiescente em qualquer uma das frações restantes de frequências $(1 - \rho)$. Se os símbolos em um intervalo de tempo forem transmitidos em um intervalo de frequência que tenha interferência, os símbolos e o intervalo de permanência serão atingidos e a probabilidade de erro do símbolo correspondente será de $1 - M^{-1} \approx 1$ para valores grandes de M.

Considerando que cada colisão resulta em L erros de símbolos, a probabilidade de um erro de pacote para sistemas usando um código $\mathcal{C}(n, k, d)$ com capacidade de decodificação de t erros [19] é

$$P_e = 1 - \sum_{j=0}^{\lfloor t/L \rfloor} \left(\begin{array}{c} M \\ j \end{array} \right) \rho^j (1-\rho)^{M-j} P(j), \tag{5.15}$$

em que $P(j)$ é a probabilidade condicional de que uma palavra recebida seja decodificada corretamente, dado que há interferência de banda parcial em j intervalos de permanência. Cada colisão resulta em L erros de símbolo, portanto, isso implica que a capacidade de correção de erros do código não será excedida se houver até t/L colisões e $P(j)$ é expressa como

$$P(j) = \sum_{i=0}^{t-Lj} \left(\begin{array}{c} n - Lj \\ i \end{array} \right) p^i (1-p)^{n-Lj-i}. \tag{5.16}$$

Macdonald e Pursley [19] consideraram a decodificação de erros e apagamentos para comparação de códigos RS e códigos de Hermite, usando o método de teste de símbolo [74] para obter informações secundárias com N símbolos de teste binários transmitidos em cada intervalo de trabalho. Se mais de um certo número γ destes símbolos de teste estiver com erro, o intervalo de trabalho será considerado não confiável e todos os símbolos nesse intervalo de tempo serão apagados.

Consideramos nesta seção a notação usada por Mcdonald e Pursley [19], em que a probabilidade de alarme falso é denotada por α e a probabilidade de detecção é denotada por β. As probabilidades α e β são definidas como segue

$$\alpha = \sum_{l=\gamma+1}^{N} \left(\begin{array}{c} N \\ l \end{array} \right) {p_0}^j (1-p_0)^{N-l} \tag{5.17}$$

e

$$\beta = 2^{-N} \sum_{l=\gamma+1}^{N} \left(\begin{array}{c} N \\ l \end{array} \right). \tag{5.18}$$

Para um código Hermitiano generalizado usando a decodificação de erros e apagamentos, consideramos a equação para a probabilidade de erro de pacote como uma única equação de modo análogo ao que foi apresentado por Macdonald e Pursley [19] para códigos de Hermite dada por

$$P_e = \sum_{j=0}^{\kappa} \left(\begin{array}{c} M \\ j \end{array} \right) \rho^j (1-\rho)^{M-j} P_3(j), \tag{5.19}$$

em que $\kappa = \lfloor (d-1)/L \rfloor$ e $P_3(j)$ é a probabilidade condicional que a palavra recebida seja decodificada, dado que a interferência de banda parcial está presente em j dos M intervalos de tempo que são usados pela transmissão. Esta probabilidade depende diretamente da probabilidade condicional que a palavra recebida seja decodificada dado que há j colisões e que i deles são detectados e da probabilidade condicional de que a palavra-código esteja correta, dado j colisões, i colisões detectadas, e s falsos alarmes, cujas equações podem são detalhadas em [19].

5.3.3 – Canal com ruído de banda parcial

Para o canal com ruído de banda parcial, a interferência é modelada como ruído gaussiano branco de banda limitada com densidade espectral de potência unilateral $\rho^{-1}N_I$. A probabilidade de erro de um símbolo que é transmitido em um intervalo de tempo com interferência é denotada por δ. A relação E_b/N_I é uma medida da força da interferência, em que E_b é a energia recebida por bit de informação e N_I é o nível de ruído. O desempenho do canal com ruído de banda parcial se aproxima do canal de interferência de banda parcial catastrófica à medida que E_b/N_I diminui e se aproxima do desempenho no canal WGN à medida que E_b/N_I aumenta. De acordo com Macdonald e Pursley [19], as expressões da probabilidade de erro por pacote com decodificação somente de erros dada para o canal catastrófico de interferência de banda parcial devem ser modificadas de tal forma que

$$P_e = 1 - \sum_{j=0}^{M} \left(\begin{array}{c} M \\ j \end{array} \right) \rho^j (1-\rho)^{M-j} P(j), \tag{5.20}$$

em que

$$P(j) = \sum_{\lambda=0}^{\lambda^*} \begin{pmatrix} Lj \\ \lambda \end{pmatrix} \delta^{\lambda}(1-\delta)^{Lj-\lambda} \cdot \sum_{i=0}^{t^*} \begin{pmatrix} n-Lj \\ i \end{pmatrix} p^i(1-p)^{n-Lj-i}. \tag{5.21}$$

O índice λ é o número de erros de símbolo nos intervalos de espera que são atingidos e o índice t é o número de erros de símbolo nos intervalos de tempo que não são atingidos. Os parâmetros λ^* e t^* são dados por [19]

$$\lambda^* = min\{t, Lj\} \tag{5.22}$$

e

$$t^* = min\{t - \lambda, n - Lj\}. \tag{5.23}$$

Para comparações de desempenho de códigos em um ambiente operacional típico de uma rede de rádio de pacote de salto de frequência em vez de usar a probabilidade de erro de bit, é mais apropriado usar a probabilidade de erro de pacote [19]. A figura 5.4 mostra os resultados das probabilidades de erros de pacotes para códigos RS, códigos de Hermite e códigos Hermitianos generalizados com $M = 64$ e taxa $1/2$ no canal AWGN. Podemos observar que a curva Hermitiana generalizada aproxima-se da curva de Hermite e, assim, apresenta melhor desempenho que o código RS nesse canal. Portanto, tais códigos podem ser uma alternativa aos códigos RS para este tipo de canal.

A figura 5.5 mostra os resultados da probabilidade de erro de pacote para decodificação somente de erro em um canal de interferência de banda parcial catastrófica para os códigos RS, códigos de Hermite e códigos Hermitianos generalizados para $M = 4096$ e taxa do código $1/2$ para alguns valores de ρ. Podemos observar que o comportamento dos gráficos quando há interferência, no máximo, em 20% das faixas de frequência, ou seja, $\rho = 0,20$ ou menos, não há diferenças significativas no comportamento do curvas. Observe que, quando há interferência em 25% das faixas de frequência, o código Hermitiano generalizado tem um desempenho menor em relação aos outros códigos.

A figura 5.6 mostra o desempenho relativo usando decodificação somente de erros e decodificação de erros e apagamentos para códigos Hermitianos generalizados para alguns valores de N e γ. Observamos que para $N = 12$ e $\gamma = 2$, a probabilidade de erro do pacote atinge o melhor desempenho.

A Figura 5.7 mostra a comparação de desempenho do código de Hermite, do código RS e do código Hermitiano generalizado sobre $\mathbb{F}_{64}$ para um canal de ruído de banda parcial com $\rho = 0.2$ e $E_b/N_I = 18dB$. Observa-se que, para este canal com decodificação somente de erro, o comportamento da curva Hermitiana generalizada é semelhante ao seu comportamento

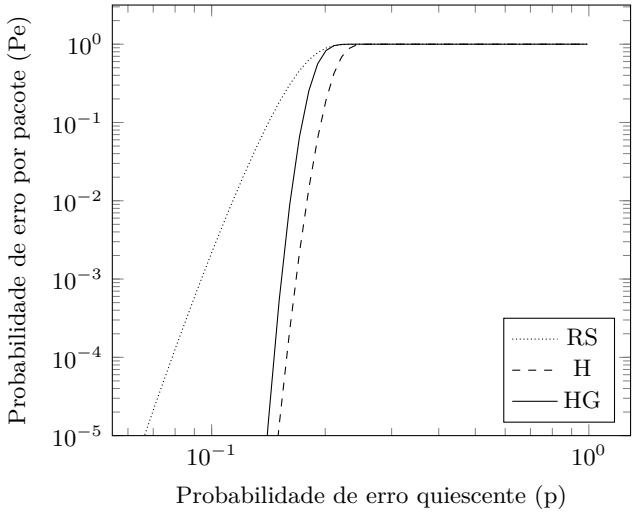

Figura 5.4 – Probabilidade de erro por pacote para decodificação de erros e apagamentos em um canal AWGN com $M = 64$.

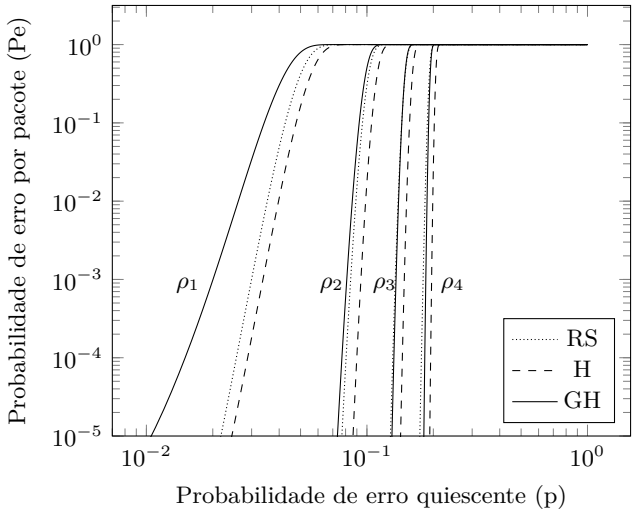

Figura 5.5 – Probabilidade de erro por pacote para decodificação de erros e apagamentos para códigos com taxa $1/2$ sobre $M = 4096$, em um canal com interferência de banda parcial catastrófico com $\rho_1 = 0.25$, $\rho_2 = 0.20$, $\rho_3 = 0.15$ e $\rho_4 = 0.10$.

no canal AWGN, pois se aproxima da curva de Hermite e mantém um desempenho melhor que os códigos RS.

Conforme pode-se observar nas figuras 5.6 e 5.7, a curva Hermitiana generalizada mantém o bom desempenho em relação aos códigos Reed-Solomon já obtido anteriormente com códigos de Hermite [19]. Além disso, apresenta a vantagem de que uma única palavra-código Hermitiano generalizado pode substituir um número maior de palavras de código RS do que o número de palavras necessárias quando um código Hermitiano é empregado. Por exemplo, para $M = 64$, um pacote com uma palavra código de um código Hermitiano generalizado pode substituir cerca de 16 palavras de um código Reed-Solomon intercaladas. Enquanto isso, o código de Hermite substitui apenas 8.

No próximo capítulo são apresentadas as considerações finais dessa pesquisa, assim como

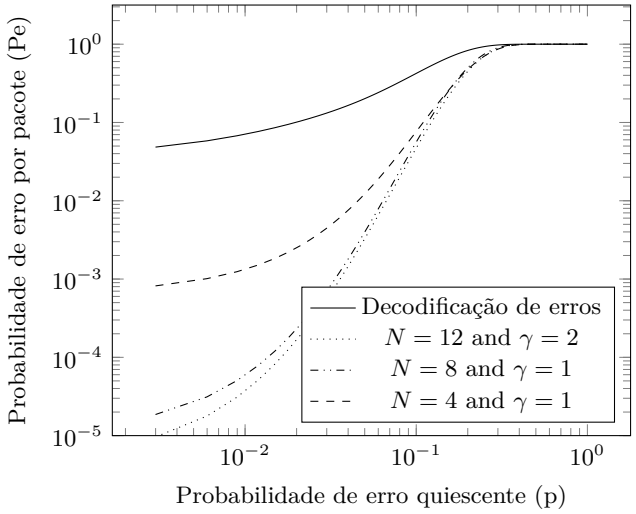

Figura 5.6 – Probabilidade de erro por pacote para decodificação de erros e apagamentos em um canal com interfer?ncia de banda parcial para códigos com taxa $1/2$ sobre $M = 8$, para alguns valores de N e γ.

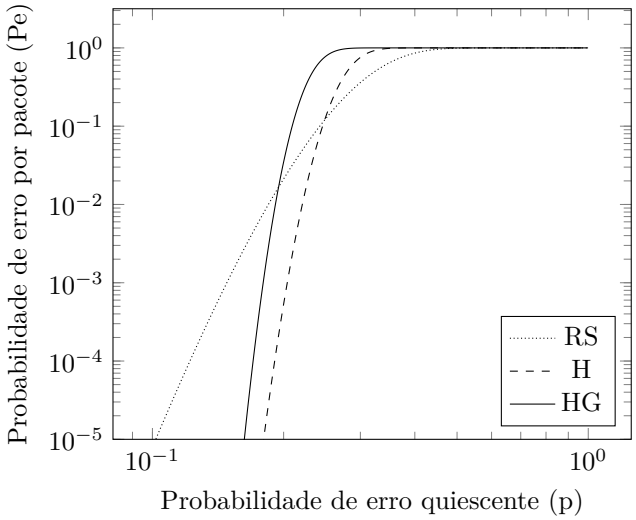

Figura 5.7 – Probabilidade de erro por pacote para decodificação de erro em um canal com interferência de banda parcial para códigos com taxa $1/2$ sobre $M = 64$, com $\rho = 0.2$ e $E_b/N_I = 18dB$.

as sugestões de trabalhos futuros.

CAPÍTULO 6

Considerações Finais

Nesta tese foram investigados códigos AG multiponto obtidos a partir de uma generalização da curva Hermitiana, que é considerada uma curva assintoticamente boa e, portanto, é capaz de gerar códigos com bons parâmetros. De modo geral, durante o desenvolvimento da pesquisa, dois problemas foram investigados: algoritmos de decodificação de lista para códigos AG multiponto e aplicações desses códigos.

Algoritmos de decodificação de lista exibem melhor desempenho do que os algoritmos de decodificação única, visto que permitem corrigir um limite de erros maior, ao considerar uma vizinhança maior da palavra recebida, tornando os algoritmos mais flexíveis. A fim de compreender a decodificação de lista para códigos AG, foram estudados os algoritmos de Shokrollahi e Wasserman [15] e de Lee e O'Sullivan [53] para códigos de Hermite.

O algoritmo de Lee e O'Sullivan [53] para códigos de Hermite de um ponto foi aplicado para a curva de F. K. Schmidt, que consiste em uma generalização da curva de Hermite. Ambos foram implementados utilizando o Macaulay2 e o SageMath ao longo desta pesquisa. Com isso, observou-se que a ordenação monomial utilizada é fundamental na implementação. A ordenação utilizada para esses algoritmos depende diretamente da valorização discreta das funções da base do espaço de Riemann-Roch no ponto que define o divisor G. Nesse sentido, buscou-se entender melhor como funcionaria a generalização dessa ordenação para códigos AG multiponto. Portanto, foi necessário realizar uma imersão do código multiponto em um código de um ponto e, assim, considerar a valorização das funções nesse ponto a fim de definir a ordenação monomial no código multiponto.

A principal contribuição desta tese consiste em um algoritmo de decodificação de lista, baseado no algoritmo proposto por Drake [1]. Este algoritmo difere do algoritmo do Drake [1] pelos seguintes fatos:

- O algoritmo de interpolação do Guruswami-Sudan foi substituído pelo algoritmo do Lee e O'Sullivan [53] para a curva de Hermite e pelo algoritmo do Lax [59] para curva Hermitiana generalizada;

- O número de passos do algoritmo foi reduzido, pois o algoritmo de fatoração (*Root-Finding*) utilizado permite obter diretamente a lista de palavras que pertence ao código AG multiponto, ao invés de obter a lista sobre o código de um ponto e, em seguida, verificar se as palavras pertencem ou não ao código AG multiponto;

- A saíde consiste em encontrar uma lista, ao invés de uma única palavra código.

Contudo, não está claro como estimar o tamanho da lista que pode ser obtida quando aumenta-se a vizinhança da palavra recebida neste algoritmo. Como trabalho futuro, pode-se investigar questões relacionadas ao raio de decodificação de lista e tamanho da lista obtida na saída do algoritmo.

O principal problema na teoria de codificação é projetar um código com o número de palavras código relativamente grande e com distância mínima d também relativamente grande, a fim de transmitir mais informação, mantendo uma boa capacidade de correção de erros. Contudo, aumentar o número de palavras em um código naturalmente diminui a distância mínima entre elas, aumentando a probabilidade de colisões entre duas palavras código. Além disso, observa-se que os parâmetros de um código AG são diretamente dependentes da curva escolhida para a construção do código. Nesse sentido, a curva Hermitiana generalizada utilizada nesta pesquisa produz códigos que alcançam bons parâmetros em comparação com os códigos de Hermite e os códigos RS quando se utiliza a mesma ordem do corpo finito. As tabelas 5.1, 5.2 e 5.3 mostram que utilizando códigos Hermitianos generalizados é possível aumentar a dimensão do código e, consequentemente, o número de usuários de um sistema FH-CDMA, com um pequeno aumento na probabilidade de colisões entre duas sequências do código.

Em sistemas de acesso múltiplo, é desejável aumentar o número de usuários sem aumentar a probabilidade de colisões entre dois usuários. Neste sentido, como trabalho futuro, gostaríamos de investigar como aproveitar o comprimento mais longo de códigos Hermitianos generalizados para obter subcódigos que gerem um número maior de usuários com a probabilidade de colisões tão pequena quanto possível.

Os códigos Hermitianos generalizados apresentam vantagens também nas comunicações de redes de rádio por pacotes. Observamos que uma única palavra código Hermitiana generalizada pode substituir um número maior de palavras do código RS do que o número de palavras necessárias quando um código de Hermite é empregado. Além disso, em todos os tipos de canais utilizados nesta pesquisa, o desempenho da probabilidade de erro de pacote para códigos Hermitianos generalizados aproxima-se do desempenho do código de Hermite. Isso permite concluir que tais códigos são uma boa alternativa aos códigos RS, que são comumente usados.

Diante do exposto, sugerimos os seguintes trabalhos futuros:

- Investigar outras generalizações da curva Hermitiana e os códigos AG multiponto obtidos, a fim de determinar a melhor generalização;

- Investigar o tamanho da lista obtida pelo algoritmo de decodificação de lista proposto e outros parâmetros, tais como o raio de decodificação de lista para este algoritmo;
- Determinar como obter subcódigos dos códigos Hermitianos generalizados com uma pequena probabilidade de colisões entre as sequências do códigos e analisar sua aplicação em sistemas de comunicação que utilizam salto em frequência.

Referências Bibliográficas

[1] N. Drake, "Decoding of multipoint algebraic geometry codes via lists," Ph.D. dissertation, Clemson University, Clemson, USA, 2009.

[2] S. Haykin, *Communication Systems*, 4th ed. Wiley, 2001, 816 p.

[3] R. E. Blahut, *Theory and Practice of Error Control Codes*. Addison-Wesley Publishing Company, MA, 1983.

[4] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 1948.

[5] L. B. da Silva Lima, "Arquitetura para um decodificador de códigos algébricos geometricos baseados em curvas de hermite," *Universidade Federal de Campina Grande*, 2004.

[6] M. A. Tsfasman, S. Vlădutx, and T. Zink, "Modular curves, shimura curves, and goppa codes, better than varshamov-gilbert bound," *Mathematische Nachrichten*, vol. 109, no. 1, pp. 21–28, 1982.

[7] I. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[8] O. Pretzel, *Codes and algebraic curves*. Oxford Science Publications, 1998, 192p.

[9] C. Hu and C.-A. Zhao, "Multi-point codes from generalized hermitian curves," *IEEE Transactions of Information Theory*, vol. 62, no. 5, pp. 2726–2736, 2016.

[10] A. Bassa, P. Beelen, A. Garcia, and H. Stichtenoth, "Towers of function fields over non-prime finite fields," *Moscow Mathematical Journal*, vol. 15, no. 1, pp. 1–29, 2015.

[11] P. Beelen and T. Høholdt, "List decoding using syndromes," in *Series on Number Theory and Its Applications*, vol. 5. World Scientific Publishing Co Pte Ltd, 2008, pp. 315–331.

[12] P. Elias, "List decoding for noisy channels," Research Laboratory of Electronics, MIT, Tech. Rep. 335, 1957.

[13] J. M. Wozencraft, "List decoding," *Quarterly Progress Report, Research Laboratory of Electronics, MIT*, vol. 48, pp. 90–95, 1958.

[14] M. Sudan, "Decoding of Reed-Solomon codes beyond the error-correction bound," *Journal of Complexity*, no. 13, pp. 180–193, 1997.

[15] M. A. Shokrollahi and H. Wasserman, "List decoding of algebraic-geometric codes," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 432–437, 1999.

[16] V. Guruswami, "List decoding of error-correcting codes," Ph.D. dissertation, Department of Electrical Engineering and Computer Science, MIT, Cambridge, US, 2001.

[17] N. Drake and G. L. Matthews, "Minimum distance decoding of general algebraic geometry codes via lists," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4335–4340, Sep. 2010.

[18] F. M. de Assis, "Hit probability between frequency hopping sequences generated by reed-solomon and hermitian codes," *Electronics Letters*, vol. 32, no. 11, pp. 962–963, May 1996.

[19] T. G. Macdonald and M. B. Pursley, "Frequency-hop spread-spectrum packet radio with hermitian codes," in *2001 MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No.01CH37277)*, vol. 2, Oct 2001, pp. 1330–1334 vol.2.

[20] V. D. Goppa, "Algebraic-geometric codes," *Math. USSR Izvestiya*, vol. 21, no. 3, pp. 75–91, 1983.

[21] H. Stichtenoth, *Algebraic function fields and codes*, 2nd ed., ser. Universitext. Springer, 2009.

[22] G. L. Matthews, "Weierstrass semigroups and codes from a quotient of the hermitian curve," *Des. Codes Cryptography*, vol. 37, no. 3, pp. 473–492, dec 2005. [Online]. Available: http://dx.doi.org/10.1007/s10623-004-4038-5

[23] J. H. V. Lint, "Algebraic geometric codes," in *Coding Theory and Design Theory, Part I, The IMA Volumes in Mathematics and Its Applications*, vol. 20. Berlin: Springer, 1990, pp. 137–162.

[24] R. R. Varshamov, "Estimate of the number of signals in error correcting codes," *Dokl. Acad. Nauk SSSR*.

[25] A. G. A. Bassa, P. Beelen and H. Stichtenoth, "Towers of function fields over non-prime finite fields," *[online] Avaliable: http://arxiv.org/abs/1202.5922*, 2012.

[26] C. Munuera, A. Sepúlveda, and F. Torres, "Generalized hermitian codes," *Designs, Codes and Cryptography*, vol. 69, no. 1, pp. 123–130, 2013.

[27] J.-P. Serre, "Sur le nombre des points rationnels dune courbe algébrique sur un corps fini," *C. R. Acad. Sci. Paris Sér. I Math.*, vol. 296, no. 9, pp. 397–402, 1983.

[28] Y. Ihara, "Some remarks on the number of rational points of algebraic curves over finite fields," *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, vol. 28, no. 3, pp. 721–724, 1982.

[29] J. Justesen, K. J. Larsen, H. E. Jensen, A. Havemose, and T. Høholdt, "Construction and decoding of a class of algebraic geometry codes," *IEEE Transactions on Information Theory*, vol. 35, no. 4, pp. 811–821, 1989.

[30] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres*, vol. 2, pp. 147–156, 1959.

[31] R. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Information and Control*, vol. 3, no. 1, pp. 68–79, 1960.

[32] S. Sakata, "Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array," *Journal of Symbolic Computation*, vol. 5, no. 3, pp. 321–337, 1988.

[33] S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen, and T. Høholdt, "Fast decoding of AG-codes up to the designed minimum distance." *IEEE Transactions Information Theory*, vol. 41, pp. 1672–1677, 1992.

[34] R. Kotter, "A fast parallel Berlekamp-Massey type algorithm for Hermitian codes," *In Proceedings Algebraic and Combinatorial Coding Theory, ACCT94*, pp. 125–128, 1994.

[35] ——, "A fast parallel implementation of a Berlekamp-Massey algorithm for algebraic-geometric codes," *IEEE Transactions Information Theory*, vol. 44, no. 4, 1998.

[36] D. M. Mandelbaum, "A method for decoding of generalized goppa codes," *IEEE Transactions on Information Theory*, vol. 23, pp. 137–140, 1977.

[37] G.-L. Feng and T. R. N. Rao, "Decoding algebraic-geometric codes up to the designed minimum distance," *IEEE Transactions on Information Theory*, vol. 39, no. 1, pp. 37–45, 1993.

[38] S. C. Porter, B.-Z. Shen, and R. Pellikaan, "Decoding geometric Goppa codes using an extra place," *IEEE Transactions on Information Theory*, vol. 38, no. 6, pp. 1663–1676, 1992.

[39] M. E. O'Sullivan, "Decoding of Hermitian codes: the key equation and efficient error evaluation," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 512–523, 2000.

[40] X.-W. Wu, M. Kuijper, and P. Udaya, "Improved decoding of algebraic-geometric codes with respect to the Lee metric," in *Communications Theory Workshop Proceedings. 6th Australian*. IEEE, 2005, pp. 119–124.

[41] A. N. Skorobogatov and S. G. Vlãdut, "On the decoding of algebraic-geometric codes," *IEEE Transactions on Information Theory*, vol. 36, no. 5, pp. 1051–1060, 1990.

[42] S. Sakata, "Extension of the Berlekamp-Massey algorithm to N dimensions," *Information and Computation*, vol. 84, no. 2, pp. 207–239, 1990.

[43] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometric codes," in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society, Washington, DC, USA, 1998, pp. 28–38.

[44] T. Høholdt and R. R. Nielsen, "Decoding Hermitian codes with Sudan's algorithm," in *AAECC*, vol. 13. Springer, 1999, pp. 260–270.

[45] S. Sakata, "On fast interpolation method for Guruswami-Sudan list decoding of one-point algebraic-geometry codes," *Applied algebra, algebraic algorithms and error-correcting codes*, vol. 2227, pp. 172–181, 2001.

[46] R. Koetter and V. Alexander, "Algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Transactions on Information Theory*, vol. 49, no. 11, pp. 2809–2825, 2003.

[47] V. Guruswami, "Algorithmic results in list decoding," *Foundations and Trends in Theoretical Computer Science*, vol. 2, no. 2, pp. 107–195, 2006.

[48] R. M. Roth and G. Ruckenstein, "Efficient decoding of Reed-Solomon codes beyond half the minimum distance," *IEEE Transactions on Information Theory*, vol. 46, no. 1, pp. 246–257, 2000.

[49] X. W. Wu and P. H. Siegel, "Efficient root-finding algorithm with application to list decoding of algebraic-geometric codes," *IEEE Transactions on Information Theory*, vol. 47, no. 6, pp. 2579–2587, 2001.

[50] H. O'Keeffe and P. Fitzpatrick, "Gröbner basis solutions of constrained interpolation problems," *Linear algebra and its applications*, vol. 351, pp. 533–551, 2002.

[51] ——, "Gröbner basis approach to list decoding of algebraic geometry codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 18, no. 5, pp. 445–466, 2007.

[52] K. Lee and M. E. O'Sullivan, "List decoding of Reed-Solomon codes from a Gröbner basis perspective," *Journal of Symbolic Computation*, vol. 43, no. 9, pp. 645–658, 2008.

[53] ——, "List decoding of Hermitian codes using Gröbner bases," *Journal of Symbolic Computation*, vol. 44, no. 12, pp. 1662–1675, 2009.

[54] M. Fujisawa and S. Sakata, "On a fast decoding of multipoint codes from algebraic curves," in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*. IEEE, 2011, pp. 1022–1026.

[55] S. Sakata and M. Fujisawa, "Fast decoding of multipoint codes from algebraic curves," *IEEE Transactions on Information Theory*, vol. 60, no. 4, pp. 2054–2064, 2014.

[56] R. Matsumoto, D. Ruano, and O. Geil, "List decoding algorithm based on voting in Gröbner bases for general one-point AG codes," *Journal of Symbolic Computation*, pp. 86–90, 2012.

[57] K. Lee, M. Bras-Amorós, and M. E. O'Sullivan, "Unique decoding of plane AG codes via interpolation," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3941–3950, 2012.

[58] R. Matsumoto, D. Ruano, and O. Geil, "Generalization of the Lee-O'Sullivan list decoding for one-point AG codes," *IEEE International Symposium on Information Theory Proceedings*, pp. 86–90, 2013.

[59] R. F. Lax, "Generic interpolation polynomial for list decoding," *Finite Fields and Their Applications*, vol. 18, pp. 167–178, 2012.

[60] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd ed. Springer Publishing Company, Incorporated, 2008.

[61] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*. New York, NY, USA: Cambridge University Press, 2001.

[62] G. Korchmáros and G. P. Nagy, "Hermitian codes from higher degree places," *Journal of Pure and Applied Algebra*, vol. 217, no. 12, pp. 2371–2381, 2013.

[63] F. M. Assis and M. S. Alencar, "Comparing algebraic geometric and reed-solomon codes for fh-cdma applications," in *Proceedings of PIMRC '96 - 7th International Symposium on Personal, Indoor, and Mobile Communications*, vol. 3, 1996, pp. 1102–1105.

[64] W. Atta, "Improved jamming-resistant frequency hopping spread spectrum systems," Ph.D. dissertation, Oct 2013.

[65] D. Torrieri, *Principles of Spread-Spectrum Communication Systems*, 3rd ed., 2015.

[66] B. Gopalakrishnan and M. A. Bhagyaveni, "Anti-jamming communication for body area network using chaotic frequency hopping," *Healthcare Technology Letters*, vol. 4, no. 6, pp. 233–237, 2017.

[67] X. Ouyang, Q. Wan, J. Cao, J. Xiong, and Q. He, "Direct tdoa geolocation of multiple frequency-hopping emitters in flat fading channels," *IET Signal Processing*, vol. 11, no. 1, pp. 80–85, 2017.

[68] L. Guan, Z. Li, J. Si, and B. Hao, "Analysis of asynchronous frequency hopping multiple-access network performance based on the frequency hopping sequences," *IET Communications*, vol. 9, no. 1, pp. 117–121, 2015.

[69] K. . Park, T. R. Park, C. D. Schmitz, and L. Sha, "Design of robust adaptive frequency hopping for wireless medical telemetry systems," *IET Communications*, vol. 4, no. 2, pp. 178–191, January 2010.

[70] X. Liu and D. Y. Peng, "Theoretical bound on frequency hopping sequence set," *Electronics Letters*, vol. 49, no. 10, pp. 654–656, May 2013.

[71] T. . Chen, "Joint signal parameter estimation of frequency-hopping communications," *IET Communications*, vol. 6, no. 4, pp. 381–389, March 2012.

[72] E. Geraniotis and M. Pursley, "Error probabilities for slow-frequency-hopped spread-spectrum multiple-access communications over fading channels," *IEEE Transactions on Communications*, vol. 30, no. 5, pp. 996–1009, May 1982.

[73] S. W. Kim and W. Stark, "Optimum rate reed-solomon codes for frequency-hopped spread-spectrum multiple-access communication systems," *IEEE Transactions on Communications*, vol. 37, no. 2, pp. 138–144, Feb 1989.

[74] M. B. Pursley, "Packet error probabilities in frequency-hop radio networks - Coping with statistical dependence and noisy side information," in *GLOBECOM '86 - Global Telecommunications Conference*, 1986, pp. 165–170.

[75] A. Hefez and M. Villela, *Códigos correctores de erros*, ser. Computação matemática. IMPA, 2008.

APÊNDICES

APÊNDICE A

Produção científica

- Souza, T. A , Assis, F. M. e Lima, L. B. S.. "Generalized Hermitian Codes for Frequency Hopping". Artigo submetido para *IET communications*.
- Souza, T. A , Assis, F. M. e Lima, L. B. S.. "Decodificação de lista para códigos de F. K. Schmidt usando Bases de Gröbner". In: XXXVI Simpósio Brasileiro de Telecomunicações. Campina Grande-PB, Setembro, 2018.
- Souza, T. A , Assis, F. M. e Lima, L. B. S.. "List Decoding of F. K. Schmidt Codes". In: Technical University of Munich. Munich, Germany, 2017.

APÊNDICE B

Fundamentação matemática

Neste Apêndice são apresentados alguns conceitos matemáticos utilizados ao longo da tese. Para maiores detalhes consultar [3, 8, 21]. Nas definições apresentadas neste capítulo denotamos $\mathbb{F}_q$ um corpo com q elementos e K e F corpos arbitrários.

B.1 – Anéis

Definição 13 Um *anel* é um conjunto não-vazio A munido de duas operações binárias

$$\begin{array}{rccc} +: & A\times A & \to & A \\ & (a,b) & \mapsto & a+b \end{array} \qquad \text{e} \qquad \begin{array}{rccc} \cdot & : A\times A & \to & A \\ & (a,b) & \mapsto & a\cdot b \end{array}$$

chamadas, respectivamente, de adição e multiplicação tal que valem as seguintes propriedades:

1. $(a+b)+c = a+(b+c), \quad \forall a,b,c \in A$ (associatividade da adição).
2. Existe um elemento neutro, chamado *zero*, denotado por 0 tal que $a+0=0+a=a$, $\forall a \in A$.
3. Existência de um elemento *inverso* para a adição: Dado $a \in A$, existe um elemento chamado *simétrico* de a e denotado por $-a$, tal que $a+(-a) = -a+a = 0$.
4. $a+b=b+a, \quad \forall a,b \in A$ (associatividade da multiplicação).
5. $(a\cdot b)\cdot c = a\cdot(b\cdot c), \quad \forall a,b,c \in A$.
6. $a\cdot(b+c) = a\cdot b + a\cdot c, \quad \forall a,b,c \in A$.

Notação: $(A,+,\cdot)$ denotará um anel A com as operações $+$ e $\cdot$.

Seja $(A,+,\cdot)$ um anel, se existe um elemento denotado por $1 \in A$ tal que $a\cdot 1 = 1\cdot a = a$, $\forall a \in A$ diremos que A é um *anel com unidade* 1.

Se um anel $(A,+,\cdot)$ satisfaz $a\cdot b = b\cdot a$, $\forall a,b \in A$ é dito *anel comutativo*.

Exemplo 22 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ munidos com as operações de adição e multiplicação usuais são exemplos de anéis. No entanto, o conjunto $\mathbb{N} = \{1, 2, 3, \ldots\}$ munido com operações de adição e multiplicação dos inteiros não forma um anel pois não existem simétricos dos elementos, nem elementro neutro para a adição.

Um anel A comutativo com unidade será chamado de *domínio de integridade* se satisfaz a seguinte condição:

$$\forall a, b \in A, \quad a \neq 0 \ \ e \ \ b \neq 0 \Rightarrow a \cdot b \neq 0.$$

Exemplo 23 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ munidos com as operações de adição e multiplicação usuais são domínios de integridade.

Definição 14 Um elemento $a \in A$, onde $(A, +, \cdot)$ é um anel, será dito *invertível* se existir um elemento $b \in A$ tal que $a \cdot b = 1$. E b é dito *inverso* de a.

Exemplo 24 Em $\mathbb{Z}$ os únicos elementos invertíveis são 1 e -1.

B.2 – Ideais de um anel

Definição 15 Um subconjunto I não vazio de um anel A é um ideal de A se:

i. $\forall a, b \in I, a + b \in I$;

ii. $\forall a \in I$ e $\forall c \in A, ca \in I$.

Note que um ideal I sempre contém o elemento zero de A, pois dado um elemento qualquer não nulo $a \in I$, temos $0 = 0a \in I$.

Também é possível observar que $I = 0$ e $I = A$ são ideais de A.

Definição 16 Seja $a \in A$, então o conjunto $I(a) = \{ca; c \in A\}$ é um ideal de A, chamado de *ideal principal* gerado por a.

Em geral, se $a_1, \cdots, a_n \in A$, então o conjunto

$$I = I(a_1, \cdots, a_n) = \{c_1a_1 + \cdots + c_na_n; c_1, \cdots, c_n \in A\}$$

é um ideal de A. Os elementos $a_1, \cdots, a_n$ são chamados de geradores de I.

B.3 – Corpos Finitos

Definição 17 Um anel onde todo elemento não nulo é invertível é chamado de *corpo*. E define-se a *ordem* do corpo como sendo o número de elementos do corpo. Um corpo com um número finito de elementos será dito *corpo finito*.

Definição 18 Seja K um corpo finito com elemento unidade 1. Considere o conjunto

$$\Lambda_K = \{n \in \mathbb{N};\ n \cdot 1 = 0\} \subset \mathbb{N}.$$

A *característica* do corpo finito K é definida como o inteiro positivo λ

$$\lambda = \min \Lambda_K = \min\{n \in \mathbb{N};\ n \cdot 1 = 0\}. \tag{B.1}$$

Proposição 4 Seja K um corpo finito, então λ é um número primo.

Demonstração 1 *Suponha que λ não seja primo, então existem $\lambda_1,\ \lambda_2 \in \mathbb{Z}$ tais que $1 < \lambda_1 < \lambda$ e $1 < \lambda_2 < \lambda$. Logo,*

$$0 = \lambda \cdot 1 = (\lambda_1 \cdot \lambda_2) \cdot 1 = \lambda_1(\lambda_2 \cdot 1) = (\lambda_1 \cdot 1)(\lambda_2 \cdot 1).$$

Como todo corpo é um domínio de integridade, então

$$(\lambda_1 \cdot 1)(\lambda_2 \cdot 1) = 0 \Leftrightarrow \lambda_1 \cdot 1 = 0 \ \textit{ou}\ \ \lambda_2 \cdot 1 = 0.$$

Mas isso é uma contradição, pois, λ é o menor inteiro positivo tal que $\lambda \cdot 1 = 0$.

Definição 19 Seja $\alpha \in K^*$, em que $K^* = K \setminus \{0\}$ e um corpo finito, define-se a *ordem* do elemento α como sendo o menor inteiro n tal que $\alpha^n = 1$.

Definição 20 Seja G um conjunto não-vazio munido da operação binária $* : G \times G \to G$. Dizemos que o par $(G, *)$ é um *grupo* se são válidas os seguintes axiomas:

a. $a * (b * c) = (a * b) * c, \quad \forall a, b, c \in G$ (Associatividade).

b. $\exists e \in G$ tal que $a * e = e * a, \quad \forall a \in G$ (Identidade).

c. $\forall a \in G, \exists b \in G$ tal que $a * b = b * a = e$ e este elemento b é dito *inverso* de a.

Os corpos finitos também são chamados de *campos de Galois* [1].

[1] Evariste Galois nasceu em 25 de outubro de 1811 na cidade de Bourg-la-Reine, na França. Filho do republicano Nicolas-Gabriel Galois e de Adelaide Marie Demante, que foi responsável por sua educação até os 12 anos de idade. Em 1823 iniciou sua educação formal no Liceu de Louis-le-Grand, em Paris. Em 1829 publicou seu primeiro artigo sobre a solução de equações algébricas. Ficou conhecido pelo seu estudo da insolubilidade das equações de graus superiores a quatro ao criar um objeto, conhecido hoje como "Grupo de Galois", que possibilita investigar se um polinômio qualquer pode ter suas soluções encontradas por meio de radicais ou não. Galois faleceu no dia 31 de maio de 1832, aos 20 anos de idade, após um duelo.

Definição 21 Sejam A e B dois anéis (ou corpos). Uma função $f : A \to B$ será chamada *homomorfismo* se, para todos os elementos $a, b \in A$, valem as seguintes condições:

(i) $f(a+b) = f(a) + f(b)$.

(ii) $f(a \cdot b) = f(a) \cdot f(b)$.

(iii) $f(1) = 1$.

Definição 22 Um homomorfismo bijetor de corpos será chamado de *isomorfismo*. Dois corpos serão ditos *isomorfos* se existir um isomorfismo entre eles.

Teorema 8 Seja α um elemento não-nulo do corpo finito $\mathbb{F}_q$. Então $\alpha^{q-1} = 1$.

Demonstração 2 *Sejam $b_1, b_2, \ldots, b_{q-1}$ os $q-1$ elementos não-nulos de $\mathbb{F}_q$. Como $\mathbb{F}_q$ é um corpo, sabemos que a operação de multiplicação é fechada, pois a multiplicação de dois elementos de $\mathbb{F}_q$ resulta em um elemento do próprio $\mathbb{F}_q$. Então, os $q-1$ elementos $\alpha \cdot b_1, \alpha \cdot b_2, \ldots, \alpha \cdot b_{q-1}$ são não-nulos e temos:*

$$(\alpha \cdot b_1)(\alpha \cdot b_2) \cdot \ldots \cdot (\alpha \cdot b_{q-1}) = b_1 \cdot b_2 \cdot \ldots \cdot b_{q-1}$$
$$\alpha^{q-1}(b_1 \cdot b_2 \cdot \ldots \cdot b_{q-1}) = b_1 \cdot b_2 \cdot \ldots \cdot b_{q-1}.$$

Como por hipótese $\alpha \neq 0$ e $b_1 \cdot b_2 \cdot \ldots \cdot b_{q-1} \neq 0$ devemos ter:

$$\alpha^{q-1} = 1.$$

Teorema 9 Seja α um elemento não-nulo do corpo finito $\mathbb{F}_q$. Seja n a ordem de α. Então n divide $q-1$.

Demonstração 3 *Suponha que n não divide $q-1$. Dividindo $q-1$ por n, obtemos $q-1 = k \cdot n + r$, onde $0 < r < n$. Então $\alpha^{q-1} = \alpha^{kn+r} = \alpha^{kn} \cdot \alpha^r = (\alpha^n)^k \cdot \alpha^r = 1^k \cdot \alpha^r = \alpha^r$. Portanto, $\alpha^{q-1} = 1$ se $\alpha^r = 1$, mas isto é impossível pois $0 < r < n$, e n é o menor inteiro tal que $\alpha^n = 1$. Logo, n divide $q-1$.*

Definição 23 Seja o corpo finito $\mathbb{F}_q$, um elemento não-nulo α de $\mathbb{F}_q$ é dito *primitivo* se a ordem de α for $q-1$, ou seja, se $\mathbb{F}_q^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$.

Portanto, as potências do elemento primitivo geram todos os elementos não-nulos de $\mathbb{F}_q$.

Teorema 10 Todo corpo finito possui elementos primitivos.

Um corpo K que contém um corpo F, tal que as operações de K, quando restritas a F, coincidam com as operações de F, é chamado de *extensão* de F. Neste caso, dizemos que F é um *subcorpo* de K. Denotaremos por K/F ou pelo diagrama

$$K$$

$$|$$

$$F$$

Neste caso, F é dito *corpo base* ou corpo fundamental da extensão.

Exemplo 25 $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, neste caso $\mathbb{C}$ é uma extensão de $\mathbb{R}$, $\mathbb{C}$ é uma extensão de $\mathbb{Q}$ e $\mathbb{R}$ é uma extensão de $\mathbb{Q}$.

B.4 – Espaços Vetoriais

Definição 24 Sejam um corpo K, cujos elementos são chamados de escalares, e um conjunto V, cujos elementos são chamados de vetores. Diremos que V é um *espaço vetorial* sobre K, ou um K*-espaço vetorial*, se existir a operação de adição em V,

$$\begin{array}{rccc} + : & V \times V & \longrightarrow & V \\ & (v, w) & \mapsto & v + w \end{array}$$

e se existir a operação de multiplicação dos elementos de V por escalares,

$$\begin{array}{rccc} \cdot : & K \times V & \longrightarrow & V \\ & (\lambda, v) & \mapsto & \lambda v \end{array}$$

satisfazendo às seguintes propriedades:

1. $(u + v) + w = u + (v + w), \quad \forall u, v, w \in V$. Associatividade da adição
2. $u + v = v + u, \quad \forall u, v \in V$. Comutatividade da adição
3. Existe um elemento *neutro* $0 \in V$ tal que

$$u + 0 = u.$$

4. Dado um elemento $u \in V$, existe um elemento inverso $-u$, chamado *simétrico* de u, tal que,

$$u + (-u) = 0.$$

5. Dados $\lambda, \mu \in K$ e $u \in V$, vale

$$(\lambda + \mu) \cdot u = \lambda \cdot u + \mu \cdot u.$$

6. Dados $\lambda \in K$ e $u, v \in V$, vale

$$\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v.$$

7. Dados $\lambda, \mu \in K$ e $u \in V$, vale

$$(\lambda \cdot \mu) \cdot u = \lambda \cdot (\mu \cdot u).$$

8. Para todo $u \in V$,

$$1 \cdot u = u,$$

onde 1 é a unidade de K.

Exemplo 26 *$\mathbb{R}$-espaços vetoriais $\mathbb{R}^n$ e $\mathbb{C}$-espaços vetoriais $\mathbb{C}^n$.*

Definição 25 Um *subespaço vetorial* de um K-espaço vetorial V é um subconjunto não vazio W de V, que, com as operações de adição e multiplicação por escalares de V, é também um K-espaço vetorial.

Podemos afirmar que um subconjunto não vazio W de um espaço vetorial V é um subespaço vetorial se é satisfeita a seguinte condição:

$$\forall u, v \in W, \quad \forall \lambda \in K, \quad u + \lambda \cdot v \in W. \tag{B.2}$$

Se V um K-espaço vetorial, dados $v_1, \ldots, v_n \in V$ dizemos que $v_1, \ldots, v_n$ são *linearmente independentes*, se for satisfeita a seguinte relação

$$\lambda_1 v_1 + \ldots + \lambda_n v_n = 0 \Rightarrow \lambda_1 = \ldots = \lambda_n = 0 \tag{B.3}$$

com $\lambda_1, \ldots, \lambda_n \in K$. E, caso contrário, $v_1, \ldots, v_n$ são ditos *linearmente dependentes*.

Diremos que um subconjunto $B \subset V$ *gera* V quando todo elemento de V puder ser escrito na forma

$$\lambda_1 v_1 + \ldots + \lambda_n v_n \tag{B.4}$$

com $v_1, \ldots, v_n \in B$ e $\lambda_1, \ldots, \lambda_n \in K$.

Quando um subconjunto $B \subset V$ gera V e os elementos de qualquer subconjunto finito de B forem linearmente independentes sobre K, diremos que B é uma *base* de V. O número de elementos de uma base será chamado *dimensão* de V sobre K e denotado por $\dim_K V$.

B.5 – Anéis de Polinômios

Definição 26 Sejam F um corpo e x uma indeterminada. Definimos o *polinômio* $p(x)$ com coeficientes em F na indeterminada x como

$$p(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n \tag{B.5}$$

em que $n \in \mathbb{Z}^+$ e $a_i \in F$, $\forall i = 0, 1, \ldots, n$.

Dados os polinômios $p(x) = a_0 + a_1x + \ldots + a_nx^n$ e $q(x) = b_0 + b_1x + \ldots + b_mx^m$, podemos dizer que $p(x) = q(x)$ se $a_i = b_i$, para todo i. Seja $F[x] = \{p(x);\ a_i \in A; \forall i = 1, \ldots, n\}$, ou seja, $F[x]$ é o conjunto de todos os polinômios na indeterminada x com coeficientes em F. Note que $F \subset F[x]$. Considere $p(x)$ e $q(x)$ definidos acima, podemos definir as seguintes operações:

$$p(x) + q(x) = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)x^i \tag{B.6}$$

$$p(x) \cdot q(x) = \sum_{i=0}^{n+m} c_i x^i \tag{B.7}$$

onde $c_i = \sum_{j=0}^{i} a_j \cdot b_{i-j}x^i$.

O conjunto $F[x]$ munido das operações definidas acima é um anel.

Se $p(x) = 0 + 0x + 0x^2 + \ldots + 0x^n$ indicaremos $p(x) \equiv 0$ e dizemos que o polinômio é *identicamente nulo* sobre F. Se $p(x) = a$, com $a \in F$, então $p(x)$ é o polinômio *constante* a. Se $p(x) \in F[x]$ tal que $a_n \neq 0$ e $a_j = 0\ \forall j > n$ dizemos que n é o grau de $p(x)$ e denotaremos por $\partial p(x) = n$.

Definição 27 Seja F um corpo e $p(x) \in F[x]$ tal que $\partial p(x) \geq 1$. Dizemos que $p(x)$ é um polinômio *irredutível* sobre F se, toda vez que $p(x) = g(x)h(x)$, tal que $g(x), h(x) \in F[x]$, então temos $g(x) = a$ constante em F ou $h(x) = b$ constante em F. Se $p(x)$ não for irredutível sobre F, dizemos que $p(x)$ é *redutível* sobre F.

Definição 28 *Seja F um corpo, o corpo das frações de $F[x]$ é definido por*

$$F(x) = \left\{ \frac{p(x)}{g(x)}; p(x), g(x) \in F[x], g(x) \neq 0 \right\}. \tag{B.8}$$

Este corpo também é chamado de corpo das funções racionais.

B.6 – Corpo de funções algébricas

Definição 29 *(Extensão algébrica) Uma extensão de corpo K/F é chamada algébrica se todo elemento de K é algébrico sobre F, isto é, se todo elemento de K é uma raiz de algum polinômio diferente de zero com coeficientes em F. Extensões de corpo que não são algébricas, isto é, que contêm elementos transcendentais, são chamadas transcendentais.*

Definição 30 *(Extensão finita) Seja K uma extensão do corpo F. Dizemos que K é uma extensão finita se $[K : F]$ é finita. Isto é, K é um espaço vetorial de dimensão finita sobre F.*

Exemplo 27 *$\mathbb{C}$ é uma extensão algébrica finita dos números reais $\mathbb{R}$, pois $[\mathbb{C} : \mathbb{R}] = 2$ e o espaço vetorial $\mathbb{C}$ sobre $\mathbb{R}$ tem base $\{1, i\}$.*

Definição 31 *Um corpo de funções algébricas K/F em uma variável sobre um corpo F é uma extensão K de F, onde K é uma extensão finita de $F(x)$ para algum $x \in K$ transcendente sobre F.*

B.7 – Curvas Algébricas

Considere ao longo dessa seção a notação seguinte:

- $\mathbb{F}_q$ (ou simplesmente $\mathbb{F}$) um corpo finito com q elementos e K o fecho algébrico de $\mathbb{F}_q$.
- $\mathbb{A}^n \rightarrow$ Espaço afim n-dimensional sobre K que consiste de todos os vetores $(x_1, x_2, \cdots, x_n)$.
- $\mathbb{P}^n \rightarrow$ Espaço projetivo n-dimensional sobre K que consiste de todos os vetores $(x_0, x_1, x_2, \cdots, x_n)$.
- No espaço projetivo as coordenadas são homogêneas, isto é, $(x_0, x_1, x_2, \cdots, x_n) \sim (cx_0, cx_1, cx_2, \cdots, cx_n)$, em que $c \in \mathbb{F}^*$.

Definição 32 *Seja $f \in K[x_1, x_2, \cdots, x_n]$. Um ponto $P = (a_1, a_2, \cdots, a_n) \in \mathbb{A}^n$ é um zero de f se $f(P) = 0$. Se f não é uma constante, então o conjunto de zeros $\mathcal{X}$ de f é chamado de variedade afim ou hipersuperfície $V(f)$ definida por f, e é dada por*

$$V(f) = \{P \in \mathbb{A}^n | f(P) = 0\}.$$

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

Exemplo 28 *Se $n = 3$ e $f = x^2 + y^2 + z^2 - 1$, então $\mathcal{X}$ é a esfera unitária em $\mathbb{A}^3$.*

Definição 33 *Uma variedade afim $\mathcal{X}$ em $\mathbb{A}^2$ é chamada de uma curva plana afim.*

Definição 34 *Dado um corpo K e o espaço afim $\mathbb{A}^2$ sobre K, uma curva algébrica plana é o conjunto de todos os pontos $P = (a, b) \in \mathbb{A}^2$ cujas coordenadas satisfazem à equação $f(x, y) = 0$, em que $f(x, y)$ é um polinômio com coeficientes sobre K.*

De modo geral, no espaço projetivo $\mathbb{P}^n$, seja $\mathcal{X}$ uma variedade afim ou projetiva, que pode ser entendida como o conjunto de zeros de uma família de polinômios.

Para uma variedade $\mathcal{X}$ (curva), definimos $K(\mathcal{X})$ o corpo de funções racionais sobre a curva. A curva $\mathcal{X}$ é caracterizada completamente pelo corpo $K(\mathcal{X})$.

Definição 35 *(Curvas Projetivas Suaves) Considere uma curva $\mathcal{X}$ em $\mathbb{A}^2$ ($\mathbb{P}^1$) definida pela equação $f(x,y)=0$ e seja $P=(a,b)$ um ponto da curva. Se pelo menos uma das derivadas f_x ou f_y for não-nula em P, então P é dito um ponto não-singular.*

Consideraremos apenas curvas não-singulares, isto é, curvas suaves, para as quais todos os pontos são não-singulares.

Seja P um ponto de $\mathcal{X}$ e U uma vizinhança de P e O_P o anel de valorização associado a um lugar (ponto) P.

Definição 36 *(Valorização discreta) Uma valorização discreta do corpo de funções racionais $K/\mathbb{F}$ é uma função $v: K/\mathbb{F} \longrightarrow \mathbb{Z}\cup\{\infty\}$ com as seguintes propriedades:*

- $v(x)=\infty$ *se, e somente se,* $x=0$.
- $v(xy)=v(x)+v(y)$, *para cada* $x,y\in K$.
- $v(x+y)>=min\{v(x),v(y)\}$ *para todo* $x,y\in K$.
- *Existe um elemento* $x\in K$ *tal que* $v(x)=1$.
- $v(a)=0$ *para todo* $a\in\mathbb{F}^*$.

Definição 37 *A função ϕ definida em U é chamada de regular em P se $\phi=\frac{f}{g}$, em que $g(P)\neq 0$ e f e g são polinômios homogêneos de mesmo grau.*

Definição 38 *O anel local O_P de ponto P em $\mathcal{X}$ é o conjunto das classes de equivalência das funções regulares em P.*

Este anel local tem um único ideal maximal m_P, que consiste das classes de funções que têm um zero em P. Além disso, os demais elementos de O_P são as unidades.

Definição 39 *Todo elemento $z\in O_P$ pode ser escrito de forma única como: $z=t^m\cdot u$, em que $t\in m_P$ e é chamado de parâmetro local e, u é uma unidade e $m\in\mathbb{N}$.*

- *Se* $m>0$, *então* P *é um zero de multiplicidade* m *de* z.
- *Se* $m<0$, *então* P *é um pólo de ordem* m *de* z.

em que $m=ord_P(z)=v_P(z)$

Exemplo 29 *Seja $\mathcal{X}$ o círculo em $\mathbb{P}^1$ com a equação $x^2+y^2=1$ e seja $P=(1,0)$. Seja $z=z(x,y)=1-x$. Esta função se anula no ponto P, portanto, $z\in m_P$.*

Afirmação: $m=ord_P(z)=2$.

Note que $x^2+y^2=1$ *pode ser reescrita como:*

$(1-x)(1+x)=y^2\Rightarrow z=1-x=y^2(\frac{1}{1+x})$

Observe que o segundo termo é uma função regular e é uma unidade em O_P.

Definição 40 *Seja K o fecho algébrico de $\mathbb{F}$ e $\mathcal{X}$ uma curva. Os pontos da curva tais que $(x, y) \in \mathbb{F}$, são chamados de pontos racionais da curva sobre $\mathbb{F}$.*

Exemplo 30 *Seja $\mathcal{X}$ uma curva com equação $x^3 + y^3 + z^3 = 0$ sobre o fecho de $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$. Existem nove pontos racionais, a saber os deslocamentos cíclicos de $(0, \gamma, 1)$, em que $\gamma \in \{1, \alpha, \alpha + 1\}$. É possível mostrar que no ponto $Q = (0, 1, 1)$ temos um parâmetro local $t = \frac{x}{z}$ para o qual a curva tem um pólo de ordem 2.*

$$\frac{x}{y+z} = t^{-2}(\frac{y^2 + yz + z^2}{z^2}) \tag{B.9}$$

B.8 – Módulo livre

Definição 41 *Um módulo M sobre um anel unitário A (abreviadamente, um A-módulo à esquerda) é um grupo abeliano $(M, +)$ em conjunto com uma operação*

$$A \times M \to M,$$

$$(a, v) \mapsto av$$

de um anel unitário A em M e satisfaz as seguintes propriedades:

- $a(v_1 + v_2) = av_1 + av_2, a \in A, v_1, v_2 \in M$
- $(a + b)v = av + bv, a, b \in A, v \in M$
- $a(bv) = (ab)v, a, b \in A, v \in M$
- $1v = v, v \in M$

De modo análogo, podemos definir os "A-módulos à esquerda". Além disso, se o anel A for comutativo, não é necessário distinguir módulos à esquerda e à direita.

Exemplo 31 *Todo ideal (à esquerda) I de um anel A é um A-módulo para a operação $A \times I \to I$ dada pela multiplicação em A: se $a \in A$ e $b \in I$, então $ab \in I$. Do mesmo modo, A/I é um A-módulo, pois se $a \in A$ e $b + I \in A/I$, então $a(b + I) = ab + I$.*

Definição 42 *Seja M um A-módulo e um conjunto não vazio $S \subseteq M$. Os elementos de S dizem-se linearmente independentes se, para toda família finita $\{v_1, \cdots, v_n\}$ de elementos de S e $a_1, \cdots, a_n \in A$, temos*

$$a_1v_1 + \cdots + a_nv_n = 0 \Rightarrow a_1 = \cdots = a_n = 0$$

Caso contrário, diz-se que os elementos de S são linearmente dependentes.

Definição 43 *Seja M um A-módulo e um conjunto não vazio $S \subseteq M$. S diz-se gerador de M se $M =< S >$. Nesse caso, qualquer elemento $v \in M$ pode ser escrito como uma combinação linear (em geral, não única) de elementos de S:*

$$v = \sum_{i=1}^{k} a_i v_i$$

em que $a_i \in A, v_i \in S$. M é dito um A-módulo de tipo finito se possui um conjunto gerador finito.

Definição 44 *Seja M um A-módulo e um conjunto não vazio $S \subseteq M$. S é uma base de M se é um conjunto gerador cujos elementos são linearmente independentes. Neste caso, qualquer elemento $v \in M$ pode ser escrito na forma única como uma combinação linear de elementos de S:*

$$v = \sum_{i=1}^{k} a_i v_i$$

em que $a_i \in A, v_i \in S$. M diz-se um A-módulo livre se possui uma base.

Exemplo 32 *Todo espaço vetorial é um módulo livre.*

Exemplo 33 *O grupo abeliano $\mathbb{Z}_n$, visto como um $\mathbb{Z}$-módulo, não é livre, pois em $\mathbb{Z}_n$ não existem conjuntos linearmente independentes. De fato, sempre existe um inteiro não-nulo m tal que $mg = 0$.*

B.9 – Bases de Gröbner

Inicialmente, como um polinômio é uma soma de monômios, desejamos arrumar os termos de um polinômio, de forma não ambígua, em ordem decrescente (ou crescente). Para isto, é necessário comparar todo par de monômios para estabelecer suas posições relativas. Deste modo, a ordenação será *linear* ou *total*. Portanto, para cada par de monômios x^α e x^β, exatamente uma das três afirmações a seguir deve ser verdadeira:

$$x^\alpha > x^\beta, x^\alpha = x^\beta, x^\alpha < x^\beta$$

Além disso, é necessário considerar o efeito da soma e do produto sobre os polinômios antes de definir a ordenação monomial. Quando somamos polinômios combinamos os termos iguais e reordenamos os termos de acordo com uma ordem apropriada. Desse modo, a soma não apresenta problemas. Contudo, o produto distribui sobre a adição e, portanto, é necessário acrescentar uma condição. Se $x^\alpha > x^\beta$ e x^γ é qualquer monômio, então iremos requerer que $x^\alpha x^\gamma > x^\beta x^\gamma$. Desse modo, podemos definir uma ordenação monomial.

Definição 45 *Uma ordenação monomial sobre $K[x_1, \cdots, x_n]$ é qualquer relação > sobre $\mathbb{Z}^n_{\geq 0}$, satisfazendo:*

- *> é uma ordenação total (ou linear) sobre $\mathbb{Z}^n_{\geq 0}$.*
- *Se $\alpha > \beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0}$, então $\alpha + \gamma > \beta + \gamma$.*
- *> é uma boa-ordenação em $\mathbb{Z}^n_{\geq 0}$.*

Lema 2 *Uma relação de ordem $>$ sobre $\mathbb{Z}^n_{\geq 0}$ é uma boa-ordenação se, e somente se, toda sequência estritamente decrescente em $\mathbb{Z}^n_{\geq 0}$*

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots$$

finalmente acaba, isto é, tem um menor elemento sobre $>$.

Definição 46 *(Ordenação Lexicográfica) Sejam $\alpha = (\alpha_1, \cdots, \alpha_n)$ e $\beta = (\beta_1, \cdots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Diremos $\alpha >_{lex} \beta$ se, no vetor diferença $\alpha - \beta \in \mathbb{Z}^n$, a coordenada mais à esquerda é não nula. Escreveremos $x^\alpha >_{lex} x^\beta$ se $\alpha >_{lex} \beta$.*

Exemplo 34 $(1, 2, 0) >_{lex} (0, 3, 4)$*, pois* $\alpha - \beta = (1, -1, -4)$.

Exemplo 35 *As variáveis $x_1, x_2, \cdots, x_n$ são ordenadas de forma usual pela ordem lex:*

$$(1, 0, \cdots, 0) >_{lex} (0, 1, 0, \cdots, 0) >_{lex} (0, \cdots, 0, 1)$$

então $x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$.

Proposição 5 *A ordenação lexicográfica sobre $\mathbb{Z}^n_{\geq 0}$ é uma ordenação monomial.*

Observe que na ordenação lexicográfica a variável domina qualquer monômio que contém variáveis menores. Por exemplo, considerando a ordenação lexicográfica com $x > y > z$, temos que $x >_{lex} y^5 z^3$.

Exemplo 36 *Considere o polinômio $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in K[x, y, z]$, então com a ordenação lexicográfica $x > y > z$, teremos $f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$.*

Definição 47 *Seja $f = \sum_\alpha a_\alpha x^\alpha$ um polinômio não nulo em $K[x_1, \cdots, x_n]$ e seja > uma ordenação monomial.*

- *O multigrau de f é $multigrau(f) = max\{\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0\}$.*
- *O coeficiente líder de f é $CL(f) = a_{multigrau(f)} \in K$.*
- *O monômio líder de f é $ML(f) = x^{multigrau(f)}$.*

- *O termo líder de f é $TL(f) = CL(f) \cdot ML(f)$.*

Exemplo 37 *Considere o polinômio $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ e seja > a ordenação lex. Então,*

$$multigrau(f) = (3, 0, 0)$$

$$CL(f) = -5$$

$$ML(f) = x^3$$

$$TL = -5x^3$$

Definição 48 *Um ideal $I \subset K[x_1, \cdots, x_n]$ é um ideal monomial se existe um subconjunto $A \subseteq \mathbb{Z}^n_{\geq 0}$ (possivelmente infinito) tal que I consiste de todos os polinômios que são somas finitas $\sum_{\alpha \in A} h_\alpha x^\alpha$, onde $h_\alpha \in K[x_1, \cdots, x_n]$. Neste caso, escreveremos $I =< x^\alpha : \alpha \in A >$.*

Definição 49 *Seja $I \subset K[x_1, \cdots, x_n]$ um ideal não nulo (diferente do {0}). Denotamos por $TL(f)$ o conjunto de termos líderes dos elementos de I. Deste modo,*

$$TL(I) = \{cx^\alpha : \exists f \in I, \text{ com } TL(f) = cx^\alpha\}.$$

Denotamos por $< TL(f) >$ o ideal gerado pelos elementos de $TL(f)$.

Definição 50 *Fixe uma ordenação monomial. Um subconjunto finito $G = \{g_1, \cdots, g_s\}$ de um ideal I é dito ser uma base de Gröbner (ou base padrão) de I, se*

$$< TL(g_1), \cdots, TL(g_s) >=< TL(I) >$$

APÊNDICE C

Códigos Corretores de Erros

Em um sistema de comunicação uma mensagem é transmitida por um canal de comunicação o qual está sujeito a interferências, comumente chamadas de ruído, e por esse motivo são necessárias medidas para garantir a confiabilidade e qualidade dessa transmissão.

Os ruídos fazem com que a mensagem recebida seja diferente da mensagem enviada e, para a transmissão da informação com confiabilidade, existe a necessidade de desenvolver métodos capazes de detectar e corrigir erros. Daí surge a codificação para o controle de erros, que envolve o uso de um codificador de canal no transmissor e um algoritmo de decodificação no receptor [75].

A taxa de um código é a razão entre a quantidade de bits que entram no codificador e a quantidade de bits que saem do codificador, denotada por R. Define-se a capacidade de um canal C como sendo a medida em bits por uso de canal. Shannon , em 1948, mostrou que se um canal tem capacidade C e uma fonte tem uma taxa de código R, então existe uma técnica de codificação apropriada tal que os símbolos produzidos pela fonte podem ser transmitidos pelo canal com uma probabilidade de erro arbitrariamente pequena [4].

Os códigos gerados pelo codificador de canal são chamados códigos corretores de erros e podem ser classificados basicamente em códigos de bloco e códigos convolucionais. Essa classificação é baseada na presença ou não de memória nos codificadores, assim, os códigos de bloco são ditos sem memória e os códigos convolucionais são ditos com memória, pois um determinado bit codificado depende de um ou mais bits de informação anteriores combinados linearmente.

C.1 – Códigos de Blocos Lineares

Seja $\mathbb{F}$ um corpo finito com q elementos. Em um codificador de bloco, a sequência de informação é segmentada em blocos de mensagens com k bits, denotados por $u = (u_0, u_1, \ldots, u_{k-1})$, em que $u_i \in \mathbb{F}_q$, $i = 0, 1, \ldots, k-1$, assim teremos q^k possíveis mensagens. Cada mensagem u é transformada em uma palavra-código v com n bits. Os

$n-k$ bits introduzidos na mensagem u são chamados bits de verificação de paridade que são a redundância utilizada para o decodificador identificar se houve erros durante a transmissão e, se possível, corrigí-los.

Definição 51 Um código de bloco de comprimento n e 2^k palavras código é dito *código linear* $\mathcal{C} \subset \mathbb{F}^n$, denotado por (n,k), quando $\mathcal{C}$ for subespaço de dimensão k de $\mathbb{F}^n$.

Seja (n,k) um código linear e seja $\{g_0, g_1, \ldots, g_{k-1}\}$ uma de suas bases, portanto, todo elemento do código se escreve de modo único na forma

$$c = u_0 g_0 + u_1 g_1 + \ldots + u_{k-1} g_{k-1}, \tag{C.1}$$

em que $u_i, i = 0, 1, \ldots, k-1$ são coordenadas da mensagem $u = (u_0, u_1, \ldots, u_{k-1})$ de comprimento k.

Os vetores da base $\{g_0, g_1, \ldots, g_{k-1}\}$ formam a *matriz geradora* do código G de ordem $k \times n$.

A partir de G, com algumas manipulações algébricas , extraímos uma matriz $H = [I_{n-k}\ P^T]$, chamada de *matriz de verificação de paridade*, que chamaremos simplesmente de *matriz de paridade*.

A matriz de paridade H é utilizada no processo de detecção e correção de erros, pois dada uma n-upla recebida v podemos afirmar que v é uma palavra código de um código (n,k) gerado pela matriz $G = [P \mid I_k]$ se, e somente se, $v \cdot H^T = 0$. Portanto, a partir da matriz H podemos identificar quando uma mensagem v pertence ou não ao código.

Considere um código linear (n,k) com matriz geradora G e matriz de paridade H. Sejam $c = (v_0, v_1, \ldots, v_{n-1})$ uma palavra código transmitida por um canal ruidoso e $v = (v_0, v_1, \ldots, v_{n-1})$ o vetor recebido no decodificador. Devido aos ruídos do canal de transmissão o vetor recebido v pode ser diferente de c. Então, podemos dizer que essa diferença é o *padrão de erro* dado por $e = c - v$.

No processo de decodificação, ao receber uma mensagem v o decodificador precisa primeiramente determinar se existem ou não erros de transmissão, para isto, o decodificador calcula a *síndrome* de v,

$$s = v \cdot H^T = (s_0, s_1, \ldots, s_{n-k-1}). \tag{C.2}$$

Se v é uma palavra código, então $s = v \cdot H^T = 0$. Nesse caso não existem erros, ou seja, $e = 0$. No entanto, a recíproca não é verdadeira. É possível haver erros que não possam ser detectados, isto é, $s = 0$ mas v não é a palavra código transmitida. Isto ocorre quando temos um padrão de erro não-nulo e que pertence ao código. Nesse caso $v = c + e$ é a soma de duas palavras código e temos $s = v \cdot H^T = 0$. Portanto, estamos diante de um *erro de decodificação*.

Podemos afirmar que $s \neq 0 \Leftrightarrow v$ contém algum erro. Além disso, um fato importante que podemos observar é que a síndrome depende apenas do padrão de erro, e não da palavra-código

transmitida, pois $s \cdot H^T = (c+e) \cdot H^T = c \cdot H^T + e \cdot H^T$, mas como c é palavra-código então $c \cdot H^T = 0$. Logo, $s = e \cdot H^T$.

Portanto, é possível detectar erros introduzidos no canal de transmissão. Contudo, nem todos os padrões de erro podem ser corretamente decodificados. A capacidade de correção de erros de um código de bloco depende diretamente de sua distância mínima, que definiremos na próxima seção.

C.2 – Distância Mínima de um Código de Bloco

Definição 52 Seja $v = (v_0, v_1, \ldots, v_{n-1}) \in V^n$, com V um espaço vetorial sobre $\mathbb{F}_q$. O *peso de Hamming* de v, denotado por $w(v)$ é definido como o número de símbolos diferentes de zero em v.

Exemplo 38 Seja $v = (1\ 0\ 0\ 1\ 0\ 1\ 0)$, então o peso de Hamming de v é $w(v) = 3$.

Definição 53 Considere $v, v' \in V^n$. A *distância de Hamming* entre v e v' denotada por $d(v, v')$ é definida como o número de coordenadas em que v e v' diferem, isto é,

$$d(v, v') = |\{i;\ v_i \neq v'_i,\ 0 \leq i \leq n-1\}|.$$

Definição 54 Dado um código $\mathcal{C} \subset V^n$, então a *distância mínima* de $\mathcal{C}$ denotada por $d_{\min}$ é dada por:

$$d_{\min} = min\{d(v, v'); v, v' \in \mathcal{C}, v \neq v'\},$$

e o *peso mínimo* do código $\mathcal{C}$, denotado por $w_{\min}$, é dado por

$$w_{\min} = \min\{w(v); v \in \mathcal{C}, v \neq 0\}.$$

A distância de Hamming é uma *métrica*, também chamada de *métrica de Hamming*, portanto, valem as seguintes propriedades para $v, v', v'' \in V^n$:

(i) $d(v, v') \geq 0$ e $d(v, v') = 0 \Leftrightarrow v = v'$.

(ii) $d(v, v') = d(v', v)$.

(iii) $d(v, v') \leq d(v, v'') + d(v'', v')$. (Desigualdade triangular)

Teorema 11 Seja $\mathcal{C}$ um código com distância mínima d. Então $\mathcal{C}$ pode corrigir até $\sqcup = \lfloor \frac{d-1}{2} \rfloor$ e detectar até $d-1$ erros.

Proposição 6 (Cota de Singleton) Os parâmetros (n, k, d) de um código linear satisfazem à desigualdade

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

.

Exemplo 39 Calcular a distância de Hamming entre a palavra-código $c = (1\ 1\ 0\ 1\ 0\ 0\ 0)$ e algumas palavras-código:

$d(1\ 1\ 0\ 1\ 0\ 0\ 0\ , 0\ 1\ 1\ 0\ 1\ 0\ 0) = 4$

$d(1\ 1\ 0\ 1\ 0\ 0\ 0\ , 1\ 1\ 1\ 0\ 0\ 1\ 0) = 3$

$d(1\ 1\ 0\ 1\ 0\ 0\ 0\ , 1\ 0\ 0\ 0\ 1\ 1\ 0) = 4$

$d(1\ 1\ 0\ 1\ 0\ 0\ 0\ , 0\ 0\ 1\ 0\ 1\ 1\ 1) = 7$

Calculando a distância de Hamming entre todas as palavras-código obtemos $d_{\min} = 3$. Este fato ocorre para qualquer código de Hamming. Portanto, todo código de Hamming é capaz de detectar até 2 erros e corrigir no máximo 1 erro.

Assim, podemos observar que os códigos de Hamming formam um classe de códigos capazes de corrigir apenas erros simples.