UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
(Doutorado)

MAYCOW GONÇALVES CARNEIRO

CÓDIGOS SOBRE O SEMI-PLANO SUPERIOR FINITO

Maringá - PR
2018

MAYCOW GONÇALVES CARNEIRO

CÓDIGOS SOBRE O SEMI-PLANO SUPERIOR FINITO.

Tese apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas, da Universidade Estadual de Maringá como requisito parcial para obtenção do título de Doutor em Matemática.

Área de concentração: Matemática Aplicada.

Orientador: Prof. Dr. Eduardo Brandani da Silva

Maringá - PR
2018

MAYCOW GONÇALVES CARNEIRO

CÓDIGOS SOBRE O SEMI-PLANO SUPERIOR FINITO

Tese apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Doutor em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Prof. Dr. Eduardo Brandani da Silva
DMA/Universidade Estadual de Maringá (Presidente)

Prof. Dr. Marcelo Muniz Silva Alves
Universidade Federal do Paraná

Profa. Dra. Sueli Irene Rodrigues Costa
Universidade Estadual de Campinas

Prof. Dr. Ednei Aparecido Santulo Junior
DMA/Universidade Estadual de Maringá

Prof. Dr. Josiney Alves de Souza
DMA/Universidade Estadual de Maringá

Aprovada em: 17 de dezembro de 2018.
Local de defesa: Auditório do Departamento de Matemática, Bloco F67, campus da Universidade Estadual de Maringá.

À minha esposa, minha mãe, irmão e irmãs.

Agradecimentos

Agradeço primeiramente à Deus por tudo! Agradeço também ao professor Eduardo Brandani por aceitar me orientar sem me conhecer pessoalmente, e sabendo que eu só teria 2 anos de afastamento para me dedicar em tempo integral ao doutorado. Também gostaria de agradecer ao professor Emerson Vitor Castelani pela ajuda com a parte computacional para gerar os exemplos apresentados. Agradeço ainda à todo apoio recebido de amigos e familiares ao longo do processo de disciplinas, qualificação e da preparação da tese. Por fim, e não menos importante, muito pelo contrário, agradeço à minha esposa, pela ajuda de todas as formas imagináveis para que eu conseguisse alcançar meus objetivos!

"O único lugar onde o sucesso vem antes do trabalho é no dicionário."

Albert Einstein

"Se A é o sucesso, então A é igual a X mais Y mais Z.
O trabalho é X; Y é o lazer; e Z é manter a boca fechada."

Albert Einstein

"Quanto mais aumenta nosso conhecimento, mais evidente fica nossa ignorância"

John F. Kennedy

"Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito.
Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes"

Marthin Luther King

Resumo

Desde que foi proposto por A. Terras em [13], o Semi-Plano Superior Finito só foi utilizado em um trabalho, [35], como ambiente para gerar códigos corretores de erros. Neste trabalho, analisamos algumas propriedades do modelo proposto por Terras para então gerar duas classes de códigos corretores de erros: a primeira baseada no trabalho de Tiu e Wallace [35], sendo lineares e binários e a segunda utilizando as propriedades geométricas do ambiente proposto por A. Terras, gerando códigos não lineares e não binários sobre o Semi-Plano Superior Finito.

Palavras-chave: *Semi-Plano Superior Finito, Códigos Lineres, Códigos não-Lineares*

Abstract

Since it was proposed by A. Terras in [13] , the finite upper half plane was used only once, [35], as an environment in order to generate error correcting codes. In the present work, we analize some properties of the model proposed by Terras to generate then two classes of error correcting codes, the first one based in the work of Tiu and Wallace [35], being linear and binary and the second one using the geometric properties of the environment proposed by A. Terras, generating non linear and non binary codes over Finite Upper Half Planes.

Keywords: *Finite Upper Half Planes, Linear Codes, Non-Linear Codes*

Sumário

Introdução

Após o trabalho de C. E. Shannon [30] em 1948, a teoria dos códigos corretores de erros passou a ser fortemente estudada por matemáticos e engenheiros.

Sempre que vamos transmitir ou armazenar dados, fazemos uso dos códigos corretores de erros, os quais introduzem dados extras aos dados originais, a fim de que possamos recuperar os dados originais de forma correta, mesmo que tenham ocorrido erros devido à ruídos durante a transmissão ou armazenamento dos dados. O estudo concentra-se então em determinar uma forma eficaz e eficiente de se introduzir tais dados extras nos dados originais.

Para se introduzir tais dados extras, tomamos um conjunto A com q elementos, chamado alfabeto, e em seguida determinamos o conjunto A^k, com k natural, e identificamos cada dado com um elemento de A^k. Tal conjunto é chamado código da fonte. Em seguida, introduzimos redundâncias aos elementos do código da fonte, que permitam detectar e corrigir erros. O novo código obtido após este processo, é então, um subconjunto próprio de A^n, com n natural e $n > k$, chamado código de canal. O canal é o meio físico pelo qual se transmitirá os dados.

Neste sentido, da transmissão dos dados pelo canal, em um sistema de comunicação, a informação transmitida é prejudicada, como mencionado, por um ruído agindo no canal de transmissão. Apesar de suas características físicas, o ruído é tratado por um modelo probabilístico, especificando sua função densidade de probabilidade. Assim, o sinal que será transmitido é processado com o objetivo de controlar a ação do ruído. Um componente muito importante do transmissor é o modulador. Para uma modulação eficiente do sinal, o modulador utiliza uma constelação de sinais, a qual é um conjunto finito associado à uma estrutura algébrica. Como mencionado, geralmente, o sistema é modulado em um ambiente Euclidiano. Porém, considerar ambientes não Euclidianos também têm se mostrado ser uma possibilidade promissora.

Uma destas possibilidades é considerar constelações de pontos no plano hiperbólico. O trabalho [32] foi o primeiro a propor um sistema de comunicação tendo como ambiente o plano hiperbólico. O principal potencial para a teoria dos códigos no plano hiperbólico é a

infinitude de tesselações essencialmente distintas, ao contrário do caso Euclidiano. Também podemos encontrar um número infinito de grupos de isometrias propriamente descontínuos que não são isomorfos uns aos outros como subgrupos abstratos. Além disso, para cada grupo de isometrias co-compacto propriamente descontínuo G, existe um número incontável de subgrupos isomorfos à G, embora não conjugados à este. Em outras palavras, para cada subgrupo destes, existe uma situação similar à essencialmente única situação encontrada em $\mathbb{R}^n$.

Depois de [32], vários trabalhos conectando geometria hiperbólica com comunicação e teoria de códigos foram publicados, [1], [9], [21], [7] entre outros. Em [10], é mostrado que é possível conceber códigos corretores mais eficientes, em temos de probabilidade de erros, se eles são elaborados a partir de uma variedade 2-dimensional com genus $g \geq 2$. Sabe-se que a geometria de tais superfícies é a geometria hiperbólica, [11].

Em meados dos anos 1980, A. Terras [13] definiu o Semi-Plano Superior Finito, o qual é definido sobre corpos finitos como análogo do semi plano superior. Em sua construção, um corpo finito de característica ímpar foi utilizado como o análogo finito da reta real e, em seguida, foi-se utilizado a raíz de um elemento não quadrado do corpo finito para gerar o Semi-Plano Superior Finito. Depois, em [14], [3], corpos com característica par foram considerados. Muitas questões foram estudadas por ela e seus colegas, principalmente funções especiais nesses planos ([4], [33]), e grafos finitos, dos quais vários resultados foram obtidos.

Em [35], Tiu e Wallace encontraram uma aplicação na teoria dos códigos. Os autores geraram um código binário linear utilizando a norma neste modelo do Semi-Plano Superior Finito. Contudo, eles consideram apenas o caso onde o Semi-Plano Superior Finito foi construído utilizando corpos finitos com característica ímpar e além disso, com p primo e da apenas da forma $p = 4m + 1$. Assim, o estudo da possibilidade de se obter resultados semelhantes, considerando-se corpos com característica par, na construção do Semi-Plano Superior Finito, apresenta-se interessante. Além disso, em nenhum momento, Tiu e Wallace levam em consideração a geometria deste novo ambiente, deixando assim esta área em aberto para estudo dentro da teoria de códigos. Como não encontramos na literatura trabalhos relacionando códigos com a estrutura geométrica do Semi-Plano Superior Finito, buscamos neste trabalho, encontrar uma aplicação para a geometria deste ambiente na construção de códigos. O trabalho está dividido da seguinte forma:

No Capítulo 1, apresentamos de forma breve alguns conceitos básicos sobre teorica dos códigos corretores de erros e de corpos finitos, os quais serão utilizados ao longo do trabalho, a fim de facilitar a compreensão do leitor que não está tão familiarizado com o tema.

No Capítulo 2, apresentamos os principais resultados sobre o Semi-Plano Superior tanto

para o caso onde o corpo finito tem característica ímpar, [13], [29], [34], quanto para o caso onde a característica é par, [2], [14]. Além disso, provamos alguns resultados que só foram considerados para o caso ímpar em [29] e [34] , mas que serão utilizados neste trabalho para o caso par.

No capítulo 3, utilizamos a idéia do trabalho de Tiu e Wallace [35], onde os autores geram um código linear binário considerando a norma dos elementos do Semi-Plano Superior Finito com a característica ímpar, tomando a entrada da matriz igual a 1 se tal norma é um não quadrado no corpo finito. Como para corpos de característica par tal construção não é possível, apresentamos então, resultados que nos mostram que conseguimos gerar códigos de forma semelhante também no caso par. Além disso, mostramos que os códigos que obtemos neste caso, são códigos quase-cíclicos, algo não apresentado por Tiu e Wallace no caso ímpar.

Por fim, no Capítulo 4, apresentamos uma nova classe de códigos considerando a geometria do Semi-Plano Superior Finito. Tais códigos não são lineares e não são binários e utilizam grupos Fuchsianos, definidos dentro deste ambiente, para serem gerados.

Capítulo 1

Códigos Corretores de Erros e Corpos Finitos

Neste capítulo, veremos alguns resultados básico sobre códigos corretores de erros bem como sobre corpos finitos, os quais serão necessários no decorrer deste trabalho. Os resultados apresentados neste capítulo sobre corpos finitos, podem ser encontrados em sua maioria em [8], [22] e [31], enquanto que os resultados sobre os códigos corretores de erros podem ser encontrados principalmente em [16], [18] e [23]

1.1 Códigos Corretores de erros

Para construirmos um código corretor de erros, precisamos de um conjunto finito A com q elementos, chamado de alfabeto. Denotaremos o número de elementos de A por $|A|$.

Um código corretor de erros é um subconjunto próprio de $A^n = \underbrace{A \times \cdots \times A}_{n}$, para algum número natural n.

1.1.1 Métrica de Hamming

Dada uma palavra de A^n, precisamos de uma forma de identificar a proximidade entre esta e outras palavras de A^n. Para isso introduzimos o conceito de Métrica de Hamming.

Definição 1.1. *Uma métrica em um conjunto X é uma função*

$$d : X \times X \longrightarrow \mathbb{R}$$

satisfazendo as seguintes propriedades:

(i) *(Positividade)* $d(x, y) \geq 0$ *para todo* $x, y \in X$*; a igualdade vale* $\Leftrightarrow x = y$*;*

(ii) *(Simetria)* $d(x, y) = d(y, x)$ *para todo* $x, y \in X$*;*

(iii) *(Desigualdade Triangular)* $d(x, y) \leq d(x, z) + d(z, y)$ *para todo* $x, y, z \in X$*.*

Definição 1.2. *Dados dois elementos* $\boldsymbol{u}$*,* $\boldsymbol{v} \in A^n$*, a distância de Hamming entre* $\boldsymbol{u}$ *e* $\boldsymbol{v}$ *é definida como*

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

Proposição 1.1. *A distância de Hamming* $d(\cdot, \cdot)$ *definida acima é uma métrica.*

Demonstração: Precisamos mostrar que a distância de Hamming satisfaz as três propriedades da definição 1.1. De fato:

(i) Temos por definição $d(\mathbf{u}, \mathbf{v}) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}| \geq 0$. Caso $d(\mathbf{u}, \mathbf{v}) = 0$ teremos $u_i = v_i$ para $i = 1, ..., n$ logo $\mathbf{u} = \mathbf{v}$. Por outro lado, se $\mathbf{u} = \mathbf{v}$ então $u_j = v_j$ para $j = 1, ..., n$ portanto $d(\mathbf{u}, \mathbf{v}) = 0$.

(ii) Pela definição temos $d(\mathbf{u}, \mathbf{v}) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}| = |\{i : v_i \neq u_i, 1 \leq i \leq n\}| = d(\mathbf{v}, \mathbf{u})$.

(iii) Para demonstrar esta propriedade podemos analisar apenas a i-ésima coordenada de $\mathbf{u}$, $\mathbf{v}$ e $\mathbf{w}$. Temos dois casos para analisar, se a contribuição de u_i e v_i para $d(\mathbf{u}, \mathbf{v})$ é zero ou um. Caso a contribuição seja zero, então a contribuição das i-ésimas coordenadas de $d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})$ certamente será maior ou igual à contribuição da i-ésima coordenada de $d(\mathbf{u}, \mathbf{v})$. Por outro lado, se a contribuição é igual a 1 então $u_i \neq v_i$, logo, se $w_i = u_i$, teremos $w_i \neq v_i$, da mesma forma, se $w_i = v_i$, teremos $w_i \neq u_i$, portanto a contribuição da i-ésima coordenada de $d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})$ certamente será maior ou igual a 1 e temos o resultado.

■

Assim a distância de Hamming entre elementos de A^n é uma métrica, também chamada de *métrica de Hamming.*

Definição 1.3. *Dados um elemento* $\boldsymbol{c} \in A^n$ *e um número real* $r > 0$ *definimos a bola e a esfera de centro* $\boldsymbol{c}$ *e raio* r *como sendo, respectivamente, os conjuntos:*

$$B(\boldsymbol{c}, r) = \{\boldsymbol{u} \in A^n : d(\boldsymbol{u}, \boldsymbol{c}) \leq r\}$$
$$S(\boldsymbol{c}, r) = \{\boldsymbol{u} \in A^n : d(\boldsymbol{u}, \boldsymbol{c}) = r\}$$

Definição 1.4. *Dado um código $\mathscr{C}$, definimos a distância mínima de $\mathscr{C}$ por*

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

Um código $\mathscr{C}$ sobre um alfabeto A, possui três parâmetros fundamentais (n, M, d), os quais se referem respectivamente, ao seu comprimento n, ou seja, o ambiente A^n onde está o código $\mathscr{C}$, o seu número de palavras M e a sua distância mínima d.

Quando trabalhamos com códigos corretores de erros, nos deparamos com duas classes de códigos: os códigos lineares e os não lineares. Ainda podemos separar tais códigos em binários ou não binários. A classe de códigos mais utilizada na prática é a dos códigos lineares. Denotaremos por $\mathbb{F}_q$ um corpo com q elementos, o qual será tomado como alfabeto. Temos assim que $\mathbb{F}_q^n$ é um $\mathbb{F}_q$-espaço vetorial de dimensão n com as operações de soma módulo q entre as entradas dos vetores e produto por escalar. Neste trabalho, construiremos duas famílias de códigos corretores de erros: a primeira, uma família de códigos lineares e binários e a segunda, uma família de códigos não lineares e não binários.

Definição 1.5. *Um código $\mathscr{C} \subset \mathbb{F}_q^n$ será chamado código linear se for um subespaço vetorial de $\mathbb{F}_q^n$.*

Como $\mathscr{C}$ é um subespaço vetorial de $\mathbb{F}_q^n$ de dimensão finita, podemos considerar a dimensão deste subespaço como sendo k, assim tomemos uma base para tal subespaço, formada pelos vetores $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$, logo para cada $\mathbf{u} \in \mathscr{C}$ teremos $\mathbf{u} = \lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_k\mathbf{v}_k$, $\lambda_i \in \mathbb{F}, i = 1, \ldots, k$.

Assim, como para cada $\lambda_i \in \mathbb{F}_q$ temos q escolhas, teremos $M = |\mathscr{C}| = q^k$ e consequentemente $\dim_{\mathbb{F}_q} \mathscr{C} = k = \log_q q^k = \log_q M$.

Definição 1.6. *Dado $\boldsymbol{x} \in \mathbb{F}_q^n$, definimos o peso de $\boldsymbol{x}$ como sendo o número inteiro*

$$\omega_H(\boldsymbol{x}) := |\{i : x_i \neq 0\}|,$$

ou seja, $\omega_H(\boldsymbol{x}) = d(\boldsymbol{x}, 0)$, onde d representa a métrica de Hamming.

Definição 1.7. *O peso de um código linear $\mathscr{C}$ é o número inteiro*

$$\omega_H(\mathscr{C}) := min\{\omega_H(\boldsymbol{x}) : x \in \mathscr{C}\backslash\{0\}\}.$$

Utilizaremos a notação com colchetes $[n, M, d]$ para representar os parâmetros de um código linear e com parênteses para representar os parâmetros de um (n, M, d)-código não linear. Além disso, para um código linear $\mathscr{C}$, o número de palavras depende da dimensão do mesmo, visto que $M = q^k$, assim podemos tomar os parâmetros desse código como sendo $[n, k, d]$ onde n é o comprimento do código, k é a dimensão e d é a distância mínima que, pela Definição 1.7 é o mesmo que o peso do código. De fato, note que para todo par de elementos $\mathbf{x}, \mathbf{y} \in \mathscr{C}$, com $\mathbf{x} \neq \mathbf{y}$, temos $\mathbf{z} = \mathbf{x} - \mathbf{y} \in \mathscr{C} \backslash \{0\}$ e $d(\mathbf{x}, \mathbf{y}) = \omega_H(\mathbf{z})$. Logo, $d = \omega(\mathscr{C})$.

Uma das formas de se descrever um subespaço vetorial em álgebra linear, é tomando o mesmo como imagem de uma transformação linear. Assim, consideremos uma base $\beta = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ de $\mathscr{C}$ e tomemos a matriz G cujas linhas são os vetores $\mathbf{v}_i = v_{i1}, \ldots, v_{in}$ para $i = 1, \ldots, k$, isto é

$$G = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}.$$

A matriz G é chamada matriz geradora do código $\mathscr{C}$ referente à base β.

Consideremos a transformação linear definida por

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ & \mathbf{x} & \mapsto & \mathbf{x}G \end{array}$$

Assim se $\mathbf{x} = (x_1, \ldots, x_k)$, teremos que $T(\mathbf{x}) = x_1\mathbf{v}_1 + \cdots + x_k\mathbf{v}_k$, ou seja, $T(\mathbb{F}_q^k) = \mathscr{C}$.

Lembrando que dada uma base de um espaço vetorial, podemos conseguir outra base para este espaço vetorial, efetuando operações elementares sobre os elementos da primeira base, dada uma matriz geradora G e acrescentando também as operações de permutação de colunas e multiplicação de uma coluna por um escalar não nulo, obtemos uma matriz G' geradora de um código $\mathscr{C}'$ equivalente ao código $\mathscr{C}$, ou seja, com os mesmos parâmetros e número de palavras, sendo que o número de palavras de peso i em $\mathscr{C}$ se mantém em $\mathscr{C}'$.

De fato, quando efetuamos as operações elementares juntamente com as duas operações descritas acima em uma base de $\mathscr{C}$, efetuamos em todas as palavras de $\mathscr{C}$.

Exemplo 1.1. Código de Hamming [7,4,3]
Um exemplo de matriz geradora de um código é a matriz abaixo, geradora do código de Hamming com parâmetros $[7, 4, 3]$.

Definição 1.8. *Dizemos que uma matriz geradora G de um código $\mathscr{C}$ está na forma padrão*

se tivermos

$$G = (Id_k|A),$$

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

Nem sempre conseguimos uma matriz geradora para um código $\mathscr{C}$ na forma padrão, porém, conseguimos um código equivalente $\mathscr{C}'$ com matriz geradora na forma padrão. Este resultado é provado em [16], página 87.

Como visto na Definição 1.5, um código é linear se for um subespaço vetorial de $\mathbb{F}_q^n$. Porém, se não tivermos tal restrição, ainda assim podemos ter um código com parâmetros (n, M, d), onde n é o comprimento do código, M é o número de palavras e d é o maior número tal que, quaisquer duas palavras do código diferem em pelo menos d coordenadas, onde utilizamos a distância de Hamming vista em 1.2. Portante, neste caso, a soma de duas palavras do código pode não ser uma palavra do mesmo, ao contrário do caso linear. Como mencionado, neste trabalho obteremos uma família de códigos lineares, onde para isto, utilizaremos um corpo finito de caracterísca par para a construção do código, tornando-o binário em seguida, conforme veremos, e uma família de códigos não lineares, onde utilizaremos um corpo podendo ter característica par ou ímpar.

1.2 Corpos Finitos

Como mencionado, no decorrer deste trabalho a estrutura algébrica mais utilizada será a de corpos finitos. Como este é um assunto exaustivamente estudado por todos os interessados em teoria de códigos, apresentaremos de forma sucinta apenas definições e resultados que serão utilizados ao longo deste trabalho.

Definição 1.9. *Um Anel é um conjunto* R *munido de duas operações binarias denotadas* $+$ *e* $\cdot$ *que satisfazem:*

i *Para quaisquer elementos* $a, b, c \in R$,

$$a + (b + c) = (a + b) + c;$$

ii *Existe um elemento neutro* $e \in R$ *com respeito à operação* $+$, *ou seja, tal que para todo* $a \in R$ *temos*

$$a + e = e + a = a;$$

iii *Para cada elemento $a \in R$ existe um elemento $d \in R$ tal que*

$$a + d = d + a = e;$$

iv *Para quaisquer elementos $a, b \in R$ temos*

$$a + b = b + a;$$

v *Para quaisquer elementos $a, b, c \in R$,*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c;$$

vi *Para quaisquer elementos $a, b, c \in R$,*

$$a \cdot (b + c) = a \cdot b + a \cdot c \ \ e \ \ (a + b) \cdots c = a \cdots c + b \cdots c.$$

Na definição acima, denotaremos o elemento neutro com respeito à operação $+$, que chamaremos de soma, por 0. Em um anel R, se existe um elemento neutro, que denotaremos por 1 com respeito à operação $\cdot$, chamada de multiplicação, ou seja, tal que $a \cdot 1 = 1 \cdot a = a \ \forall a \in R$, dizemos que o anel R é um *anel com unidade*. Além disso, se a operação $\cdot$ é tal que $a \cdot b = b \cdot a \ \forall a, b \in R$, dizemos que R é um *anel comutativo*.

Definição 1.10. *Um corpo $\mathbb{F}$ é um anel comutativo com unidade tal que:*

i *Para quaisquer $a, b \in \mathbb{F}$ se $a \cdot b = 0$ então $a = 0$ ou $b = 0$;*

ii *Para cada elemento $a \in \mathbb{F}$ existe um elemento $a^{-1} \in \mathbb{F}$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.*

Neste trabalho, utilizaremos apenas corpos finitos, ou seja, um corpo $\mathbb{F}$ com um número finito de elementos.

Definição 1.11. *Seja p primo, $\mathbb{F}_p$ o conjunto composto pelos números $\{0, 1, 2, \ldots, p-1\}$ e considere a aplicação $\phi : \mathbb{Z}/(p) \to \mathbb{F}_p$ dada por $\phi([a]) = a$. Então $\mathbb{F}_p$ munido da estrutura de corpo induzida por ϕ é um corpo finito, chamado Corpo de Galois de ordem p.*

Definição 1.12. *A característica do corpo $\mathbb{F}$ é o menor inteiro n tal que $n.a = 0$ para todo $a \in \mathbb{F}$. Se não existe tal inteiro, dizemos que $\mathbb{F}$ tem característica 0.*

Teorema 1.2. *[22] Um corpo finito possui como característica um número primo.*

Se p é primo, então a característica de $\mathbb{F}_p$ é o próprio p. Neste trabalho, utilizaremos para a construção de uma família de códigos lineares, corpos finitos com $q = 2^r$ elementos, ou seja, corpos com característica 2, enquanto que para a construção da família de códigos não lineares a característica poderá ser ímpar.

Teorema 1.3. *[23] Em qualquer corpo de característica p, temos que*

$$(a + b)^p = a^p + b^p.$$

O resultado anterior pode ser estendido para $(a + b)^{p^n} = a^{p^n} + b^{p^n}$. Como mencionado anteriormente, trabalharemos com corpos da forma $\mathbb{F}_{2^r}$, ou seja, um corpo de característica 2. Assim, pelo teorema anterior, obtemos $(x + y)^2 = x^2 + y^2$.

Pela Definição 1.11, para p primo, podemos tomar $\mathbb{F}_p = \{0, 1, 2, \ldots, p - 1\}$, ou seja, o conjunto dos inteiros módulo p. Porém, como trabalharemos com $\mathbb{F}_{p^r}$, e p^r não é primo para $r > 1$, precisaremos de outra forma para representar os elementos do corpo $\mathbb{F}_{p^r}$. Para isto, precisamos da noção de polinômios irredutíveis sobre corpos finitos.

Primeiramente, lembramos que um polinômio sobre o corpo $\mathbb{F}$ é uma expressão da forma $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a^nx^n$ onde $a_i \in \mathbb{F}$ para $0 \leq i \leq n$ e $n \in \mathbb{N}$. O anel formado por polinômios sobre $\mathbb{F}$ com as operações de soma e multiplicação de polinômios, é chamado anel de polinômios sobre $\mathbb{F}$ e denotado por $\mathbb{F}[x]$.

Definição 1.13. *Um polinômio $p(x) \in \mathbb{F}[x]$ é dito irredutível sobre $\mathbb{F}$ (ou irredutível em $\mathbb{F}[x]$), se $p(x)$ tem grau positivo e $p(x) = f(x)g(x)$ com $f(x), g(x) \in \mathbb{F}[x]$, implica que $f(x)$ ou $g(x)$ é um polinômio constante.*

Uma raíz de um polinômio $p(x) \in \mathbb{F}[x]$ em $\mathbb{F}$ é um elemento $\alpha \in \mathbb{F}$ que satisfaz $p(\alpha) = 0$. Note que um polinômio irredutível sobre um corpo $\mathbb{F}$ não possui raíz sobre este corpo.

Definição 1.14. *Seja $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{F}[x]$. Então a derivada de $p(x)$ é dado por $p'(x)$ onde $p'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in \mathbb{F}[x]$.*

Teorema 1.4. *[22] Um elemento $\alpha \in \mathbb{F}$ é uma raíz múltipla de um polinômio $p(x) \in \mathbb{F}[x]$ se, e somente se, é raíz de ambos, $p(x)$ e $p'(x)$.*

Definição 1.15. *Um conjunto $K \subseteq \mathbb{F}$, que munido das operações de $\mathbb{F}$ é ainda um corpo, é chamado de subcorpo de $\mathbb{F}$. Se $K \neq \mathbb{F}$ dizemos que K é um subcorpo próprio de $\mathbb{F}$ e ainda neste contexto, dizemos que $\mathbb{F}$ é uma extensão de K.*

Dizemos que um elemento $\zeta \in \mathbb{F}$ é algébrico sobre K se este elemento satisfaz uma equação polinomial não trivial sobre K, ou seja, $a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1} + a_n\zeta^n = 0$, com $a_i \in K$ não todos nulos. Uma extensão L de K, onde todos os elementos são algébricos sobre K, é chamada de extensão algébrica de K.

Afim de construirmos o corpo $\mathbb{F}_{p^r}$, utilizaremos estes conceitos conforme o resultado abaixo.

Teorema 1.5. *[22] Seja $p(x) \in \mathbb{F}[x]$ um polinômio irredutível sobre $\mathbb{F}$. Então existe uma extensão algébrica simples de $\mathbb{F}$ com uma raíz de $p(x)$ como elemento definidor.*

Assim, dado um polinômio irredutível de grau m sobre um corpo primo $\mathbb{F}_p$, ou seja, um corpo onde p é primo, podemos construir uma extensão algébrica simples de $\mathbb{F}_p$ adicionando a raíz de tal polinômio, conseguindo assim um corpo finito com p^m elementos.

Exemplo 1.2. Consideremos $p(x) = x^2 + x + 1$ o qual é irredutível sobre $\mathbb{F}_2$ e consideremos ζ uma raiz deste polinômio, ou seja, tal que $\zeta^2 + \zeta + 1 = 0$, então podemos considerar o corpo $\mathbb{F}_2(\zeta)$ que contém os elementos $\{0, 1, \zeta, \zeta + 1\}$. Temos então que $\mathbb{F}_2(\zeta)$ é uma extensão algébrica simples de $\mathbb{F}_2$ a qual é um corpo com $2^2 = 4$ elementos.

Teorema 1.6. *[23] Seja $p(x)$ um polinômio irredutível de grau r sobre $\mathbb{F}_p$. Então o conjunto de todos os polinômios de grau menor ou igual a $r - 1$ com coeficientes em $\mathbb{F}_p$ e operações realizadas módulo $p(x)$, formam um corpo de ordem p^r.*

Se tomarmos por exemplo, um polinômio irredutível $p(x)$ de grau r sobre o corpo $\mathbb{F}_p$, o conjunto de todos os polinômios mônicos de grau $\leq r - 1$ com coeficientes em $\mathbb{F}_p$, forma o corpo $\mathbb{F}_{p^r}$.

Exemplo 1.3. Como exemplo, vejamos o caso de $\mathbb{F}_8 = \mathbb{F}_{2^3}$, para isto consideremos o polinômio $p(x) = x^3 + x + 1$ que é irredutível sobre $\mathbb{F}_2$, então os polinômios mônicos de grau menor ou igual a $3-1 = 2$ são: $0, 1, x, x^2, 1+x, 1+x^2, 1+x+x^2, x+x^2$ e considerando as operações de soma e multiplicação destes polinômios módulo $p(x)$, obtemos a representação dos elementos de $\mathbb{F}_8$ como polinômios, $\mathbb{F}_8 = \{0, 1, x, x^2, 1 + x, 1 + x^2, 1 + x + x^2, x + x^2\}$. Note que se considerarmos ζ uma raíz do polinômio $p(x) = x^3 + x + 1$ obtemos uma extensão algébrica de $\mathbb{F}_2$ dada por $\mathbb{F}_2(\zeta) = \{0, 1, \zeta, \zeta^2, 1 + \zeta, 1 + \zeta + \zeta^2, \zeta + \zeta^2\}$.

Note que, no exemplo anterior, os corpos obtidos foram essencialmente os mesmo, apenas representados de forma diferente. Além disso, se tomarmos outro polinômio irredutível para construirmos o corpo, obteremos um corpo isomorfo ao anterior, o que é confirmado pelo teorema a seguir.

Lembrando que a ordem de um corpo finito é o número de elementos deste corpo, temos o seguinte resultado.

Teorema 1.7. *[23] Todos os corpos de mesma ordem p^r são isomorfos.*

Consideremos o corpo finito $\mathbb{F}_q$. Denotaremos por $\mathbb{F}_q^*$ o conjunto dos elementos não nulos de $\mathbb{F}_q$.

Lembremos que um grupo multiplicativo finito é cíclico se o mesmo consiste dos elementos $1, a, a^2, \ldots, a^{q-1}$ com $a^q = 1$, onde a é um elemento não nulo do grupo. Neste caso, a é o gerador do grupo e escrevemos $G = \langle a \rangle$.

Teorema 1.8. *[23] $\mathbb{F}_q^*$ é um grupo multiplicativo cíclico de ordem $p^r - 1$, dado que $q = p^r$.*

Definição 1.16. *Um gerador do grupo multiplicativo cíclico $\mathbb{F}_q^*$ é chamado elemento primitivo de $\mathbb{F}_q$.*

Teorema 1.9. *[23] Todo corpo $\mathbb{F}_q$ possui um elemento primitivo.*

Teorema 1.10. *[22] Seja $\mathbb{F}_p$ um corpo finito e $\mathbb{F}_q$ uma extensão finita do corpo. Então $\mathbb{F}_q$ é uma extensão algébrica simples de $\mathbb{F}_p$ e todo elemento primitivo de $\mathbb{F}_q$ serve como um elemento definidor de $\mathbb{F}_q$ sobre $\mathbb{F}_p$.*

Pelos teoremas acima, se tomarmos α um elemento primitivo de $\mathbb{F}_{p^r}$, então este será um elemento definidor de $\mathbb{F}_{p^r}$ sobre $\mathbb{F}_p$, ou seja, os elementos de $\mathbb{F}_{p^r}$ serão dados por $\mathbb{F}_{p^r} = \{0, \alpha^0 = 1, \alpha, \alpha^2, \ldots, \alpha^{p^r-2}\}$. Utilizaremos esta representação para os elementos de $\mathbb{F}_{p^r}$, ou seja, como potências de um elemento primitivo.

Assim, para construirmos os elementos de $\mathbb{F}_{p^r}$, tomaremos um polinômio irredutível $p(x)$ de grau r sobre $\mathbb{F}_p$ cuja raíz, digamos α, em $\mathbb{F}_{p^r}$ é um elemento primitivo de $\mathbb{F}_{p^r}$. Neste caso teremos a representação desejada dos elementos de $\mathbb{F}_{p^r}$ como potências de um único elemento.

Exemplo 1.4. Novamente, se utilizarmos $p(x) = x^3+x+1$ para construirmos o corpo $\mathbb{F}_8 = \mathbb{F}_{2^3}$, então, tomando α uma raíz deste polinômio, podemos escrever os elementos de $\mathbb{F}_8$ como sendo potências de α. Temos que $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. Note que, como $p(\alpha) = 0$, obtemos $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^2 + \alpha + 1$ e $\alpha^6 = \alpha^2 + 1$, e assim podemos representar os elementos de $\mathbb{F}_8$ como potências de α mais o elemento nulo, ou seja, $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ e este corpo é essencialmente o mesmo obtido no Exemplo 1.3. Porém $q(x) = x^3 + x^2 + 1$ também é irredutível sobre $\mathbb{F}_2$, logo também pode ser utilizado para construir um corpo com 8 elementos, onde se γ é uma raíz de $q(x)$, então os elementos deste corpo serão $\{0, 1, \gamma, \gamma^2, \gamma^3 = \gamma^2 + 1, \gamma^4 = 1 + \gamma + \gamma^2, \gamma^5 = 1 + \gamma, \gamma^6 = \gamma + \gamma^2\}$. Note

que γ^3 também é raíz de $p(x)$, logo podemos tomar a aplicação que leva $\alpha \leftrightarrow \gamma^3$ a qual é um isomorfismo e assim os corpos são isomorfos.

Como vimos no exemplo acima, o corpo construído é essencialmente o mesmo, independente do polinômio definidor escolhido, porém por praticidade nas contas desenvolvidas, escolheremos o polinômio com base nos resultados que seguirão. No exemplo anterior, a escolha do polinômio irredutível não fez diferença para escrevermos os elementos do corpo como potências de uma raíz do polinômio, porém, como mencionado, a raíz precisa ser um elemento primitivo, e nem sempre isto ocorre.

Exemplo 1.5. Consideremos o polinômio $p(x) = x^4 + x^3 + x^2 + x + 1$ que é irredutível sobre $\mathbb{F}_2$, então podemos utilizar este polinômio para escrever uma extensão algébrica de grau 4 sobre $\mathbb{F}_2$ adicionando a raíz deste polinômio, ou seja, se α é uma raíz de $p(x)$, temos que a extensão algébrica de grau 4 será $\mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha^2, \alpha^3, 1+\alpha, 1+\alpha^2, 1+\alpha^3, \alpha+\alpha^2, \alpha+\alpha^3, \alpha^2+\alpha^3, 1+\alpha+\alpha^2, 1+\alpha+\alpha^3, 1+\alpha^2+\alpha^3, \alpha+\alpha^2+\alpha^3, 1+\alpha+\alpha^2+\alpha^3\}$. Porém, não podemos escrever os elementos deste corpo como potências de α visto que $\alpha^5 = 1$, ou seja, uma raíz deste polinômio irredutível não é um elemento primitivo.

Se por outro lado tomarmos $q(x) = x^4 + x^3 + 1$, o qual também é irredutível sobre $\mathbb{F}_2$ então podemos tomar α como sendo uma raíz deste polinômio e conseguiremos escrever $\mathbb{F}_{16} = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}$.

Na literatura existem diversos trabalhos sobre polinômios irredutíveis primitivos sobre corpos finitos, os quais podem ser utilizados para a construção do corpo finito desejado com os elementos dados por potências de uma raíz do mesmo. Neste trabalho, optaremos por utilizar a representação de elementos de um corpo $\mathbb{F}_q$ como potências de um elemento primitivo. Assim, vejamos mais alguns resultados que nos auxiliarão a determinar qual polinômio irredutível escolher de forma a obtermos um elemento primitivo.

Primeiramente, lembremos que se m é um número inteiro positivo, então podemos fatorar este número como produto de potências de números primos, $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Então, a função de Euler do número m é dada por

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

Assim conseguimos o seguinte resultado.

Teorema 1.11. *[22] O corpo finito $\mathbb{F}_q$ possui $\phi(q-1)$ elementos primitivos.*

Assim, utilizamos este resultado para determinar se podemos escolher qualquer polinômio irredutível de grau r sobre $\mathbb{F}_p$ na construção do corpo $\mathbb{F}_{p^r}$.

Exemplo 1.6. Consideremos o corpo $\mathbb{F}_8$. Então, pelo teorema anterior, este corpo possui $\phi(7) = 7(1 - \frac{1}{7}) = 6$ elementos primitivos, como este corpo possui 8 elementos, se tirarmos os elementos 0 e 1, todos os demais elementos serão elementos primitivos, logo para qualquer polinômio irredutível de grau 3 sobre $\mathbb{F}_2$ que escolhermos, vamos ter que uma raíz será um elemento primitivo.

Por outro lado, como vimos, $\mathbb{F}_{16}$ terá $\phi(15) = 15(1 - \frac{1}{3})(1 - \frac{1}{5}) = 8$ elementos primitivos, e como este corpo possui 16 elementos, não podemos escolher qualquer polinômio irredutível para tomarmos uma raíz.

Caso não possamos escolher qualquer polinômio irredutível de grau r na construção de $\mathbb{F}_{p^r}$, utilizaremos os seguintes resultados.

Teorema 1.12. *[22] Seja $q = p^r$. Então o corpo finito $\mathbb{F}_q$ é o $(q-1)$-ésimo corpo ciclotômico sobre $\mathbb{F}_p$.*

Temos que o $(q-1)$-ésimo corpo ciclotômico sobre $\mathbb{F}_p$ é o corpo de divisão de $x^{q-1} - 1$ sobre $\mathbb{F}_p$, ou seja, uma extensão $\mathbb{F}_q$ de $\mathbb{F}_p$ que possui todas as raízes deste polinômio, isto é, tal que $x^{q-1} - 1$ pode ser escrito como produto de fatores lineares em $\mathbb{F}_q[x]$. Assim, se fatorarmos o polinômio $x^{q-1} - 1$ sobre $\mathbb{F}_p$ em polinômios irredutíveis sobre $\mathbb{F}_p$ conseguiremos encontrar o polinômio desejado. Para isto, vamos utilizar os polinômios ciclotômicos.

Primeiramente, se $\mathbb{F}_q$ é o corpo de divisão de $x^{q-1} - 1$ sobre $\mathbb{F}_p$, então as raízes de $x^{q-1} - 1$ em $\mathbb{F}_q$ são chamadas de raízes $(q-1)$-ésimas da unidade. Além disso, temos que

$$x^{q-1} - 1 = \prod_{d|(q-1)} Q_d(x),$$

onde $q - 1$ não é divisível pela característica de $\mathbb{F}_q$, ou seja, por p e $Q_d(x)$ é o d-ésimo polinômio ciclotômico sobre $\mathbb{F}_q$, com coeficiente no corpo $\mathbb{F}_p$. Para encontrarmos tais polinômios utilizaremos um resultado que necessita da Função de Moebius, a qual é definida como:

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ (-1) & \text{se n se escreve como produto de k primos distintos} \\ 0 & \text{se n se escreve como o quadrado de um primo} \end{cases}$$

Assim, temos o seguinte resultado.

Teorema 1.13. *[22] Seja $\mathbb{F}_q$ um corpo com característica p e n um inteiro não divisível por p. Então o n-ésimo polinômio ciclotômico $Q_n(x)$ sobre $\mathbb{F}_q$ satisfaz*

$$Q_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)} = \prod_{d|n}(x^{d/n} - 1)^{\mu(d)}.$$

Exemplo 1.7. Consideremos o corpo $\mathbb{F}_{16}$ e $n = 15$, então temos que o polinômio ciclotômico $Q_{15}(x)$ sobre $\mathbb{F}_{16}$ é dado por

$$Q_{15}(x) = \prod_{d|n}(x^d-1)^{\mu(n/d)} = (x-1)^{\mu(15)}(x^3-1)^{\mu(5)}(x^5-1)^{\mu(3)}(x^{15}-1)^{\mu(1)} = \frac{(x^{15}-1)(x-1)}{(x^5-1)(x^3-1)} = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1.$$

Teorema 1.14. *[22] Considere o $(q-1)$-ésimo corpo ciclotômico $\mathbb{F}_q$ sobre $\mathbb{F}_p$. Então este é uma extensão algébrica simples sobre $\mathbb{F}_p$ e além disso, se $MDC(p, q-1) = 1$ então $Q_{q-1}(x)$ se fatora em $\frac{\phi(q-1)}{d}$ polinômios irredutíveis de mesmo grau d sobre $\mathbb{F}_p[x]$, onde d é tal que $p^d = 1 mod(q-1)$ e assim $\mathbb{F}_q$ é o corpo de divisão sobre $\mathbb{F}_p$ de qualquer um desses fatores.*

Pelo teorema anterior, para encontrarmos um elemento primitivo para gerarmos o corpo $\mathbb{F}_q$, basta encontramos $Q_{q-1}(x)$ e fatorarmos este polinômio em polinômios irredutíveis de grau r, onde $q = p^r$, sobre $\mathbb{F}_2$ e tomarmos o elemento primitivo como sendo uma raíz de qualquer um destes polinômios.

Exemplo 1.8. No exemplo anterior vimos que $\mathbb{F}_{16}$ é o 15-ésimo corpo ciclotômico. Como $16 = 2^4$ e $Q_{15}(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$, o qual se fatora em $\frac{\phi(15)}{4} = 2$ polinômio irredutíveis de grau 4 sobre $\mathbb{F}_2[x]$, e $f(x) = x^4 + x^3 + 1$ é irredutível sobre $\mathbb{F}_2[x]$ temos que $Q_{15}(x) = (x^4 + x^3 + 1)(x^4 + x + 1)$ e podemos utilizar a raíz de qualquer um destes dois polinômios como elemento primitivo.

Teorema 1.15. *[22] Seja f um polinômio irredutível sobre $\mathbb{F}_p$ de grau r. Então f possui uma raíz α na extensão $\mathbb{F}_{p^r}$ e além disso todas as raízes de f são dadas pelos r elementos distintos $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{r-1}}$ de $\mathbb{F}_{p^r}$.*

No decorrer do trabalho estaremos interessados em particular, em polinômios de grau 2, irredutíveis sobre um corpo $\mathbb{F}_q$. Pois utilizaremos tais polinômios na construção do Semi-Plano Superior Finito H_q quando $q = 2^r$, apresentado no próximo capítulo. Assim, vejamos alguns resultados específicos que nos auxiliarão.

Primeiramente, precisamos da noção de traço e norma de um elemento de um corpo finito.

Definição 1.17. *Seja $\mathbb{F}_{p^r}$ uma extensão de $\mathbb{F}_p$ e $\alpha \in \mathbb{F}_{p^r}$. Então os elementos α, α^p, α^{p^2}, ..., $\alpha^{p^{r-1}}$ são chamados conjugados de α com respeito a $\mathbb{F}_p$.*

Definição 1.18. *Para $\alpha \in \mathbb{F}_{p^r}$, onde $\mathbb{F}_p$ é o subcorpo primo de $\mathbb{F}_{p^r}$, o traço $Tr_{\mathbb{F}_p}(\alpha)$ de α sobre $\mathbb{F}_p$ é dado por*

$$Tr_{\mathbb{F}}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{r-1}}.$$

Assim, o traço de um elemento α sobre $\mathbb{F}_p$ é a soma dos seus conjugados. Outra definição importante é a da norma de um elemento, que nada mais é que o produto de seus conjugados.

Definição 1.19. *Para $\alpha \in \mathbb{F}_{p^r}$, onde $\mathbb{F}_p$ é o subcorpo primo de $\mathbb{F}_{p^r}$, a norma $N_{\mathbb{F}}(\alpha)$ de α sobre $\mathbb{F}_p$ é dada por*

$$N_{\mathbb{F}_p}(\alpha) = \alpha \cdot \alpha^p \cdot \cdots \cdot \alpha^{p^{r-1}}.$$

De posse destas definições, podemos agora apresentar alguns resultados específicos para polinômios de grau 2, como mencionado.

Teorema 1.16. *[22] Seja $\mathbb{F}_q$ um corpo finito com característica p e $a \in \mathbb{F}_q$. Então o trinômio $x^p - x - a$ é irredutível em $\mathbb{F}_q[x]$ se, e somente se, $Tr_{\mathbb{F}}(a) \neq 0$.*

Como iremos trabalhar com o corpo $\mathbb{F}_{2^r}$, cuja característica é 2, e em $\mathbb{F}_{2^r}$ temos que $-1 = 1$, o resultado anterior nos diz que o polinômio $x^2 + x + a$ é irredutível sobre $\mathbb{F}_{2^r}$ se, e somente se, $Tr_{\mathbb{F}}(a) \neq 0$. Além disso, trabalharemos com a representação dos elementos de $\mathbb{F}_{2^r}$ como potências de um elemento primitivo. Assim, o próximo resultados nos auxiliará na escolha de tal elemento primitivo.

Teorema 1.17. *[23] $\mathbb{F}_{2^r}$ contém um elemento primitivo de traço igual a 1.*

Tal resultado aparece em [23] como um corolário e sua demonstração pode ser encontrada em [26].

Assim, ao construirmos o corpo $\mathbb{F}_{2^r}$, escolheremos como elemento definidor α, um elemento primitivo com traço igual a 1, obtendo assim o polinômio irredutível $p(x) = x^2 + x + \alpha$ sobre $\mathbb{F}_{2^r}$.

Exemplo 1.9. Pelo exemplo 1.8, temos duas opções de polinômios irredutíveis sobre $\mathbb{F}_2$ de grau 4 para construirmos $\mathbb{F}_{16}$, onde os elementos de $\mathbb{F}_{16}$ serão dados por potências de uma raíz de um destes polinômios. Se tomarmos o polinômio $f(x) = x^4 + x + 1$ e γ uma raíz deste, então $Tr_{\mathbb{F}_2}(\gamma) = \gamma + \gamma^2 + \gamma^4 + \gamma^8 = 0$, porém se tomarmos $p(x) = x^4 + x^3 + 1$ e α uma raíz deste, teremos $Tr_{\mathbb{F}_2}(\alpha) = \alpha + \alpha^2 + \alpha^4 + \alpha^8 = 1$. Logo escolheremos α para gerar $\mathbb{F}_{16}$ e neste caso, pelo teorema anterior teremos que $x^2 + x + \alpha$ será irredutível sobre $\mathbb{F}_{16}$.

Outros resultados relacionados à corpos finitos que utilizaremos em nosso trabalho são apresentados a seguir.

Definição 1.20. *Para qualquer corpo finito $\mathbb{F}_q$, a função valor inteiro υ em $\mathbb{F}_q$ é definida por*

$$\upsilon(b) = -1, \;\; b \in \mathbb{F}_q^* \;\; e \;\; \upsilon(0) = q - 1.$$

Lema 1.18. *[22] Seja q par e $a \in \mathbb{F}_q$ com $Tr_{\mathbb{F}_q}(a) = 1$ e $b \in \mathbb{F}_q$. Então o número de soluções em $\mathbb{F}_q$ de $x^2 + xy + ay^2 = b$ é dado por $q - \upsilon(b)$.*

Ao longo do trabalho, denotaremos o número de soluções de $x^2 + xy + ay^2 = b$ em $\mathbb{F}_q$, com as hipóteses do teorema acima, por $S(x^2 + xy + ay^2 = b)$.

Além dos conceitos e resultados apresentados sobre corpos finitos, outra estrutura que será muito utilizada ao longo do trabalho é a do Grupo Linear Geral, $GL_2(\mathbb{F}_q)$ das matrizes não singulares 2×2 com entradas em $\mathbb{F}_q$.

Como $GL_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \;\; a, b, c, d \in \mathbb{F}_q, \;\; ad - bc \neq 0 \right\}$, então se a, b, c, d são todos não nulos, basta tomarmos $a \neq d^{-1}bc$, o que nos dá $(q-1)^3(q-2)$ escolhas, se exatamente uma das entradas é nula, então as outras 3 podem ser qualquer elemento não nulo o que nos dá um total de $4(q-1)^3$ elementos, por fim, se duas entradas são nulas, elas devem estar na posição oposta uma da outra para que a matriz seja inversível, e as outras duas podem ser qualquer elemento não nulo, logo temos $2(q-1)^2$ escolhas. Portanto o número total de elementos de $GL_2(\mathbb{F}_q)$ é

$$|GL_2(\mathbb{F}_q)| = (q-1)^3(q-2) + 4(q-1)^3 + 2(q-1)^2 = (q^2-1)(q^2-q).$$

Definição 1.21. *Dados dois elementos x e y de um grupo G, dizemos que estes elementos são conjugados se existe $g \in G$ tal que $gxg^{-1} = y$.*

Esta é uma relação de equivalência e assim podemos considerar classes de equivalência com relação à conjugação. Temos que a classe de equivalência de $x \in G$ com relação à conjugação é dada por

$$C_x = \{y \in G \mid \exists g \in G \text{ tal que } gxg^{-1} = y\}.$$

Se X é um conjunto qualquer e G um grupo, então uma ação de G sobre o conjunto X é

uma aplicação

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \mapsto & gx \end{array}.$$

Neste caso, se considerarmos $X = GL_2(\mathbb{F}_q)$, $G = GL_2(\mathbb{F}_q)$ e a ação dada pela conjugação, ou seja, $\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \mapsto & aba^{-1} \end{array}$, teremos que as classes de equivalência serão as G-órbitas, também chamadas de classes de conjugação. O número de classes de conjugação de $G = GL_2(\mathbb{F}_q)$ é o número de G-órbitas ou classes de conjugação distintas e pode ser determinado analisando o polinômio característico $p(x)$ e minimal $m(x)$ de $g \in G$.

Proposição 1.19. *[17] Seja $G = GL_2(\mathbb{F}_q)$. Então:*

(i) *Se $g \in GL_2(\mathbb{F}_q)$ é tal que $p(x) = (x-a)^2$ e $m(x) = x - a$, um representante para a classe de conjugação de g é $g = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ e o número de classes é $q-1$ cada uma com 1 elemento;*

(ii) *Se $g \in GL_2(\mathbb{F}_q)$ é tal que $p(x) = m(x) = (x-a)^2$, um representante para a classe de conjugação de g é $g = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ e o número de classes é $q-1$ cada uma com (q^2-1) elementos;*

(iii) *Se $g \in GL_2(\mathbb{F}_q)$ é tal que $p(x) = m(x) = (x-a)(x-b)$ com $a \neq b$, um representante para a classe de conjugação de g é $g = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ e o número de classes é $\frac{1}{2}(q-1)(q-2)$ cada uma com q^2+q elementos;*

(iv) *Se $g \in GL_2(\mathbb{F}_q)$ é tal que $p(x) = x^2 + ax + b$ é irredutível sobre $\mathbb{F}_q$, então considerando a extensão quadrática $\mathbb{F}_{q^2}$ e $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, um representante para a classe de conjugação de g é $g = \begin{pmatrix} 0 & \alpha^{q+1} \\ -1 & \alpha + \alpha^q \end{pmatrix}$ e o número de classes é $\frac{q^2-q}{2}$ cada uma com $q^2 - q$ elementos.*

Capítulo 2

Modelo do Semi-Plano Superior Finito

O Semi-Plano Superior Finito foi introduzido por Terras em [13], e foi posteriormente estudado em uma série de trabalhos, Celniker [12], Poulos [27], Angel e Velasquez [3], [4], Terras [33], [34] onde consideram $q = p^r$ um número ímpar com p primo e $\mathbb{F}_q$ um corpo com q elementos, e em seguida analisam as propriedades geométricas e analíticas do que chamam de Semi Plano Superior Finito, o qual é obtido substituindo-se $\mathbb{R}$ por $\mathbb{F}_q$ no Semi Plano de Poincaré. Angel [2] e Evans [14] também consideram os casos de corpos com característica par. Inicialmente, veremos os resultados para p ímpar e em seguida para $p = 2$.

Quando estudamos geometria hiperbólica, nos deparamos com o modelo do Semi-Plano Superior ou, também chamado por alguns como Semi-Plano Superior de Poincaré. Tal Semi-Plano Superior é definido como

$$H = \{x + iy,\ \ x, y \in \mathbb{R},\ \ y > 0\}, \quad \text{onde } i = \sqrt{-1}.$$

Terras et al. [13] consideram então, um modelo semelhante, substituindo-se $\mathbb{R}$ por um corpo finito $\mathbb{F}_p$, com p ímpar e i por $\sqrt{\varsigma}$ onde ς é um não quadrado em $\mathbb{F}_p$ e analisam as propriedades de tal modelo. A seguir introduziremos os principais resultados obtidos em [13], [34] e em seguida, apresentaremos nossos resultados para o caso par com destaque para o Lema 2.6 e o Teorema 2.7.

Definição 2.1. *Sejam p um número primo ímpar, $q = p^r$, $\mathbb{F}_q$ um corpo finito com q elementos e ς um não quadrado em $\mathbb{F}_q$. Definimos o Semi-Plano Superior Finito H_q como*

$$H_q = \{x + y\sqrt{\varsigma},\ \ x \in \mathbb{F}_q,\ \ y \in \mathbb{F}_q^*\}.$$

Note que, pela definição, H_q possui $q(q-1)$ elementos. Seguindo o modelo do Semi-Plano

Superior, define-se uma "pseudo-distância" em H_q. Considerando $z = x + y\sqrt{\varsigma} \in H_q$, assim como no modelo do Semi-Plano Superior, dizemos que a parte imaginária de z é $Im(z) = y$. Tomamos ainda $\overline{z} = x - y\sqrt{\varsigma}$ e consideramos a norma $N(z) = z\overline{z}$. Com tais elementos obtemos uma definição para uma distância neste modelo proposto.

Definição 2.2. *Sejam $z, w \in H_q$. Definimos a "distância" entre z e w por*

$$d(z,w) = \frac{N(z-w)}{Im(z)Im(w)}.$$

Vale ressaltar que esta distância retorna um elemento do corpo, por isso consideramos a mesma como uma "pseudo-distância".

Exemplo 2.1. Consideremos $\mathbb{F}_3 = \{0,1,2\}$, então 2 é um não quadrado em $\mathbb{F}_3$ e temos que $H_3 = \{z_1 = \sqrt{2}, z_2 = 2\sqrt{2}, z_3 = 1+\sqrt{2}, z_4 = 1+2\sqrt{2}, z_5 = 2+\sqrt{2}, z_6 = 2+2\sqrt{2}\}$. Logo, $d(z_3,z_6) = \dfrac{N(z_3-z_6)}{Im(z_3)Im(z_4)} = \dfrac{N((1+\sqrt{2})-(2+2\sqrt{2}))}{1.2} = \dfrac{N(2+2\sqrt{2})}{2} = \dfrac{(2+2\sqrt{2})(2-2\sqrt{2})}{2} = 1.$

Considerando o grupo linear geral $GL(2,\mathbb{F}_q)$ das matrizes 2×2 com entradas em $\mathbb{F}_q$ e determinante não nulo, obtemos que a distância é invariante por transformações fracionárias lineares, ou seja, se $g \in GL(2,\mathbb{F}_q)$, temos que $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ age em H_q por $g(z) = \dfrac{az+b}{cz+d}$ e assim, $d(z,w) = d(g(z),g(w))$.

De fato, sejam $z = x + y\sqrt{\varsigma}$ e $w = u + v\sqrt{\varsigma}$ pertencentes a H_q. Então, pelas definições dadas, temos que $Im(z) = y$, $Im(w) = v$, $g(z) = \dfrac{az+b}{cz+d}$, $g(w) = \dfrac{aw+b}{cw+d}$, $Im(g(z)) = \dfrac{(ad-bc)Im(z)}{N(cz+d)}$, $Im(g(w)) = \dfrac{(ad-bc)Im(w)}{N(cw+d)}$.

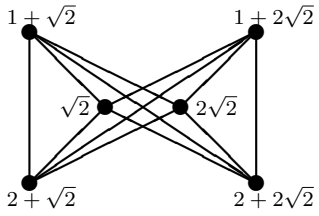
Assim

$$\begin{aligned} d(g(z),g(w)) &= \frac{N(g(z)-g(w))}{Im(g(z))Im(g(w))} = \frac{N\left(\frac{(az+b)(cw+d)-(aw+b)(cz+d)}{(cz+d)(cw+d)}\right)}{\frac{(ad-bc)^2Im(z)Im(w)}{N(cz+d)N(cw+d)}} = \\ &= \frac{N((az+b)(cw+d)-(aw+b)(cz+d))}{(ad-bc)^2Im(z)Im(w)} = \frac{N((ad-bc)(z-w))}{(ad-bc)^2Im(z)Im(w)} = \\ &= \frac{N(z-w)}{Im(z)Im(w)} = d(z,w). \end{aligned}$$

O Semi-Plano Superior Finito está intimamente ligado à teoria dos grafos, e isso foi uma das motivações para sua definição.

Definição 2.3. *Fixe $a \in \mathbb{F}_q$, com $a \neq 0, 4\varsigma$. Define-se o grafo $X_q(\varsigma, a)$ como sendo o grafo tendo como vértices os elementos de H_q e dois vértices z e w sendo adjacentes se $d(z, w) = a$.*

Exemplo 2.2. Consideremos o Semi-Plano Superior Finito H_3, construído no exemplo 2.1. Como $\varsigma = 2$, e o único $a \in \mathbb{F}_3$ tal que $a \neq 0, 4\varsigma$ é $a = 1$, o único grafo que conseguimos neste caso é o $X_3(2, 1)$. Neste caso teremos dois vértices adjacentes se $d(z, w) = 1$ e obtemos o seguinte grafo:



Os artigos [13], [33], [34], trabalham em sua maioria, com propriedades destes grafos para q ímpar. Como neste trabalho não utilizaremos tanto os conceitos de grafos, iremos omitir a maioria dos resultados, apresentando apenas alguns a seguir.

Primeiramente vejamos alguns conceitos gerais sobre grafos. Dizemos que o grau de um vértice v de um grafo é o número de vértices que são adjacentes à este vértice v no grafo. Se este número é o mesmo, digamos k, para todos os vértices, dizemos que o grafo é k-regular, além disso, se para quaisquer dois vértices v e u conseguirmos um caminho formado por vértices adjacentes começando em v e terminando em u, dizemos que o grafo é conexo. Temos ainda que se G é um grupo finitamente gerado e S é um subgrupo gerador, então o grafo tendo como vértices os elementos de G e vértices adjacentes v e u se $u = sv$, com $s \in S$, é chamado grafo de Cayley.

Agora colocaremos em um único teorema, vários resultados obtidos para os grafos construídos em $\mathbf{H}_q$.

Teorema 2.1. *[33] Sejam $q = p^r$, com p primo ímpar, $\mathbb{F}_q$ um corpo com q elementos, ς um não quadrado em $\mathbb{F}_q$ e $a \in \mathbb{F}_q$.*

i *Se $a \neq 0, 4\varsigma$, então $X_q(\varsigma, a)$ é um grafo $(q+1)-$regular;*

ii *Os grafos $X_q(\varsigma, a)$ e $X_q(\varsigma.c^2, a.c^2)$ são isomorfos;*

iii *Seja τ um elemento do grupo de Galois $Gal(\mathbb{F}_q/\mathbb{F}_p)$, então os grafos $X_q(\varsigma, a)$ e $X_q(\tau(\varsigma), \tau(a)$ são isomorfos;*

iv *Se $a \neq 0, 4\varsigma$, o grafo $X_q(\varsigma, a)$ é conexo. Na verdade, $X_q(\varsigma, a)$ é um grafo de Cayley para o grupo afim*

$$Aff(q) = \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} | x, y \in \mathbb{F}_q, \ \ y \neq 0 \right\}$$

usando os geradores

$$S_q(\varsigma, a) = \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} | x, y \in \mathbb{F}_q, \ \ y \neq 0, x^2 = ay + \varsigma(y-1)^2 \right\}.$$

Outro resultado importante obtido é o próximo teorema. Lembrando que um grafo conexo k-regular é Ramanujan se o segundo maior auto-valor, em módulo, da matriz de adjacência do grafo satisfaz $|\lambda| \leq 2\sqrt{k-1}$.

Teorema 2.2. *[19] Seja ς um não quadrado em $\mathbb{F}_q$, com $q = p^r$ potência de um primo ímpar e $a \in \mathbb{F}_q$, $a \neq 0, 4\varsigma$. Então o grafo $X_q(\varsigma, a)$ é Ramanujan.*

Muitos outros resultados analíticos e geométricos foram obtidos para os grafos em H_q, com muitos teoremas sobre a matriz de adjacência dos grafos, seus autovalores entre outros. Não utilizaremos estes resultados neste trabalho. Assim, seguimos com o estudo de H_q para q par.

Note que na definição do Semi-Plano Superior Finito H_q, é necessário um elemento não quadrado em $\mathbb{F}_q$. Tal elemento não existe se a característica do corpo é par.

De fato, como trabalharemos com $\mathbb{F}_{2^r}$, a característica do corpo é 2, e neste caso todo elemento $a \in \mathbb{F}_{2^r}$ satisfaz $a^{2^r} = a$, ou seja, para todo elemento do corpo, existe um elemento que elevado ao quadrado resulta no anterior, neste caso, $a = (a^{2^{r-1}})^2$. Assim, a fim de definir o Semi-Plano Superior Finito para potências de 2, precisamos de algumas modificações.

Tais modificações foram apresentadas por Evans [14] e Angel [2], os resultados apresentados a seguir podem ser encontrados nestas referências.

Primeiramente, para $q = 2^r$, o corpo $\mathbb{F}_q$ não é isomorfo aos inteiros módulo q. Assim, a fim de construir tal corpo, como visto no capítulo anterior, tomamos um polinômio irredutível de grau r sobre $\mathbb{F}_2$, cuja raíz é um elemento primitivo de $\mathbb{F}_{2^r}$.

Considere então o corpo $\mathbb{F}_{2^r}$ assim obtido. Como não há um elemento não quadrado, para contornar este "problema", consideramos então um novo polinômio irredutível, agora quadrático, sobre $\mathbb{F}_{2^r}$ e θ uma raíz deste polinômio sobre a extensão quadrática de $\mathbb{F}_{2^r}$ e definimos o Semi-Plano Superior Finito de forma análoga por:

Definição 2.4. *Seja x^2+tx+n um polinômio irredutível sobre $\mathbb{F}_q$, com $q=2^r$ e θ uma raíz deste polinômio sobre a extensão quadrática $\mathbb{F}_{q^2}$. O Semi-Plano Superior Finito H_q é definido como*

$$H_q=\{x+\theta y|\ x,y\in\mathbb{F}_q,\ \ y\neq 0\}.$$

Note que, como θ é raíz de x^2+tx+n sobre $\mathbb{F}_{q^2}[x]$, então θ^q também é uma raíz. Assim, podemos tomar $n=\theta\theta^q$ e $t=\theta+\theta^q$, uma vez que $x^2+tx+n=(x+\theta)(x+\theta^q)$ em $\mathbb{F}_{q^2}[x]$.

Pode-se mostrar que a escolha do polinômio quadrático irredutível não interfere nos resultados obtidos. Sendo assim, uma vez que optamos no capítulo 1, após os resultados do Teorema 1.16 e Teorema 1.17, construir o corpo $\mathbb{F}_{2^r}$ com os elementos sendo potências de um elemento primitivo α, com $Tr(\alpha)=1$ e vimos que neste caso $x^2+x+\alpha$ é irredutível sobre $\mathbb{F}_{2^r}$, optaremos por construir o Semi-Plano Superior H_{2^r} com θ raíz do polinômio $x^2+x+\alpha$. Neste caso teremos $\theta\theta^q=\alpha$ e $\theta+\theta^q=1$, o que facilitará nossas contas ao longo do trabalho.

Exemplo 2.3. Considere o corpo $\mathbb{F}_8=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$ construído no exemplo 1.4 tendo α como raíz do polinômio irredutível x^3+x^2+1 sobre $\mathbb{F}_2$. Neste caso temos que $Tr(\alpha)=1$ e assim, pelo Teorema 1.16, $x^2+x+\alpha$ é irredutível sobre $\mathbb{F}_8$. Logo, tomando θ uma raíz deste polinômio sobre $\mathbb{F}_{8^2}$ construímos o Semi-Plano Superior Finito H_8 como sendo

$H_8=\{\theta,\ \theta\alpha,\ \theta\alpha^2,\ \theta\alpha^3,\ \theta\alpha^4,\ \theta\alpha^5,\ \theta\alpha^6,$
$1+\theta,\ 1+\theta\alpha,\ 1+\theta\alpha^2,\ 1+\theta\alpha^3,\ 1+\theta\alpha^4,\ 1+\theta\alpha^5,\ 1+\theta\alpha^6,$
$\alpha+\theta,\ \alpha+\theta\alpha,\ \alpha+\theta\alpha^2,\ \alpha+\theta\alpha^3,\ \alpha+\theta\alpha^4,\ \alpha+\theta\alpha^5,\ \alpha+\theta\alpha^6,$
$\alpha^2+\theta,\ \alpha^2+\theta\alpha,\ \alpha^2+\theta\alpha^2,\ \alpha^2+\theta\alpha^3,\ \alpha^2+\theta\alpha^4,\ \alpha^2+\theta\alpha^5,\ \alpha^2+\theta\alpha^6,$
$\alpha^3+\theta,\ \alpha^3+\theta\alpha,\ \alpha^3+\theta\alpha^2,\ \alpha^3+\theta\alpha^3,\ \alpha^3+\theta\alpha^4,\ \alpha^3+\theta\alpha^5,\ \alpha^4+\theta\alpha^6,$
$\alpha^4+\theta,\ \alpha^4+\theta\alpha,\ \alpha^4+\theta\alpha^2,\ \alpha^4+\theta\alpha^3,\ \alpha^4+\theta\alpha^4,\ \alpha^4+\theta\alpha^5,\ \alpha^4+\theta\alpha^6,$
$\alpha^5+\theta,\ \alpha^5+\theta\alpha,\ \alpha^5+\theta\alpha^2,\ \alpha^5+\theta\alpha^3,\ \alpha^5+\theta\alpha^4,\ \alpha^5+\theta\alpha^5,\ \alpha^5+\theta\alpha^6,$
$\alpha^6+\theta,\ \alpha^6+\theta\alpha,\ \alpha^6+\theta\alpha^2,\ \alpha^6+\theta\alpha^3,\ \alpha^6+\theta\alpha^4,\ \alpha^6+\theta\alpha^5,\ \alpha^6+\theta\alpha^6\}.$

Para $z=x+\theta y\in H_{2^r}$, utilizaremos a notação $\overline{\theta}=\theta^{2^r}$ e obtemos o "conjugado"de z como sendo $\overline{z}=x+y\overline{\theta}$. Então, assim como no caso q ímpar, temos $\mathrm{Im}(z)=y$ e se considerarmos a "norma" $N(z)=z\overline{z}=z^{2^r+1}$, temos também a definição de uma "pseudo-distância" dada por $d(z,w)=\frac{N(z-w)}{Im(z)Im(w)}$. Neste caso também temos que o grupo $GL(2,\mathbb{F}_{2^r})$ age em H_{2^r} por transformações lineares fracionárias, ou seja, se $g=\begin{bmatrix} a & b\\ c & d\end{bmatrix}$ então a ação de g em H_q é dada por $g(z)=\frac{az+b}{cz+d}$ e novamente temos $d(z,w)=d(g(z),g(w))$.

Definimos também o grafo $X_{2^r}(\theta,a)$ tendo como vértices os elementos de H_{2^r} e tendo dois vértices z e w adjacentes se $d(z,w)=a$.

Como as propriedades que utilizaremos, em sua maioria, valem para ambos os casos, vamos considerar

$$\mathbf{H}_q = \{x + \delta y |\ x, y \in \mathbb{F}_q,\ y \neq 0\},\ \delta = \begin{cases} \sqrt{\varsigma},\ \varsigma \text{ não quadrado em } \mathbb{F}_q & \text{se q é ímpar} \\ \theta,\ \text{raíz de } x^2 + x + \alpha \text{ em } \mathbb{F}_{q^2} & \text{se q é par} \end{cases} \tag{2.1}$$

No próximo capítulo construiremos nossas famílias de códigos, como mencionado anteriormente, construiremos uma família de códigos lineares para o caso em que q é par, e uma família de códigos não lineares considerando ambos os casos. Assim, vejamos mais alguns resultados sobre $\mathbf{H}_q$ para ambos os casos. Primeiramente, vejamos um resultado sobre a distância definida, provado por Evans em [14] para o caso par e por Terras em [13] para o caso ímpar. Utilizaremos $\mathbf{H}_q$ como apresentado em (2.1), e vamos considerar como origem de $\mathbf{H}_q$ o elemento $z_0 = \delta$.

Lema 2.3. *Os elementos $z = x + \delta y$ e $z_0 = \delta$ pertencentes à $\boldsymbol{H}_q$ são adjacentes em $X_q(\delta, a)$ se, e somente se,*

$$\begin{cases} x^2 + x(y-1) + \alpha(y-1)^2 = ya & \textit{para } q \textit{ par} \\ x^2 - \delta^2(y-1)^2 = ya & \textit{para } q \textit{ ímpar} \end{cases}$$

Demonstração: De fato, temos que $Im(z) = y$, $Im(z_0) = 1$ e que por definição do grafo $X_q(\delta, a)$, os elementos são adjacentes se, e somente se, $d(z, z_0) = a$ para ambos os casos. Assim temos

$$a = d(z, z_0) \Leftrightarrow a = \frac{N(z - z_0)}{Im(z)Im(z_0)} \Leftrightarrow a = \frac{N(x + \delta y - \delta)}{y.1} \Leftrightarrow ay = N(x + \delta(y-1)).$$

Agora, se q é par, temos $\delta = \theta$ e assim

$$\begin{aligned} &ay = N(x + \delta(y-1)) \Leftrightarrow ay = [x + \theta(y-1)][x + \theta^q(y-1)] \Leftrightarrow \\ &ay = x^2 + (\theta + \theta^q)x(y-1) + \theta\theta^q(y-1)^2 \Leftrightarrow \\ &ay = x^2 + x(y-1) + \alpha(y-1)^2. \end{aligned}$$

Se q é ímpar, temos

$$ay = [x + \delta(y-1)][x - \delta(y-1)] \Leftrightarrow ay = x^2 - \delta^2(y-1)^2.$$

■

Em [2], Angel prova separadamente, vários resultados sobre os grafos para o caso p par, entre eles os resultados do Teorema 2.1 para q par. Assim, como fizemos no Teorema 2.1, colocaremos vários destes resultados como itens de um único teorema e utilizaremos o Semi-Plano Superior Finito $\mathbf{H}_q$ apresentado em (2.1).

Teorema 2.4. *[2] Seja $q = 2^r$, $\mathbb{F}_{2^r}$ um corpo com 2^r elementos, $a \in \mathbb{F}_{2^r}$, $\boldsymbol{H}_{2^r}$ como em (2.1) e considere o conjunto $S(\delta, a) = \{z \in \boldsymbol{H}_{2^r} | d(z, \delta) = a\}$.*

(i) *Se $a \neq 0, 1$, então $X_{2^r}(\delta, a)$ é um grafo $(q+1)-$regular;*

(ii) *Se $\delta_1 = c + d\delta_2$, com $c, d \in \mathbb{F}_{2^r}$, então $X_{2^r}(\delta_1, a) = X_{2^r}(\delta_2, \frac{a}{d^2})$;*

(iii) *Seja $\tau \in Gal(\mathbb{F}_{2^r}/\mathbb{F}_2)$, então os grafos $X_{2^r}(\delta, a)$ e $X_{2^r}(\delta, \frac{\tau(a)}{(Im\tau(\delta))^2})$ são isomorfos;*

(iv) *Se $z \in S(\delta, a)$ então $\overline{z} \in S(\delta, 1 + a)$;*

(v) $\sqrt{a} + \delta \in S(\delta, a)$;

(vi) *Se $a \neq 0, 1$, então o grafo $X_{2^r}(\delta, a)$ é conexo. Na verdade $X_{2^r}(\delta, a)$ é um grafo de Cayley para o grupo afim, $Aff(\mathbb{F}_{2^r})$ usando os geradores*

$$S = \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} | x + \delta y \in S(\delta, a) \right\}$$

Teorema 2.5. *[14] Seja $a \in \mathbb{F}_{2^r}$ com $a \neq 0,\ 1$. Então o grafo $X(\delta, a)$ é Ramanujan.*

Para a construção da família de códigos não lineares e não binários que faremos no capítulo 4, utilizaremos os conceitos geométricos apresentados por Terras em [34] e Shaheen em [29], [28]. Nos referidos trabalhos considera-se apenas o caso q ímpar, porém consideraremos também o caso onde q é par, e por isso provaremos os resultados.

Quando estudamos a geometria hiperbólica no Semi-Plano Superior, nos deparamos com os grupos fuchsianos e os domínios fundamentais para a ação destes grupos sobre o Semi-Plano Superior. Nos referidos trabalhos [34], [29], [28], os autores adaptam estes conceitos ao Semi-Plano Superior Finito. Como estamos trabalhando com corpos finitos, e qualquer subconjunto finito de $GL(2, \mathbb{F}_q)$ é discreto, estes serão grupos fuchsianos. Então, assim como no caso do Semi-Plano Superior, podemos definir um domínio fundamental para a ação de um grupo discreto $\Gamma \subseteq GL(2, \mathbb{F}_q)$ sobre $\mathbf{H}_q$.

Antes de falarmos sobre o domínio fundamental para $\mathbf{H}_q$, precisamos definir uma ordem em $\mathbb{F}_q$. Para isto, consideremos α um elemento primitivo, logo, gerador do grupo multiplicativo

$\mathbb{F}_q^*$ e então, consideremos a ordem

$$0 < 1 < \alpha < \alpha^2 < \alpha^3 < \cdots < \alpha^{q-2}. \tag{2.2}$$

Agora, seja $\Gamma \subseteq GL(2, \mathbb{F}_q)$ um subgrupo e Γ' o conjunto dos elementos não triviais de Γ, ou seja, diferentes de múltiplos da identidade e $z_0 \in \mathbf{H}_q$ um ponto que não é fixado por nenhum elemento de Γ', ou seja, tal que $\gamma(z_0) \neq z_0 \forall \gamma \in \Gamma'$, definimos os conjuntos:

$$D_\Gamma(z_0) = \{w \in \mathbf{H}_q | d(z_0, w) < d(\gamma z_0, w), \ \ \forall \gamma \in \Gamma'\},$$
$$\overline{D_\Gamma(z_0)} = \{w \in \mathbf{H}_q | d(z_0, w) \leq d(\gamma z_0, w), \ \ \forall \gamma \in \Gamma'\}.$$

Note que na definição dos conjuntos acima, precisamos de um elemento $z_0 \in \mathbf{H}_q$ que não é fixado por nenhum elemento de Γ', o qual sempre existe.

De fato, pela Proposição 1.19 temos que os representantes para as classes de conjugação de $\mathrm{GL}(2, \mathbb{F}_q)$, que não são múltiplos da identidade, são $g_1 = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$, $g_2 = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ com $a, b \in \mathbb{F}_q$, $a \neq b$ e $g_3 = \begin{pmatrix} 0 & \alpha^{q+1} \\ -1 & \alpha + \alpha^q \end{pmatrix}$ com $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Agora note que se γ pertence à classe de conjugação de g_1 ou g_2 então nenhum elemento de $\mathbf{H}_q$ é fixado, pois $\gamma(z) = z \Leftrightarrow a'z + b' = c'z^2 + d'z$ a qual não tem solução nestes dois casos. Se γ pertence à classe de conjugação de g_3, então $\gamma(z) = z \Leftrightarrow z^2 - (\alpha + \alpha^q)z + \alpha^{q+1} = 0$, a qual possui como solução a origem de $\mathbf{H}_q$ e seu "conjugado". Portanto qualquer elemento de $\mathbf{H}_q$ diferente da origem ou seu conjugado, não é fixado por nenhum elemento de Γ'.

Temos então que os conjuntos apresentados são os análogos às regiões de Dirichlet, para o semi-plano superior finito. Outro resultado obtido por Terras em [34] nos ajuda a definir um dominínio fundamental para $\mathbf{H}_q$ e o mesmo é provado pelos autores apenas para q ímpar, assim apresentamos a demonstração considerando-se também o caso par.

Lema 2.6. *Dado $z \in \boldsymbol{H}_q$, existe $\gamma \in \Gamma$ tal que $\gamma z \in \overline{D_\Gamma(z_0)}$. Além disso, se $z, w \in D_\Gamma(z_0)$ e $\gamma z = w$ para algum $\gamma \in \Gamma$, então γ é um elemento trivial.*

Demonstração: Seja $\gamma \in \Gamma$ tal que $d(z_0, \gamma z) \leq d(z_0, \gamma' z) \ \ \forall \gamma' \in \Gamma$. Tal γ existe pois Γ é finito. Como múltiplos da identidade fixam todos os elementos de $\mathbf{H}_q$, podemos supor que $\gamma \in \Gamma'$ ou que $\gamma = I$, onde I é a matriz identidade. Vamos provar que este é o γ procurado.

De fato, escolha outro elemento $\gamma' \in \Gamma'$, pela invariância de d sob a ação de Γ, temos que $d(\gamma' z_0, \gamma z) = d(z_0, (\gamma')^{-1}\gamma z)$. Temos então dois casos para analisarmos:

Caso 1: $\gamma = I$

Neste caso, pela invariância de d sob a ação de Γ e pela escolha de $\gamma = I$, obtemos:

$$d(\gamma^{'} z_0, z) = d(z_0, (\gamma^{'})^{-1} z) \geq d(z_0, z).$$

Caso 2: $\gamma \neq I$

Novamente, pela invariância de d sob a ação de Γ, temos $d(\gamma^{'} z_0, \gamma z) = d(z_0, (\gamma^{'} \gamma z))$. Agora, se $\gamma^{'} \gamma \in \Gamma^{'} \cup \{I\}$, pela escolha de γ, temos que $d(z_0, \gamma^{'} \gamma z) \geq d(z_0, \gamma z)$ e assim

$$d(z_0, \gamma z) \leq d(\gamma^{'} z_0, \gamma z).$$

Agora, se $\gamma^{'} \gamma = \lambda I$, então $\gamma^{'} = \gamma \circ (\lambda I)$, donde segue que $\gamma^{'} z = \gamma z$ e então

$$d(\gamma^{'} z_0, \gamma z) = d(\gamma^{'} z_0, \gamma^{'} z) = d(z_0, z) \geq d(z_0, \gamma z).$$

Portanto, $\gamma z \in \overline{D_\Gamma(z_0)}$.

Para a segunda parte, suponha que $z, w \in \overline{D_\Gamma(z_0)}$ com $w = \gamma z$ e $\gamma \in \Gamma^{'}$. Então, $d(z_0, z) < d(\gamma z_0, z) \ \ \forall \gamma \in \Gamma^{'}$. Por outro lado, como $\gamma z \in D_\Gamma(z_0)$, então

$$d(\gamma^{-1} z_0, z) = d(z_0, \gamma z) < d(\gamma z_0, \gamma z) = d(z_0, z),$$

absurdo. Portanto γ é trivial.

■

Com este lema, temos que $\overline{D_\Gamma(z_0)}$ é quase um domínio fundamental para a ação de $\Gamma \subseteq GL(2, \mathbb{F}_q)$ sobre $\mathbf{H}_q$, sendo necessário, em alguns casos, retirar alguns elementos de forma a satisfazer as condições da seguinte definição, obtida a partir da definição no Semi-Plano Superior.

Definição 2.5. *Seja $\Gamma \subseteq GL(2, \mathbb{F}_q)$ um subgrupo e $z_0 \in \boldsymbol{H}_q$ um ponto que não é fixado por nenhum $\gamma \in \Gamma'$. Diremos que $\mathfrak{D}$ é um Domínio Fundamental para Γ sobre $\boldsymbol{H}_q$, se $\mathfrak{D}$ for um menor subconjunto tal que $D_\Gamma(z_0) \subseteq \mathfrak{D} \subseteq \overline{D_\Gamma(z_0)}$ e satisfaz:*

1. $\bigcup_{\gamma \in \Gamma} \gamma(\mathfrak{D}) = \boldsymbol{H}_q$;
2. *se $z, w \in D_\Gamma(z_0)$ e $\gamma z = w$ para algum $\gamma \in \Gamma$, então γ é um elemento trivial, ou seja, $\overset{\circ}{\mathfrak{D}} \cap \gamma(\overset{\circ}{\mathfrak{D}}) = \emptyset, \ \ \forall \gamma \in \Gamma'$.*

Basicamente, um domínio fundamental conterá um elemento de cada γ-órbita. Exemplos para o caso q ímpar podem ser encontrados em [28]. Vejamos um exemplo para q par.

Exemplo 2.4. Seja $q = 4$ e considere $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ onde α é raíz de $x^2 + x + 1$, ou seja, elemento primitivo de $\mathbb{F}_4$. Então tomamos $x^2 + x + \alpha$, irredutível sobre $\mathbb{F}_4$, e δ raíz deste. Assim teremos:

$\mathbf{H}_4 = \{x + \delta y |\ x, y \in \mathbb{F}_4,\ y \neq 0\} = \{\delta,\ \delta\alpha,\ \delta\alpha^2,\ 1+\delta,\ 1+\delta\alpha,\ 1+\delta\alpha^2,\ \alpha+\delta,\ \alpha+\delta\alpha,\ \alpha+\delta\alpha^2,\ \alpha^2+\delta,\ \alpha^2+\delta\alpha,\ \alpha^2+\delta\alpha^2\}$.

Considere agora o subgrupo $\Gamma \subset GL(2, \mathbb{F}_4)$ dado por $\Gamma = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F}_4 \right\}$ e $z_0 = 1+\delta$. Temos que:

$$\Gamma = \left\{ \gamma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \gamma_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \gamma_3 = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \gamma_4 = \begin{pmatrix} 1 & \alpha^2 \\ 0 & 1 \end{pmatrix} \right\},$$

$$D_\Gamma(z_0) = \{1+\delta\} \quad ,$$

$$\overline{D_\Gamma(z_0)} = \{z_0 = 1+\delta,\ z_1 = 1+\delta\alpha,\ z_2 = 1+\delta\alpha^2,\ z_3 = \alpha+\delta\alpha,\ z_4 = \alpha^2+\delta\alpha^2\}.$$

Então

$\Gamma(z_0) = \{\gamma_1 z_0 = 1+\delta,\ \gamma_2 z_0 = \delta,\ \gamma_3 z_0 = \alpha^2+\delta,\ \gamma_4 z_0 = \alpha+\delta\}$,
$\Gamma(z_1) = \{\gamma_1 z_1 = 1+\alpha\delta,\ \gamma_2 z_1 = \alpha\delta,\ \gamma_3 z_1 = \alpha^2+\alpha\delta,\ \gamma_4 z_1 = \alpha+\alpha\delta\}$,
$\Gamma(z_2) = \{\gamma_1 z_2 = 1+\alpha^2\delta,\ \gamma_2 z_2 = \alpha^2\delta,\ \gamma_3 z_2 = \alpha^2+\alpha^2\delta,\ \gamma_4 z_2 = \alpha+\alpha^2\delta\}$,
$\Gamma(z_3) = \{\gamma_1 z_3 = \alpha+\alpha\delta,\ \gamma_2 z_3 = \alpha^2+\alpha\delta,\ \gamma_3 z_3 = \alpha\delta,\ \gamma_4 z_3 = 1+\alpha\delta\}$,
$\Gamma(z_4) = \{\gamma_1 z_4 = \alpha^2+\alpha^2\delta,\ \gamma_2 z_4 = \alpha+\alpha^2\delta,\ \gamma_3 z_4 = 1+\alpha^2\delta,\ \gamma_4 z_4 = \alpha^2\delta\}$.

Se tomarmos $\overline{D_\Gamma(z_0)}$, teremos que $\bigcup_{\gamma\in\Gamma} \gamma(\overline{D_\Gamma(z_0)}) = \mathbf{H}_4$, $\mathring{\mathfrak{D}} \cap \gamma(\mathring{\mathfrak{D}}) = \emptyset,\ \forall \gamma \in \Gamma'$. Porém visto que $\Gamma(z_1) = \Gamma(z_3)$ e $\Gamma(z_2) = \Gamma(z_4)$, então $\overline{D_\Gamma(z_0)}$ não é um menor subconjunto que satisfaz as condições da definição, ou seja, precisamos excluir elementos.

Portanto, se tomarmos $\mathfrak{D} = \{1+\delta,\ 1+\delta\alpha,\ 1+\delta\alpha^2\}$, que é um conjunto com um representante de cada γ-órbita, teremos que $\bigcup_{\gamma\in\Gamma} \gamma(\mathfrak{D}) = \mathbf{H}_4$ e como $\mathring{\mathfrak{D}} = \{1+\delta\}$ então $\mathring{\mathfrak{D}} \cap \gamma(\mathring{\mathfrak{D}}) = \emptyset,\ \forall \gamma \in \Gamma'$ e assim $\mathfrak{D}$ será um menor subconjunto que satisfaz as propriedades da definição. Logo obtemos um domínio fundamental para a ação de Γ sobre $\mathbf{H}_4$.

Exemplo 2.5. Por outro lado, no exemplo anterior, se considerarmos

$$\Gamma = K = \{g \in GL(2, \mathbb{F}_4) |\ g(\delta) = \delta\} = \left\{ \begin{pmatrix} c+d & c\alpha \\ c & d \end{pmatrix}, c, d \in \mathbb{F}_4, cd + d^2 + c^2\alpha \neq 0 \right\} =$$

$$\left\{\gamma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \gamma_2 = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \gamma_3 = \begin{pmatrix} \alpha^2 & 0 \\ 0 & \alpha^2 \end{pmatrix}, \gamma_4 = \begin{pmatrix} 1 & \alpha \\ 1 & 0 \end{pmatrix}, \gamma_5 = \begin{pmatrix} 0 & \alpha \\ 1 & 1 \end{pmatrix}, \gamma_6 = \begin{pmatrix} \alpha^2 & \alpha \\ 1 & \alpha \end{pmatrix}$$
$$\gamma_7 = \begin{pmatrix} \alpha & \alpha \\ 1 & \alpha^2 \end{pmatrix}, \gamma_8 = \begin{pmatrix} \alpha & \alpha^2 \\ \alpha & 0 \end{pmatrix}, \gamma_9 = \begin{pmatrix} \alpha^2 & \alpha^2 \\ \alpha & 1 \end{pmatrix}, \gamma_{10} = \begin{pmatrix} 0 & \alpha^2 \\ \alpha & \alpha \end{pmatrix}, \gamma_{11} = \begin{pmatrix} 1 & \alpha^2 \\ \alpha & \alpha^2 \end{pmatrix},$$
$$\gamma_{12} = \begin{pmatrix} \alpha^2 & 1 \\ \alpha^2 & 0 \end{pmatrix}, \gamma_{13} = \begin{pmatrix} \alpha & 1 \\ \alpha^2 & 1 \end{pmatrix}, \gamma_{14} = \begin{pmatrix} 1 & 1 \\ \alpha^2 & \alpha \end{pmatrix}, \gamma_{15} = \begin{pmatrix} 0 & 1 \\ \alpha^2 & \alpha^2 \end{pmatrix}\right\},$$

teremos que δ e $1+\delta$ serão fixados por todos os elementos de K, assim, tomando-se o ponto $z_0 = \alpha + \delta$, obtemos

$$D_\Gamma(z_0) = \{\alpha+\delta,\ \alpha^2+\delta\} \quad , \quad \overline{D_\Gamma(z_0)} = \{\alpha+\delta,\ \alpha^2+\delta,\ \delta,\ 1+\delta\}.$$

Assim, se tomarmos $\mathbf{F} = \overline{D_\Gamma(z_0)} = \{z_0 = \alpha+\delta,\ z_1 = \delta,\ z_2 = 1+\delta,\ , z_3 = \alpha^2+\delta\}$, teremos:

$$\gamma_1(\mathbf{F}) = \gamma_2(\mathbf{F}) = \gamma_3(\mathbf{F}) = \{\alpha+\delta,\ \alpha^2+\delta,\ \delta,\ 1+\delta\},$$

$$\gamma_4(\mathbf{F}) = \gamma_8(\mathbf{F}) = \gamma_{12}(\mathbf{F}) = \{\alpha^2+\alpha^2\delta,\ \alpha^2\delta,\ \delta,\ 1+\delta\},$$

$$\gamma_5(\mathbf{F}) = \gamma_{10}(\mathbf{F}) = \gamma_{15}(\mathbf{F}) = \{1+\alpha^2\delta,\ \alpha+\alpha^2\delta,\ \delta,\ 1+\delta\},$$

$$\gamma_6(\mathbf{F}) = \gamma_{11}(\mathbf{F}) = \gamma_{13}(\mathbf{F}) = \{1+\alpha\delta,\ \alpha^2+\alpha\delta,\ \delta,\ 1+\delta\},$$

$$\gamma_7(\mathbf{F}) = \gamma_9(\mathbf{F}) = \gamma_{14}(\mathbf{F}) = \{\alpha+\alpha\delta,\ \alpha\delta,\ \delta,\ 1+\delta\}.$$

Note que, neste caso, não podemos retirar pontos de $\overline{D_\Gamma(z_0)}$ pois a condição (1) da definição 2.5 não será satisfeita. Além disso, é fácil verificar que a condição (2) é satisfeita, logo $\mathfrak{D} = \overline{D_\Gamma(z_0)}$ é um domínio fundamental para $\Gamma = K$ sobre $\mathbf{H}_4$.

Como mencionado, outros exemplos de domínios fundamentais para $\mathbf{H}_q$ com q ímpar, podem ser encontrados em [28], [29], [34].

O resultado a seguir também é necessário neste trabalho. Observamos que originalmente ele foi enunciado somente para q ímpar, e apresentamos a demonstração para q qualquer.

Primeiramente, acrescentamos à $\mathbf{H}_q$ os elementos de $\mathbb{F}_q$ e o elemento ∞. Seja T a aplica-

ção, denominada de cross-ratio, dada por

$$T(z, z_1, z_2, z_3) = \frac{(z - z_1)(z_2 - z_3)}{(z - z_3)(z_2 - z_1)},$$

onde $z_1, z_2, z_3 \in \mathbf{H}_q$ são três pontos distintos de $\mathbf{H}_q$ e neste caso, são levados respectivamente em $0, 1, \text{e}\infty$. Com esta aplicação e considerando-se $\mathbb{F}_{q^2} = \mathbb{F}_q(\delta)$, onde δ é dado em (2.1), conseguimos o seguinte resultado.

Teorema 2.7. *Dados distintos $z_1, z_2, z_3 \in \boldsymbol{H}_q$ e distintos $u_1, u_2, u_3 \in \boldsymbol{H}_q$ existe $\gamma \in GL(2, \mathbb{F}_{q^2})$ tal que $\gamma z_1 = u_1$, $\gamma z_2 = u_2$ e $\gamma z_3 = u_3$. Além disso, γ é única a menos de multiplicação por constante e pode ser representada por*

$$\gamma = \begin{pmatrix} \left(\dfrac{u_1(z_2 - z_1)}{u_2 - u_1} - \dfrac{u_3(z_2 - z_3)}{u_2 - u_3}\right) & \left(\dfrac{u_3 z_1(z_2 - z_3)}{u_2 - u_3} - \dfrac{u_1 z_3(z_2 - z_1)}{u_2 - u_1}\right) \\ \left(\dfrac{(z_2 - z_1)}{u_2 - u_1} - \dfrac{(z_2 - z_3)}{u_2 - u_3}\right) & \left(\dfrac{z_1(z_2 - z_3)}{u_2 - u_3} - \dfrac{z_3(z_2 - z_1)}{u_2 - u_1}\right) \end{pmatrix}.$$

Demonstração: De fato, primeiramente acrescentamos $\mathbb{F}_q$ e ∞ à $\mathbf{H}_q$ e consideramos as aplicações cross-ratio $T(z, z_1, z_2, z_3) = \dfrac{(z - z_1)(z_2 - z_3)}{(z - z_3)(z_2 - z_1)}$ e $G(z, u_1, u_2, u_3) = \dfrac{(z - u_1)(u_2 - u_3)}{(z - u_3)(u_2 - u_1)}$, como $T(z_1) = 0, T(z_2) = 1, T(z_3) = \infty$ e $G(u_1) = 0, G(u_2) = 1, G(u_3) = \infty$, basta tomarmos $\gamma = G^{-1} \circ T : \mathbf{H}_q \to \mathbf{H}_q$ e teremos $\gamma z_1 = u_1$, $\gamma z_2 = u_2$ e $\gamma z_3 = u_3$ bem como a expressão apresentada. Para a segunda afirmação, seja $\gamma' \in GL(2, \mathbb{F}_{q^2})$ outra aplicação tal que $\gamma' z_1 = u_1$, $\gamma' z_2 = u_2$ e $\gamma' z_3 = u_3$. Então temos que z_1, z_2, z_3 são distintos e fixados por $\gamma^{-1} \circ \gamma'$. Note que $z \in \mathbf{H}_q$ é fixado se, e somente se, satisfaz $\dfrac{az + b}{cz + d} = z$, a qual claramente possui 3 soluções se, e somente se, $a = d$ e $b = c = 0$, de onde segue que $\gamma' = a\gamma$, $a \in \mathbb{F}_{q^2}$. ∎

Exemplo 2.6. Consideremos os resultados obtidos no Exemplo 2.5 e tomemos os elementos $z_1 = \alpha + \delta$, $z_2 = \alpha^2 + \delta$, $z_3 = 1 + \delta$, $u_1 = \alpha + \alpha\delta$, $u_2 = \alpha\delta$, $u_3 = 1 + \delta$ todos elementos de $\mathbf{H}_4$ satisfazendo as condições do Teorema 2.7. Seja $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ como no teorema, então, lembrando que em corpos de característica par, $-1 = 1$, temos:

$$a = \frac{(\alpha + \alpha\delta)((\alpha^2 + \delta) + (\alpha + \delta))}{(\alpha\delta) + (\alpha + \alpha\delta)} + \frac{(1 + \delta)((\alpha^2 + \delta) + (1 + \delta))}{(\alpha\delta) + (1 + \delta)} = \alpha\delta$$

$$b = \frac{(1 + \delta)(\alpha + \delta)((\alpha^2 + \delta) + (1 + \delta))}{(\alpha\delta) + (1 + \delta)} + \frac{(\alpha + \alpha\delta)(1 + \delta)((\alpha^2 + \delta) + (\alpha + \delta))}{(\alpha\delta) + (\alpha + \alpha\delta)} = \alpha\delta$$

$$c = \frac{(\alpha^2+\delta)+(\alpha+\delta)}{(\alpha\delta)+(\alpha+\alpha\delta)} + \frac{(\alpha^2+\delta)+(1+\delta)}{(\alpha\delta)+(1+\delta)} = \delta$$
$$d = \frac{(\alpha+\delta)((\alpha^2+\delta)+(1+\delta))}{(\alpha\delta)+(\alpha+\alpha\delta)} + \frac{(1+\delta)((\alpha^2+\delta)+(\alpha+\delta))}{(\alpha\delta)+(\alpha+\alpha\delta)} = \alpha^2\delta.$$

Como γ é única a menos de multiplicação por constante, podemos tomar $\gamma \in GL(2,\mathbb{F}_4)$ dada por $\gamma = \begin{pmatrix} \alpha & \alpha \\ 1 & \alpha^2 \end{pmatrix}$ que é a aplicação γ_7 no Exemplo 2.5 e vemos pelo Exemplo 2.5 que de fato $\gamma_7(z_1) = u_1$, $\gamma_7(z_2) = u_2$ e $\gamma_7(z_3) = u_3$. Se multiplicarmos γ por α ou por α^2 obtemos respectivamente γ_9 e γ_{14}, confirmando novamente o que foi encontrado no Exemplo 2.5.

Terras [34], ainda comenta que podemos considerar Γ-tessalações ao tomarmos $q = p^r$, com $r > 1$ e $\Gamma \subseteq GL(2,\mathbb{F}_p)$ para o caso ímpar.

No capítulo 4, consideraremos este caso e também o caso par na construção de nossos códigos não-lineares. Além disso, veremos que podemos considerar $\Gamma = GL(2,\mathbb{F}_q)$ agindo sobre $\mathbf{H}_{q^2}$ tanto para q ímpar quanto para q par e que os códigos não-lineares obtidos dessa forma são os melhores para nosso método de construção.

Capítulo 3

Códigos Lineares Quase-Cíclicos sobre $\mathbf{H}_q$

Neste capítulo veremos uma família de códigos quase-cíclicos que podem ser obtidos trabalhando-se com o Semi-Plano Superior Finito $\mathbf{H}_q$. Iremos considerar $q = 2^r$ e construiremos uma família de códigos quase-cíclicos binários sobre $\mathbf{H}_q$.

3.1 Códigos Quase-Cíclicos sobre $\mathbf{H}_q$ utilizando a norma

Em [35], Tiu e Wallace apresentaram uma nova família de códigos baseados no Semi-Plano Superior Finito $\mathbf{H}_q$ com q ímpar. Esses códigos foram chamados de NQR, Resíduos Nâo Quadráticos. Na construção de tais códigos, os autores consideram a norma dos elementos de $\mathbf{H}_q$ e tomam aqueles cuja norma é um resíduo não quadrático módulo q. Porém, como para q par, todo elemento do corpo $\mathbb{F}_q$ é um resíduo quadrático, não podemos utilizar o mesmo método de construção para o Semi-Plano Superior Finito $\mathbf{H}_q$ com q par. Podemos no entanto, considerar apenas a norma ou a distância até a "origem"de $\mathbf{H}_q$ e relacioná-las com elementos previamente escolhidos do corpo $\mathbb{F}_q$.

3.1.1 Construção

Consideremos o corpo $\mathbb{F}_{2^r} = \{0, 1 = \alpha^0, \alpha, \alpha^2, \ldots, \alpha^{2^r-2}\}$ construído como no capítulo anterior, α um elemento primitivo com $Tr(\alpha) = 1$. Como vimos, a fim de construirmos H_{2^r}, tomamos o polinômio $x^2 + x + \alpha$, que pelo Teorema 1.16 é irredutível sobre $\mathbb{F}_{2^r}$, e considerando θ uma raíz deste polinômio sobre a extensão quadrática de $\mathbb{F}_{2^r}$. Assim temos que $H_{2^r} = \{x + \theta y |\ x, y \in \mathbb{F}_{2^r},\ y \neq 0\}$. A fim de melhorarmos a notação ao longo do capítulo, vamos identificar os elementos de $\mathbf{H}_{2^r}$ por $z_{ij} = x + \theta y$, onde i, j são as potência de α tais que $x = \alpha^i$ e $y = \alpha^j$, caso $x = 0$, tomaremos $i = *$, ou seja, representaremos $0 = \alpha^*$.

Exemplo 3.1. Considere $\mathbf{H}_4$ como no Exemplo 2.4, então

$\mathbf{H}_4 = \{x + \delta y |\ x, y \in \mathbb{F}_4,\ y \neq 0\} =$
$\{\delta,\ \delta\alpha,\ \delta\alpha^2,\ 1+\delta,\ 1+\delta\alpha,\ 1+\delta\alpha^2,\ \alpha+\delta,\ \alpha+\delta\alpha,\ \alpha+\delta\alpha^2,\ \alpha^2+\delta,\ \alpha^2+\delta\alpha,\ \alpha^2+\delta\alpha^2\} =$
$\{z_{*0},\ z_{*1},\ z_{*2},\ z_{00},\ z_{01},\ z_{02},\ z_{10},\ z_{11},\ z_{12},\ z_{20},\ z_{21},\ z_{22}\}$.

Como os elementos de $\mathbb{F}_{2^r}$ podem ser escritos da forma $\mathbb{F}_{2^r} = \{0 = \alpha^*, 1 = \alpha^0, \alpha, \alpha^2, \ldots, \alpha^{2^r-2}\}$, vamos ordenar os elementos de $\mathbf{H}_{2^r}$ utilizando a ordem dada em 2.2 para elementos de $\mathbb{F}_{2^r}$, ou seja, $\alpha^* = 0 < \alpha^0 = 1 < \alpha^1 < \alpha^2 < \cdots < \alpha^{2^r-2}$. Note que $\alpha^i < \alpha^j \Leftrightarrow i < j$ e estamos considerando $* < 0$. Então os elementos de $\mathbf{H}_{2^r}$ serão ordenados como:

$$z_{ij} < z_{uv} \Leftrightarrow i < u \text{ ou } j < v \text{ caso } i = u. \tag{3.1}$$

Note que no exemplo acima, os elementos estão ordenados segundo esta ordem.

Agora, para cada elemento $\alpha^i \in \mathbb{F}_q$, consideremos o bloco:

$$C_i = \{z_{i0}, z_{i1}, \ldots, z_{i(2^r-2)}\}$$

.

Como $\theta + \theta^{2^r} = 1$ e $\theta\theta^{2^r} = \alpha$, temos que, para $z = x + y\theta \in H_{2^r}$, $N(x + y\theta) = x^2 + (\theta + \overline{\theta})xy + \theta\overline{\theta}y^2 = x^2 + xy + \alpha y^2$.

Podemos então passar à construção da Matriz G que utilizaremos para gerar nosso código. Faremos isto da seguinte forma:

A primeira linha de G, denotada por L_0, será formada pelos blocos C_i ordenados da seguinte maneira, $L_0 = [C_*\ C_0\ C_1\ \cdots C_{2^r-2}]$. As próximas $2^r - 1$ linhas serão obtidas através de um shift para a direita, dos blocos da linha anterior, ou seja, $L_1 = [C_{2^r-2}\ C_*\ C_0\ \cdots C_{2^r-3}]$, $\cdots$, $L_{2^r-1} = [C_0\ C_1\ C_2\ \cdots C_*]$.

Assim, a matriz G será da forma:

$$G = \begin{bmatrix} C_* & C_0 & C_1 & C_2 & \cdots & C_{2^r-2} \\ C_{2^r-2} & C_* & C_0 & C_1 & \cdots & C_{2^r-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ C_0 & C_1 & C_2 & C_3 & \cdots & C_* \end{bmatrix} \tag{3.2}$$

Teorema 3.1. *Seja G a matriz (3.2). A matriz $A_{2^r \times 2^r}$ construída tomando-se a coluna k, com $1 \leq k \leq 2^r - 1$ e as colunas $k + (2^r - 1)m$, com $1 \leq m \leq 2^r - 1$ é uma matriz circular.*

Demonstração: De fato, note primeiramente que, em blocos, G é circular. Temos ainda que cada bloco C_i possui o mesmo comprimento $2^r - 1$ e, a entrada referente à coluna k em cada bloco, é o elemento $z_{i(k-1)}$. Assim, tomando em cada bloco a k-ésima coluna, obtemos a matriz

$$A_k = \begin{bmatrix} z_{*(k-1)} & z_{0(k-1)} & z_{1(k-1)} & \cdots & z_{(2^r-2)(k-1)} \\ z_{(2^r-2)(k-1)} & z_{*(k-1)} & z_{0(k-1)} & \cdots & z_{(2^r-3)(k-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ z_{0(k-1)} & z_{1(k-1)} & z_{2(k-1)} & \cdots & z_{*(k-1)} \end{bmatrix}, \tag{3.3}$$

que é circular. ■

Exemplo 3.2. Se considerarmos o Exemplo 3.1 então a matriz G será dada por

$$G = \begin{bmatrix} C_* & C_0 & C_1 & C_2 \\ C_2 & C_* & C_0 & C_1 \\ C_1 & C_2 & C_* & C_0 \\ C_0 & C_1 & C_2 & C_* \end{bmatrix}$$

$$= \begin{bmatrix} z_{*0} & z_{*1} & z_{*2} & z_{00} & z_{01} & z_{02} & z_{10} & z_{11} & z_{12} & z_{20} & z_{21} & z_{22} \\ z_{20} & z_{21} & z_{22} & z_{*0} & z_{*1} & z_{*2} & z_{00} & z_{01} & z_{02} & z_{10} & z_{11} & z_{12} \\ z_{10} & z_{11} & z_{12} & z_{20} & z_{21} & z_{22} & z_{*0} & z_{*1} & z_{*2} & z_{00} & z_{01} & z_{02} \\ z_{00} & z_{01} & z_{02} & z_{10} & z_{11} & z_{12} & z_{20} & z_{21} & z_{22} & z_{*0} & z_{*1} & z_{*2} \end{bmatrix}$$

$$= \begin{bmatrix} \theta & \alpha\theta & \alpha^2\theta & 1+\theta & 1+\alpha\theta & 1+\alpha^2\theta & \alpha+\theta & \alpha+\alpha\theta & \alpha+\alpha^2\theta & \alpha^2+\theta & \alpha^2+\alpha\theta & \alpha^2+\alpha^2\theta \\ \alpha^2+\theta & \alpha^2+\alpha\theta & \alpha^2+\alpha^2\theta & \theta & \alpha\theta & \alpha^2\theta & 1+\theta & 1+\alpha\theta & 1+\alpha^2\theta & \alpha+\theta & \alpha+\alpha\theta & \alpha+\alpha^2\theta \\ \alpha+\theta & \alpha+\alpha\theta & \alpha+\alpha^2\theta & \alpha^2+\theta & \alpha^2+\alpha\theta & \alpha^2+\alpha^2\theta & \theta & \alpha\theta & \alpha^2\theta & 1+\theta & 1+\alpha\theta & 1+\alpha^2\theta \\ 1+\theta & 1+\alpha\theta & 1+\alpha^2\theta & \alpha+\theta & \alpha+\alpha\theta & \alpha+\alpha^2\theta & \alpha^2+\theta & \alpha^2+\alpha\theta & \alpha^2+\alpha^2\theta & \theta & \alpha\theta & \alpha^2\theta \end{bmatrix}.$$

Como consequência, o código linear gerado a partir de G será um código quasi-cíclico de ordem 2^r.

A partir da matriz G construída acima, podemos obter códigos lineares. Como mencionado, tais códigos serão quasi-cíclicos de ordem 2^r. A família de códigos que apresentaremos será obtida utilizando-se a norma dos elementos. Tal código será um código binário e para isto, escolheremos um elemento não nulo de $\mathbb{F}_{2^r}$, digamos α^l para um l fixado.

Para obtermos o código linear binário, vamos calcular a norma de cada elemento de G e, se a norma do elemento for igual ao α^l escolhido, colocaremos um 1 no lugar do elemento correspondente na matriz G, caso contrário colocaremos um 0. Desta forma, ficaremos com uma matriz que denotaremos por $N(G)$, com todas as entradas sendo 1's ou 0's. Note que tal matriz terá $2^r(2^r-1)$ colunas e 2^r linhas, porém ainda não tomaremos esta matriz como a matriz geradora do código, visto que conseguiremos eliminar algumas colunas desta matriz, diminuindo assim o comprimento do código.

Lema 3.2. *O peso da cada linha da matriz $N(G)$ é igual a 2^r.*

Demonstração: De fato, note primeiramente que escolhemos α como elemento primitivo de $\mathbb{F}_{2^r}$ com $Tr(\alpha) = 1$ e em cada linha da matriz G temos todos os blocos C_i, sem repetição, com $i \in \{*, 0, 1, \ldots, 2^r - 2\}$. Além disso, para cada elemento z_{ij} de cada bloco C_i fazemos j percorrer todos os elementos de $\{0, 1, 2, \ldots, 2^r - 2\}$. Logo, estamos interessados em saber o número de soluções da equação $N(x + \theta y) = \alpha^l$ quando x e y percorrem os elementos de $\mathbb{F}_{2^r}$ com $y \neq 0$. Mas $N(x + \theta y) = \alpha^l \Leftrightarrow x^2 + xy + \alpha y^2 = \alpha^l$.

Pelo Lema 1.18, o número de soluções de tal equação é : $S(x^2 + xy + \alpha y^2 = \alpha^l) = 2^r - \upsilon(\alpha^l) = 2^r + 1$. Porém, como em $\mathbb{F}_{2^r}$ todo elemento pode ser escrito como quadrado de outro então, para $y = 0$ temos que existe um elemento $x \in \mathbb{F}_{2^r}$ tal que $x^2 = \alpha^l$, mas em H_{2^r} tomamos $y \neq 0$, então devemos excluir este x. O número de soluções se torna então 2^r e portanto o peso de cada linha de $N(G)$ é 2^r ∎

A partir do Lema 3.2 vemos que o número de 1's tomando todos os blocos C_i é 2^r. Agora, se considerarmos a matriz $N(G)$, vemos que verticalmente, a cada $2^r - 1$ colunas temos todos os blocos C_i como linhas, logo o número de 1's em cada bloco de linhas também é 2^r. Assim obtemos o próximo resultado.

Teorema 3.3. *Seja $N(G)$ a matriz obtida de G colocando-se um 1 na entrada do elemento cuja norma é α^l e 0 caso contrário. Então, dentre as $2^r(2^r - 1)$ colunas de $N(G)$, apenas 2^{2r-1} são não nulas. Além disso, as colunas nulas ocorrem na mesma posição em cada bloco.*

Demonstração: Note que precisamos analisar apenas as primeiras $2^r - 1$ colunas, visto que as mesmas se repetem a menos da ordem de seus elementos, umas vez que a matriz A_k em (3.3) é circular. Agora, como consequência do lema anterior, temos que existem 2^r 1's entre as entradas destas primeiras $2^r - 1$ colunas. Temos ainda que os elementos da k-ésima coluna são da forma $z_{i(k-1)}$, onde i percorre todos os elementos de $\{*, 0, 1, \ldots, 2^r - 1\}$. Logo, a k-ésima coluna terá um 1 na entrada $z_{i(k-1)}$ se $(\alpha^i)^2 + \alpha^i \alpha^{k-1} + \alpha^{2k-1} = \alpha^j$, ou seja, se considerarmos $\alpha^i = x$, temos uma equação de grau 2 em uma variável x e tal equação possui duas ou nenhuma solução em $\mathbb{F}_{2^r}$, uma vez que $(a+b)^2 = a^2 + b^2$ em $\mathbb{F}_{2^r}$. Assim, cada coluna não nula possui 0 ou duas entradas não nulas. Agora, temos 2^r entradas não nulas no bloco analisado, portanto temos $\frac{2^r}{2} = 2^{r-1}$ colunas não nulas entre as primeiras $2^r - 1$ colunas, as quais se repetem nos blocos seguintes. Portanto, apenas 2^{2r-1} colunas de $N(G)$ são não nulas. A segunda parte segue diretamente da matriz G ser circular por blocos. ∎

Assim, podemos excluir as colunas nulas da matriz $N(G)$ e conseguimos uma nova matriz G' com 2^r linhas e 2^{2r-1} colunas, a qual será a matriz geradora do código.

Exemplo 3.3. Consideremos a matriz G obtida no Exemplo 3.2. Devemos escolher um elemento $\alpha^l \in \mathbb{F}_4^*$ e em seguida colocar 1 na entrada z_{ij} se $N(z_{ij}) = \alpha^l$ e 0 caso contrário. Vamos escolher o elemento $\alpha^2 \in \mathbb{F}_4^*$. Então temos que os elementos $z_{ij} \in \mathbf{H}_4$ tais que $N(z_{ij}) = \alpha^2$ são $\{z_{*1}, z_{10}, z_{20}, z_{22}\}$. Então, como

$$G = \begin{bmatrix} z_{*0} & z_{*1} & z_{*2} & z_{00} & z_{01} & z_{02} & z_{10} & z_{11} & z_{12} & z_{20} & z_{21} & z_{22} \\ z_{20} & z_{21} & z_{22} & z_{*0} & z_{*1} & z_{*2} & z_{00} & z_{01} & z_{02} & z_{10} & z_{11} & z_{12} \\ z_{10} & z_{11} & z_{12} & z_{20} & z_{21} & z_{22} & z_{*0} & z_{*1} & z_{*2} & z_{00} & z_{01} & z_{02} \\ z_{00} & z_{01} & z_{02} & z_{10} & z_{11} & z_{12} & z_{20} & z_{21} & z_{22} & z_{*0} & z_{*1} & z_{*2} \end{bmatrix}, \text{ teremos}$$

$$N(G) = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \text{ e}$$

$$G' = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Já sabemos que o comprimento do código é 2^{2r-1}, vejamos resultados sobre os outros parâmetros código.

Teorema 3.4. *Seja G' a matriz $2^r \times 2^{2r-1}$ obtida de $N(G)$. Então, entre as 2^r linhas de G', quaisquer $2^r - 1$ linhas são linearmente independentes.*

Demonstração: Com efeito, suponha que no processo de obtenção de G', a k-ésima coluna do primeiro bloco de $N(G)$ era não nula e considere a matriz A_k obtida em (3.3) a partir desta coluna. Basta mostrarmos que tal matriz possui posto $2^r - 1$ e assim, como encontramos uma submatriz de G' com posto $2^r - 1$, então o posto de G' deve ser maior ou igual a $2^r - 1$. Por outro lado, note que ao somarmos todas as linhas de G', obtemos o vetor nulo, uma vez que cada coluna possui apenas dois 1's, logo o posto de G' é menor que 2^r e assim, obteremos o resultado desejado. Seja então A a matriz obtida tomando-se a k-ésima coluna (não nula) de $N(G)$ e as colunas $k + (2^r - 1)m$, com $1 \leq m \leq 2^r - 1$, após trocarmos as entradas por 1's e 0's. Vimos que tal matriz é circular e por Macwillians e Sloane [23], página 201, considerando

a matriz de Vandermonde sobre $GF(2^r)$

$$M = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_0 & a_1 & \cdots & a_{2^r-1} \\ a_0^2 & a_1^2 & \cdots & a_{2^r-1}^2 \\ a_0^{2^r-1} & a_1^{2^r-1} & \cdots & a_{2^r-1}^{2^r-1} \end{bmatrix},$$

onde $a_0 = 1$ e a_i são as 2^r-ésimas raízes da unidade, e sendo $f(x) = f_0 + f_1 x + \cdots + f_{2^r-1}x^{2^r-1}$ com a primeira linha de A_k sendo dada por $[\ f_0 \quad f_1 \quad \cdots \quad f_{2^r-1}\ ]$, temos que $M^{-1}A_kM$ é a matriz diagonal $M^{-1}A_kM = diag[f(a_0), f(a_1), \ldots, f(a_{2^r-1})]$. Agora, note que apenas dois f_i's são não nulos, logo $f(a_0) = 0$ e $f(a_i) \neq 0$ para $1 \leq i \leq 2^r - 1$, visto que os a_i's são as 2^r-ésimas raízes da unidade. Logo a matriz A_k tem posto $2^r - 1$ e como encontramos uma submatriz de G' com posto $2^r - 1$ temos que $2^r - 1 \leq \text{posto}(G') < 2^r$ e portanto quaisquer $2^r - 1$ linhas de G' são linearmente independentes. ■

De posse de tais resultados, conseguimos então nosso código.

Teorema 3.5. *Seja $\mathscr{C}$ o código linear binário cuja matriz geradora é a matriz G' obtida nos resultados anteriores. Então $\mathscr{C}$ é um $[2^{2r-1}, 2^r - 1, 2^r]$-código quasi-cíclico.*

Demonstração: De fato, pelo Teorema 3.3 temos que o comprimento do código é 2^{2r-1} e pelo Teorema 3.4 que a dimensão do código é $2^r - 1$. Além disso, pela forma como a matriz foi construída, obtemos diretamente que o código é quasi-cíclico. Resta provarmos que a distância mínima é 2^r. Pelo Lema 3.2 temos que $\omega(\mathscr{C}) \leq 2^r$. Assim, resta provarmos que $\omega(\mathscr{C}) \geq 2^r$. Para isto, considere as 2^{r-1} matrizes circulares A_k formadas como em 3.3, a partir das 2^{r-1} primeiras colunas de G'. Para cada uma dessas matrizes, temos que o peso de cada linha e cada coluna é 2, e além disso, como o posto de cada uma destas matrizes é $2^r - 1$, a soma de quaisquer l linhas, $1 \leq l \leq 2^r - 1$, deve ter peso par. Assim, para cada uma das 2^{r-1} matrizes circulares o peso deve ser maior que, ou igual a 2, ao considerarmos todas as matrizes circulares obtidas, ao mesmo tempo, devemos ter $\omega(\mathscr{C}) \geq (2^{r-1})2 = 2^r$. Portanto a distância mínima do código é 2^r. ■

Apesar do código obtido não possuir uma distância mínima e um dimensão tão elevados a princípio, o método de decodificação torna-se muito simples como veremos a seguir. Também veremos que conseguimos melhorar a distância mínima, chegando bem próximo dos parâmetros dos melhores códigos quasi-cíclicos conhecidos.

3.2 Códigos Quase-Cíclicos sobre $\mathbf{H}_q$ utilizando a distância

Na construção dos códigos quase-cíclicos da seção anterior, consideramos a norma dos elementos de $\mathbf{H}_q$. Porém, podemos utilizar o mesmo método de construção para a matriz G e para obtermos a matriz seguinte, utilizarmos a distância até um elemento fixo de $\mathbf{H}_q$.

Consideremos então a matriz G obtida em (3.2). Fixado um elemento $z_{uv} \in \mathbf{H}_q$, vamos construir uma matriz $D_l^{uv}(G)$ a partir de G tomando as entradas da matriz $D_l^{uv}(G)$ como sendo 1 se $d(z_{ij}, z_{uv}) = \alpha^l$ e 0 caso contrário.

Teorema 3.6. *Se $l \neq *, 0$, então o peso de cada linha da matriz $D_l^{uv}(G)$ é $2^r + 1$.*

Demonstração: De fato, segue diretamente do Teorema 2.4, uma vez que o grafo $X_{2^r}(\delta, \alpha^l)$ é um grafo $(q+1)-$regular se $\alpha^l \neq 0, 1$. ■

Proposição 3.7. *Entre as colunas não nulas de cada bloco da matriz $D_l^{uv}(G)$, uma coluna possui peso 1 e as demais possuem peso 2.*

Demonstração: De fato, vamos analisar o primeiro bloco da matriz, assim como no caso da norma. Primeiramente, note que se $z_{ij} = x + \delta y$ e $z_{uv} = m + \delta n$ então

$$d(z_{ij}, z_{uv}) = \alpha^l \Leftrightarrow \alpha^l ny = (x+m)^2 + (x+m)(y+n) + \alpha(y+n)^2.$$

Agora, $m = \alpha^u$ e $n = \alpha^v$ são fixos, e se a k-ésima coluna é não nula então $y = \alpha^{k-1}$ também é fixo, o que nos deixa com uma equação do segundo grau em uma variável. Tal equação possui apenas uma solução se $y = n$, neste caso teremos $\alpha^l n^2 + m^2 = x^2 \Leftrightarrow (\alpha^{\frac{l}{2}} v + m)^2 = x^2 \Leftrightarrow x = \alpha^{\frac{l}{2}} v + u$, caso contrário a equação terá duas soluções, provando assim o resultado. ■

Como consequência deste resultado temos:

Corolário 3.8. *O posto da matriz $D_l^{uv}(G)$ é 2^r.*

Demonstração: De fato, considere a submatriz A_k formada tomando-se todas as colunas com apenas um elemento não nulo. Então, como esta é uma matriz circular, seu posto é 2^r e consequentemente a matriz $D_l^{uv}(G)$ também terá posto 2^r. ■

Proposição 3.9. *A matriz $D_l^{uv}(G)$ possui $2^r(2^{r-1} - 2)$ colunas nulas.*

Demonstração: De fato, pela Proposição 3.7, entre as colunas não nulas de cada bloco, uma possui peso 1 e as outras peso 2. Agora, pelo Teorema 3.6, cada bloco tem 2^r+1 coordenadas não nulas, o que nos fornece por bloco, 1 coluna com peso 1 e 2^{r-1} colunas com peso 2. Logo, em cada bloco temos

$$2^r - 1 - (1 + 2^{r-1}) = 2^{r-1} - 2$$

colunas nulas e como temos 2^r blocos, então a matriz possui $2^r(2^{r-1} - 2)$ colunas nulas. ■

Vamos denotar por $D_l^{uv}(G')$ a matriz obtida ao se excluir as colunas nulas de $D_l^{uv}(G)$. Então conseguimos o seguinte resultado.

Teorema 3.10. *Seja $\mathscr{C}$ o código linear binário cuja matriz geradora é a matriz $D_l^{uv}(G')$ obtida nos resultados anteriores. Então $\mathscr{C}$ é um $[2^r(1 + 2^{r-1}), 2^r, 2^r]$-código quasi-cíclico.*

Demonstração: A demonstração é análoga ao caso da norma. Pelo Teorema 3.6 temos que $\omega(\mathscr{C}) \leq 2^r + 1$. Porém, ao somarmos todas as linhas, como existe uma coluna com peso 1 em cada bloco, e as demais com peso 2, obteremos um elemento com peso 2^r, portanto $\omega(\mathscr{C}) \leq 2^r$. Agora, considerando-se novamente as matrizes A_k, obtemos $\omega(\mathscr{C}) \geq 2^r$, provando-se o resultado. ■

Exemplo 3.4. Considere o corpo $\mathbb{F}_8 = \{\alpha^* = 0, \alpha^0 = 1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ onde α é raíz do polinômio x^3+x^2+1, irredutível sobre $\mathbb{F}_2$ e tomemos θ raíz de $x^2+x+\alpha$ irredutível sobre $\mathbb{F}_8$. Então $\mathbf{H}_8 = \{z_{ij} = \alpha^i+\theta\alpha^j |\ j \neq *\} = \{z_{*0}, z_{*1}, z_{*2}, z_{*3}, z_{*4}, z_{*5}, z_{*6}, z_{00}, z_{01}, z_{02}, z_{03}, z_{04}, z_{05}, z_{06}, z_{10}, z_{11}, z_{12}, z_{13}, z_{14}, z_{15}, z_{16}, z_{20}, z_{21}, z_{22}, z_{23}, z_{24}, z_{25}, z_{26}, z_{30}, z_{31}, z_{32}, z_{33}, z_{34}, z_{35}, z_{36}, z_{40}, z_{41}, z_{42}, z_{43}, z_{44}, z_{45}, z_{46}, z_{50}, z_{51}, z_{52}, z_{53}, z_{54}, z_{55}, z_{56}, z_{60}, z_{61}, z_{62}, z_{63}, z_{64}, z_{65}, z_{66}\}$. Então teremos

$$G = \begin{bmatrix} C_* & C_0 & C_1 & C_2 & C_3 & C_4 & C_5 & C_6 \\ C_6 & C_* & C_0 & C_1 & C_2 & C_3 & C_4 & C_5 \\ C_5 & C_6 & C_* & C_0 & C_1 & C_2 & C_3 & C_4 \\ C_4 & C_5 & C_6 & C_* & C_0 & C_1 & C_2 & C_3 \\ C_3 & C_4 & C_5 & C_6 & C_* & C_0 & C_1 & C_2 \\ C_2 & C_3 & C_4 & C_5 & C_6 & C_* & C_0 & C_1 \\ C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_* & C_0 \\ C_0 & C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_* \end{bmatrix}$$

onde
$$\begin{aligned}
C_* &= [z_{*0}\ z_{*1}\ z_{*2}\ z_{*3}\ z_{*4}\ z_{*5}\ z_{*6}]\\
C_0 &= [z_{00}\ z_{01}\ z_{02}\ z_{03}\ z_{04}\ z_{05}\ z_{06}]\\
C_1 &= [z_{10}\ z_{11}\ z_{12}\ z_{13}\ z_{14}\ z_{15}\ z_{16}]\\
C_2 &= [z_{20}\ z_{21}\ z_{22}\ z_{23}\ z_{24}\ z_{25}\ z_{26}]\\
C_3 &= [z_{30}\ z_{31}\ z_{32}\ z_{33}\ z_{34}\ z_{35}\ z_{36}]\\
C_4 &= [z_{40}\ z_{41}\ z_{42}\ z_{43}\ z_{44}\ z_{45}\ z_{46}]\\
C_5 &= [z_{50}\ z_{51}\ z_{52}\ z_{53}\ z_{54}\ z_{55}\ z_{56}]\\
C_6 &= [z_{60}\ z_{61}\ z_{62}\ z_{63}\ z_{64}\ z_{65}\ z_{66}]
\end{aligned}$$

Agora, se escolhermos o elemento $z_{*0} = \theta$ e na matriz G colocarmos 1 no lugar do elemento z_{ij} se $d(z_{ij}, z_{*0}) = \alpha$ e zero caso contrário, obteremos os blocos C_i dados por

$$\begin{aligned}
C_* &= [0\ 0\ 0\ 0\ 0\ 0\ 0]\\
C_0 &= [0\ 0\ 1\ 0\ 0\ 1\ 0]\\
C_1 &= [0\ 0\ 0\ 0\ 1\ 0\ 0]\\
C_2 &= [0\ 0\ 1\ 0\ 1\ 0\ 0]\\
C_3 &= [0\ 0\ 0\ 0\ 0\ 0\ 0]\\
C_4 &= [1\ 0\ 0\ 1\ 0\ 0\ 0]\\
C_5 &= [0\ 0\ 0\ 1\ 0\ 1\ 0]\\
C_6 &= [0\ 0\ 0\ 0\ 0\ 0\ 0]
\end{aligned}.$$

Assim, excluindo a segunda e a sétima coluna em cada bloco, obtemos a matriz $D_1^{*0}(G')$ com 40 colunas não nulas, cada linha tendo peso 9, à cada 5 colunas uma coluna com peso 1 e 4 com peso 2, o que nos deixa com um código com peso 8, confirmando os resultados anteriores.

3.3 Decodificação

Vejamos então como decodificar nosso código para ambos os casos.

Suponha que temos o código $\mathscr{C}$ com paramêtros $[2^{2r-1}, 2^r - 1, 2^r]$ construído como explicado ao longo da primeira seção deste capítulo, ou seja, estamos utilizando a norma. Agora, note que o peso de cada coluna da matriz G' é 2 e considere as 2^{r-1} matrizes circulares A_k, $1 \leq k \leq 2^{r-1}$ obtidas a partir das primeiras 2^{r-1} colunas de G'. Temos que em cada uma destas matrizes, se na primeira coluna temos as posições referentes às linhas L_i e L_j não nulas, $0 \leq i, j \leq 2^r - 1$, então na próxima coluna teremos as posições referentes às linhas $L_{(i+1)mod2^r}$ e $L_{(j+1)mod2^r}$ sendo não nulas, e assim sucessivamente para as demais colunas de cada uma destas matrizes circulares.

Agora suponha que a palavra c foi codificada via matriz G' e que recebemos a palavra $r = c + e$, onde e foi o erro introduzido no decorrer da transmissão. Vamos representar cada uma das $2^r(2^r - 1)$ entradas da palavra r por r_{xy} onde x representa o bloco C_x e y a coluna deste bloco, referente à primeira linha da matriz G'. Assim, para cada matriz A_k, tomaremos uma sequência de coordenadas da palavra r, sendo esta sequência dada por r_{*k}, r_{0k}, $r_{1k}, \ldots,$ $r_{(2^r-2)k}$ e resolveremos o sistema

$$\begin{cases} (L_i + L_j)mod2 & = & r_{*k} \\ (L_{(i+1)mod2^r} + L_{(j+1)mod2^r})mod2 & = & r_{0k} \\ \vdots & \vdots & \vdots \\ (L_{(i+2^{r-1})mod2^r} + L_{(j+2^{r-1})mod2^r})mod2 & = & r_{(2^r-2)k} \end{cases}$$

Note que resolver tal sistema é muito simples, uma vez que nossa matriz $A_k$tem 2^r linhas e posto 2^{r-1}, ao somarmos todas as linhas temos a palavra nula. Assim, se r é combinação de l linhas de $N(G)$, também podemos escrever r como combinação das linhas complementares, uma vez que ao somarmos as l linhas com as suas complementares o resultado deve ser a palavra nula. Portanto, tanto faz a escolha que fazemos para começar a resolver o sistema. Por exemplo, se $r_{*k} = 1$, tanto faz tomarmos $L_i = 1$ e $L_j = 0$ ou $L_i = 0$ e $L_j = 1$ e a partir da solução escolhida para a primeira linha do sistema, determinamos as demais. Note que $L_i = 1$ e $L_j = 0$ significa que estamos tomando a linha i para escrever a combinação linear que resulta na palavra r e não estamos tomando a linha j. Assim escolhemos uma das opções e vamos substituindo nas demais linhas do sistema de forma a resolvermos o sistema. Além disso, não precisamos, a princípio, resolver todos os sistemas. Podemos escolher um k e resolver.

Agora, se para o k escolhido o sistema for possível e possuir apenas duas soluções, obtenha a palavra c' que é combinação das linhas de G' referentes à uma das soluções do sistema e calcule $c' + r$. Se $\omega(c' + r) \leq \left\lfloor \frac{2^r-1}{2} \right\rfloor$, a palavra enviada foi c'. Se $\omega(c' + r) > \left\lfloor \frac{2^r-1}{2} \right\rfloor$, ou o sistema é impossível, repita o processo para outro k. Temos ainda a opção do sistema possuir mais que duas soluções, neste caso encontramos as possíveis soluções e verificamos qual destas soluções satisfaz $\omega(c' + r) \leq \left\lfloor \frac{2^r-1}{2} \right\rfloor$ ou escolhemos outro k.

Como a distância mínima é 2^r, temos que $\mathscr{C}$ corrige até $\left\lfloor \frac{2^r-1}{2} \right\rfloor$ erros. Agora, $\left\lfloor \frac{2^r-1}{2} \right\rfloor < 2^{r-1}$, e como temos 2^{r-1} colunas em cada bloco da matriz G', conseguiremos corrigir até $\left\lfloor \frac{2^r-1}{2} \right\rfloor$ erros. Se o sistema for impossível para todos os valores de k, ou possível mas $\omega(c'+r) > \left\lfloor \frac{2^r-1}{2} \right\rfloor$ para toda solução do sistema, então ocorreram mais que $\left\lfloor \frac{2^r-1}{2} \right\rfloor$ erros e não conseguimos determinar a palavra enviada.

Exemplo 3.5. Considere a matriz G' obtida no Exemplo 3.3, ou seja,

$$G' = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

e suponha que a palavra $r = [0\ 1\ 0\ 0\ 0\ 1\ 1\ 0]$ foi recebida.

Identificamos $r = [r_{*1}\ r_{*2}\ r_{01}\ r_{02}\ r_{11}\ r_{12}\ r_{21}\ r_{22}]$ e tomando $k = 1$ vemos que na primeira coluna de G' as linhas L_1 e L_2 são não nulas, logo montamos o sistema:

$$\begin{cases} (L_1 + L_2)\text{mod}2 = 0 \\ (L_2 + L_3)\text{mod}2 = 0 \\ (L_3 + L_0)\text{mod}2 = 0 \\ (L_0 + L_1)\text{mod}2 = 1 \end{cases}$$

Assim, tomando $L_1 = 1$ e $L_2 = 1$ devemos ter $L_3 = 1$, $L_0 = 1$ e $L_1 = 0$ um absurdo, logo o sistema é impossível e ocorreu um erro em ao menos uma destas posições.

Agora tomando $k = 2$, obtemos o sistema

$$\begin{cases} (L_0 + L_1)\text{mod}2 = 1 \\ (L_1 + L_2)\text{mod}2 = 0 \\ (L_2 + L_3)\text{mod}2 = 1 \\ (L_3 + L_0)\text{mod}2 = 0 \end{cases}$$

Então, se tomarmos $L_0 = 1$ e $L_1 = 0$ na primeira linha, obtemos $L_2 = 0$, $L_3 = 1$ e $L_0 = 1$, ou seja, sistema possível e obtemos a palavra $c' = L_0 + L_3 = [0\ 1\ 1\ 0\ 0\ 1\ 1\ 0]$. Note que então temos $r + c' = [0\ 0\ 1\ 0\ 0\ 0\ 0\ 0]$ e como $\omega(r + c') \leq 1$, a palavra enviada foi $e = [0\ 1\ 1\ 0\ 0\ 1\ 1\ 0]$.

Se a matriz foi construída utilizando a distância, então o procedimento se torna o mesmo se o k escolhido for referente à uma coluna com peso 2.

3.4 Melhorando a distância

Como vimos nas seções anteriores deste capítulo, conseguimos construir códigos lineares sobre o Semi-Plano Superior Finito $\mathbf{H}_q$ utilizando tanto a norma como a distância até um elemento fixado e para isto escolhemos um elemento do corpo $\mathbb{F}_{2^r}$ para tomar a entrada da matriz igual 1 se a norma ou distância até o elemento fixado for igual ao elemento do corpo escolhido ou zero caso contrário. Com isto, utilizando a norma, vimos que obtemos um código

quasi-cíclico $\mathscr{C}$ com parâmetros $[2^{2r-1}, 2^r - 1, 2^r]$ e se utilizarmos a distância, obtemos um código quasi-cíclico $\mathscr{C}$ com parâmetros $[2^{2r-1} + 2^r, 2^r, 2^r]$.

Note que em ambos os métodos, escolhemos um elemento e apenas um elemento do corpo $\mathbb{F}_{2^r}$ e neste caso restringimos a distância mínima a ser no máximo 2^r. Porém, se ao invés de escolhermos apenas um elemento, tomarmos mais elementos, podemos melhorar a distância, porém, aumentaremos o comprimento do nosso código.

Se estivermos utilizando a norma para gerar a matriz $N(G)$, então, se escolhermos colocar 1 na entrada cuja norma é igual a qualquer elemento de um conjunto com t elementos, então nossa distância passará a ser limitada superiormente pelo número $2^r.t$.

A questão que fica agora é: que número t escolher de forma a se obter o melhor código possível?

Em [35] Tiu e Wallace escolhem colocar 1 se a norma é um resíduo quadrático e 0 caso contrário. Como provado em [23], metade dos elementos de um corpo com característica ímpar são resíduos quadrático, logo Tiu e Wallace estão escolhendo o número t como sendo $t = \frac{q}{2}$.

Naturalmente seguiremos a mesma idéia, porém como todo elemento é um resíduo quadrático em corpos com característica par, devemos escolher os elementos de outra forma. Com a ajuda do professor Emerson Vitor Castelani, o qual escreveu um algoritmo no Software livre Julia, para nos ajudar a determinar os elementos que fornecem a melhor distância possível para alguns exemplos criados, somos levados a crer que este número t deve ser $t = 2^{r-1}$ ou $t = 2^{r-1} - 1$.

Na escolha destes números, vamos tomar os t elementos de forma que uma coluna ao menos, tenho peso 2, garantindo assim a dimensão do código em $2^r - 1$. Também, não tomaremos todos os elementos de uma mesma coluna, ou seja, em todas as colunas o peso deve ser menor que $2^r - 2$.

Para construirmos alguns exemplos, utilizamos o software livre GAP para fazermos as operações sobre os corpos finitos.

Exemplo 3.6. Vamos construir o corpo $\mathbb{F}_{16}$ com o polinômio $x^4 + x^3 + 1$ irredutível sobre $\mathbb{F}_2$. Em seguida encontraremos todas as soluções de $N(x+\theta y) = \alpha^i$ para $* < 0 < i < 14$ no GAP conforme apresentado no apêndice A e construiremos a matriz G.

Agora, a partir da matriz G, utilizaremos o software Julia com as linhas de comando apresentadas no apêndice A, elaboradas pelo professor Emerson, para obtermos todas as distâncias possíveis para escolhas de 8 dos 15 elementos não nulos de $\mathbb{F}_{16}$ para construirmos a matriz $N(G)$, e vemos que se escolhermos 8 elementos, aqueles que nos fornecem a melhor

distância, a qual é 100, são os elementos

$1, \alpha, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{13}$.

Obtemos ainda que se tomarmos apenas 7 elementos, também conseguimos a distância 100 e os elementos que podem ser escolhidos são:
$1, \alpha, \alpha^2, \alpha^4, \alpha^5, \alpha^7, \alpha^9 - [240, 15, 100]$
$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^{12}, \alpha^{13} - [240, 15, 100]$

Com este exemplo vemos que podemos melhorar a distância do nosso código, porém teremos que utilizar todas as colunas, aumentando então o comprimento do nosso código. Com isso, ficamos com a distância mínima muito próxima da distância do melhor código binário quasi-cíclico conhecido com mesmo comprimento e dimensão que neste caso é 104.

Com o exemplo para $q = 8$, obtemos um código binário quasi-cíclico de comprimento 56, dimensão 7 e distância mínima 24 se escolhemos 3 ou 4 elementos para construirmos a matriz $N(G)$. Os elementos escolhidos para obtermos estes resultados neste caso são:

3 elementos :
$1, \alpha, \alpha^3 - [56, 7, 24]$
$1, \alpha^2, \alpha^4 - [56, 7, 24]$
$1, \alpha^3, \alpha^4 - [56, 7, 24]$
$1, \alpha^3, \alpha^5 - [56, 7, 24]$
$1, \alpha^5, \alpha^6 - [56, 7, 24]$
$\alpha, \alpha^2, \alpha^3 - [56, 7, 24]$
$\alpha, \alpha^2, \alpha^4 - [56, 7, 24]$
$\alpha, \alpha^4, \alpha^6 - [56, 7, 24]$
$\alpha^2, \alpha^3, \alpha^4 - [56, 7, 24]$
$\alpha^3, \alpha^4, \alpha^6 - [56, 7, 24]$

4 elementos
$1, \alpha, \alpha^3, \alpha^5 - [56, 7, 24]$
$1, \alpha, \alpha^4, \alpha^6 - [56, 7, 24]$
$1, \alpha^2, \alpha^4, \alpha^6 - [56, 7, 24]$
$1, \alpha^4, \alpha^5, \alpha^6 - [56, 7, 24]$
$\alpha, \alpha^2, \alpha^3, \alpha^4 - [56, 7, 24]$
$\alpha, \alpha^3, \alpha^4, \alpha^6 - [56, 7, 24]$

$\alpha^3, \alpha^4, \alpha^5, \alpha^6 - [56, 7, 24]$

Os exemplos mostram-se promissores com relação aos códigos binários já existentes. Porém ainda não conseguimos uma relação entre os elementos que devem ser escolhidos.

Para o caso onde construímos a matriz G utilizando a distância, podemos fazer o mesmo procedimento. Porém vemos que se escolhermos um número ímpar de elementos, a distância será sempre fixa em q. Assim, podemos acrescentar como sendo 1 também a entrada cuja distância até o elemento fixado é 0 ou 1, porém fazendo isto, reduzimos a dimensão do código e também conseguimos obter os mesmos parâmetros do caso utilizando a norma.

Uma desvantagem de melhorarmos a distância desta forma é que o método de decodificação também não poderá mais ser utilizado, sendo necessário a busca por outro método.

Capítulo 4

Códigos Não-Lineares e Não-Binários sobre $\mathbf{H}_q$

Neste capítulo construiremos uma nova família de códigos sobre $\mathbf{H}_q$ porém, diferentemente do capítulo anterior, estes códigos não são lineares, não são binários e q pode ser ímpar. Além disso, aqui não utilizaremos a notação do capítulo anterior.

4.1 Construção

Seja $\mathbf{H}_q$ construído como em (2.1), $\Gamma \subseteq GL(2, \mathbb{F}_q)$ e $\mathfrak{D}$ um domínio fundamental para a ação de Γ sobre $\mathbf{H}_q$. Considerando a ordem apresentada em (2.2), iremos ordenar os elementos de $\mathbf{H}_q$ da seguinte forma: dados $z = x + \delta y,\ w = u + \delta v \in \mathbf{H}_q$, diremos que $z < w$ se, e somente se, $x < u$ ou $y < v$ caso $x = u$.

Agora, seja $\mathfrak{D}$ um domínio fundamental para a ação de Γ sobre $\mathbf{H}_q$ e consideremos os elementos de $\mathfrak{D}$ ordenados em ordem crescente, ou seja, sejam $z_1 < z_2 < \cdots < z_n$ os elementos de $\mathfrak{D}$ e tomemos o vetor $c_0 = [z_1, z_2, \ldots, z_n]$, onde $|\mathfrak{D}| = n$. Tal vetor será o vetor gerador de nosso código.

Para obtermos as palavras do código, tomaremos $\gamma \in \Gamma$ e aplicaremos em todas as entradas de c_0. Note, pelos exemplos no Capítulo 2, que podemos ter $\gamma_i(c_0) = \gamma_j(c_0)$, para isto, basta que $\gamma_i^{-1} \circ \gamma_j = c.Id$. Então, tomaremos como palavras do código todos os elementos distintos obtidos ao se aplicar $\gamma \in \Gamma$ em c_0.

Exemplo 4.1. Consideremos o Exemplo 2.5 no capítulo 2. Encontramos que $\overline{D_\Gamma(z_0)} = \{\alpha + \delta,\ \alpha^2 + \delta,\ \delta,\ 1 + \delta\}$ é um domínio fundamental para a ação de $\Gamma = K$ sobre $\mathbf{H}_4$. Ordenando estes elementos teremos $c_0 = [\delta, 1 + \delta, \alpha + \delta, \alpha^2 + \delta]$ e então, aplicando os

elementos de Γ em c_0 obtemos as palavras distintas do código dadas por:
$c_1 = [\delta,\ 1+\delta,\ \alpha+\delta,\ \alpha^2+\delta]$
$c_2 = [\delta,\ 1+\delta,\ \alpha^2+\alpha^2\delta,\ \alpha^2\delta]$
$c_3 = [\delta,\ 1+\delta,\ 1+\alpha^2\delta,\ \alpha+\alpha^2\delta]$
$c_4 = [\delta,\ 1+\delta,\ 1+\alpha\delta,\ \alpha^2+\alpha\delta]$
$c_5 = [\delta,\ 1+\delta,\ ,\alpha+\alpha\delta,\ \alpha\delta]$

Consideremos agora o código com parâmetros (n, M, d) criado, onde n é o comprimento, M o número de palavras do código e d a distância mínima do código, utilizamos a distância de Hamming. Vejamos alguns resultados sobre tais parâmetros.

Primeiramente, o comprimento do código será dado por $n = |\mathfrak{D}|$. Agora, temos pelo Lema de Burnside, para um grupo finito Γ agindo em $\mathbf{H}_q$ com $\mathrm{Fix}(\gamma) = \{z \in \mathbf{H}_q | \gamma(z) = z\}$, que $n = |\Gamma \backslash H_q| = \dfrac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} |\mathrm{Fix}(\gamma)|$.

Assim, utilizaremos as classes de conjugação de $GL(2, \mathbb{F}_q)$ apresentadas no Proposição 1.19 e determinaremos $\mathrm{Fix}(\gamma)$. Pela Proposição1.19 conseguimos construir a seguinte tabela:

Tabela 4.1: Tabela de Classes de Conjugação de $GL(2, \mathbb{F}_q)$

Tipo	Representante	# Classes	#elementos na classe
1	$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, $a \in \mathbb{F}_q$, $a \neq 0$	$q-1$	1
2	$\begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$, $a \in \mathbb{F}_q$, $a \neq 0$	$q-1$	q^2-1
3	$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $a, b \in \mathbb{F}_q$, $a \neq b$	$\frac{1}{2}(q-1)(q-2)$	$q(q+1)$
4	$\begin{bmatrix} 0 & w^{q+1} \\ -1 & w+w^q \end{bmatrix}$, $w \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$	$\frac{1}{2}q(q-1)$	$q(q-1)$

Em [34] Terras apresenta uma tabela para o caso q ímpar. Porém, como neste trabalho utilizamos ambos os casos, consideraremos a tabela acima.

Proposição 4.1. *Seja $\gamma \in GL(2, \mathbb{F}_q)$ e $\boldsymbol{H}_q$ dado em (2.1). Então*

$$|Fix(\gamma)| = \begin{cases} q(q-1) & se\ \ \gamma\ é\ do\ tipo\ 1 \\ 0 & se\ \ \gamma\ é\ do\ tipo\ 2\ ou\ 3 \\ 2 & se\ \ \gamma\ é\ do\ tipo\ 4 \end{cases}$$

Demonstração: De fato, se γ é do tipo 1 então $\gamma = a.Id$, logo $\gamma(z) = \frac{az}{a} = z$, ou seja, $\text{Fix}(\gamma) = \mathbf{H}_q \Rightarrow |\text{Fix}(\gamma)| = q(q-1)$. Se γ é do tipo 2, então $\gamma(z) = z \Leftrightarrow az + 1 = az$, a qual não possui solução, logo $|\text{Fix}(\gamma)| = 0$. Analogamente, se γ é do tipo 3, então $\gamma(z) = z \Leftrightarrow az = bz$ que não possui solução, uma vez que $a \neq b$. Para γ do tipo 4 temos que $\gamma(z) = z \Leftrightarrow z^2 - (w + w^q)z + w^{q+1} = 0$. Agora, em (2.1), se q é ímpar, tomamos $\delta = \sqrt{\varsigma}$, onde ς é um não quadrado, ou seja, $x^2 - \varsigma$ é irredutível sobre $\mathbb{F}_q$, logo $\sqrt{\varsigma} \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, e assim podemos considerar $w = \sqrt{\varsigma}$ de onde segue que $w + w^q = 0$, $w^{q+1} = \varsigma$ e assim, $\pm\sqrt{\varsigma}$ são as soluções da equação. Como $\pm\sqrt{\varsigma} \in \mathbf{H}_q$, temos que $|\text{Fix}(\gamma)| = 2$. Analogamente, se q é par, então em (2.1) tomamos $\delta = \theta$ onde θ é raíz do polinômio irredutível $x^2 + x + \alpha$ sobre $\mathbb{F}_q$, ou seja, $\delta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, assim, tomando $w = \delta$, teremos $w + w^q = 1$, $w^{q+1} = \alpha$, logo δ e δ^q satisfazem $z^2 - (w + w^q)z + w^{q+1} = 0$, como $\delta, \delta^q \in \mathbf{H}_q$, então $|\text{Fix}(\gamma)| = 2$ ■

Como consequência deste resultado temos:

Corolário 4.2. *Um domínio fundamental $\mathfrak{D}$ para a ação de $\Gamma = GL(2, \mathbb{F}_q)$ agindo sobre $\boldsymbol{H}_q$ contém apenas um elemento.*

Demonstração: De fato, pelo Lema de Burnside e da tabela acima temos:

$$|\mathfrak{D}| = |\Gamma \backslash \mathbf{H}_q| = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} |\text{Fix}(\gamma)| =$$

$$= \frac{1}{(q^2-1)(q^2-q)} \left[q(q-1)(q-1) + 0 + 0 + \frac{1}{2} q(q-1)q(q-1)2 \right] =$$

$$= \frac{(q-1)^2(q^2+q)}{(q^2-1)(q^2-q)} = 1$$

■

Vemos pelo Corolário 4.2 que não obtemos um bom código ao tomarmos $\Gamma = GL(2, \mathbb{F}_q)$ agindo sobre $\mathbf{H}_q$, visto que teremos n=1, mesmo se consideramos $\Gamma \subset GL(2, \mathbb{F}_q)$, os parâmetros do código obtido não serão bons, visto que da forma como o código foi construído, o número de palavras será baixo.

Exemplo 4.2. Consideremos os subgrupos

$$\Gamma_1 = N = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F}_q \right\}$$

$$\Gamma_2 = K = \{ g \in GL(2, \mathbb{F}_q) \mid g(\delta) = \delta \},$$

então, utilizando os resultados da Tabela 4.1 e o Lema de Burnside, sendo $\mathfrak{D}_1$ e $\mathfrak{D}_2$ os

respectivos domínios fundamentais, teremos que $|\mathfrak{D}_1| = |\Gamma_1\backslash\mathbf{H}_q| = q-1$ e $|\mathfrak{D}_2| = |\Gamma_2\backslash\mathbf{H}_q| = q$. Agora, como $\mathbf{H}_q$ possui $q(q-1)$ elementos, então teremos q palavras no código tomando-se $\mathfrak{D}_1$ como domínio fundamental e distância mínima q, visto que neste caso, nenhum elemento de $\mathfrak{D}_1$ é fixado por elementos de $\Gamma_1 = N$, logo o número de palavras é dado por $M = \frac{q(q-1)}{q-1} = q$ e tomamos apenas as palavras distintas, então temos que $\gamma_i(z_k) \neq \gamma_j(z_k)$, logo $d = q-1$. Assim, conseguimos um código com parâmetros $(q-1, q, q-1)$.

Se considerarmos $\mathfrak{D}_2$ como domínio fundamental, como visto, temos dois elementos que são fixados por γ do tipo 4, logo o número de palavras será $M = \frac{q(q-1)-2}{q-2}$ e neste caso a distância mínima será $d = q-2$. Assim, conseguimos um código com parâmetros $(q, \frac{q(q-1)-2}{q-2}, q-2)$, o que se confirma no Exemplo 4.1.

O exemplo acima nos mostra que os parâmetros de fato não são bons devido ao baixo número de palavras no código. Podemos melhorar tal número de palavras para até $n-1$ vezes o número original, mantendo o comprimento n e distância mínima d obtidos. Aqui estamos considerando a distância de Hamming. Para se obter tal aumento no número de palavras, podemos considerar o vetor gerador do código $c_0 = [z_1, z_2, \ldots, z_n]$ e obter mais $n-2$ vetores fazendo-se um "shift"para a direita em cada coordenada, obtendo-se os vetores $c_1 = [z_n, z_1, \ldots, z_{n-1}], \ldots, c_{n-2} = [z_2, z_3, \ldots, z_1]$, em seguida, aplicamos o procedimento de criação do código nesses vetores. Assim, teremos $M(n-1)$ palavras no novo código obtido. Veremos mais adiante um método de decodificação para o primeiro caso, porém tal método é perdido se fizermos tal procedimento no aumento do número de palavras, como veremos.

Contudo, se considerarmos Γ-Tesselações, por exemplo, $\Gamma = GL(2, \mathbb{F}_q)$ agindo sobre $\mathbf{H}_{q^2}$ então teremos resultados melhores nos parâmetros e poderemos manter o método de decodificação que veremos.

Para analisarmos o caso de Γ-Tesselações, vamos considerar os corpos finitos $\mathbb{F}_q$ e $\mathbb{F}_{q^2} = \mathbb{F}_q(\delta)$ onde δ é dado como em (2.1). Note que agora, para construirmos $\mathbf{H}_{q^2}$, precisaremos de um elemento δ_1 raíz de um polinômio irredutível $x^2 + t_1 x + n_1$ sobre $\mathbb{F}_{q^2}$ se q é par ou $\delta_1 = \sqrt{\varsigma_1}$ se q é ímpar, onde ς_1 é um não quadrado em $\mathbb{F}_{q^2}$, ou seja, $\mathbf{H}_{q^2} = \{x + \delta_1 y \mid x, y \in \mathbb{F}_{q^2} = \mathbb{F}_q(\delta),\ y \neq 0\}$.

Proposição 4.3. *Sejam $\gamma \in GL(2, \mathbb{F}_q)$ e $\boldsymbol{H}_{q^2}$ como acima. Então*

$$|Fix(\gamma)| = \begin{cases} q^2(q^2-1) & \text{se } \gamma \text{ é do tipo 1} \\ 0 & \text{se } \gamma \text{ é do tipo 2, 3 ou 4} \end{cases}$$

Demonstração: De fato, a demonstração é essencialmente a mesma da Proposição 4.1. Porém agora, como $|\mathbf{H}_{q^2}| = q^2(q^2-1)$, se γ é do tipo 1, então $|\mathrm{Fix}(\gamma)| = q^2(q^2-1)$ e como

$\mathbf{H}_{q^2} = \{x + \delta_1 y \mid x, y \in \mathbf{F}_{q^2} = \mathbf{F}_q(\delta),\ y \neq 0\}$, os pontos fixados para γ do tipo 4, continuam sendo $\pm\delta$ para q ímpar e $\delta,\ \delta^q$ para q par, os quais não pertencem à $\mathbf{H}_{q^2}$. Logo, $|\mathrm{Fix}(\gamma)| = 0$. ■

Lema 4.4. *Seja $\mathfrak{D}$ um domínio fundamental para a ação de $\Gamma = GL(2, \mathbb{F}_q)$ agindo sobre $\boldsymbol{H}_{q^2}$. Então*

$$|\mathfrak{D}| = |\Gamma \backslash \boldsymbol{H}_{q^2}| = q$$

Demonstração: O resultado segue diretamente do Lema de Burnside e da Proposição 4.3. Segue destes resultados que $|\mathfrak{D}| = \dfrac{1}{(q^2-1)(q^2-q)}[(q-1)q^2(q^2-1)] = q$ ■

Teorema 4.5. *Sejam $\mathfrak{D}$ um domínio fundamental para a ação de $\Gamma = GL(2, \mathbb{F}_q)$ sobre $\boldsymbol{H}_{q^2}$ e $c_0 = [z_1, z_2, \ldots, z_n]$ o vetor com elementos de $\mathfrak{D}$ em ordem crescente. Então o código $\mathscr{C}$ obtido tomando-se os elementos distintos, após aplicarmos os elementos de Γ em c_0, possui parâmetros $(n = q, M = q(q^2-1), d = q)$.*

Demonstração: De fato, o comprimento $n = q$ decorre diretamente do Lema 4.4. Para o número de palavras, como tomamos $\mathfrak{D}$ um domínio fundamental, temos que $|\mathbf{H}_q| = q^2(q^2-1)$ e, pela Proposição 4.3, segue que $M = \frac{q^2(q^2-1)}{q} = q(q^2-1)$. Para a distância mínima temos que se $\gamma \in \Gamma$, então $\gamma^{-1} \in \Gamma$. Assim, suponha que existem $\gamma_i, \gamma_j \in \Gamma$ com $\gamma_i(z_k) = \gamma_j(z_k)$ para algum $z_k \in \mathfrak{D}$, então z_k é fixado por $\gamma_i^{-1} \circ \gamma_j$, e pela Proposição 4.3 temos que $\gamma_i^{-1} \circ \gamma_j = c.Id$, logo $\gamma_i^{-1} \circ \gamma_j$ fixa todos os elementos de $\mathfrak{D}$, ou seja, $\gamma_i(z_k) = \gamma_j(z_k)\ \forall\ z_k \in \mathfrak{D}$ e assim $\gamma_i(c_0) = \gamma_j(c_0)$, absurdo pois tomamos as palavras distintas. Portanto a distância mínima será $d = q$. ■

Note que novamente, neste caso, podemos aumentar o número de palavras do código para até $q-1$ vezes o número original fazendo o "shift"$q-1$ vezes para a direita nas coordenadas das palavras do código original. Porém, assim como mencionado anteriormente, perdemos o método de decodificação que será apresentado a seguir.

4.1.1 Decodificação

Para decodificarmos uma palavra recebida $\mathbf{r}$, utilizaremos a Proposição 2.7. Assim, sejam $\mathbf{e} = [e_1, e_2, \ldots, e_n]$ e $\mathbf{r} = [r_1, r_2, \ldots, r_n]$ as palavras enviada e recebida respectivamente. Note que $\mathbf{e} = \gamma(c_0)$, ou seja, $e_i = \gamma(z_i),\ i = 1, 2, \ldots, n$ para alguma $\gamma \in \Gamma$. Logo, pela Proposição 2.7 basta tomarmos $r_i,\ r_j,\ r_k$ e determinarmos γ' tal que $\gamma'(z_i) = r_i,\ \gamma'(z_j) = r_j,\ \gamma'(z_k) = r_k$. Em seguida verificamos se $\gamma' \in GL(2, \mathbb{F}_q)$, em caso negativo, ao menos um erro ocorreu

e tomamos outra combinação de r_i, r_j, r_k. Se $\gamma' \in GL(2, \mathbb{F}_q)$, verificamos se $\omega(\gamma'(c_0) - \mathbf{r}) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$, onde $\omega(w)$ é o peso de Hamming de w. Em caso afirmativo a palavra enviada foi $\mathbf{e} = \gamma'(c_0)$. Caso contrário as três coordenadas estão erradas e escolhemos outros elementos r_i, r_j, r_k diferentes destes. Em seguida realizamos o procedimento novamente. Note que, para que este método consiga corrigir até $\left\lfloor \frac{d-1}{2} \right\rfloor$ erros, precisamos tomar $q \geq 4$ se $n = d = q$ ou $q \geq 5$ se $d = q - 2$, pois neste caso existirão ao menos três elementos que foram enviados corretamente e pela unicidade de γ dada na Proposição 2.7, conseguiremos determinar a aplicação γ correta.

Utilizando este método, teremos no máximo $\frac{q(q-1)(q-2)}{6}$ comparações, se precisarmos fazer todas as combinações de $n = q$ elementos tomados 3 a 3.

Capítulo 5

Considerações Finais

Ao longo deste trabalho, estudamos o Semi-Plano Superior Finito proposto por A. Terras [13] e encontramos duas classes de códigos corretores de erros obtidos sobre este modelo. A primeira classe, dos códigos lineares e binários obtidos no Capítulo 3, considerando-se $\mathbf{H}_q$ com q par e a segunda classe, dos códigos obtidos no Capítulo 4 considerando-se $\mathbf{H}_q$ com q podendo ser par ou ímpar.

No que se refere aos códigos lineares obtidos, vemos que os parâmetros se aproximam muito dos melhores códigos existentes com mesmo comprimento e dimensão quando tomamos $\frac{q}{2}$ elementos para considerar na construção do código. Assim, essa classe de códigos mostra-se promissora. Porém, como vimos, determinar quais são esses elementos que devem ser escolhidos no caso geral ainda não foi possível. Além disso, perdemos o método de decodificação proposto quando aumentamos o número de elementos tomados. Logo, sugerimos como possíveis trabalhos futuros, determinar uma ligação, caso exista, entre os elementos que devem ser escolhidos bem como determinar um método de decodificação para o nosso código, bem como para o código apresentado por Tiu e Wallace [35], visto que este também não possui um método de decodificação específico.

Quanto aos códigos obtidos no Capítulo 4, não conseguimos comparar tais códigos com outros devido às suas especificidades. Este códigos têm seus parâmetros facilmente determinados, inclusive quanto à distância mínima, o que é uma vantagem. Além disso, o método de decodificação proposto, apresenta um número reduzido de comparações em relação ao método ML. Novamente, ao aumentarmos o número de palavras, perdemos o método utilizado na decodificação. Assim como sugestão de trabalho futuro, propomos determinar um método utilizando as propriedades geométricas de $\mathbf{H}_q$ para decodificar o código após o aumento do

número de palavras.

Vemos então que o modelo de Semi-Plano Superior Finito pode ser utilizado na construção de códigos corretores de erros com bons parâmetros e que este ainda pode ser utilizado dentro da teoria de códigos.

Apêndice A

Linhas de Comando GAP e Julia

Com mencionado no Capítulo 3, ainda não conseguimos dizer quais os elementos tomar na melhora da distância através de uma relação entre os mesmos, assim, apresentamos aqui as linhas de comando utilizadas no GAP para determinar a matriz G e também as linhas de comando utilizadas no Julia para determinar quais elementos tomar.

H_{16}

$gap > x := X(GF(2), "x");$
x
$gap > defin := x^4 + x^3 + 1;; Factors(defin);$
$[x^4 + x^3 + Z(2)^0]$
$gap > RootsOfUPol(GF(16), defin);$
$[Z(2^4)^7, Z(2^4)^{11}, Z(2^4)^{13}, Z(2^4)^{14}]$
$gap > a := last[4];$
$Z(2^4)^{14}$
$gap > res1 := List(Elements(GF(16)), x- > [x, Filtered(Elements(GF(16)), y- > x^2 + x * y + a * y^2 = Z(2)^0)]);$
$gap > resa := List(Elements(GF(16)), x- > [x, Filtered(Elements(GF(16)), y- > x^2 + x * y + a * y^2 = a)]);$
$\vdots$
$gap > resa14 := List(Elements(GF(16)), x- > [x, Filtered(Elements(GF(16)), y- > x^2 + x * y + a * y^2 = a^{14})]);$

Em seguida, determinamos os elementos como pares (x, y) no GAP:

$gap > Concatenation(List(res1, x- > List(x[2], y- > [x[1], y])));$

$[[0*Z(2), Z(2^4)^8], [Z(2)^0, 0*Z(2)], [Z(2)^0, Z(2^4)], [Z(2^2)^2, Z(2^4)^2], [Z(2^2)^2, Z(2^4)^9], [Z(2^4), Z(2^4)^3],$
$[Z(2^4), Z(2^4)^6], [Z(2^4)^4, Z(2^4)], [Z(2^4)^4, Z(2^4)^2], [Z(2^4)^8, Z(2^4)^8], [Z(2^4)^8, Z(2^4)^{12}], [Z(2^4)^9, Z(2^4)^3],$
$[Z(2^4)^9, Z(2^4)^{12}], [Z(2^4)^{11}, Z(2^4)^4], [Z(2^4)^{11}, Z(2^4)^6], [Z(2^4)^{13}, Z(2^4)^4], [Z(2^4)^{13}, Z(2^4)^9]]$
$\vdots$
$gap > Concatenation(List(resa14, x- > List(x[2], y- > [x[1], y])));$

$[[0*Z(2), Z(2^4)], [Z(2^4), Z(2^2)], [Z(2^4), Z(2^4)], [Z(2^4)^2, Z(2^2)], [Z(2^4)^2, Z(2^4)^{11}], [Z(2^4)^3, Z(2^2)^2],$
$[Z(2^4)^3, Z(2^4)^2], [Z(2^4)^4, Z(2^4)^{12}], [Z(2^4)^4, Z(2^4)^{14}], [Z(2^4)^6, Z(2^4)^2], [Z(2^4)^6, Z(2^4)^{12}], [Z(2^4)^8, 0*$
$Z(2)],$
$[Z(2^4)^8, Z(2^4)^9], [Z(2^4)^9, Z(2^4)^{11}], [Z(2^4)^9, Z(2^4)^{14}], [Z(2^4)^{12}, Z(2^2)^2], [Z(2^4)^{12}, Z(2^4)^9]]$

Agora tomamos os blocos C_i, e construindo a matriz G, podemos utilizar o algoritmo criado pelo professor Emerson no software Julia, para obtermos os elementos que devem ser escolhidos de forma a obtermos a melhor distância possível.

As linhas de comando do algoritmo são:

$usingCombinatorics$
$include("arvore.jl")$
$functionsomamod2(ind, mat, n)$
$vs = zeros(n)$
$foriinind$
$vs = vs + mat[i, :]$
end
$returnsum(mod.(vs, 2))$
end

$functionbusca(ent, mat)$
$(m, n) = size(mat)$
$saida = zeros(m, n)$
$foriinent$

```
for k = 1 : m
for j = 1 : n
if i == mat[k, j]
saida[k, j] = 1
end
end
end
end
lista = buildtree(m)
aux_vsum = 0.0
vsum = 2000.0
for el in lista
vi = find(el)
aux_vsum = somamod2(vi, saida, n)
if vsum > aux_vsum&&aux_vsum > 0.0
vsum = aux_vsum
end
end
return vsum
end

    function main(nc, mat)
v = [0, 1, "a", "a2", "a3", "a4", "a5", "a6", "a7", "a8", "a9", "a10", "a11", "a12", "a13", "a14"]
output = "output_combinations_$nc.dat"
outputg100 = "output_combinations_g100_$nc.dat"
g = open(output, "w")
g100 = open(outputg100, "w")
list = combinations(v, nc)
for comb in list
sol = busca(comb, mat)
println(comb, , sol)
println(g, comb, , sol)
if sol >= 100
println(g100, comb, , sol)
end
```

end
$close(g)$
$close(g100)$
end
$A = readdlm(\text{"}tab1.csv\text{"})$
$main(8, A)$

Nesta última linha de comando especificamos quantos elementos estamos tomando para gerar todas as combinações possíveis com estes elementos.

Referências Bibliográficas

[1] Albuquerque, C. D. Palazzo Jr., R., and Silva, E. B. Topological quantum codes on compact surfaces with genus g > 2. *Journal of Mathematical Physics vol. 50* (2009), p. 023513.

[2] Angel, J. Finite upper half planes over finite fields. *Finite Fields and Their Applications 2*, 1 (1996), 62 – 86.

[3] Angel, J. Celniker, N. P. S. T. A. T. C., and Velasquez, E. Special functions on finite upper half planes. *Contemp. Math. 138* (1992), 1–26.

[4] Angel, J. Poulos, S. T. A. T. C., and Velasquez, E. Spherical functions and transforms on finite upper half planes: Eigenvalues of of the combinatorial laplacian, uncertainty, traces. *Contemp. Math. 173* (1994), 15–70.

[5] Baldi, M. *QC-LDPC Code-Based Cryptography*. Springer Publishing Company, Incorporated, 2014.

[6] Bhandari, M. C., Gupta, M. K., and Lal, A. K. Some results on nqr codes. *Designs, Codes and Cryptography 16*, 1 (Jan 1999), 5–9.

[7] Blanco-Chacon, I. Rem ´ on, D. H. C., and Alsinac ´, M. Nonuniform fuchsian codes for noisy channels. *J. Frankl. Inst. 351* (2014), 5076–5098.

[8] Carmichael, R. D. *Introducion to the Theory of Groups of Finite Order*. Dover Publications, Inc., 2000.

[9] Carvalho, E. D., and Andrade, A. A. Hyperbolic lattices: A new propose for coding theory. *Internat. J. App. Math v. 24* (2011), p. 65–72.

[10] Cavalcante, R. G. Lazari, H. L. J. D., and R. Palazzo, . A new approach to the design of digital communication systems. *AMS-DIMACS Series v. 68* (2005), p. 145–177.

[11] Cavalcante, R. G., and Palazzo Jr., R. Performance analysis of mpsk signal constellations in riemannian varieties. *Lect. Notes Comp. Science vol. 2643* (2003), 191–203.

[12] Celniker, N. *Ph.D. thesis*. PhD thesis, University of California, San Diego, 1991.

[13] Celniker, N., Poulos, S., Terras, A., Trimble, C., and Velasquez, E. Is there life on finite upper half planes. *Contemp. Math. 143* (01 1993), 65 – 88.

[14] Evans, R. Spherical functions for finite upper half planes with characteristic 2. *Finite Fields and Their Applications 1*, 3 (1995), 376 – 394.

[15] HAMMING, R. W. Error detecting and error correcting codes. *BELL SYSTEM TECHNICAL JOURNAL 29*, 2 (1950), 147–160.

[16] Hefez, A., and Villela, M. *Códigos correctores de erros*. Computação e matematica. IMPA, 2008.

[17] Hesbo, O. E., and Oduor, O. M. On cunjugacy and order structure of certain classes of finite groups. *International Journal of Pure and Applied Mathematics 91*, 4 (2014), 435–458.

[18] Huffman, W., and Pless, V. *Fundamentals of Error-Correcting Codes*. Cambridge, Ma University Press, 2003.

[19] Katz, N. Estimates for soto–andrade sums. *J. Reine Angew. Math. 438* (1993), 143–161.

[20] Lane, S., and Birkhoff, G. *Algebra*. Chelsea Publishing Series. Chelsea Publishing Company, 1999.

[21] Lazari, H., and Palazzo Jr., R. Geometrically uniform hyperbolic codes. *Comp. Appl. Math vol. 24(2)* (2005), 173–192.

[22] Lidl, R., and Niederreiter, H. *Finite Fields*. No. v. 20,pt. 1 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.

[23] MacWilliams, F., and Sloane, N. *The Theory of Error-Correcting Codes*, 2nd ed. Northholland Publishing Company, 1978.

[24] Martin, P. A. *Grupos, corpos e teoria de galois*, vol. 2. Editora Livraria da Física, 2010.

[25] Medrano, A., Myers, P., Stark, H., and Terras, A. Finite analogues of euclidean space. *Journal of Computational and Applied Mathematics 68*, 1 (1996), 221 – 238.

[26] Moreno, O. On primitive elements of trace equal to 1 in gf(2m). *Discrete Mathematics 41*, 1 (1982), 53 – 56.

[27] Poulos, S. *Ph.D. thesis*. PhD thesis, University of California, San Diego, 1991.

[28] Shaheen, A. M. *Finite Planes and Finite Upper Half Planes: Their Geometry, a Trace Formula, Modular Forms, and Eisenstein Series.* PhD thesis, University of California, San Diego, 2005.

[29] Shaheen, A. M. A trace formula for finite upper half planes. *J. Ramanujan Math. Soc. 4* (2006), 343–363.

[30] Shannon, C. E. A mathematical theory of communication. *Bell System Technical Journal 27* (1948), 379–423.

[31] Shparlinski, I. *Finite Fields: Theory and Computation The Meeting Point of Number Theory, Computer Science, Coding Theory and Cryptography*, 1st ed. Springer Publishing Company, Incorporated, 2010.

[32] Silva, E. B. Firer, M. C. S. R., and Palazzo Jr., R. Signal constellations in the hyperbolic plane: A proposal for new communication systems. *J. Franklin Inst. 343* (2006), 69–82.

[33] Terras, A. *Fourier Analysis on Finite Groups and Applications*. London Mathematical Society St. Cambridge University Press, 1999.

[34] Terras, A. *Harmonic Analysis on Symmetric Spaces - Euclidean Space, the Sphere, and the Poincaré Upper Half-Plane*. Springer New York, 2013.

[35] Tiu, P. D., and Wallace, D. I. Norm quadratic-residue codes. *IEEE Transactions on Information Theory 40*, 3 (May 1994), 946–949.

[36] Yucas, J. L., and Mullen, G. L. Irreducible polynomials over gf(2) with prescribed coefficients. *Discrete Mathematics 274*, 1 (2004), 265 – 279.