UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

UMA MELHORA DAS COTAS DE FENG-RAO E DE MIURA PARA A DISTÂNCIA MÍNIMA DE CÓDIGOS DEFINIDOS SOBRE UMA VARIEDADE AFIM

Por

ALINE MOTA DE MESQUITA

ORIENTADOR:
PROF. DR. PAULO HENRIQUE DE AZEVEDO RODRIGUES

DISSERTAÇÃO DE MESTRADO EM MATEMÁTICA

GOIÂNIA, GOIÁS
2007

UFG

sistema de bibliotecas ufg

Termo de Ciência e de Autorização para Disponibilizar as Teses e Dissertações Eletrônicas (TEDE) na Biblioteca Digital da UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás–UFG a disponibilizar gratuitamente através da Biblioteca Digital de Teses e Dissertações – BDTD/UFG, sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira. a partir desta data.

1. Identificação do material bibliográfico: **[X] Dissertação** **[ ] Tese**

2. Identificação da Tese ou Dissertação

Autor(a):	Aline Mota de Mesquita				
CPF:		E-mail:	amm.aline@gmail.com		
Seu e-mail pode ser disponibilizado na página? [X]Sim [ ] Não					
Vínculo Empregatício do autor					
Agência de fomento:	Coord. de Aperf. de Pessoal de Nível Superior			Sigla:	CAPES
País:	Brasil	UF:	GO	CNPJ:	00889834\0001-08
Título:	Uma melhora das cotas de Feng-Rao e de Miura para a distância mínima de códigos definidos sobre uma variedade afim.				
Palavras-chave:	Códigos sobre uma variedade afim; cota de Feng-Rao; cota de Miura.				
Título em outra língua:	An improvement of the Feng-Rao and Miura's bounds on minimum distance for codes defined an affine variety.				
Palavras-chave em outra língua:	Codes on affine variety; Feng-Rao bound; Miura bound.				
Área de concentração:	Álgebra				
Data defesa: (dd/mm/aaaa)	18/12/2007				
Programa de Pós-Graduação:	Mestrado em Matemática				
Orientador(a):	Professor Doutor Paulo Henrique de Azevedo Rodrigues				
CPF:		E-mail:	paulo@mat.ufg.br		
Co-orientador(a):					
CPF:		E-mail:			

3. Informações de acesso ao documento:

Liberação para disponibilizacão?[1] [X] total [ ] parcial

Em caso de disponibilização parcial, assinale as permissões:

[ ] Capítulos. Especifique: _____

[ ] Outras restrições: _____

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC da tese ou dissertação.

O Sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses e ou dissertações, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.

Aline Mota de Mesquita

Assinatura do(a) autor(a)

Data: 18 / 12 / 2007.

[1] Em caso de restrição, esta poderá ser mantida por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Todo resumo e metadados ficarão sempre disponibilizados.

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
COORDENAÇÃO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Uma melhora das cotas de Feng-Rao e de Miura para a distância mínima de códigos definidos sobre uma variedade afim

Por

Aline Mota de Mesquita

Área de concentração: Álgebra
Orientador: Prof. Dr. Paulo Henrique de Azevedo Rodrigues

Dissertação submetida à Banca Examinadora designada pelo Conselho Diretor do Instituto de Matemática e Estatística, como parte dos requisitos necessários à obtenção do grau de Mestre em Matemática.

GOIÂNIA, GOIÁS
2007

Dados Internacionais de Catalogação-na-Publicação (CIP)

(GPT/BC/UFG)

Mesquita, Aline Mota de.
M582m Uma melhora das cotas de Feng-Rao e de Miura para a distância mínima de códigos definidos sobre uma variedade afim / Aline Mota de Mesquita. – 2007.

77f.

Orientador: Prof. Dr. Paulo Henrique de Azevedo Rodrigues.

Dissertação (Mestrado) – Universidade Federal de Goiás. **Instituto de Matemática e Estatística**, 2007.

Bibliografia: f. 75-77.

1.Códigos lineares – Códigos sobre uma variedade afim 2. Cota de Feng-Rao 3. Cota de Miura 4. Álgebra I. Rodrigues, Paulo Henrique de Azevedo. II. Universidade Federal de Goiás. **Instituto de Matemática e Estatística.** III. Título.

CDU: 512

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
COORDENAÇÃO DO PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA-MESTRADO

"UMA MELHORA DAS COTAS DE FENG-RAO E DE MIURA PARA A DISTÂNCIA MÍNIMA DE CÓDIGOS DEFINIDOS SOBRE UMA VARIEDADE AFIM"

por

Aline Mota de Mesquita

Dissertação submetida à Banca Examinadora designada pelo Conselho Diretor do Instituto de Matemática e Estatística, como parte dos requisitos necessários à obtenção do grau de Mestre em Matemática.

Goiânia, 18 de dezembro de 2007.

Banca Examinadora:

Prof. Dr. Paulo Henrique de Azevedo Rodrigues - IME/UFG
(Orientador)

Prof. Dr. Flávio Leonardo Cavalcanti de Moura – UnB

Prof. Dr. Mário José de Souza - IME/UFG

A meus pais: **Neuza** e **Divino**.

DEDICO

Agradecimentos

A Deus, o dono da minha vida, quem me criou e me capacitou a chegar até aqui.

Ao Professor Doutor Paulo Henrique de Azevedo Rodrigues pela grande atenção, paciência e dedicação que teve comigo durante as orientações. Seu auxílio foi fundamental no meu desenvolvimento. Muito obrigada!

À minha família, em especial aos meus pais Neuza e Divino que sempre me apoiaram incondicionalmente, me incentivando a cada dia. Eu os amo muito.

Aos professores do Corpo Docente do Mestrado em especial àqueles com quem cursei alguma disciplina.

Aos meus colegas que, durante o período de aula, tanto contribuíram para a minha formação em momentos formidáveis de estudo.

À Banca Examinadora pela disponibilidade e atenção dispensada ao meu trabalho.

À Capes pelo apoio financeiro.

Resumo

Nesta dissertação apresentamos alguns códigos lineares e tratamos de parâmetros de famílias de códigos cíclicos que conduzem à caracterização dos códigos de Goppa, para o qual descrevemos cotas para a distância mínima quando este é dado sobre uma variedade afim. Quando tal código é assim definido, dizemos que ele é um código geométrico de Goppa melhorado. A primeira das cotas mencionada neste trabalho foi dada por Feng e Rao em [6] (cota de Feng-Rao), posteriormente melhorada por Miura em [18],[19] (cota fraca de Feng-Rao), que por sua vez foi melhorada por G. Salazar, D. Dunn e S. B. Graham em [22] (cota indicativa e estimativa indicativa forte), sendo que neste último artigo está fundamentada esta dissertação. Encerramos nosso trabalho exibindo famílias de códigos para as quais verificamos a veracidade das melhoras das cotas.

Abstract

In this work we present some linear codes and we discuss about parameters of cyclic codes families that lead to the characterization of the Goppa codes, which we describe minimum distance bounds when it is given for an affine variety. When this code is defined like this, we say that it is an improved geometric Goppa code. The first bounds mentioned in this work was given by Feng and Rao in [6] (Feng-Rao bound), later improved by Miura in [18],[19] (weakly Feng-Rao bound), that in its turn has been improved by G. Salazar, D. Dunn and S. B. Graham in [22] (advisory bound and strong advisory estimate). This work was based in this last article. We finishing the dissertation showing families of codes for which we verified the veracity of the improvement of bounds.

Sumário

Notações

A_r	número indicativo formado pela soma $\widetilde{N}_r + E_r$
$\mathcal{B}_r$	conjunto dos índices (i,j) tais que $h_{i,j} \in S_r$ e para todo (u,v) tal que $u = i$ e $v < j$ ou $u < i$ e $v = j$ temos que $h_{u,v} \notin S_r$
$\mathcal{B}_r^*$	conjunto dos índices (i,j) tais que $h_{i,j} \in S_r^*$ e $h_{i,j}$ é fracamente bem comportado
$\mathcal{C}_r$	conjunto das submatrizes $M_{(a,b)}$ tais que $(a,b) \in \mathcal{P}_r$
$\mathcal{C}_r'$	conjunto das submatrizes $[S_c]_{(a,b)}$ tais que $(a,b) \in \mathcal{P}_r$
$\mathcal{D}_r$	conjunto dos divisores de h_r
$\Delta(I_q)$	conjunto de todos os monômios de $\mathbb{F}_q[x_1,\ldots,x_k]$ que não são líderes de nenhum polinômio não nulo de I_q
δ	distância mínima designada
δ_{FR}	cota de Feng-Rao
δ_{WFR}	cota fraca de Feng-Rao ou cota de Miura
δ_A	cota indicativa
δ_{A^+}	estimativa indicativa forte
$\mathcal{E}_r$	conjunto dos pares $(a,b) \in \mathcal{P}_r$ tais que $M_{(a,b)}$ é extrema para h_r
H	sequência crescente (sobre $<_t$) dos elementos de $\Delta(I_q)$
I_q	conjunto gerado por um ideal $I \subseteq \mathbb{F}_q[x_1,\ldots,x_k]$ e pelos polinômios $x_1^q - x_1, \ldots, x_k^q - x_k$
$lm(f)$	monômio líder do polinômio f
$L(\underline{r})$	subespaço linear de R gerado por $\{\overline{h}_1,\ldots,\overline{h}_r\}$
MDS	Separado pela Máxima Distância

M	matriz simétrica $n \times n$ de monômios $h_{i,j}$
$M_{(a,b)}$	submatriz de M cujas entradas $h_{i,j}$ são tais que $i \in W_a$ e $b \in W_b$
$\mathcal{N}_r$	conjunto dos índices dos monômios bem comportados
$\widetilde{\mathcal{N}}_r$	conjunto dos índices dos monômios fracamente bem comportados
$\mathcal{P}_r$	conjunto dos pares $(a, b) \in W$ tais que $a + b = w(h_r)$
R	anel coordenado de $V(I_q)$
S_r	conjunto de consistência de h_r
S_r^*	subconjunto de S_r formado por todos os monômios $m \in S_r$ tais que $m <_t h_{r+1}$
$s_i(c)$	valor síndrome para c
$s_{i,j}(c)$	valor síndrome para c
S_c	matriz $n \times n$ de síndromes para c cujas entradas são valores síndrome $s_{i,j}(c)$
$[S_c]_{(a,b)}$	submatriz de S_c cujas entradas $s_{i,j}(c)$ são tais que $i \in W_a$ e $j \in W_b$
T^k	conjunto de todos os monômios de $\mathbb{F}_q[x_1, \ldots, x_k]$
$V(I_q)$	variedade afim de I_q
W	sequência não decrescente dos pesos dos elementos de H
W_a	conjunto dos índices i tais que $w(h_i) = a$
w_i	elemento de uma base de $\mathbb{F}_q^n$
$\sim$	consistente
$<_t$	ordenação peso e lexicográfica
$<,>$	produto interno usual de K^n, onde K é um corpo
$\langle * \rangle$	conjunto gerado por $*$

Introdução

A teoria dos códigos corretores de erros é um ramo da matemática em pleno desenvolvimento, possuindo várias ramificações que utilizam diversas ferrametas matemáticas, tais como álgebra linear, teoria de anéis e corpos, teoria dos números, combinatória, probabilidade, análise, geometria e várias outras. Sempre utilizamos códigos quando queremos transmitir ou armazenar dados, desta forma, eles estão presentes em nosso cotidiano de inúmeras maneiras, por exemplo, quando assistimos a um programa de televisão, quando ouvimos um CD de música, falamos ao telefone, assistimos a um filme em DVD, navegamos pela internet, enfim, sempre que fazemos o uso de informações digitalizadas.

A teoria dos códigos iniciou o com matemático americano Claude E. Shannon, do Laboratório Bell, em um trabalho publicado em 1948 [23]. O trabalho inicial para a obtenção das primeiras classes de bons códigos foi árduo, pois exigia um profundo conhecimento de Álgebra Abstrata e Teoria de Probabilidade, sendo desenvolvido por um grupo restrito composto basicamente por matemáticos nas décadas de 50 e 60, embora a importância prática daquele tema já fosse reconhecida pelos engenheiros de comunicações da época. Entretanto, só com as pesquisas espaciais e a grande popularização dos computadores, ocorridos na década de 70, é que os engenheiros começaram a se interessar por essa teoria. A partir de então, pesquisadores vêm procurando famílias de bons códigos e desenvolvendo decodificadores eficientes para os mesmos.

Na prática, a classe mais utilizada é a dos códigos lineares devido aos seus bons algoritmos de codificação e decodificação. Os algoritmos são ditos bons no sentido

que eles são mais eficientes e não possuem um elevado custo computacional. O desenvolvimento mais importante na teoria de códigos corretores de erros nos últimos anos foi a introdução de métodos para a construção de códigos lineares sobre curvas algébricas geométricas. Estes são chamados códigos algébricos geométricos (códigos AG) e foram introduzidos por V. D. Goppa entre 1977 e 1982. Em 1982, Tsfasman, Vladut e Zink mostraram a existência de uma sequência de códigos AG que excedem a cota de Gilbert-Varshamov [14]. Desde então, surgiram vários artigos tratando de códigos AG e sua decodificação.

Feng e Rao apresentaram um eficiente algoritmo de decodificação para códigos AG [5] e, em seguida, salientaram que pode-se aumentar a dimensão do código sem diminuir sua capacidade de correção de erros deletando linhas desnecessárias na matriz teste de paridade [6]. Esta última construção é dita código geométrico de Goppa melhorado que, para alguns casos, possui parâmetros melhores que os do código de Goppa. Para tais códigos, Feng e Rao encontraram uma cota para a distância mínima, conhecida como cota de Feng-Rao. Miura observou que os resultados de Feng e Rao podem ser obtidos usando somente álgebra linear [18],[19] e melhorou a cota por eles dada criando a cota fraca de Feng-Rao [16] (ou cota de Miura) que, por sua vez, foi melhorada por G. Salazar, D. Dunn e S. B. Graham e denominada cota indicativa, a qual, em alguns casos, ainda pode ser melhorada, não se tornando uma cota para a distânica mínima, mas uma estimativa para tal, dita estimativa indicativa forte [22].

Nesta dissertação apresentamos as referidas melhoras da cota de Feng-Rao para a distância mínima de códigos geométricos de Goppa melhorados quando este é dado sobre uma variedade afim. A estrutura deste trabalho é dividida como a seguir.

O Capítulo 1 traz uma introdução à teoria de códigos corretores de erros, bem como algumas classes de códigos lineares, enfatizando os parâmetros desses códigos e tendo o código de Goppa como a classe mais importante para o nosso estudo. Convém salientar que uma parte considerável das demonstrações deste capítulo foram omitidas visto utilizarem resultados elementares de álgebra linear ou serem

muito técnicas, além de constarem em excelentes livros-texto oportunamente citados.

Em seguida, no Capítulo 2, definimos códigos sobre uma variedade afim, que são os códigos geométricos de Goppa melhorados, e apresentamos alguns conceitos e resultados que conduzem à melhora da cota de Feng-Rao para a distância mínima de tais códigos descrita por G. Salazar, D. Dunn e S. B. Graham em [22] (cota indicativa e estimativa indicativa forte), artigo este que foi a base de nossos estudos. Além de apresentarmos esta melhora, descrevemos também a cota de Feng-Rao e a cota fraca de Feng-Rao ou cota de Miura, que é também uma cota para a distância mínima inferior à cota indicativa.

Finalizamos no Capítulo 3 apresentando três famílias de códigos para as quais se aplicam as cotas dadas no Capítulo 2. Para cada uma delas construímos códigos para determinadas distâncias mínimas designadas verificando, através dos exemplos, que os códigos cuja cota para a distância mínima é a cota indicativa são códigos melhores.

Capítulo 1

Preliminares

Iniciamos este capítulo apresentando conceitos e resultados básicos da teoria de códigos corretores de erros, seguidos de uma classe desses códigos, que são os códigos lineares os quais possuem algumas subclasses dentre elas a dos códigos cíclicos que por sua vez é dividido em várias famílias: códigos BCH, Reed-Solomon, Reed-Solomon generalizados, alternantes e códigos de Goppa. Propriedades desses códigos, que nos serão úteis para o desenvolvimento deste trabalho, serão apresentadas neste capítulo, tudo com a finalidade de compreender a melhora da cota de Feng-Rao, a qual é uma cota para a distânica mínima de códigos de Goppa sobre variedades afins.

1.1 Códigos corretores de erros

O ponto de partida para a construção de um código corretor de erros é dar um conjunto finito $A \neq \emptyset$ chamado de *alfabeto*. O número de elementos de A, denotado por $|A|$, será simbolizado por q. Um código corretor de erros C é qualquer subconjunto próprio de A^n, para algum número natural n, e uma palavra $u \in A^n$ será representada por $(u_1, \ldots, u_n)$. Com o intuito de tornar precisa a noção de proximidade entre palavras, apresentamos a seguir um modo de medir a distância entre palavras em A^n e, em seguida, alguns conceitos e resultados básicos da teoria de códigos corretores

de erros.

Definição 1.1. Dados $u, v \in A^n$, a *distância de Hamming* entre u e v é definida como

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

E a *distância mínima de um código* C é o número

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

A distânica de Hamming é uma métrica em A^n de fácil verificação.

Definição 1.2. Dado um código C com distância mínima d, define-se $\kappa := \lfloor \frac{d-1}{2} \rfloor$ onde $\lfloor t \rfloor$ representa a parte inteira de um número real t.

Veja que se $u \in A^n$ e $d(u, c) \leq \kappa$ para algum $c \in C$, então c é a única palavra do código satisfazendo $d(u, c) \leq \kappa$. De fato, suponhamos que exista $c' \in C$ com $c' \neq c$ tal que $d(u, c') \leq \kappa$, logo, $d(c, c') \leq d(c, u) + d(u, c') \leq 2\kappa \leq d - 1$, o que é um absurdo, pois $d(c, c') \geq d$.

Teorema 1.3. *Seja C um código com distância mínima d. Então C pode corrigir até κ erros e detectar até $d - 1$ erros.*

Demonstração: Se ao transmitirmos uma palavra c do código cometemos t erros com $t \leq \kappa$ e recebemos a palavra r, então $d(c, r) = t \leq \kappa$, enquanto que a distância de r a qualquer outra palavra do código é maior do que κ. Isso determina c de modo único a partir de r.

Por outro lado, dada uma palavra do código, podemos nela introduzir até $d - 1$ erros sem encontrar outra palavra do código e assim, a detecção do erro será possível. □

Note que, em virtude do teorema acima, um código terá maior capacidade de correção de erros quanto maior for a sua distância mínima. Portanto, é fundamental para a teoria de códigos poder calcular d ou pelo menos determinar uma cota inferior para ele.

1.2 Códigos lineares

A classe dos códigos lineares é a mais utilizada na prática, vem daí a sua importância. Para o desenvolvimento desta seção, consideremos o corpo finito K com q elementos como sendo o alfabeto. Portanto, temos, para cada número natural n, um K-espaço vetorial de dimensão n, denotado por K^n.

Definição 1.4. Um código $C \subset K^n$ será chamado de *código linear* se for um subespaço vetorial de K^n. Os elementos de C são chamados de *palavras código*.

Definição 1.5. Dado $u \in K^n$, define-se o *peso* de u como sendo o número inteiro

$$\omega(u) := d(u, \mathbf{0}) = |\{i : u_i \neq 0, 1 \leq i \leq n\}|.$$

O *peso do código* C é o inteiro

$$\omega := min\{\omega(u) : u \in C, u \neq \mathbf{0}\}.$$

Como $d(u, v) = d(u-v, \mathbf{0}) = \omega(u-v)$ e C é um espaço linear, a distância mínima de C é equivalente a

$$d := min\{w(x) : x \in C, x \neq \mathbf{0}\}$$

A terna de inteiros $[n, k, d]$ é chamada de *parâmetros do código linear* C, onde n é o comprimento das palavras de C, k é a dimensão de C sobre K e d é a distância mínima de C. Note que o número de elementos de C é igual a q^k, onde q é o número de elementos de K.

Em álgebra linear uma maneira de descrever subespaços vetoriais de um espaço vetorial K^n é como imagem de transformações lineares. Para estas transformações podemos determinar uma matriz, dita matriz da transformação. Em teoria dos códigos, tal matriz é chamada de matriz geradora do código e definida como a seguir.

Definição 1.6. Uma *matriz geradora* de um código linear C com parâmetros $[n, k, d]$ é uma matriz G de ordem $k \times n$ cujas linhas formam uma base para C.

Exemplo 1.7. O código binário $C = \{0000, 1011, 0101, 1110\}$ é gerado pelo conjunto $\{1011, 0101\}$, logo, sua matriz geradora é

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Definição 1.8. Seja $C \subset K^n$ um código linear com parâmetros $[n, k, d]$.
i) O *código dual* de C, $C^{\perp}$, é o complemento ortogonal do subespaço C de K^n,

$$C^{\perp} = \{v \in K^n :< v, u >= 0, \forall u \in C\},$$

onde $<,>$ denota o produto interno usual de K^n.
ii) Uma *matriz teste de paridade* H para um código linear C é uma matriz geradora para o código dual $C^{\perp}$, cuja ordem é $(n-k) \times n$.

Se tomarmos a matriz G acima descrita e nela realizarmos operações do tipo permutação de duas linhas, multiplicação de uma linha por um escalar não nulo e adição de um múltiplo escalar de uma linha a outra, de forma a obtermos uma matriz do tipo $G' = (Id_k \,|\, A)$, onde Id_k é a matriz identidade $k \times k$ e A é uma matriz $k \times (n-k)$, temos uma matriz padrão de G, ou seja, $G' = (Id_k \,|\, A)$ é a matriz G na forma padrão. Entretanto, realizando somente essas operações, nem sempre encontramos uma matriz padrão de G. Nesses casos, utiliza-se operações, além das já mencionadas, do tipo permutação de duas colunas e multiplicação de uma coluna por um escalar não nulo, obtendo uma matriz padrão de um código equivalente ao código C. A partir da matriz G' obtemos que a matriz teste de paridade H é da forma $H = (-A^t \,|\, Id_{n-k})$.

Lema 1.9. *Se $C \subset K^n$ é um código linear com matriz geradora G, então*
i) $C^{\perp}$ é um subespaço vetorial de K^n;
ii) $x \in C^{\perp}$ se, e somente se, $Gx^t = \boldsymbol{0}$.

Demonstração: Ver Lema 1, Capítulo 5 de [10]. □

Como consequência do Lema 1.9 temos que para determinar se uma palavra c está no código C precisamos verificar se ela está no dual de $C^{\perp}$, ou seja, em $(C^{\perp})^{\perp}$ que é igual a C, para isso temos que verificar se $Hc^t = 0$, uma vez que H é a matriz geradora de $C^{\perp}$. Isto é exatamente o que nos diz a próxima proposição.

Proposição 1.10. *Seja C um código linear e suponhamos que H seja uma matriz geradora de $C^{\perp}$. Temos então, que $v \in C$ se, e somente se, $Hv^t = \boldsymbol{0}$.*

Demonstração: Temos, pelo fato de que $(C^{\perp})^{\perp} = C$ e pelo Lema 1.9 acima item (ii), que $v \in C$ se, e somente se, $v \in (C^{\perp})^{\perp}$ se, e somente se, $Hv^t = \mathbf{0}$. □

Deste modo, o método para determinar se uma palavra v pertence ou não a um código C se tornou mais simples. Assim, H tem a finalidade de diminuir os cálculos relacionados a um código C. O vetor Hv^t é chamado de *síndrome* de v.

Exemplo 1.11. Seja dado o código C sobre $\mathbb{F}_2$ com matriz geradora

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Como G está na forma padrão é fácil calcular uma matriz teste de paridade H. Temos que $H = (-A^t \,|\, Id_{n-k})$, logo,

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

Dados $v = (100111)$ e $v' = (010101)$, como

$$Hv^t = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \qquad e \qquad H(v')^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \neq \mathbf{0},$$

segue que $v \in C$ e $v' \notin C$.

Teorema 1.12. *Seja H a matriz teste de paridade de um código C.*
i) O peso de C é maior ou igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.
ii) O peso de C é igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.

Demonstração: Para o item (i) ver Proposição 5, Capítulo 5 de [10] e para o item (ii) ver Teorema 2, Capítulo 5 de [10]. □

Teorema 1.13. (Cota de Singleton). *Os parâmetros $[n, k, d]$ de um código linear satisfazem à desigualdade $d \leq n - k + 1$.*

Demonstração: Se H é uma matriz teste de paridade, então ela tem posto $n-k$. Como quaisquer $d-1$ colunas de H são linearmente independentes, $d-1$ é menor ou igual ao posto de H, ou seja, $d-1 \leq n-k$, então, $d \leq n-k+1$. □

Um código será dito MDS (*Separado pela Máxima Distância*) se valer a igualdade $d = n - k + 1$.

1.3 Códigos cíclicos

Os códigos cíclicos são muito utilizados nas aplicações por formarem uma classe de códigos lineares que possui bons algoritmos de codificação e de decodificação. No que se segue, representaremos as coordenadas de K^n por $(a_0, \ldots, a_{n-1})$ para estabelecermos um isomorfismo entre essas n-uplas e um anel de polinômios, uma vez que, por questão de notação, o termo independente de um polinômio é representado com índice zero.

Definição 1.14. Um código linear $C \subset K^n$ será um *código cíclico* se, dada a permutação π de $\{0, \ldots, n-1\}$ definida por

$$\pi(i) = \begin{cases} i-1, & se \quad i \geq 1 \\ n-1, & se \quad i = 0 \end{cases},$$

e sendo $T_\pi(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2})$, temos que $T_\pi c \in C$ para todo $c \in C$; ou seja, $T_\pi C \subseteq C$.

Exemplo 1.15. Os seguintes códigos são cíclicos:

i) Os códigos triviais $\{\mathbf{0}\}$ e K^n.

ii) O $[3, 2, 2]$-código linear $\{000, 110, 101, 011\}$ sobre $\mathbb{F}_2$.

Exemplo 1.16. Seja $v \in K^n$. O espaço vetorial

$$\langle v \rangle = Kv + KT_\pi v + \cdots + KT_\pi^{n-1} v$$

é claramente um código cíclico (note que $T_\pi^n = Id$).

Como exemplo numérico considere $K = \mathbb{F}_2$ e seja $v = (10011001) \in K^8$. Assim,

$$\langle v \rangle = K(10011001) + K(11001100) + K(01100110) + K(00110011).$$

Algumas questões imediatamente surgem no contexto dos códigos cíclicos, tais como: todo código cíclico é da forma $\langle v \rangle$ para algum v? Como calcular o peso de um código cíclico? A primeira pergunta será respondida logo abaixo, entretanto, a segunda é muito difícil de ser respondida e é, em parte, uma questão em aberto, existindo apenas cotas para a distância mínima de algumas classes especiais de códigos, tais como os códigos BCH e os códigos de Goppa, que é o alvo de nosso estudo.

A técnica para lidar com os códigos cíclicos consiste em enriquecer a estrutura de espaço vetorial de K^n como segue.

Defina R_n como sendo o anel das classes residuais em $K[x]$ módulo $\langle x^n - 1 \rangle$ e considere o isomorfismo

$$\begin{array}{rccc} \nu : & K^n & \to & R_n \\ & (a_0, \ldots, a_{n-1}) & \mapsto & \overline{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}} \end{array}.$$

Temos então, que todo código linear $C \subset K^n$ pode ser imerso em R_n mediante o isomorfismo ν.

Considerando $I = I(\overline{g(x)})$, onde $g(x) = g_0 + g_1x + \cdots + g_sx^s$ é um divisor de $x^n - 1$, facilmente verificamos que $\overline{g(x)}, \overline{xg(x)}, \overline{x^2g(x)}, \ldots, \overline{x^{n-s-1}g(x)}$ é uma base de I como espaço vetorial sobre K, consequentemente, temos que dado um código cíclico C, existe $v \in C$, $v = \nu^{-1}(\overline{g(x)})$, tal que $C = \langle v \rangle = \nu^{-1}(I)$, deste modo, C tem matriz geradora

$$G = \begin{pmatrix} \nu^{-1}(\overline{g(x)}) \\ \nu^{-1}(\overline{xg(x)}) \\ \vdots \\ \nu^{-1}(\overline{x^{n-s-1}g(x)}) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_s & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{s-1} & g_s & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & g_0 & g_1 & \cdots & g_s \end{pmatrix}$$

e $dim_K I = n - s$.

O dual de um código cíclico é ainda um código cíclico.

Seja

$$\begin{aligned} \mu : \quad K^s \quad &\to K[x]_{s-1} \subset K[x] \\ (a_0, \ldots, a_{s-1}) &\mapsto \sum_{i=0}^{s-1} a_i x^i \end{aligned}$$

o isomorfismo de K-espaços vetoriais, onde $K[X]_{s-1}$ é o espaço vetorial dos polinômios de grau menor ou igual a $s-1$. Esse isomorfismo será de grande utilidade no próximo teorema.

Teorema 1.17. *Seja $C \subset K^n$ um código cíclico. Suponhamos que $C = \nu^{-1}(I)$, onde $I = (\overline{g(x)})$, com $g(x)$ um divisor de $x^n - 1$ de grau s. Seja R a matriz $(n-s) \times s$ cuja i-ésima linha é*

$$R_i = -\mu^{-1}(r_i(x)), \qquad 1 \leq i \leq n - s,$$

onde $r_i(x)$ é o resto da divisão de x^{s-1+i} por $g(x)$. Então, $(R \,|\, Id_{n-s})$ é uma matriz geradora de C na forma padrão.

Demonstração: Sejam $q_i(x)$ e $r_i(x)$ o quociente e o resto da divisão de x^{s-1+i} por $g(x)$. Logo,

$$x^{s-1+i} = g(x)q_i(x) + r_i(x),$$

com $r_i(x) = 0$ ou $gr(r_i(x)) \leq s-1$.

Portanto, $\overline{x^{s-1+i} - r_i(x)}$ pertence a I e é evidente que esses vetores, para $i = 1, \ldots, n-s$, são linearmente independentes sobre K. Como $\nu^{-1}(\overline{x^{s-1+i} - r_i(x)}) = e_{s-1+i} - \mu^{-1}(r_i(x))$, temos que a matriz

$$\begin{pmatrix} -\mu^{-1}(r_1(x)) & 1 & 0 & \cdots & 0 \\ -\mu^{-1}(r_2(x)) & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -\mu^{-1}(r_{n-s}(x)) & 0 & 0 & \cdots & 1 \end{pmatrix}$$

é uma matriz geradora de C. □

Como consequência do teorema acima, temos que uma matriz teste de paridade de C é da forma $H = (Id_s \mid -R^t)$.

1.4 Códigos BCH

A classe de códigos Bose, Chaudhuri e Hocquenghem (BCH) binários foram primeiramente discorridos por A. Hocquenghem [11] em 1959 e independentemente por R. C. Bose e D. K. Ray-Chaudhuri [1] em 1960. Generalizações dos códigos BCH binários para códigos q-ários foram obtidos por D. Gorenstein e N. Zierler [8] em 1961.

Definição 1.18. Seja α um elemento primitivo de $\mathbb{F}_{q^m}$ e denote por $M^{(i)}(x)$ o polinômio minimal de α^i com respeito a $\mathbb{F}_q$. Um *código BCH* (primitivo) sobre $\mathbb{F}_q$ de comprimento $n = q^m - 1$ e distância designada δ é um código cíclico q-ário gerado por $g(x) := mmc(M^{(a)}(x), M^{(a+1)}(x), \ldots, M^{(a+\delta-2)}(x))$ para algum inteiro a. Além disso, o código é dito no sentido estrito se $a = 1$.

Quanto aos parâmetros de um código BCH, temos que seu comprimento é claramente $q^m - 1$. Os próximos teoremas nos fornecem uma cota para a dimensão e para a distância mínima. Suas demonstrações consistem de alguns resultados básicos da álgebra linear e anéis de polinômios.

Teorema 1.19. *Um código BCH q-ário de comprimento q^m-1 e distância designada δ tem dimensão pelo menos $q^m - 1 - m(\delta - 1)$.*

Demonstração: Ver Teorema 8.1.9 (ii) de [14]. □

Teorema 1.20. *Um código BCH com distância designada δ tem distância mínima pelo menos δ.*

Demonstração: Ver Teorema 8.1.18 de [14]. □

Seja α um elemento primitivo de $\mathbb{F}_{q^m}$ e seja C um código BCH com distância mínima d pelo menos δ, gerado por $g(x) = mmc(M^{(a)}(x), M^{(a+1)}(x), \ldots, M^{(a+\delta-2)}(x))$. É claro que os elementos $\alpha^a, \ldots, \alpha^{a+\delta-2}$ são raízes de $g(x)$. Seja $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ uma palavra não nula de C tal que $w(c(x)) = d$. Assim, $c(x) = g(x)t(x)$ para algum $t(x) \in \mathbb{F}_q[x]$ e as raízes de $g(x)$ são raízes de $c(x)$, ou seja, $c(\alpha^i) = 0$ para todo $i = a, \ldots, a + \delta - 2$. Em forma matricial temos:

$$\begin{pmatrix} 1 & \alpha^a & (\alpha^a)^2 & \cdots & (\alpha^a)^{n-1} \\ 1 & \alpha^{a+1} & (\alpha^{a+1})^2 & \cdots & (\alpha^{a+1})^{n-1} \\ 1 & \alpha^{a+2} & (\alpha^{a+2})^2 & \cdots & (\alpha^{a+2})^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{a+\delta-2} & (\alpha^{a+\delta-2})^2 & \cdots & (\alpha^{a+\delta-2})^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{pmatrix} = \mathbf{0}$$

Deste modo, a matriz

$$\begin{pmatrix} 1 & \alpha^a & (\alpha^a)^2 & \cdots & (\alpha^a)^{n-1} \\ 1 & \alpha^{a+1} & (\alpha^{a+1})^2 & \cdots & (\alpha^{a+1})^{n-1} \\ 1 & \alpha^{a+2} & (\alpha^{a+2})^2 & \cdots & (\alpha^{a+2})^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{a+\delta-2} & (\alpha^{a+\delta-2})^2 & \cdots & (\alpha^{a+\delta-2})^{n-1} \end{pmatrix}$$

é uma matriz teste de paridade de um código BCH.

1.5 Códigos Reed-Solomon

A subclasse mais importante dos códigos BCH é a classe dos códigos Reed-Solomon (RS). Códigos RS foram introduzidos por I. S. Reed e G. Solomon [21] independentemente do trabalho de R. C. Bose, D. K. Ray-Chaudhuri e A. Hocquenghem.

Considere um código BCH q-ário C de comprimento $q^m - 1$ gerado por $g(x) := mmc(M^{(a)}(x), M^{(a+1)}(x), \ldots, M^{(a+\delta-2)}(x))$, onde $M^{(i)}(x)$ é o polinômio minimal de α^i com respeito a $\mathbb{F}_q$ para um elemento primitivo α de $\mathbb{F}_{q^m}$. Se $m = 1$, temos um código BCH q-ário de comprimento $q - 1$. Neste caso, α é um elemento primitivo de $\mathbb{F}_q$ e, além disso, o polinômio minimal de α^i com respeito a $\mathbb{F}_q$ é $x - \alpha^i$. Deste modo, para $\delta \leq q - 1$ o polinômio gerador é

$$\begin{aligned} g(x) &= mmc(x - \alpha^a, x - \alpha^{a+1}, \ldots, x - \alpha^{a+\delta-2}) \\ &= (x - \alpha^a)(x - \alpha^{a+1}) \cdots (x - \alpha^{a+\delta-2}) \end{aligned}$$

onde $\alpha^a, \alpha^{a+1}, \ldots, \alpha^{a+\delta-2}$ são dois a dois distintos.

Definição 1.21. Um *código Reed-Solomon* q-ário (código RS) é um código BCH q-ário de comprimento $q - 1$ gerado por

$$g(x) = (x - \alpha^a)(x - \alpha^{a+1}) \cdots (x - \alpha^{a+\delta-2}),$$

com $a \geq 1$ e $2 \leq \delta \leq q - 1$, onde α é um elemento primitivo de $\mathbb{F}_q$.

Nunca consideramos códigos RS binários, pois se assim fosse, ele teria comprimento $q - 1 = 1$.

Exemplo 1.22. Considere o código RS 7-ário de comprimento 6 com polinômio gerador $g(x) = (x - 3)(x - 3^2)(x - 3^3) = 6 + x + 3x^2 + x^3$. Este código possui uma matriz geradora

$$G = \begin{pmatrix} 6 & 1 & 3 & 1 & 0 & 0 \\ 0 & 6 & 1 & 3 & 1 & 0 \\ 0 & 0 & 6 & 1 & 3 & 1 \end{pmatrix}.$$

Uma matriz teste de paridade

$$H = \begin{pmatrix} 1 & 4 & 1 & 1 & 0 & 0 \\ 0 & 1 & 4 & 1 & 1 & 0 \\ 0 & 0 & 1 & 4 & 1 & 1 \end{pmatrix}$$

é obtida por $h(x) = (x^6 - 1)/g(x) = 1 + x + 4x^2 + x^3$. Quaisquer 3 colunas de H é linearmente independentes e quaisquer 4 colunas é linearmente dependente. Assim, este é um [6,3,4]-código MDS 7-ário.

Teorema 1.23. *Códigos Reed-Solomon são MDS, isto é, um código Reed-Solomon q-ário de comprimento $q-1$ gerado por $g(x) = \prod_{i=a}^{a+\delta-2}(x - \alpha^i)$ é um $[q-1, q-\delta, \delta]$-código cíclico para qualquer $2 \leq \delta \leq q-1$.*

Demonstração: Como o grau de $g(x)$ é $\delta - 1$, a dimensão do código é exatamente $k := q - 1 - (\delta - 1) = q - \delta$ e a distância mínina é pelo menos δ. Por outro lado, pela cota de Singleton, a distância mínima é no máximo $(q-1) + 1 - k = \delta$. Logo, o código RS é MDS. □

1.6 Códigos Reed-Solomon generalizados

Considere o código RS definido na seção anterior com $a = 1$. Neste caso, existe uma descrição alternativa para tal código que é conveniente para o nosso propósito nesta seção.

Teorema 1.24. *Seja α um elemento primitivo do corpo finito $\mathbb{F}_q$ e seja $2 \leq \delta \leq q-1$. O código q-ário RS no sentido estrito com polinômio gerador*

$$g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{\delta-1})$$

é igual a

$$\{(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-2})) : f(x) \in \mathbb{F}_q[x] \text{ e } gr(f(x)) < q - \delta\}. \qquad (1.1)$$

Demonstração: É fácil verificar que o conjunto (1.1) é um $\mathbb{F}_q$-espaço vetorial. Primeiro mostraremos que ele está contido no código RS gerado por $g(x)$.

A palavra código $c = (f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-2}))$ corresponde ao polinômio $c(x) = \sum_{i=0}^{q-2} f(\alpha^i)x^i \in \mathbb{F}_q[x]/(x^n - 1)$. Precisamos mostrar que $g(x)$ divide $c(x)$ para que $c \in C$, isto é, $c(\alpha) = c(\alpha^2) = \cdots = c(\alpha^{\delta-1}) = 0$.

Note que, para $1 \leq k \leq q-2$, temos que

$$\sum_{i=0}^{q-2} \alpha^{ik} = \frac{(\alpha^k)^{q-1} - 1}{\alpha^k - 1} = 0$$

Escreva $f(x) = \sum_{j=0}^{q-\delta-1} f_j x^j$. Então, para $1 \leq l \leq \delta - 1$,

$$c(\alpha^l) = \sum_{i=0}^{q-2} f(\alpha^i)(\alpha^l)^i = \sum_{i=0}^{q-2}(\sum_{j=0}^{q-\delta-1} f_j \alpha^{ij})\alpha^{il} = \sum_{j=0}^{q-\delta-1} f_j(\sum_{i=0}^{q-2} \alpha^{i(j+l)}) = 0,$$

com $1 \leq j + l \leq q - 2$.

A aplicação $f \longmapsto (f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-2}))$ proveniente do conjunto de polinômios em $\mathbb{F}_q[x]$ de grau menor que $q - \delta$ para o conjunto em (1.1) é injetora (qualquer $f(x)$ no núcleo desta aplicação deve ter, pelo menos $q - 1 > q - \delta > gr(f(x))$ zeros, mas isso somente é possível se $f(x)$ é identicamente nulo). Esta aplicação é claramente sobrejetora, assim ela é um isomorfismo entre $\mathbb{F}_q$-espaços vetoriais. Portanto, a dimensão sobre $\mathbb{F}_q$ do espaço vetorial em (1.1) é $q - \delta$, que é a dimensão do código RS gerado por $g(x)$. Assim, segue o teorema. □

O seguinte corolário fornece explicitamente uma matriz geradora para o código RS.

Corolário 1.25. *Seja α um elemento primitivo de $\mathbb{F}_q$, e seja $2 \leq \delta \leq q - 1$. A matriz*

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{(q-2)2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{q-\delta-1} & \alpha^{2(q-\delta-1)} & \ldots & \alpha^{(q-2)(q-\delta-1)} \end{pmatrix}$$

é uma matriz geradora para o código RS gerado pelo polinômio

$$g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{\delta - 1}).$$

Uma fácil generalização da descrição do código RS no Teorema 1.24 é conduzida a uma classe mais geral de códigos que também são MDS.

Definição 1.26. Seja $n \leq q$. Seja $\alpha = (\alpha_1, \ldots, \alpha_n)$, onde α_i $(1 \leq i \leq n)$ são elementos distintos de $\mathbb{F}_{q^m}$. Seja $v = (v_1, \ldots, v_n)$, onde $v_i \in \mathbb{F}_{q^m}^*$ para todo $1 \leq i \leq n$. Para $k \leq n$, o *código Reed-Solomon generalizado* $GRS_k(\alpha, v)$ é definido por

$$\{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) : f(x) \in \mathbb{F}_{q^m}[x] \ e \ gr(f(x)) < k\}.$$

Teorema 1.27. *O código generalizado RS,* $GRS_k(\alpha, v)$ *tem parâmetros* $[n, k, n - k + 1]$*, assim, ele é um código MDS.*

Demonstração: É óbvio que $GRS_k(\alpha, v)$ tem comprimento n. O mesmo argumento da prova do Teorema 1.24 mostra que sua dimensão é k. Falta mostrar que a distância mínima é $n - k + 1$.

Para fazer isso, contamos o número máximo de zeros em uma palavra não nula do código. Suponha que $f(x)$ não seja identicamente nulo. Como $gr(f(x)) < k$, o polinômio $f(x)$ só pode ter, no máximo, $k - 1$ zeros, isto é, a palavra código $(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n))$ tem no máximo $k-1$ zeros em suas coordenadas. Em outras palavras, o peso é pelo menos $n - k + 1$, assim a distância mínima d de $GRS_k(\alpha, v)$ satisfaz $d \geq n - k + 1$. Por outro lado, a cota de Singleton, Teorema 1.13, mostra que $d \leq n - k + 1$, assim, $d = n - k + 1$. Portanto, $GRS_k(\alpha, v)$ é MDS. □

Teorema 1.28. *O dual do código generalizado RS,* $GRS_k(\alpha, v)$*, sobre* $\mathbb{F}_{q^m}$ *de comprimento* n *é* $GRS_{n-k}(\alpha, v')$ *para algum* $v' \in (\mathbb{F}_{q^m}^*)^n$.

Demonstração: Primeiro, seja $k = n-1$. Pelo Teorema 1.27, o dual de $GRS_{n-1}(\alpha, v)$ é um código MDS de dimensão 1, assim, ele tem parâmetros $[n, 1, n]$. Em particular, sua base consiste de um vetor $v' = (v_1', \ldots, v_n')$, onde $v_i' \in \mathbb{F}_q^*$ para todo $1 \leq i \leq n$. Claramente, este código dual é $GRS_1(\alpha, v')$.

Segue, em particular, que para todo $f(x) \in \mathbb{F}_q[x]$ de grau menor que $n-1$, temos

$$< v^{'}, c >= v_1 v_1^{'} f(\alpha_1) + \cdots + v_n v_n^{'} f(\alpha_n) = 0,$$

onde $v = (v_1, \ldots, v_n)$ e $<,>$ denota o produto interno usual de $\mathbb{F}_{q^m}^n$.

Agora, para um k arbitrário, afirmamos que $GRS_k(\alpha, v)^{\perp} = GRS_{n-k}(\alpha, v^{'})$.

Uma palavra típica de $GRS_k(\alpha, v)$ é $(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n))$, onde $f(x) \in \mathbb{F}_q[x]$ e $gr(f(x)) \leq k-1$, embora uma palavra típica de $GRS_{n-k}(\alpha, v^{'})$ tenha a forma $(v_1^{'} g(\alpha_1), \ldots, v_n^{'} g(\alpha_n))$, com $g(x) \in \mathbb{F}_q[x]$ de grau menor ou igual a $n-k-1$. Visto que $gr(f(x)g(x)) \leq n-2 < n-1$, temos

$$< (v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)), (v_1^{'} g(\alpha_1), \ldots, v_n^{'} g(\alpha_n)) >=$$

$$v_1 v_1^{'} f(\alpha_1) g(\alpha_1) + \cdots + v_n v_n^{'} f(\alpha_n) g(\alpha_n) = 0$$

Portanto,$GRS_{n-k}(\alpha, v^{'}) \subseteq GRS_k(\alpha, v)^{\perp}$. Comparando as dimensões de ambos os códigos, temos que $GRS_k(\alpha, v)^{\perp} \subseteq GRS_{n-k}(\alpha, v^{'})$. □

Corolário 1.29. *A matriz teste de paridade de $GRS_k(\alpha, v)$ é*

$$\begin{pmatrix} v_1^{'} & v_2^{'} & \cdots & v_n^{'} \\ v_1^{'}\alpha_1 & v_2^{'}\alpha_2 & \cdots & v_n^{'}\alpha_n \\ v_1^{'}\alpha_1^2 & v_2^{'}\alpha_2^2 & \cdots & v_n^{'}\alpha_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ v_1^{'}\alpha_1^{n-k-1} & v_2^{'}\alpha_2^{n-k-1} & \cdots & v_n^{'}\alpha_n^{n-k-1} \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{pmatrix} \begin{pmatrix} v_1^{'} & 0 & \cdots & 0 \\ 0 & v_2^{'} & \cdots & 0 \\ & & \cdots & \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & v_n^{'} \end{pmatrix}.$$

Observação 1.30. Observe que $v^{'} = (v_1^{'}, \ldots, v_n^{'})$ é qualquer vetor que gera o dual de $GRS_k(\alpha, v)$, assim, ele não é único. Em particular, a matriz teste de paridade do corolário acima não é única.

1.7 Códigos alternantes

Uma interessante família de códigos que surge por meio dos códigos generalizados RS da seção anterior é a classe dos códigos alternantes. Esta é uma grande família que inclui os códigos BCH.

Definição 1.31. Um *código alternante* $A_k(\alpha, v^{'})$ sobre um corpo finito $\mathbb{F}_q$ é o subcódigo no subcorpo $GRS_k(\alpha, v)|_{\mathbb{F}_q}$, onde $GRS_k(\alpha, v)$ é um código generalizado RS sobre $\mathbb{F}_{q^m}$, para algum $m \geq 1$.

A Observação 1.33 abaixo explica porque escolhemos $v^{'}$ na notação do código alternante em vez de v.

Proposição 1.32. *O código alternante* $A_k(\alpha, v^{'})$ *tem parâmetros* $[n, k^{'}, d]$, *onde* $mk - (m-1)n \leq k^{'} \leq k$ *e* $d \geq n - k + 1$.

Demonstração: Pelo Teorema 1.27, $GRS_k(\alpha, v)$ tem parâmetros $[n, k, n-k+1]$. Assim, $A_k(\alpha, v^{'})$ claramente tem comprimento n e sua dimensão $k^{'}$ trivialmente satisfaz $k^{'} \leq k$. Como $A_k(\alpha, v^{'})$ é um subconjunto de $GRS_k(\alpha, v)$, é claro que a distância mínima de $A_k(\alpha, v^{'})$ é pelo menos a distância mínima de $GRS_k(\alpha, v)$, isto é, $d \geq n - k + 1$. Agora, $A_k(\alpha, v^{'}) = GRS_k(\alpha, v)|_{\mathbb{F}_q} := GRS_k(\alpha, v) \cap \mathbb{F}_q^n$, assim,

$$\begin{aligned}
k^{'} &= dim_{\mathbb{F}_q} A_k(\alpha, v^{'}) = dim_{\mathbb{F}_q}(GRS_k(\alpha, v) \cap \mathbb{F}_q^n) \\
&= dim_{\mathbb{F}_q} GRS_k(\alpha, v) + dim_{\mathbb{F}_q}\mathbb{F}_q^n - dim_{\mathbb{F}_q}(GRS_k(\alpha, v) + \mathbb{F}_q^n) \\
&\geq \log_q |GRS_k(\alpha, v)| + n - dim_{\mathbb{F}_q}(\mathbb{F}_{q^m}^n) \\
&= \log_q(q^m)^k + n - \log_q(q^m)^n \\
&= mk + n - mn = mk - (m-1)n.
\end{aligned}$$

□

Observação 1.33. Segue diretamente da Definição 1.31 e do Corolário 1.29 que $A_k(\alpha, v^{'})$ não é nada mais que

$$\{c \in \mathbb{F}_q^n : Hc^t = \mathbf{0}\},$$

onde H é a matriz do corolário citado. Como H é determinada por α e $v^{'}$, é apropriado que a notação de código alternante seja expressa em termos de α e $v^{'}$.

Note que todo elemento $\beta \in \mathbb{F}_{q^m}$ pode ser escrito unicamente na forma $\sum_{i=0}^{m-1} \beta_i \alpha^i$, onde α é um elemento primitivo de $\mathbb{F}_{q^m}$ e $\beta_i \in \mathbb{F}_q$, para todo $0 \leq i \leq m-1$. Portanto, se substituirmos cada entrada β de H por um vetor coluna $(\beta_o, \ldots, \beta_{m-1})^t$, obtemos uma matriz $\bar{H}$ $(n-k)m \times n$ com entradas em $\mathbb{F}_q$, tal que $A_k(\alpha, v^{'})$ é

$$\{c \in \mathbb{F}_q^n : \bar{H}c^t = \mathbf{0}\}.$$

A matriz $\bar{H}$ faz o papel da matriz teste de paridade de $A_k(\alpha, v^{'})$, exceto que suas linhas não são necessariamente linearmente independentes, assim reprimimos chamando-a de uma matriz teste de paridade de $A_k(\alpha, v^{'})$.

Uma outra matriz teste de paridade para os códigos alternantes é obtida se multiplicarmos a matriz H definida no Corolário 1.29 por uma matriz quadrada D não singular, sobre $\mathbb{F}_{q^m}$. Assim,

$$\begin{aligned}
\tilde{H} = DH &= \begin{pmatrix} d_{11} & d_{12} & \cdots & d_{1r} \\ d_{21} & d_{22} & \cdots & d_{2r} \\ d_{31} & d_{32} & \cdots & d_{3r} \\ \vdots & \vdots & \vdots & \vdots \\ d_{r1} & d_{r2} & \cdots & d_{rr} \end{pmatrix} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_n^{r-1} \end{pmatrix} \begin{pmatrix} v_1^{'} & 0 & \cdots & 0 \\ 0 & v_2^{'} & \cdots & 0 \\ & & \cdots & \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & v_n^{'} \end{pmatrix} \\
&= \begin{pmatrix} v_1^{'}h_1(\alpha_1) & v_2^{'}h_1(\alpha_2) & \cdots & v_n^{'}h_1(\alpha_n) \\ v_1^{'}h_2(\alpha_1) & v_2^{'}h_2(\alpha_2) & \cdots & v_n^{'}h_2(\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \\ v_1^{'}h_r(\alpha_1) & v_2^{'}h_r(\alpha_2) & \cdots & v_n^{'}h_r(\alpha_n) \end{pmatrix},
\end{aligned}$$

onde $r = n - k$ e

$$h_i(x) = d_{i1} + d_{i2}x + d_{i3}x^2 + \cdots + d_{ir}x^{r-1}, \;\; i = 1, \ldots, r$$

é um polinômio de grau menor ou igual a $r-1$ com coeficientes em $\mathbb{F}_{q^m}$.

Se escolhermos qualquer submatriz de ordem r de $\tilde{H}$ e calcularmos o seu determinante, obtemos o produto do determinante de D pelo determinate de Vandermonde com elementos distintos e pelo determinante de uma submatriz diagonal. Determinantes desta forma são conhecidos como alternantes e, por esta razão, os códigos determinados por matrizes desta forma são conhecidos como códigos alternantes.

Vejamos agora alguns exemplos de códigos alternantes.

Exemplo 1.34. Para qualquer q e m, um código BCH sobre $\mathbb{F}_q$ é um código que consiste de todo $c \in \mathbb{F}_q^n$ que satisfaz $Hc^t = \mathbf{0}$, onde

$$
\begin{aligned}
H &= \begin{pmatrix}
1 & \alpha^{a} & \alpha^{2a} & \cdots & \alpha^{a(n-1)} \\
1 & \alpha^{a+1} & \alpha^{2(a+1)} & \cdots & \alpha^{(a+1)(n-1)} \\
1 & \alpha^{a+2} & \alpha^{2(a+2)} & \cdots & \alpha^{(a+2)(n-1)} \\
\vdots & \vdots & \vdots & \cdots & \vdots \\
1 & \alpha^{a+\delta-2} & \alpha^{2(a+\delta-2)} & \cdots & \alpha^{(a+\delta-2)(n-1)}
\end{pmatrix} \\
&= \begin{pmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \alpha & \alpha^{2} & \cdots & \alpha^{n-1} \\
1 & \alpha^{2} & \alpha^{4} & \cdots & \alpha^{(n-1)2} \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
1 & \alpha^{\delta-2} & \alpha^{2(\delta-2)} & \cdots & \alpha^{(n-1)(\delta-2)}
\end{pmatrix}
\begin{pmatrix}
1 & 0 & \cdots & 0 \\
0 & \alpha^{a} & \cdots & 0 \\
 & & \cdots & \\
\vdots & & \ddots & \vdots \\
0 & 0 & \cdots & \alpha^{a(n-1)}
\end{pmatrix},
\end{aligned}
$$

que está exatamente na forma do Corolário 1.29. Portanto, um código BCH é também um código alternante.

Exemplo 1.35. Seja $q = 2$ e $m = 3$ e tome $n = 6$. Seja θ um elemento primitivo de $\mathbb{F}_8$ que satisfaz $\theta^3 + \theta + 1 = 0$. Tome $v' = (1, \ldots, 1)$ e $\alpha = (\theta, \theta^2, \ldots, \theta^6)$. Então $A_3(\alpha, v') = \{c \in \mathbb{F}_2^6 : Hc^t = \mathbf{0}\}$, onde

$$
H = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
\theta & \theta^2 & \theta^3 & \theta^4 & \theta^5 & \theta^6 \\
\theta^2 & \theta^4 & \theta^6 & \theta^8 & \theta^{10} & \theta^{12}
\end{pmatrix}.
$$

Então

$$\bar{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

que tem a seguinte forma escalonada:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Assim, segue que $A_3(\alpha, v')$ tem matriz geradora

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

e que é um $[6, 2, 4]$-código.

1.8 Códigos de Goppa

Uma das subclasses mais importantes dos códigos alternantes é a família dos códigos de Goppa, introduzida por V.D. Goppa [7] nos anos de 1970, os quais possuem bons

parâmetros. Códigos de Goppa são usados também em criptografia - os sistemas criptográficos McEliece e Niederreiter são exemplos de sistemas criptográficos de chave pública que usam códigos de Goppa.

Definição 1.36. Seja $g(x)$ um polinômio em $\mathbb{F}_{q^m}[x]$ para algum m fixo e seja $L = \{\alpha_1, \ldots, \alpha_n\}$ um subconjunto de $\mathbb{F}_{q^m}$, onde os α_i são dois a dois distintos e tais que $g(\alpha_i) \neq 0$ para $i = 1, \ldots, n$. O *Código de Goppa* $\Gamma(L, g)$ é definido como

$$\Gamma(L, g) = \{(c_1, \ldots, c_n) \in \mathbb{F}_q^n : \sum_{i=1}^{n} c_i \frac{g(x) - g(\alpha_i)}{x - \alpha_i} g(\alpha_i)^{-1} = 0\}.$$

É claro que $\Gamma(L, g)$ é um subespaço vetorial de $\mathbb{F}_q^n$ e, portanto, é um código linear. O polinômio $g(x)$ é dito o *polinômio de Goppa*. Quando $g(x)$ é irredutível, $\Gamma(L, g)$ é dito um código de Goppa *irredutível*.

A próxima proposição mostra imediatamente que os Códigos de Goppa são exemplos de códigos alternantes.

Proposição 1.37. *Para um dado polinômio de Goppa $g(x)$ de grau t e $L = \{\alpha_1, \ldots, \alpha_n\}$, temos $\Gamma(L, g) = \{c \in \mathbb{F}_q^n : Hc^t = \boldsymbol{0}\}$, onde*

$$H = \begin{pmatrix} g(\alpha_1)^{-1} & \cdots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \cdots & \alpha_n g(\alpha_n)^{-1} \\ \vdots & \vdots & \vdots \\ \alpha_1^{t-1} g(\alpha_1)^{-1} & \cdots & \alpha_n^{t-1} g(\alpha_n)^{-1} \end{pmatrix}.$$

Demonstração: Ver Proposição 9.3.3 de [14]. □

Corolário 1.38. *Para um dado polinômio de Goppa $g(x)$ de grau t e $L = \{\alpha_1, \ldots, \alpha_n\}$, o código de Goppa $\Gamma(L, g)$ é um código alternante $A_{n-t}(\alpha, v')$, onde $\alpha = (\alpha_1, \ldots, \alpha_n)$ e $v' = (g(\alpha_1)^{-1}, \ldots, g(\alpha_n)^{-1})$.*

Pela Proposição 1.32 e pelo Corolário 1.38 damos imediatamente uma cota para a dimensão e para a distância mínima de um código de Goppa.

Corolário 1.39. *Para um dado polinômio de Goppa $g(x)$ de grau t e $L = \{\alpha_1, \ldots, \alpha_n\}$, o código de Goppa $\Gamma(L, g)$ é um código linear sobre $\mathbb{F}_q$ com parâmetros $[n, k, d]$, onde $k \geq n - mt$ e $d \geq t + 1$.*

Exemplo 1.40. Para qualquer t tome $g(x) = x^t$ e seja $L = \{1, \alpha^{-1}, \alpha^{-2}, \ldots, \alpha^{-(q^m-2)}\}$, onde α é um elemento primitivo de $\mathbb{F}_{q^m}$ (visto que $n = q^m - 1$). Então $\Gamma(L, g) = \{c \in \mathbb{F}_q^n : Hc^t = \mathbf{0}\}$, onde

$$H = \begin{pmatrix} 1 & \alpha^t & \alpha^{2t} & \cdots & \alpha^{(n-1)t} \\ 1 & \alpha^{t-1} & \alpha^{2(t-1)} & \cdots & \alpha^{(n-1)(t-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \end{pmatrix}.$$

Note que H é uma matriz teste de paridade para um código BCH, assim, $\Gamma(L, g)$ é precisamente o código BCH.

Exemplo 1.41. Seja $q = 2$ e tome $g(x) = \alpha^3 + x + x^2$, onde α é um elemento primitivo de $\mathbb{F}_8$ que satisfaz $\alpha^3 + \alpha + 1 = 0$. Seja $L = \mathbb{F}_8$, assim, $n = 8$ e $m = 3$. Então $\Gamma(L, g) = \{c \in \mathbb{F}_2^8 : Hc^t = \mathbf{0}\}$, onde

$$H = \begin{pmatrix} \alpha^4 & \alpha^4 & \alpha & 1 & \alpha & \alpha^2 & \alpha^2 & 1 \\ 0 & \alpha^4 & \alpha^2 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^6 \end{pmatrix}.$$

Substituindo cada entrada de H por um vetor coluna em $\mathbb{F}_2^3$, obtemos

$$\bar{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix},$$

que tem a seguinte forma escalonada

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Deste modo, $\Gamma(L, g)$ tem matriz geradora

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Portanto, $\Gamma(L, g)$ tem parâmetros $[8, 2, 5]$.

Capítulo 2

Cotas para a distância mínima de códigos definidos sobre uma variedade afim

2.1 Uma melhora da cota de Feng-Rao para a distância mínima

Esta seção tem por finalidade introduzir algumas definições básicas para a teoria de códigos sobre variedades afins. Até a segunda definição utilizaremos uma terminologia geral para códigos algébricos geométricos. A partir deste ponto adotaremos a terminologia de Feng-Rao no contexto de códigos sobre variedades afins. Os conceitos e resultados serão apresentados com a finalidade de obtermos a cota fraca de Feng-Rao (cota de Miura) para códigos duais de tais códigos. Para isso, seja $\mathbb{F}_q$ um corpo com q elementos e $\mathbb{F}_q^k$ o conjunto de todas as k-uplas de elementos em $\mathbb{F}_q$.

Definição 2.1. Seja I um ideal do anel de polinômios $\mathbb{F}_q[x_1, \ldots, x_k]$. Ponha

$$I_q := I + \langle x_1^q - x_1, \ldots, x_k^q - x_k \rangle.$$

A *variedade afim* de I_q, denotada por $V(I_q)$, é dada por

$$V(I_q) := \{(a_1, \ldots, a_k) \in \mathbb{F}_q^k : f(a_1, \ldots, a_k) = 0, \textit{ para todo } f \in I_q\}.$$

Para os exemplos que seguem, faremos $x_1 = x$, $x_2 = y$ e $x_3 = z$. Deste modo, consideraremos as variáveis x, y e z ordenadas lexicograficamente.

Exemplo 2.2. Considere o ideal $I = \langle x^2 + x + y^2 + y \rangle \subset \mathbb{F}_4[x, y]$. Então

$$I_4 = \langle x^2 + x + y^2 + y, x^4 - x, y^4 - y \rangle.$$

Dado $f(x, y) \in I_4$ temos que

$$f(x, y) = t_1(x, y)(x^2 + x + y^2 + y) + t_2(x, y)(x^4 - x) + t_3(x, y)(y^4 - y)$$

para algum $t_1, t_2, t_3 \in \mathbb{F}_4[x, y]$. Note que todo $(x, y) \in \mathbb{F}_4^2$ é raiz de $x^4 - x$ e $y^4 - y$, uma vez que $a^4 = a$ em $\mathbb{F}_4$, assim determinar as raízes de f se reduz a encontrar as raízes de $x^2 + x + y^2 + y$. Para isso, consideremos $\mathbb{F}_4 = \mathbb{F}_2(\theta)$, onde $\theta^2 = \theta + 1$ para algum θ, logo $\mathbb{F}_4 = \{0, 1, \theta, \theta^2\}$ e as raízes de $x^2 + x + y^2 + y$ são $(0, 0), (0, 1), (1, 0), (1, 1), (\theta, \theta), (\theta^2, \theta^2), (\theta, \theta^2)$ *e* (θ^2, θ). Deste modo, a variedade afim $V(I_4)$ é o conjunto formado por estes 8 pontos.

Seja R o *anel coordenado* da variedade afim $V(I_q)$; isto é,

$$R = \frac{\mathbb{F}_q[x_1, \ldots, x_k]}{I_q}.$$

Suponha que $P_1, \ldots, P_n$ seja uma ordenação dos pontos de $V(I_q)$. Definimos a aplicação

$$\begin{array}{rccc} \phi: & R & \to & \mathbb{F}_q^n \\ & \overline{f} & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

onde $\overline{f}$ representa a classe de equivalência $f + I_q$. Note que ϕ é bem definida e

injetora, uma vez que

$$\begin{aligned}
\overline{f} = \overline{g} &\Leftrightarrow f + I_q = g + I_q \\
&\Leftrightarrow f - g \in I_q \\
&\Leftrightarrow ((f-g)(P_1), \ldots, (f-g)(P_n)) = (0, \ldots, 0),\ P_1, \ldots, P_n \in V(I_q) \\
&\Leftrightarrow (f(P_1), \ldots, f(P_n)) = (g(P_1), \ldots, g(P_n)) \\
&\Leftrightarrow \phi(\overline{f}) = \phi(\overline{g}).
\end{aligned}$$

A aplicação ϕ também é sobrejetora. De fato, pois podemos escrever

$$f(x_1, \ldots, x_k) = \sum_{t=0}^{m} \sum_{l_1+\cdots+l_k=t} a_{l_1 \cdots l_k} x_1^{l_1} \cdots x_k^{l_k},$$

onde $m = gr(f)$ e $l_i \geq 0$ para $i = 1, \ldots, k$. Escolha m suficientemente grande de forma que o sistema linear ($a_{l_1 \cdots l_k}$ são as incógnitas)

$$\begin{cases}
f(P_1) &= \alpha_1 \\
\quad \vdots & \\
f(P_n) &= \alpha_n
\end{cases}$$

tenha solução. Assim, para todo $(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n$, existe $f \in \mathbb{F}_q[x_1, \ldots, x_k]$ tal que $f(P_1, \ldots, P_n) = (\alpha_1, \ldots, \alpha_n)$.

E, por último, ϕ é linear:

$$\begin{aligned}
\phi(\alpha\overline{f} + \overline{g}) &= ((\alpha f + g)(P_1), \ldots, (\alpha f + g)(P_n)) \\
&= (\alpha f(P_1), \ldots, \alpha f(P_n)) + (g(P_1), \ldots, g(P_n)) \\
&= \alpha(f(P_1), \ldots, f(P_n)) + (g(P_1), \ldots, g(P_n)) \\
&= \alpha\phi(\overline{f}) + \phi(\overline{g}).
\end{aligned}$$

Portanto, a aplicação ϕ é um isomorfismo de $\mathbb{F}_q$-espaços vetoriais. Na realidade, ϕ é um isomorfismo de anéis no caso em que consideramos a multiplicação em $\mathbb{F}_q^n$ feita coordenada a coordenada.

Seja L um $\mathbb{F}_q$-subespaço vetorial do anel coordenado R.

Definição 2.3. Os *códigos* $C(I,L)$ e $C^{\perp}(I,L)$ *sobre uma variedade afim* são definidos como:

$$C(I,L) = \phi(L) \quad e \quad C^{\perp}(I,L) = \phi(L)^{\perp},$$

onde $\phi(L)^{\perp}$ é o complemento ortogonal de $\phi(L)$ com respeito ao produto interno usual sobre $\mathbb{F}_q^n$. Tais códigos são ditos *códigos geométricos de Goppa melhorados.*

Em 1995, Feng e Rao determinaram uma cota inferior para a distância mínima de um código da forma $C^{\perp}(I,L)$ sobre uma variedade afim e mostraram como tais códigos são construídos [6] (tal construção será mostrada no Capítulo 3 Seção 2). Para introduzir essa cota de Feng-Rao começamos com as seguintes definições, adotando a terminologia de Feng e Rao no contexto de códigos sobre variedades afins.

Definição 2.4. Seja T^k o *conjunto dos monômios* de $\mathbb{F}_q[x_1,\ldots,x_k]$. Em outras palavras,

$$T^k := \{x_1^{\alpha_1}\cdots x_k^{\alpha_k} : \alpha_i \in \mathbb{N} \; para \; 1 \leq i \leq k\}.$$

Definiremos uma ordenação total sobre todos os elementos de T^k de acordo com a ordenação peso e lexicográfica do monômio analisado. Para isso, seja o peso de cada variável x_i um inteiro positivo $w(x_i)$. O peso do monômio $x_1^{\alpha_1}\cdots x_k^{\alpha_k}$ é definido como:

$$w(x_1^{\alpha_1}\cdots x_k^{\alpha_k}) = \sum_{i=1}^{k} \alpha_i w(x_i).$$

Obviamente, $w(1) = w(x^0) = 0$. Aqui, peso de um monômio é um número inteiro positivo, que, apesar da mesma notação, não é a mesma definição de peso de uma palavra código.

Exemplo 2.5. Para o polinômio $f(x,y) = xy^3 + x^3 + y$ consideremos $w(x) = 3$ e $w(y) = 2$, deste modo, $w(xy^3) = w(x) + 3w(y) = 9$ e $w(x^3) = 3w(x) = 9$.

Considere dois monômios $x_1^{\alpha_1}\cdots x_k^{\alpha_k}$ e $x_1^{\beta_1}\cdots x_k^{\beta_k}$ quaisquer. Definimos uma relação (denotada $<_t$) destes monômios como mostrado abaixo:

$$x_1^{\alpha_1}\cdots x_k^{\alpha_k} <_t x_1^{\beta_1}\cdots x_k^{\beta_k} \;\; se$$

1. $w(x_1^{\alpha_1} \cdots x_k^{\alpha_k}) < w(x_1^{\beta_1} \cdots x_k^{\beta_k})$ *ou*

2. $w(x_1^{\alpha_1} \cdots x_k^{\alpha_k}) = w(x_1^{\beta_1} \cdots x_k^{\beta_k})$ *e existe um* m *tal que* $\alpha_l = \beta_l$ *para* $1 \leq l < m$ *e* $\alpha_m < \beta_m$.

Facilmente verifica-se que esta relação é uma ordenação total, dita *ordenação peso e lexicográfica.*

Exemplo 2.6. Considere monômios em três variáveis, x, y e z. Seja $w(x) = 4$, $w(y) = 3$ e $w(z) = 2$. Uma comparação segundo a ordenação total de dois monômios x^2yz^3 e x^2y^3 pode ser definida como a seguir: temos que $w(x^2yz^3) = w(x^2y^3) = 17$, $\alpha_1 = \beta_1$ e $\alpha_2 < \beta_2$, então $x^2yz^3 <_t x^2y^3$.

Definição 2.7. O Δ-*conjunto* de um ideal $I \subseteq \mathbb{F}_q[x_1, \ldots, x_k]$, denotado por $\Delta(I)$, é definido por

$$\Delta(I) := T^k \setminus \{lm(f) : f \in I,\ f \neq 0\},$$

onde $lm(f)$ denota o *monômio líder* de f sob a ordenação $<_t$.

Dado um ideal I, consideraremos duas sequências provenientes de $\Delta(I_q)$.

Definição 2.8. Para $I \subseteq \mathbb{F}_q[x_1, \ldots, x_k]$, definimos a sequência H como

$$H := \{h_i\}_{i=1}^n,$$

que é uma sequência crescente (sobre $<_t$) dos elementos de $\Delta(I_q)$. A sequência peso é definida por

$$W := \{w(h_i)\}_{i=1}^n.$$

Pela definição acima temos que W é uma sequência não decrescente, visto H ser uma sequência crescente e dois ou mais elementos de H poderem ter o mesmo peso.

Proposição 2.9. *O conjunto* $\overline{H} = \{\overline{h}_1, \ldots, \overline{h}_n\}$ *é uma base para* R.

Demonstração: Precisamos mostrar que os elementos de $\overline{H}$ são linearmente independentes e que eles geram R. Primeiramente, seja $\alpha_1, \ldots, \alpha_n$ elementos de $\mathbb{F}_q$,

então se $\alpha_1\overline{h}_1+\cdots+\alpha_n\overline{h}_n=\overline{\mathbf{0}}$ em R e $\overline{h}_i=h_i+I_q$, temos que $\alpha_1h_1+\cdots+\alpha_nh_n\in I_q$. Supondo $\alpha_n\neq 0$ temos que h_n é o líder, absurdo, logo $\alpha_n=0$. Supondo $\alpha_{n-1}\neq 0$ temos que h_{n-1} é o líder, absurdo, logo $\alpha_{n-1}=0$. Repetindo esse processo sucessivamente, obtemos $\alpha_1=\cdots=\alpha_n=0$. Logo, tal conjunto é linearmente independente.

Consideremos $\mathcal{L}=\{lm(f):f\in I_q, f\neq 0\}$, assim podemos escrever $\Delta(I_q)=T^k\setminus\mathcal{L}$. Suponhamos que $\overline{H}$ não gera R. Deste modo, existe $\overline{f}\in R$, $\overline{f}=f+I_q$, com $f\in\mathbb{F}_q[x_1,\ldots,x_k]$, tal que $f\notin[H]+I_q$ ($[H]$ denota o subespaço gerado pelos elementos de H). De fato, pois se $f\in[H]+I_q$, então existe $m_1\in[H]$ e $m_2\in I_q$ tal que $f=m_1+m_2$, logo, $\overline{f}=m_1+m_2+I_q=m_1+I_q$, ou seja, $\overline{f}\in[\overline{H}]$, o que é uma contradição. Escolha f de forma que seu monômio líder seja o menor possível. Podemos ter $lm(f)\in H$ ou $lm(f)\in\mathcal{L}$. Se $lm(f)\in H$, tome $g=f-lm(f)$, $g\in\mathbb{F}_q[x_1,\ldots,x_k]$, logo $lm(g)<_t lm(f)$, assim, $g\notin[H]+I_q$, pois se assim fosse teríamos $g=t_1+t_2$, com $t_1\in[H]$ e $t_2\in I_q$, resultando que $f=g+lm(f)=(t_1+lm(f))+t_2\in[H]+I_q$, o que é uma contradição, portanto, $lm(f)\notin H$. Se $lm(f)\in\mathcal{L}$, então existe $t\in I_q$ tal que $lm(f)=lm(t)$. Tome $u=f-t$, logo, $lm(u)<_t lm(f)$. Deste modo, $u\notin[H]+I_q$, pois se assim fosse teríamos $u=p_1+p_2$ com $p_1\in[H]$ e $p_2\in I_q$, resultando que $f=u+t=p_1+(p_2+t)\in[H]+I_q$, o que é uma contradição, portanto, $lm(f)\notin\mathcal{L}$. Com isso concluímos que se $lm(f)\notin H$ e $lm(f)\notin\mathcal{L}$, então não podemos ter $R\neq[\overline{H}]$. Portanto, $\overline{H}$ gera R. □

Exemplo 2.10. Considerando a mesma situação do Exemplo 2.2 e o peso designado $w(x)=w(y)=1$ temos, analisando $f(x,y)=t_1(x,y)(x^2+x+y^2+y)+t_2(x,y)(x^4-x)+t_3(x,y)(y^4-y)$, que os únicos monômios que não são líderes de algum $f\in I_4$ são $1,x,y,y^2,y^3,xy,xy^2$ *e* xy^3, portanto, $\Delta(I_4)=\{x^ay^b:0\leq a\leq 1\ e\ 0\leq b\leq 3\}$ e $H=\{1,y,x,y^2,xy,y^3,xy^2,xy^3\}$. Calculando o peso de cada monômio de H obtemos a sequência $W=\{0,1,1,2,2,3,3,4\}$.

Definição 2.11. Denotemos por $L(\underline{r})$ o *subespaço linear* de dimensão r de R gerado pelo conjunto $\{\overline{h}_1,\ldots,\overline{h}_r\}$. Mais geralmente, denotemos por $L(\underline{r},v_1,\ldots,v_l)$ o subespaço de dimensão $r+l$ gerado por $\{\overline{h}_1,\ldots,\overline{h}_r,\overline{h}_{v_1},\ldots,\overline{h}_{v_l}\}$, onde $r+1<v_1<$

$\cdots < v_l$ para algum $l \geq 0$.

Note que se $l = 0$, então $L(\underline{r}, v_1, \ldots, v_l) = L(\underline{r})$.

Definição 2.12. Um monômio m é dito *consistente* com h_r se $w(m) = w(h_r)$ e $\overline{m} \in L(\underline{r}) \setminus L(\underline{r-1})$. Se m é consistente com h_r, então escrevemos $m \sim h_r$.

Exemplo 2.13. Tome $h_6 \in H$, onde H é dada no Exemplo 2.10. Determinemos todos os monômios consistentes com $h_6 = y^3$. Para isso precisamos encontrar todos os monômios $m \in T^2$ tais que $m \sim h_6$. Os possíveis candidatos são: x^3, y^3, x^2y e xy^2, visto possuírem o mesmo peso que h_6. Assim, basta determinar quais deles possuem sua classe de equivalência em $L(\underline{6}) \setminus L(\underline{5})$.

- x^3: para $\alpha_i \in \mathbb{F}_4$, com $i = 1, ..., 6$,

$$\begin{aligned} \overline{x^3} &= \alpha_1\overline{1} + \alpha_2\overline{y} + \alpha_3\overline{x} + \alpha_4\overline{y^2} + \alpha_5\overline{xy} + \alpha_6\overline{y^3} \\ &\Leftrightarrow \; x^3 + \alpha_1 1 + \alpha_2 y + \alpha_3 x + \alpha_4 y^2 + \alpha_5 xy + \alpha_6 y^3 \in I_4, \end{aligned}$$

  mas é impossível escrever esse polinômio na forma de um elemento de I_4, deste modo $\overline{x^3} \notin L(\underline{6}) \setminus L(\underline{5})$;

- y^3: é o próprio h_6, consequentemente, consistente com ele mesmo;

- x^2y: para $\alpha_i \in \mathbb{F}_4$, com $i = 1, ..., 6$,

$$\begin{aligned} \overline{x^2y} &= \alpha_1\overline{1} + \alpha_2\overline{y} + \alpha_3\overline{x} + \alpha_4\overline{y^2} + \alpha_5\overline{xy} + \alpha_6\overline{y^3} \\ &\Leftrightarrow \; x^2y + \alpha_1 1 + \alpha_2 y + \alpha_3 x + \alpha_4 y^2 + \alpha_5 xy + \alpha_6 y^3 \\ &= \; (x^2 + \alpha_5 x + \alpha_6 y^2 + \alpha_4 y)y + \alpha_1 + \alpha_2 y + \alpha_3 x \in I_4, \end{aligned}$$

  tomando $\alpha_1 = \alpha_2 = \alpha_3 = 0$ e $\alpha_4 = \alpha_5 = \alpha_6 = 1$ temos

$$(x^2 + x + y^2 + y)y \in I_4$$

  e como $\alpha_6 \neq 0$, $\overline{x^2y} \in L(\underline{6}) \setminus L(\underline{5})$;

- xy^2: é o h_7, assim $\overline{xy^2} \in L(\underline{7})$.

Portanto, os monômios consistentes com $h_6 = y^3$ são o próprio h_6 e o monômio x^2y.

Lema 2.14. *Se $m <_t h_r$, então $\overline{m} \in L(\underline{r-1})$.*

Demonstração: Suponha $m <_t h_r$ e $\overline{m} \in L(\underline{s}) \setminus L(\underline{s-1})$ para algum $s \geq r$. Então $m + I_q = \sum_{i=1}^{s}(k_i h_i) + I_q$ para algum $k_i \in \mathbb{F}_q$, com $1 \leq i \leq s$ e $k_s \neq 0$. Deste modo, $f = \sum_{i=1}^{s}(k_i h_i) - m \in I_q$ e $lm(f) = h_s$, com $k_s \neq 0$ e $m <_t h_r \leq_t h_s$. Assim, $h_s \notin \Delta(I_q)$ o que é uma contradição. □

Como uma consequência, obtemos o seguinte resultado.

Corolário 2.15. *Se $m \sim h_r$, então $h_r \leq_t m$.*

Demonstração: Suponhamos $m <_t h_r$, então, pelo Lema 2.14, $\overline{m} \in L(\underline{r-1})$, assim, m não é consistente com h_r, o que é uma contradição. □

Definição 2.16. Para $h_r = x_1^{\alpha_1} \cdots x_k^{\alpha_k} \in H$, denotemos por $\mathcal{D}_r$ o *conjunto dos divisores* de h_r e escrevamos

$$D_r := |\mathcal{D}_r| = \prod_{i=1}^{k}(\alpha_i + 1).$$

Para h_i e h_j em H, denotaremos o produto $h_i h_j$ simplesmente como $h_{i,j}$.

Resultados equivalentes aos do Apêndice A podem ser obtidos no anel coordenado R mediante o isomorfismo

$$\begin{array}{rccc} \phi: & R & \rightarrow & \mathbb{F}_q^n \\ & \overline{f} & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

considerando que:

1. $\phi(\overline{h}_i) = w_i,\ 1 \leq i \leq n$;

2. $\phi(\overline{h}_{i,j}) = (h_{i,j}(P_1), \ldots, h_{i,j}(P_n)) = (h_i h_j(P_1), \ldots, h_i h_j(P_n))$
$= (h_i(P_1), \ldots, h_i(P_n))(h_j(P_1), \ldots, h_j(P_n)) = \phi(\overline{h_i})\phi(\overline{h_j}) = w_i w_j$;

3. $\phi(L(\underline{r})) = \mathcal{W}(\underline{r})$ (A definição de $\mathcal{W}(\underline{r})$ encontra-se no Apêndice A).

Definição 2.17. Suponha $h_{i,j}$ um monômio tal que $h_{i,j} \sim h_r$. O monômio $h_{i,j}$ é *bem comportado* se para cada (u, v), onde $1 \leq u \leq i$ e $1 \leq v \leq j$, com $(u, v) \neq (i, j)$, temos que $\overline{h}_{u,v} \in L(\underline{r-1})$.

Definição 2.18. Suponha $h_{i,j}$ um monômio tal que $h_{i,j} \sim h_r$. O monômio $h_{i,j}$ é *fracamente bem comportado* se para cada (u, v), onde $u < i$ e $v = j$ ou $u = i$ e $v < j$, temos que $\overline{h}_{u,v} \in L(\underline{r-1})$.

Consequentemente, $h_{i,j}$ é bem comportado em R se, e somente se, (w_i, w_j) é bem comportado em relação a ω (analogamente para fracamente bem comportado).

Definição 2.19. Para cada monômio $h_r \in H$ defina

$$\mathcal{N}_r := \{(i, j) : h_{i,j} \sim h_r \text{ e } h_{i,j} \text{ é bem comportado}\}.$$

Analogamente, defina

$$\widetilde{\mathcal{N}}_r := \{(i, j) : h_{i,j} \sim h_r \text{ e } h_{i,j} \text{ é } fracamente \text{ bem comportado}\}.$$

Ponha $N_r := |\mathcal{N}_r|$ e $\widetilde{N}_r := |\widetilde{\mathcal{N}}_r|$.

O inteiro N_r é devido a Feng e Rao e o inteiro $\widetilde{N}_r$ é devido a Miura. Além disso, por construção, vemos que $N_r \leq \widetilde{N}_r$.

Exemplo 2.20. Consideremos ainda o monômio $h_6 = y^3 \in H$, onde H é a sequência dada no Exemplo 2.10. Determinemos os monômios bem comportados e fracamente bem comportados com h_6. Pelo Exemplo 2.13 temos que $x^2y \sim h_6$. Note que $h_{3,5} = x^2y$, mas $h_{3,5}$ não é fracamente bem comportado, pois $h_{2,5} = xy^2 = h_7$ e $\overline{h}_7 \in L(\underline{7})$, consequentemente, $h_{3,5}$ não é bem comportado. Agora, $h_{1,6} = h_6$ é fracamente bem comportado, uma vez que $\overline{h}_{1,v} \in L(\underline{5})$ para $1 \leq v \leq 5$ e $L(\underline{1}) \subset L(\underline{2}) \subset L(\underline{3}) \subset L(\underline{4}) \subset L(\underline{5})$, consequentemente, $h_{1,6}$ é também bem comportado. Resta analisar $h_{2,4} = h_6$. Temos que $h_{2,3} = h_5$, $h_{1,4} = h_{2,2} = h_4$, $h_{1,3} = h_3$ e $h_{1,2} = h_{2,1} = h_2$. Logo, $\overline{h}_{2,3} \in L(\underline{5})$, $\overline{h}_{1,4}, \overline{h}_{2,2} \in L(\underline{4}) \subset L(\underline{5})$, $\overline{h}_{1,3} \in L(\underline{3}) \subset L(\underline{5})$

e $\overline{h}_{1,2}, \overline{h}_{2,1} \in L(\underline{2}) \subset L(\underline{5})$. Deste modo, $h_{2,4}$ é bem comportado e fracamente bem comportado. Portanto,

$$\mathcal{N}_6 = \widetilde{\mathcal{N}}_6 = \{(1,6),(2,4),(4,2),(6,1)\}.$$

Lema 2.21. *Seja h_i, h_j e $h_r \in H$. Se $h_{i,j} = h_r$, então $h_{i,j}$ é bem comportado e consistente com h_r.*

Demonstração: Suponha h_i, h_j e $h_r \in H$ tais que $h_{i,j} = h_r$, então $w(h_{i,j}) = w(h_r)$ e $\overline{h}_{i,j} \in L(\underline{r}) \setminus L(\underline{r-1})$, resultando que $h_{i,j} \sim h_r$. Consideremos (u,v) tal que $1 \leq u \leq i$ e $1 \leq v \leq j$, com $(u,v) \neq (i,j)$. Então $h_{u,v} <_t h_{i,j} = h_r$. Assim, pelo Lema 2.14, $\overline{h}_{u,v} \in L(\underline{r-1})$, ou seja, $h_{i,j}$ é bem comportado. □

Corolário 2.22. *Para $h_r \in H$, temos $D_r \leq N_r$. Isto é, N_r é pelo menos o número de monômios divisores de h_r.*

Exemplo 2.23. Considere o ideal $I = \langle g \rangle \subset \mathbb{F}_q[x,y]$, onde $g = x^a + cy^b + f(x,y)$, e o peso designado $w(x) = b$ e $w(y) = a$. Suponha que $mdc(a,b) = 1$, $c \neq 0$ e $w(lm(f)) < ab$. Note que $lm(g) = x^a$ e, consequentemente, temos

$$\Delta(I_q) \subseteq \{x^{\alpha_1}y^{\alpha_2} : 0 \leq \alpha_1 < a \text{ e } 0 \leq \alpha_2 < q\}.$$

Quaisquer dois monômios distintos neste conjunto possuem pesos diferentes. De fato, consideremos $m_1 = x^{\alpha_1}y^{\alpha_2}$ e $m_2 = x^{\beta_1}y^{\beta_2}$ monômios distintos em tal conjunto, assim,

$$w(m_1) = \alpha_1 w(x) + \alpha_2 w(y) = b\alpha_1 + a\alpha_2 \quad e$$

$$w(m_2) = \beta_1 w(x) + \beta_2 w(y) = b\beta_1 + a\beta_2.$$

Logo, $w(m_1) \neq w(m_2)$, pois $mdc(a,b) = 1$, $0 \leq \alpha_1, \beta_1 < a$, $0 \leq \alpha_2, \beta_2 < q$ e $\alpha_1 \neq \beta_1$ ou $\alpha_2 \neq \beta_2$. Como um resultado, W é uma sequência estritamente crescente.

Suponha $h_i, h_j, h_r \in H$ com $w(h_i) + w(h_j) = w(h_r)$. Se $h_{i,j} = h_r$, então, pelo Lema 2.21, sabemos que $(i,j) \in \mathcal{N}_r$. Se $h_{i,j} = x^{e_1}y^{e_2} \neq h_r$, então, pela estrutura de

$\Delta(I_q)$, observe que $h_r = x^{e_1-a}y^{e_2+b}$ e que multiplicando g por $x^{e_1-a}y^{e_2}$, obtemos:

$$\begin{aligned} x^{e_1-a}y^{e_2}g &= x^{e_1-a}y^{e_2}x^a + x^{e_1-a}y^{e_2}cy^b + x^{e_1-a}y^{e_2}f(x,y) \\ &= x^{e_1}y^{e_2} + x^{e_1-a}y^{e_2+b}c + x^{e_1-a}y^{e_2}f(x,y) \\ &= h_{i,j} + ch_r + x^{e_1-a}y^{e_2}f(x,y) \in I. \end{aligned}$$

Logo,

$$h_{i,j} = x^{e_1-a}y^{e_2}g - ch_r - x^{e_1-a}y^{e_2}f(x,y).$$

Como $c \neq 0$ temos que $-c\overline{h}_r \in L(\underline{r})$. Logo, $\overline{h}_{i,j} \in L(\underline{r}) \setminus L(\underline{r-1})$ e $h_{i,j} \sim h_r$.

Como W é uma sequência estritamente crescente, $h_{i,j} \sim h_r$ implica que $h_{i,j}$ é bem comportado. Com isso e pela Definição 2.12, temos que:

$$\mathcal{N}_r = \{(i,j) : h_{i,j} \sim h_r\} = \{(i,j) : w(h_i) + w(h_j) = w(h_r)\},$$

consequentemente,

$$N_r = |\{(a,b) : a,b \in W \ \ e \ \ a+b = w(h_r)\}|.$$

Dadas estas definições e resultados, podemos agora definir a cota de Feng-Rao e a cota fraca de Feng-Rao para a distância mínima.

Definição 2.24. Considere o código $C^{\perp}(I,L)$, onde $L = L(\underline{r}, v_1, \ldots, v_l)$. Defina

$$\delta_{FR} := min\{N_v : v \notin \{1, \ldots, r, v_1, \ldots, v_l\}\}$$

e

$$\delta_{WFR} := min\{\widetilde{N}_v : v \notin \{1, \ldots, r, v_1, \ldots, v_l\}\}.$$

O inteiro δ_{FR} é a *cota de Feng-Rao* para a distância mínima do código $C^{\perp}(I,L)$, onde $L = L(\underline{r}, v_1, \ldots, v_l)$. Isso está demonstrado em [6], que é o artigo em que Feng e Rao definem código sobre uma variedade afim e também determinam uma cota para a distância mínima de tais códigos, que é justamente a cota mencionada acima, δ_{FR}. O número δ_{WFR} será referido como a *cota fraca de Feng-Rao* ou *cota de Miura*.

Note que, como $\mathcal{N}_r \subseteq \widetilde{\mathcal{N}}_r$, temos que $\delta_{FR} \leq \delta_{WFR}$. No Capítulo 3, Seções 2 e 3 discutiremos duas famílias de códigos nas quais podem ser vistas tal desigualdade.

Proposição 2.25. *A distância mínima do código $C^{\perp}(I, L)$, onde $L = L(\underline{r}, v_1, \ldots, v_l)$, é, pelo menos, δ_{WFR}.*

Demonstração: Análoga à demonstração da Proposição .9 do Apêndice A, considerando o isomorfismo entre R e $\mathbb{F}_q^n$ já mencionado anteriormente e que $\phi(L(\underline{r}, v_1, \ldots, v_l)) = C(I, L) = C(\mathcal{W})$, onde $\mathcal{W} = \{\phi(\overline{h}_1), \ldots, \phi(\overline{h}_r), \phi(\overline{h}_{v_1}), \ldots, \phi(\overline{h}_{v_l})\}$. □

2.2 Uma melhora da cota de Miura para a distância mínima

Nesta seção novas definições e conceitos serão introduzidos, os quais conduzirão ao ápice deste trabalho, que é descrever uma cota para a distância mínima melhor que a cota fraca de Feng-Rao (cota de Miura).

Definição 2.26. Denotamos por $S_r := \{m_1, \ldots, m_{l_r}\}$ o conjunto completamente ordenado de monômios consistentes com h_r tais que $m_1 <_t m_2 <_t \cdots <_t m_{l_r}$. Chamamos S_r de *conjunto de consistência* de h_r.

Pelo Corolário 2.15 e Lema 2.21 devemos ter $m_1 = h_r$. Em geral, a maioria dos códigos sobre variedades afins foram, no passado, considerados não tendo mais que dois elementos em S_r, para todo r tal que $1 \leq r \leq n$.

Exemplo 2.27. Pelo Exemplo 2.13 temos que os monômios consistentes com $h_6 = y^3$ são o próprio h_6 e o monômio x^2y. Note que $y^3 <_t x^2y$, portanto, $S_6 = \{y^3, x^2y\}$.

Definição 2.28. Ponha $\mathcal{B}_r := \{(i, j) : h_{i,j} = m_p \in S_r$ *e não existe um* $h_u \in H$ *tal que* $h_{i,u}$ *ou* $h_{u,j}$ *seja igual a* $m_v \in S_r$ *para algum* $v < p\}$. Denote por B_r a cardinalidade de $\mathcal{B}_r$.

Observação 2.29. Visto que $v < p$ se, e somente se, $m_v <_t m_p$, uma descrição alternativa de $\mathcal{B}_r$ é a seguinte: $\mathcal{B}_r = \{(i, j) : h_{i,j} \in S_r$ *e para todo* (u, v) *tal que* $u = i$ *e* $v < j$ *ou* $u < i$ *e* $v = j$, *temos que* $h_{u,v} \notin S_r\}$.

Exemplo 2.30. Considerando o conjunto $S_6 = \{y^3, x^2y\}$ dado no Exemplo 2.27, obtemos $\mathcal{B}_6 = \{(1,6),(2,4),(3,5),(4,2),(5,3),(6,1)\}$.

Definição 2.31. Denotamos por $S_r^* := \{m_1, \ldots, m_s\}$ o conjunto completamente ordenado de todos os monômios $m_p \in S_r$ tais que $m_p <_t h_{r+1}$, ou seja, $h_r = m_1 <_t \cdots <_t m_s <_t h_{r+1}$. Como $S_r^* \subseteq S_r$, também chamamos S_r de *conjunto de consistência* de h_r.

Note que se $r = n$, então temos, por convenção, que $S_r^* = S_r$.

Definição 2.32. Defina $\mathcal{B}_r^* := \{(i,j) : h_{i,j} = m_p \in S_r^*$ *e não existe um* $h_u \in H$ *tal que* $h_{i,u}$ *ou* $h_{u,j}$ *seja igual a* $m_v \in S_r^*$ *para algum* $v < p\}$. Denote por B_r^* a cardinalidade de $\mathcal{B}_r^*$.

Observação 2.33. Como $h_r \in S_r^*$, temos que $\{(i,j) : h_{i,j} = h_r\} \subseteq \mathcal{B}_r^* \subseteq \mathcal{B}_r$ e portanto, $D_r \leq B_r^* \leq B_r$.

Uma outra maneira de ver $\mathcal{B}_r^*$ é dada na seguinte proposição.

Proposição 2.34. *Seja* $h_r \in H$ *e* S_r^* *seu correspondente conjunto de consistência. Então* $\mathcal{B}_r^* = \{(i,j) : h_{i,j} \in S_r^*$ *e* $h_{i,j}$ *é fracamente bem comportado*$\}$.

Demonstração: Ponha $\mathcal{B}'_r := \{(i,j) : h_{i,j} \in S_r^*$ *e* $h_{i,j}$ *é fracamente bem comportado*$\}$. Mostraremos por contradição que $\mathcal{B}'_r \subseteq \mathcal{B}_r^*$. Suponha $(i,j) \in \mathcal{B}'_r$. Sem perda de generalidade, assuma que existe um h_u tal que $h_{i,u} \in S_r^*$, com $h_{i,u} <_t h_{i,j}$. Portanto, $u < j$ e $h_{i,u} \sim h_r$ implica que $\overline{h}_{i,u} \in L(\underline{r}) \setminus L(\underline{r-1})$. Assim, $h_{i,j}$ não é fracamente bem comportado, o que é uma contradição. Deste modo, $\mathcal{B}'_r \subseteq \mathcal{B}_r^*$.

Suponha $(i,j) \in \mathcal{B}_r^*$. Seja (u,v) tal que $u = i$ e $v < j$ ou $u < i$ e $v = j$. Visto que $h_{u,v} <_t h_{i,j} <_t h_{r+1}$ e $w(h_{i,j}) = w(h_r)$, temos que $w(h_{u,v}) \leq w(h_r)$. Se $w(h_{u,v}) < w(h_r)$, então $h_{u,v} <_t h_r$ e, pelo Lema 2.14, temos $\overline{h}_{u,v} \in L(\underline{r-1})$. Se $w(h_{u,v}) = w(h_r)$, então $\overline{h}_{u,v} \in L(\underline{r-1})$ uma vez que $h_{u,v} <_t h_{r+1}$ e $h_{u,v} \notin S_r^*$. Assim, $h_{i,j}$ é fracamente bem comportado. Portanto, $\mathcal{B}_r^* \subseteq \mathcal{B}'_r$. □

Teorema 2.35. *Para cada* $h_r \in H$ *temos* $\mathcal{B}_r^* \subseteq \widetilde{\mathcal{N}}_r \subseteq \mathcal{B}_r$.

Demonstração: Pela descrição de $\mathcal{B}_r^*$ na Proposição 2.34 vemos que $\mathcal{B}_r^* \subseteq \widetilde{\mathcal{N}}_r$. A seguir mostraremos por contradição que $\widetilde{\mathcal{N}}_r \subseteq \mathcal{B}_r$. Suponha $(i,j) \in \widetilde{\mathcal{N}}_r$. Sem perda de generalidade, assuma que existe um h_u tal que $h_{i,u} \in S_r$ com $h_{i,u} <_t h_{i,j}$. Portanto, $u < j$ e $h_{i,u} \sim h_r$ implica que $\overline{h}_{i,u} \in L(\underline{r}) \setminus L(\underline{r-1})$. Assim, $h_{i,j}$ não é fracamente bem comportado, o que é uma contradição. □

Note que, em virtude do Teorema 2.35 acima temos que $\widetilde{\mathcal{N}}_r \subseteq \mathcal{B}_r$, entretanto, $\mathcal{B}_r \nsubseteq \widetilde{\mathcal{N}}_r$. De fato, seja $(i,j) \in \mathcal{B}_r$, então $h_{i,j} \in S_r$ e para todo (u,v) tal que $u < i$ e $v = j$ ou $u = i$ e $v < j$ temos que $h_{u,v} \notin S_r$. Agora, $h_{u,v} \notin S_r$ implica que $h_{u,v} \nsim h_r$ que por sua vez implica em:

1. $w(h_{u,v}) \neq w(h_r)$ e $\overline{h}_{u,v} \in L(\underline{r}) \setminus L(\underline{r-1})$, logo $\overline{h}_{u,v} \notin L(\underline{r-1})$ e $\overline{h}_{i,j}$ não é fracamente bem comportado;

2. $w(h_{u,v}) = w(h_r)$ e $\overline{h}_{u,v} \notin L(\underline{r}) \setminus L(\underline{r-1})$, logo $\overline{h}_{u,v} \in L(\underline{s})$ com $s \geq r+1$ ou $s \leq r-1$. Quando $s = r+1$ temos que $h_{i,j}$ é fracamente bem comportado, nos outros casos, $h_{i,j}$ não é fracamente bem comportado;

3. $w(h_{u,v}) \neq w(h_r)$ e $\overline{h}_{u,v} \notin L(\underline{r}) \setminus L(\underline{r-1})$, é a mesma análise do item 2.

Corolário 2.36. *Seja $h_r \in H$ e $S_r = \{m_1, \ldots, m_{l_r}\}$ seu correspondente conjunto de consistência. Se $m_{l_r} <_t h_{r+1}$, então $\mathcal{B}_r^* = \widetilde{\mathcal{N}}_r = \mathcal{B}_r$.*

Demonstração: Suponha que $m_{l_r} <_t h_{r+1}$. Então $S_r^* = S_r$ implica que $\mathcal{B}_r^* = \mathcal{B}_r$. Com isso e pela inclusão estabelecida no Teorema 2.35 obtemos $\mathcal{B}_r^* = \widetilde{\mathcal{N}}_r = \mathcal{B}_r$. □

Corolário 2.37. *Se W é uma sequência estritamente crescente, então para todo $r \leq n$ temos $\mathcal{B}_r^* = \mathcal{B}_r = \mathcal{N}_r = \widetilde{\mathcal{N}}_r = \{(i,j) : h_{i,j} \sim h_r\}$.*

Demonstração: Seja $h_r \in H$ e $S_r = \{m_1, \ldots, m_{l_r}\}$ seu correspondente conjunto de consistência. Se W é estritamente crescente, então temos que $w(m_{l_r}) = w(h_r) < w(h_{r+1})$. Além disso, $m_{l_r} <_t h_{r+1}$ e, pelo Corolário 2.36, temos $\mathcal{B}_r^* = \widetilde{\mathcal{N}}_r = \mathcal{B}_r$.

Suponha $h_{i,j} \sim h_r$. Seja (u,v) tal que $u \leq i$ e $v \leq j$, com $(u,v) \neq (i,j)$. Como W é crescente, temos $w(h_{u,v}) < w(h_{i,j}) = w(h_r)$. Então $h_{u,v} <_t h_r$ e, pelo Lema

2.14, $\overline{h}_{u,v} \in L(\underline{r-1})$. Deste modo, $h_{i,j}$ é bem comportado. Agora, seja (u,v) tal que $u < i$ e $v = j$ ou $u = i$ e $v < j$, com $(u,v) \neq (i,j)$. Como W é crescente, $w(h_{u,v}) < w(h_{i,j}) = w(h_r)$. Assim, $h_{u,v} <_t h_r$ e, pelo Lema 2.14, $\overline{h}_{u,v} \in L(\underline{r-1})$, logo $h_{i,j}$ é fracamente bem comportado. Portanto, pela Definição 2.19, temos que $\mathcal{N}_r = \widetilde{\mathcal{N}}_r = \{(i,j) : h_{i,j} \sim h_r\}$. □

Corolário 2.38. *Se $|S_r| = 1$, então $\mathcal{B}_r^* = \mathcal{B}_r = \mathcal{N}_r = \widetilde{\mathcal{N}}_r$ com cardinalidade D_r.*

Demonstração: Suponha $|S_r| = 1$. Então h_r é o único elemento de S_r e $h_r <_t h_{r+1}$. Assim, pelo Corolário 2.36, $\mathcal{B}_r^* = \widetilde{\mathcal{N}}_r = \mathcal{B}_r$. Analisando os divisores de h_r vemos que $\{(i,j) : h_{i,j} = h_r\} = \mathcal{B}_r$. Pela Observação 2.33, $B_r^* = B_r = \widetilde{N}_r = D_r$. Pelo Lema 2.21, temos $\{(i,j) : h_{i,j} = h_r\} \subseteq \mathcal{N}_r$, que, pelo que acabamos de provar, resulta em $\widetilde{\mathcal{N}}_r \subseteq \mathcal{N}_r$. Por outro lado, $\mathcal{N}_r \subseteq \widetilde{\mathcal{N}}_r$. Deste modo, temos a igualdade. □

Observação 2.39. Se $|S_r| = 2$ (isto é, $S_r = \{h_r, m_2\}$), então, pela Definição 2.28, sabemos que $\mathcal{B}_r$ pode ser expresso como a união disjunta de dois conjuntos, a saber,

$$\mathcal{B}_r = \{(i,j) : h_{i,j} = h_r\} \cup \{(i,j) : h_{i,j} = m_2, \text{ com } h_i, h_j \notin \mathcal{D}_r\}.$$

Definição 2.40. Definimos a *matriz de produtos $n \times n$ simétrica* como sendo a matriz

$$M := [h_{i,j}], \quad \text{para } 1 \leq i,j \leq n.$$

Definição 2.41. Para todo $a \in W$, defina $W_a := \{i : w(h_i) = a\}$.

Definição 2.42. Para $a, b \in W$, defina $M_{(a,b)}$ como sendo a submatriz de M formada por todas as entradas $h_{i,j}$ tais que $i \in W_a$ e $j \in W_b$. Referiremos a $M_{(a,b)}$ como uma *submatriz de elementos de mesmo peso.*

Lema 2.43. *Se existe pelo menos um $h_{i,j} \in M_{(a,b)}$ tal que $h_{i,j} \sim h_r$ então existe pelo menos um $h_{u,v} \in M_{(a,b)}$ tal que $(u,v) \in \mathcal{B}_r$.*

Demonstração: Para $S_r = \{m_1, \ldots, m_{l_r}\}$ ponha $p' = min\{p : m_p \in M_{(a,b)}\}$. Então $h_{u,v} = m_{p'} \in M_{(a,b)}$ implica que $(u,v) \in \mathcal{B}_r$. □

Definição 2.44. Dizemos que a submatriz $M_{(a,b)}$ é *extrema* para h_r se existir pelo menos um $h_{i,j} \in M_{(a,b)}$ com $h_{i,j} \sim h_r$ e, para todos os $h_{i,j}$, temos que $h_{i,j}$ não é fracamente bem comportado.

Definição 2.45. Defina $\mathcal{P}_r := \{(a,b) : a,b \in W \text{ e } a+b = w(h_r)\}$. Denote por $\mathcal{C}_r$ o seguinte conjunto de submatrizes de M:

$$\mathcal{C}_r := \{M_{(a,b)} : (a,b) \in \mathcal{P}_r\}.$$

Note que não há duas submatrizes em $\mathcal{C}_r$ que compartilham uma linha ou coluna comum com M. Também, para cada $M_{(a,b)} \in \mathcal{C}_r$ temos $M_{(b,a)} = M^t_{(a,b)} \in \mathcal{C}_r$, visto que M é simétrica.

Definição 2.46. Defina $\mathcal{E}_r := \{(a,b) \in \mathcal{P}_r : M_{(a,b)} \textit{ é extrema para } h_r\}$ e $E_r = |\mathcal{E}_r|$.

Definição 2.47. Defina $A_r := \widetilde{N}_r + E_r$. Dizemos que A_r é o *número indicativo* para h_r.

Pelo Lema 2.43 e pela Definição 2.44 temos que toda matriz extrema para h_r contém um elemento $h_{u,v}$ tal que $(u,v) \in \mathcal{B}_r$, mas não há um elemento $h_{i,j}$ tal que $(i,j) \in \widetilde{\mathcal{N}}_r$. Portanto, $\widetilde{N}_r \leq A_r \leq B_r$.

Observação 2.48. Suponha $h_{i,j} \in M_{(a,b)}$ com $h_{i,j} \sim h_r$. Então, pela Definição 2.44, $M_{(a,b)}$ contém um termo fracamente bem comportado consistente com h_r ou é extrema para h_r. Assim,

$$A_r \geq |\{M_{(a,b)} : \textit{existe um } h_{i,j} \in M_{(a,b)} \textit{ com } h_{i,j} \sim h_r\}|.$$

Como consequência do Lema 2.43, sabemos que se cada $h_{u,v}$, tal que $(u,v) \in \mathcal{B}_r$, ocupa uma posição em uma submatriz de elementos de mesmo peso, então $B_r \leq A_r$, logo, $B_r = A_r$.

Definição 2.49. Para um código sobre variedade afim $C^{\perp}(I,L)$, onde $L = L(\underline{r}, v_1, \ldots, v_l)$, definimos dois números:

$$\delta_A := min\{A_v : v \notin \{1, \ldots, r, v_1, \ldots, v_l\}\}$$

e

$$\delta_{A^+} := min\{B_v : v \notin \{1, \ldots, r, v_1, \ldots, v_l\}\}.$$

Dizemos que δ_A é a *cota indicativa* e δ_{A^+} é a *estimativa indicativa forte*.

Note que, como $\widetilde{N}_r \leq A_r \leq B_r$, temos que $\delta_{WFR} \leq \delta_A \leq \delta_{A^+}$. O número δ_{A^+} parece ser um bom preditor da verdadeira distância mínima de $C^{\perp}(I, L)$. Entretanto, no geral, δ_{A^+} pode ser uma estimativa superior da cota dada na Proposição 2.25.

Exemplo 2.50. Analisemos a distância mínima do código $C^{\perp}(I, L(\underline{5}))$, onde I é o ideal dado no Exemplo 2.2 e $L(\underline{5})$ é o subespaço gerado por $\{h_1, \ldots, h_5\}$ com $h_i \in H$, H dada no Exemplo 2.10. Para isso, determinemos δ_{A^+}, que é sua estimativa superior. Antes, note que $dimC^{\perp}(I, L(\underline{5})) = 3$, pois $dimC(I, L(\underline{5})) = 5$ e a base de $L(\underline{5})$ está contida na base de R que tem 8 elementos, conforme determinação de H no Exemplo 2.10. Agora, elementos de $C^{\perp}(I, L(\underline{5}))$ são imagens de elementos de $L(\underline{5})$ mediante o isomorfismo ϕ, o qual pega um elemento de $L(\underline{5})$ e aplica nos 8 pontos de $V(I_4)$, dados no Exemplo 2.2, assim, o comprimento de $C(I, L(\underline{5}))$ é igual 8, consequentemente, o comprimento de $C^{\perp}(I, L(\underline{5}))$ também é igual a 8.

Determinemos δ_{A^+}. Para isso, precisamos determinar todos os B_v tais que $h_v \in H$ mas $h_v \notin \{h_1, \ldots, h_5\}$. O Exemplo 2.30 nos fornece $B_6 = 6$. Com $h_7 = xy^2$ e $h_8 = xy^3$ temos que $\mathcal{D}_7 = \{1, x, y, y^2xy, xy^2\}$ e $\mathcal{D}_8 = \{1, x, y, y^2, y^3, xy, xy^2, xy^3\}$. Logo, pela Observação 2.33, temos que $B_7 \geq D_7 = 6$ e $B_8 \geq D_8 = 8$. Portanto, $\delta_{A^+} = min\{B_6, B_7, B_8\} = 6$. Mas, pela Cota de Griesmer (cf [14] e [9]) não existe um código quaternário com parâmetros $[8, 3, 6]$. Assim, δ_{A^+} é uma estimativa superior da verdadeira distância mínima.

Provaremos que δ_A é uma cota inferior para a distância mínima e, deste modo, um melhoramento de δ_{WFR}. No Capítulo 3, Seção 2, examinaremos uma família de códigos para as quais podemos demonstrar que δ_{A^+} também pode ser usada como uma cota inferior.

Definição 2.51. Para cada $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ e $1 \leq i, j \leq n$, defina o seguinte *valor síndrome*: $s_i(c) := \phi(\overline{h}_i)c^t$ e $s_{i,j}(c) := \phi(\overline{h}_{i,j})c^t$.

Observação 2.52. Note que c é uma palavra código de $C^{\perp}(I, L)$, onde $L = L(\underline{r}, v_1, \ldots, v_l)$ se, e somente se, $s_i(c) = 0$ para todo $i \in \{1, \ldots, r, v_1, \ldots, v_l\}$. Note também que $s_{i,j}(c) = 0$ se $\overline{h}_{i,j} \in L(\underline{r}, v_1, \ldots, v_l)$.

Definição 2.53. Definimos a matriz síndrome $n \times n$ $S_c := [s_{i,j}(c)]$. Tal matriz é dita a *matriz de síndromes* para c.

Observação 2.54. Um fato importante que temos é que como c é uma palavra código, o posto da matriz síndrome é precisamente o peso da palavra código.

Definição 2.55. Para $a, b \in W$, denote por $[S_c]_{(a,b)}$ a submatriz de S_c de todas as entradas $s_{i,j}(c)$ tais que $i \in W_a$ e $j \in W_b$.

Definição 2.56. Denote por $\mathcal{C}_r'$ o seguinte conjunto de submatrizes de S_c:

$$\mathcal{C}_r' = \{[S_c]_{(a,b)} : (a, b) \in \mathcal{P}_r\}.$$

Note que toda submatriz $[S_c]_{(a,b)}$ de $\mathcal{C}_r'$ corresponde de maneira natural a uma submatriz $M_{(a,b)}$ de $\mathcal{C}_r$. Além disso, não há duas submatrizes de $\mathcal{C}_r'$ compartilhando uma linha ou coluna comum de S_c. E ainda, para cada $[S_c]_{(a,b)} \in \mathcal{C}_r'$, temos $[S_c]_{(a,b)} = [S_c]_{(a,b)}^t \in \mathcal{C}_r'$, visto que S_c é simétrica.

Teorema 2.57. *Suponha que c seja uma palavra não nula do código $C^{\perp}(I, L)$. Suponha que $s_z(c) \neq 0$ e $s_v(c) = 0$ para todo $v < z$. Então $w(c) \geq A_z$.*

Demonstração: Pelas observações acima temos que

$$\begin{aligned} w(c) &= \textit{posto } S_c \geq \sum_{(a,b)\in\mathcal{P}_z} \textit{posto } [S_c]_{(a,b)} \\ &= \sum_{(a,b)\in\mathcal{P}_z\setminus\mathcal{E}_z} \textit{posto } [S_c]_{(a,b)} + \sum_{(a,b)\in\mathcal{E}_z} \textit{posto } [S_c]_{(a,b)}. \end{aligned}$$

Para cada $(i, j) \in \widetilde{\mathcal{N}}_z$, sabemos que para todo (u, v) tal que $u < i$ e $v = j$ ou $u = i$ e $v < j$, temos $\overline{h}_{u,v} \in L(\underline{z-1})$ e portanto, $s_{u,v}(c) = 0$. Por outro lado, $h_{i,j} \sim h_z$ e

$s_z(c) \neq 0$ implica que $s_{i,j}(c) \neq 0$. Como não existe dois elementos $(i,j),(i^{'},j^{'}) \in \widetilde{\mathcal{N}}_z$ tal que $i = i^{'}$ ou $j = j^{'}$, temos que em cada linha e em cada coluna de S_c existe, no máximo, um elemento cujo índice está em $\widetilde{\mathcal{N}}_z$. Portanto, existe $\widetilde{\mathcal{N}}_z$ linhas de S_c que têm sua primeira entrada não nula em colunas diferentes. Agora, cada matriz $M_{(a,b)}$ que não é extrema para h_z contém pelo menos uma entrada cujos índices estão em $\widetilde{\mathcal{N}}_z$, logo, *posto* $[S_c]_{(a,b)} \geq 1$. Assim,

$$\sum_{(a,b)\in\mathcal{P}_z\setminus\mathcal{E}_z} posto\ [S_c]_{(a,b)} \geq \widetilde{N}_z.$$

Como cada matriz $M_{(a,b)}$ extrema para h_z contém uma entrada consistente com h_z, segue que $[S_c]_{(a,b)}$ é não nula e assim, *posto* $[S_c]_{(a,b)} \geq 1$. Portanto, temos

$$\sum_{(a,b)\in\mathcal{E}_z} posto\ [S_c]_{(a,b)} \geq E_z.$$

Deste modo, $w(c) \geq \widetilde{N}_z + E_z = A_z$. □

Note que se c é uma palavra de $C^{\perp}(I,L)$ tal que $s_v(c) = 0$ para $1 \leq v \leq n$ então, pela Observação 2.52, c também é uma palavra do código zero-dimensional $C^{\perp}(I,L(\underline{n}))$. Deste modo, c deve ser o vetor nulo.

Teorema 2.58. *A distância mínima do código sobre variedade afim $C^{\perp}(I,L)$, onde $L = L(\underline{r}, v_1, \ldots, v_l)$, é pelo menos δ_A.*

Demonstração: Seja c uma palavra não nula do código e z o único índice tal que $s_v(c) = 0$ para todo $v < z$ e $s_z(c) \neq 0$. Pela Observação 2.52 devemos ter $z \notin \{1,\ldots,r,v_1,\ldots v_l\}$, visto que c é uma palavra do código. Portanto, pelo Teorema 2.57, temos que

$$w(c) \geq A_z \geq min\{A_t : t \notin \{1,\ldots,r,v_1,\ldots v_l\}\} = \delta_A.$$

□

Observação 2.59. Seja z tal que $A_z \neq B_z$. Se pudermos mostrar que

$$posto\ S_c \geq \sum_{(a,b)\in\mathcal{P}_z} posto\ [S_c]_{(a,b)} \geq B_z$$

para todo c que satisfaz $z = min\{v : s_v(c) \neq 0\}$, então poderemos reafirmar o Teorema 2.57 com B_z no lugar de A_z. Se isso for verificado para cada tal z, então poderemos reescrever o Teorema 2.58 com δ_{A^+} no lugar de δ_A.

Um método possível para mostrar a desigualdade acima é provar que

$$posto\ [S_c]_{(a,b)} \geq |\{h_{i,j} \in M_{(a,b)} : (i,j) \in \mathcal{B}_z\}|$$

para todo $(a,b) \in \mathcal{P}_z$. De fato, pelo Lema 2.21 e a prova do Teorema 2.57, precisaremos examinar somente esses $(a,b) \in \mathcal{P}_z$ para os quais $M_{(a,b)}$ contém uma entrada $h_{u,v}$ tal que $(u,v) \in \mathcal{B}_z$, com $h_{u,v} \neq h_r$. No Capítulo 3, Seção 2, forneceremos um exemplo para o qual isso pode ser verificado. Deste modo, a estimativa indicativa forte pode ser usada como uma cota inferior para a distância mínima.

Capítulo 3

Aplicações

Neste capítulo descreveremos certas famílias de códigos para as quais mostraremos as diferenças entre os códigos construídos com cada uma das cotas mencionadas no Capítulo 2, deixando claro que o código cuja cota para distância mínima é a indicativa é maior que os construídos com as cotas de Feng-Rao e Miura. Mostraremos também uma família de códigos na qual se aplica a estimativa indicativa forte como cota para a distânica mínima.

3.1 Polinômios definidos em $\mathbb{F}_q$

Iniciaremos descrevendo duas famílias de polinômios que foram definidas por Rédei [20] e que nos auxiliarão na descrição de códigos $C^{\perp}(I, L)$.

Definição 3.1. Seja $\mathbb{F}_s$ um subcorpo de $\mathbb{F}_q$. Um polinômio $f(x) \in \mathbb{F}_q[x]$ é dito um $(\mathbb{F}_q, \mathbb{F}_s)$-*polinômio* se, para cada $\gamma \in \mathbb{F}_q$, temos $f(\gamma) \in \mathbb{F}_s$.

É bem sabido que cada aplicação de $\mathbb{F}_q$ em $\mathbb{F}_q$ pode ser representada unicamente por um polinômio em $\mathbb{F}_q[x]$ de grau menor que q. Consideraremos $(\mathbb{F}_4, \mathbb{F}_2)$-polinômios de grau no máximo 3 e $(\mathbb{F}_8, \mathbb{F}_2)$-polinômios de grau no máximo 7.

A proposição abaixo caracteriza os $(\mathbb{F}_4, \mathbb{F}_2)$-polinômios e os $(\mathbb{F}_8, \mathbb{F}_2)$-polinômios. Faremos somente a demonstração do item (i), visto que a do item (ii) é análoga e

pode ser encontrada em [20].

Proposição 3.2. *(i) O polinômio* $f(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \beta_3 x^3 \in \mathbb{F}_4[x]$ *é um* $(\mathbb{F}_4, \mathbb{F}_2)$*-polinômio se, e somente se,* $\beta_0, \beta_3 \in \mathbb{F}_2$ *e* $\beta_2 = \beta_1^2$.
(ii) O polinômio $g(x) = \beta_0 + \beta_1 x + \cdots + \beta_6 x^6 + \beta_7 x^7 \in \mathbb{F}_8[x]$ *é um* $(\mathbb{F}_8, \mathbb{F}_2)$*-polinômio se, e somente se,* $\beta_0, \beta_7 \in \mathbb{F}_2$, $\beta_2 = \beta_1^2$, $\beta_4 = \beta_2^2$, $\beta_6 = \beta_3^2$ *e* $\beta_3 = \beta_5^2$.

Demonstração: (i) Consideremos $\mathbb{F}_4 = \mathbb{F}_2(\theta)$, onde $\theta^2 = \theta + 1$. Assim, $\mathbb{F}_4 = \{0, 1, \theta, \theta^2\}$.

Primeiramente, suponhamos que $f(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \beta_3 x^3$ seja um $(\mathbb{F}_4, \mathbb{F}_2)$-polinômio. Avaliando $f(x)$ em cada elemento de $\mathbb{F}_4$ e usando a Definição 3.1, obtemos:

$$\begin{aligned} f(0) &= \beta_0 \in \mathbb{F}_2 && (3.1)\\ f(1) &= \beta_0 + \beta_1 + \beta_2 + \beta_3 \in \mathbb{F}_2 && (3.2)\\ f(\theta) &= \beta_0 + \beta_1\theta + \beta_2\theta^2 + \beta_3 \in \mathbb{F}_2 && (3.3)\\ f(\theta^2) &= \beta_0 + \beta_1\theta^2 + \beta_2\theta + \beta_3 \in \mathbb{F}_2 && (3.4)\\ f(\theta) + f(1) &= \beta_1\theta^2 + \beta_2\theta \in \mathbb{F}_2 && (3.5) \end{aligned}$$

Como (3.4) e (3.5) estão em $\mathbb{F}_2$ podemos escrevê-las na forma

$$\begin{aligned} \beta_0 + \beta_1\theta^2 + \beta_2\theta + \beta_3 &= \alpha_1 && (3.6)\\ \beta_1\theta^2 + \beta_2\theta &= \alpha_2 && (3.7) \end{aligned}$$

com $\alpha_1, \alpha_2 \in \mathbb{F}_2$. Assim, obtemos $\beta_3 = \alpha_1 + \alpha_2 + \beta_0$, logo, $\beta_3 \in \mathbb{F}_2$. Resta mostrar que $\beta_2 = \beta_1^2$.

De (3.2) e pelo fato de que $\beta_0, \beta_3 \in \mathbb{F}_2$ obtemos $\beta_1 + \beta_2 \in \mathbb{F}_2$, então

$$\beta_1 = \alpha_3 + \beta_2 \qquad (3.8)$$

com $\alpha_3 \in \mathbb{F}_2$.

Quando $\alpha_2 = 0$ temos $\beta_2 = \beta_1\theta$. Usando (3.8) obtemos $\beta_2 = \alpha_3\theta + \beta_2\theta$, consequentemente, $\beta_2\theta = \alpha_3$. Deste modo, se $\alpha_3 = 0$, então $\beta_2 = 0$, $\beta_1 = 0$ e $\beta_2 = \beta_1^2$. Se $\alpha_3 = 1$, então $\beta_2 = \theta^2$, $\beta_1 = \theta$ e $\beta_2 = \beta_1^2$.

Quando $\alpha_2 = 1$ temos $\beta_2\theta = 1+\beta_1\theta^2$. Usando (3.8) obtemos $\beta_2 = \theta^2+\alpha_3\theta+\beta_2\theta$. Se $\alpha_3 = 0$, então $\beta_2 = \theta^2 + \beta_2\theta$, logo, $\beta_2 = 1$, $\beta_1 = 1$ e $\beta_2 = \beta_1^2$. Se $\alpha_3 = 1$, então $\beta_2 = \theta^2+\theta+\beta_2\theta$, consequentemente, $\beta_2 = \theta$, $\beta_1 = \theta^2$ e $\beta_2 = \beta_1^2$. Portanto, em todos os casos, $\beta_2 = \beta_1^2$.

Por outro lado, suponhamos $\beta_0, \beta_3 \in \mathbb{F}_2$ e $\beta_2 = \beta_1^2$. Observe que $0^2 + 0 = 0$, $1^2 + 1 = 0$, $\theta^2 + \theta = 1$ e $(\theta^2)^2 + \theta^2 = 1$. Assim,

$$f(0) = \beta_0 \in \mathbb{F}_2 \qquad e \qquad f(1) = \beta_0 + \beta_1 + \beta_1^2 + \beta_3 \in \mathbb{F}_2.$$

Agora, $\beta_1\theta \in \mathbb{F}_4$, então, pela observação acima, $(\beta_1\theta)^2 + \beta_1\theta \in \mathbb{F}_2$. Portanto,

$$f(\theta) = \beta_3 + \beta_1\theta + \beta_1^2\theta^2 + \beta_3 = \beta_0 + \beta_1\theta + (\beta_1\theta)^2 + \beta_3 \in \mathbb{F}_2.$$

Temos que $\theta^4 = \theta$, deste modo, $\beta_1^2\theta = \beta_1^2\theta^4$. Logo, pela observação acima,

$$f(\theta^2) = \beta_0 + \beta_1\theta^2 + \beta_1^2\theta + \beta_3 = \beta_0 + \beta_1\theta^2 + (\beta_1\theta^2)^2 + \beta_3 \in \mathbb{F}_2.$$

Portanto, $f(x)$ é um $(\mathbb{F}_4, \mathbb{F}_2)$-polinômio.
(ii) Ver Teorema 2, página 14 de [20]. □

Teorema 3.3. (Teorema de König-Rados). *Seja* $f(x) = a_0 + a_1x + \cdots + a_{q-2}x^{q-2} \in \mathbb{F}_q[x]$. *Então o número de soluções não nulas da equação* $f(x) = 0$ *em* $\mathbb{F}_q$ *é igual a* $q - 1 - r$, *onde* r *é o posto da matriz*

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{q-3} & a_{q-2} \\ a_1 & a_2 & \cdots & a_{q-2} & a_0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{q-2} & a_0 & \cdots & a_{q-4} & a_{q-3} \end{pmatrix}.$$

Demonstração: Ver Teorema 6.1 de [13]. □

3.2 Uma família de códigos para curvas não singulares

Seja $\mathcal{F}$ o conjunto de polinômios dado por $\mathcal{F} = \{f(x) + g(y) : f \text{ e } g \text{ são } (\mathbb{F}_8, \mathbb{F}_2) - \text{polinômios com } gr(f) = 4 \text{ e } gr(g) = 6\}$. Pela descrição de $f(x)$ e $g(y)$ dada em $\mathcal{F}$, podemos escrever $f(x) = a_0 + a_1x + a_1x^2 + a_1x^4$, com $a_0 \in \mathbb{F}_2$ e $a_1 \in \mathbb{F}_8^*$, e $g(y) = b_0 + b_1y + b_1^2y^2 + b_5^2y^3 + b_1^4y^4 + b_5y^5 + b_5^4y^6$, com $b_0 \in \mathbb{F}_2$, $b_1 \in \mathbb{F}_8$ e $b_5 \in \mathbb{F}_8^*$. Deste modo, temos 14 polinômios de grau 4 e 112 polinômios de grau 6. Por combinação, segue que a família $\mathcal{F}$ tem 784 membros.

Afirmamos que todo $(\mathbb{F}_8, \mathbb{F}_2)$-polinômio quaternário tem 4 raízes distintas sobre $\mathbb{F}_8$. De fato, seja $f(x)$ um $(\mathbb{F}_8, \mathbb{F}_2)$-polinômio quaternário, então $f(x) = a_0 + a_1x + a_1^2x^2 + a_1^4x^4$, com $a_0 \in \mathbb{F}_2$ e $a_1 \in \mathbb{F}_8^*$.

Tomando $a_0 = 1$ temos que $x = 0$ não é solução de $f(x)$, assim, pelo Teorema de König-Rados, o número de soluções de $f(x)$ é $N = 7 - r$, onde r é o posto da matriz

$$A = \begin{pmatrix} 1 & a_1 & a_1^2 & 0 & a_1^4 & 0 & 0 \\ a_1 & a_1^2 & 0 & a_1^4 & 0 & 0 & 1 \\ a_1^2 & 0 & a_1^4 & 0 & 0 & 1 & a_1 \\ 0 & a_1^4 & 0 & 0 & 1 & a_1 & a_1^2 \\ a_1^4 & 0 & 0 & 1 & a_1 & a_1^2 & 0 \\ 0 & 0 & 1 & a_1 & a_1^2 & 0 & a_1^4 \\ 0 & 1 & a_1 & a_1^2 & 0 & a_1^4 & 0 \end{pmatrix}.$$

Escalonando A obtemos

$$A^{'} = \begin{pmatrix} 1 & 0 & 0 & a_1^3 & a_1^4 & a_1^5 & 0 \\ 0 & 1 & a_1 & a_1^2 & 0 & a_1^4 & 0 \\ 0 & 0 & 1 & a_1 & a_1^2 & 0 & a_1^4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

que implica que $r = 3$, logo, $N = 4$.

Tomando $a_0 = 0$ podemos escrever $f(x)$ na forma $f(x) = x(a_1 + a_1^2 x + a_1^4 x^3) = xg(x)$. Claramente, $x = 0$ é uma solução de $f(x)$. As demais soluções de $f(x)$ são as soluções de $g(x) = a_1 + a_1^2 x + a_1^4 x^3$. Note que $x = 0$ não é solução de $g(x)$, uma vez que $a_1 \neq 0$. Deste modo, o número de soluções de $f(x)$ é $N = N^{'} + 1$, onde $N^{'}$ é o número de soluções de $g(x)$ e, pelo Teorema de König-Rados, $N^{'} = 7 - r$, com r igual o posto da matriz

$$B = \begin{pmatrix} a_1 & a_1^2 & 0 & a_1^4 & 0 & 0 & 0 \\ a_1^2 & 0 & a_1^4 & 0 & 0 & 0 & a_1 \\ 0 & a_1^4 & 0 & 0 & 0 & a_1 & a_1^2 \\ a_1^4 & 0 & 0 & 0 & a_1 & a_1^2 & 0 \\ 0 & 0 & 0 & a_1 & a_1^2 & 0 & a_1^4 \\ 0 & 0 & a_1 & a_1^2 & 0 & a_1^4 & 0 \\ 0 & a_1 & a_1^2 & 0 & a_1^4 & 0 & 0 \end{pmatrix}.$$

Escalonando B obtemos a matriz

$$B' = \begin{pmatrix} 1 & 0 & 0 & 0 & a_1^4 & 0 & a_1^2 \\ 0 & 1 & 0 & a_1^2 & a_1^3 & a_1^4 & 0 \\ 0 & 0 & 1 & a_1 & 0 & a_1^3 & 0 \\ 0 & 0 & 0 & 1 & a_1 & 0 & a_1^3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

que implica que $r = 4$, logo, $N' = 3$ e $N = 4$. Portanto, em ambos os casos, temos $N = 4$.

Agora, cada membro de nossa família tem 32 raízes em $\mathbb{F}_8^2$, pois para cada $a \in \mathbb{F}_8$, $f(x) + g(a)$ é um $(\mathbb{F}_8, \mathbb{F}_2)$-polinômio, assim, $f(x) + g(a) = 0$ tem 32 raízes, uma vez que $f(x)$ tem 4 raízes distintas e temos 8 escolhas diferentes para a.

Escolha um $t \in \mathcal{F}$ e seja $I = \langle t \rangle$. Ponha $w(x) = 3$ e $w(y) = 2$. Consequentemente, os monômios x^4 e y^6 têm peso máximo dentre todos os monômios no suporte de t (monômios que compõem t). Observe que $t \in I_8$, com $lm(t) = x^4$. Como um resultado

$$\Delta(I_8) = \{x^a y^b : 0 \leq a \leq 3 \ e \ 0 \leq b \leq 7\}.$$

A sequência H é:

$$\begin{aligned} H = \ & \{1, y, x, y^2, xy, y^3, x^2, xy^2, y^4, x^2y, xy^3, x^3, y^5, x^2y^2, xy^4, x^3y, y^6, x^2y^3, xy^5, \\ & x^3y^2, y^7, x^2y^4, xy^6, x^3y^3, x^2y^5, xy^7, x^3y^4, x^2y^6, x^3y^5, x^2y^7, x^3y^6, x^3y^7\} \end{aligned}$$

e cada um de seus monômios pode ser relacionado na seguinte tabela:

PESO	MONÔMIOS	PESO	MONÔMIOS
0	$h_1 = 1$	12	$h_{17} = y^6,\ h_{18} = x^2y^3$
2	$h_2 = y$	13	$h_{19} = xy^5,\ h_{20} = x^3y^2$
3	$h_3 = x$	14	$h_{21} = y^7,\ h_{22} = x^2y^4$
4	$h_4 = y^2$	15	$h_{23} = xy^6,\ h_{24} = x^3y^3$
5	$h_5 = xy$	16	$h_{25} = x^2y^5$
6	$h_6 = y^3,\ h_7 = x^2$	17	$h_{26} = xy^7,\ h_{27} = x^3y^4$
7	$h_8 = xy^2$	18	$h_{28} = x^2y^6$
8	$h_9 = y^4,\ h_{10} = x^2y$	19	$h_{29} = x^3y^5$
9	$h_{11} = xy^3,\ h_{12} = x^3$	20	$h_{30} = x^2y^7$
10	$h_{13} = y^5,\ h_{14} = x^2y^2$	21	$h_{31} = x^3y^6$
11	$h_{15} = xy^4,\ h_{16} = x^3y$	23	$h_{32} = x^3y^7$

Tabela 3.1: Elementos de H e seus respectivos pesos.

Note que há muitos $h_r \in H$ satisfazendo $|S_r| = 1$. Neste caso, pelo Corolário 2.38, sabemos que B_r é minimal, a saber, $B_r = D_r$. Existem exatamente 8 monômios em H que têm conjunto de consistência não trivial. São eles $h_{17} = y^6$, $h_{21} = y^7$, $h_{23} = xy^6$, $h_{26} = xy^7$, $h_{28} = x^2y^6$, $h_{30} = x^2y^7$, $h_{31} = x^3y^6$ e $h_{32} = x^3y^7$. Examinemos individualmente cada um desses monômios juntamente com seus números associados N_r, $\widetilde{N}_r$, A_r e B_r. Pelo Lema 2.21, precisamos somente examinar os $h_{i,j}$ tais que $h_{i,j} \sim h_r$, mas $h_{i,j} \neq h_r$.

Para $h_{17} = y^6$, os possíveis monômios que estão no seu conjunto de consistência, exceto o próprio h_{17} são x^2y^3 e x^4, visto possuírem mesmo peso. Mas $x^2y^3 = h_{18}$, consequentemente, $\overline{x^2y^3} \in L(\underline{18})$, logo $x^2y^3 \notin S_{17}$. Analisemos x^4. As contas feitas a seguir são análogas às do Exemplo 2.13. Para $\alpha_i \in \mathbb{F}_8$, $i = 1, \ldots, 17$,

$$
\begin{aligned}
\overline{x^4} = \;& \alpha_1\overline{1} + \alpha_2\overline{y} + \alpha_3\overline{x} + \alpha_4\overline{y^2} + \alpha_5\overline{xy} + \alpha_6\overline{y^3} + \alpha_7\overline{x^2} + \alpha_8\overline{xy^2} + \alpha_9\overline{y^4} + \\
& \alpha_{10}\overline{x^2y} + \alpha_{11}\overline{xy^3} + \alpha_{12}\overline{x^3} + \alpha_{13}\overline{y^5} + \alpha_{14}\overline{x^2y^2} + \alpha_{15}\overline{xy^4} + \alpha_{16}\overline{x^3y} + \alpha_{17}\overline{y}^6 \\
\Leftrightarrow \;& x^4 + \alpha_1 + \alpha_2 y + \alpha_3 x + \alpha_4 y^2 + \alpha_5 xy + \alpha_6 y^3 + \alpha_7 x^2 + \alpha_8 xy^2 + \alpha_9 y^4 + \\
& \alpha_{10}x^2y + \alpha_{11}xy^3 + \alpha_{12}x^3 + \alpha_{13}y^5 + \alpha_{14}x^2y^2 + \alpha_{15}xy^4 + \alpha_{16}x^3y + \alpha_{17}y^6 \\
= \;& (x^4 + \alpha_7 x^2 + \alpha_3 x + \alpha_1)1 + (\alpha_{17}y^6 + \alpha_{13}y^5 + \alpha_9 y^4 + \alpha_6 y^3 + \alpha_4 y^2 + \alpha_2 y)1 + \\
& \alpha_5 xy + \alpha_8 xy^2 + \alpha_{10}x^2y + \alpha_{11}xy^3 + \alpha_{12}x^3 + \alpha_{14}x^2y^2 + \alpha_{15}xy^4 + \alpha_{16}x^3y \in I_8
\end{aligned}
$$

Tomando $\alpha_5 = \alpha_8 = \alpha_{10} = \alpha_{11} = \alpha_{12} = \alpha_{14} = \alpha_{15} = \alpha_{16} = 0$ e $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = \alpha_6 = \alpha_7 = \alpha_9 = \alpha_{13} = \alpha_{17} = 1$ temos

$$(x^4 + x^2 + x + 1)1 + (y^6 + y^5 + y^4 + y^3 + y^2 + y)1 \in I_8$$

e como $\alpha_{17} \neq 0$, $\overline{x^4} \in L(\underline{17}) \setminus L(\underline{16})$. Consequentemente, $x^4 \in S_{17}$.

Portanto, $S_{17} = \{y^6, x^4\}$ e

$$\mathcal{B}_{17} = \{(1,17),(2,13),(4,9),(6,6),(9,4),(13,2),(17,1)\} \cup \{(3,12),(7,7),(12,3)\}.$$

Assim $B_{17} = 10$ e, pelo Lema 2.21, $N_{17} = 7$.

Considere as duas submatrizes de elementos de mesmo peso $M_{(3,9)}$ e $M_{(6,6)}$ (ver Definição 2.42). Primeiro,

$$M_{(3,9)} = \begin{pmatrix} x^2y^3 & x^4 \end{pmatrix} = \begin{pmatrix} h_{18} & x^4 \end{pmatrix}.$$

Note que $h_{3,12} = x^4 \in M_{(3,9)}$ não é fracamente bem comportado, visto que $h_{3,11} = h_{18}$. Deste modo, $M_{(3,9)}$ é extrema para h_{17}. Como $M_{(9,3)} = M_{(3,9)}^t$ temos que $M_{(9,3)}$ também é extrema para h_{17}. Segundo,

$$M_{(6,6)} = \begin{pmatrix} y^6 & x^2y^3 \\ x^2y^3 & x^4 \end{pmatrix} = \begin{pmatrix} h_{17} & h_{18} \\ h_{18} & x^4 \end{pmatrix}.$$

Note que $h_{7,7} = x^4 \in M_{(6,6)}$ não é fracamente bem comportado uma vez que $h_{7,6} = h_{18}$. Entretanto, $M_{(6,6)}$ não é extrema para h_{17}, pois $h_{1,17} = h_{17} \in M_{(6,6)}$. Assim, $E_{17} = 2$, $\widetilde{N}_{17} = 7$ e $A_{17} = 9$.

Para $h_{21} = y^7$ temos $S_{21} = \{y^7, x^4y\}$, com

$$\begin{aligned}\mathcal{B}_{21} = \ & \{(1,21),(2,17),(4,13),(6,9),(9,6),(13,4),(17,2),(21,1)\} \\ & \cup\{(3,16),(5,12),(7,10),(10,7),(12,5),(16,3)\}.\end{aligned}$$

Examinemos as três submatrizes $M_{(3,11)}$, $M_{(5,9)}$ e $M_{(6,8)}$. Primeiro,

$$M_{(3,11)} = \begin{pmatrix} x^2y^4 & x^4y \end{pmatrix} = \begin{pmatrix} h_{22} & x^4y \end{pmatrix}.$$

Note que $h_{3,16} = x^4y \in M_{(3,11)}$ não é fracamente bem comportado, visto que $h_{3,15} = h_{22}$. Portanto, $M_{(3,11)}$ e $M_{(11,3)}$ são extremas para h_{21}. Segundo,

$$M_{(5,9)} = \begin{pmatrix} x^2y^4 & x^4y \end{pmatrix} = \begin{pmatrix} h_{22} & x^4y \end{pmatrix}.$$

Observe que $M_{(5,9)} = M_{(3,11)}$, consequentemente, nem $h_{5,12} = x^4y \in M_{(5,9)}$ nem $h_{12,5} \in M_{(5,9)}$ são fracamente bem comportados, pois $h_{11,5} = h_{5,11} = h_{22}$. Com isso, $M_{(5,9)}$ e $M_{(9,5)}$ são extremas para h_{21}. Terceiro,

$$M_{(6,8)} = \begin{pmatrix} y^7 & x^2y^4 \\ x^2y^4 & x^4y \end{pmatrix} = \begin{pmatrix} h_{21} & h_{22} \\ h_{22} & x^4y \end{pmatrix}.$$

Note que $h_{7,10} = x^4y \in M_{(6,8)}$ não é fracamente bem comportado, visto que $h_{7,9} = h_{22}$. Porém, $M_{(6,8)}$ não é extrema para h_{21}, uma vez que $h_{1,21} = h_{21} \in M_{(6,8)}$. Por simetria, $h_{10,7}$ não é fracamente bem comportado e $M_{(8,6)}$ não é extrema para h_{21}. Como resultado temos $N_{21} = \widetilde{N}_{21} = 8$, $A_{21} = 12$ e $B_{21} = 14$.

Para $h_{23} = xy^6$ temos $S_{23} = \{xy^6, x^5\}$, com $B_{23} = 16$. Como

$$\mathcal{D}_{23} = \{1, x, y, y^2, y^3, y^4, y^5, y^6, xy, xy^2, xy^3, xy^4, xy^5, xy^6\}$$

e $D_{23} = 14$, precisamos examinar somente $h_{7,12}$ e $h_{12,7}$. Considere a submatriz

$$M_{(6,9)} = \begin{pmatrix} xy^6 & x^3y^3 \\ x^3y^3 & x^5 \end{pmatrix} = \begin{pmatrix} h_{23} & h_{24} \\ h_{24} & x^5 \end{pmatrix}.$$

Podemos ver que $h_{7,12} = x^5 \in M_{(6,9)}$ não é fracamente bem comportado, pois $h_{7,11} = h_{24}$. Além disso, $M_{(6,9)}$ não é extrema para h_{23}, visto que $h_{23} \in M_{(6,9)}$. Por simetria,

$h_{12,7}$ não é fracamente bem comportado e $M_{(9,6)}$ não é extrema para h_{23}. Logo, $N_{23} = \widetilde{N}_{23} = A_{23} = 14$.

Para $h_{26} = xy^7$ temos $S_{26} = \{xy^7, x^2y\}$, com $B_{26} = 20$ e $D_{26} = 16$. Precisamos examinar $h_{7,16}$, $h_{10,12}$, $h_{12,10}$ e $h_{16,7}$. Considere as duas submatrizes $M_{(6,11)}$ e $M_{(8,9)}$. Primeiro,

$$M_{(6,11)} = \begin{pmatrix} xy^7 & x^3y^4 \\ x^3y^4 & x^5y \end{pmatrix} = \begin{pmatrix} h_{26} & h_{27} \\ h_{27} & x^5y \end{pmatrix}.$$

Note que $h_{7,16} = x^5y \in M_{(6,11)}$ não é fracamente bem comportado, pois $h_{7,15} = h_{27}$. Além disso, $M_{(6,11)}$ não é extrema para h_{26}, pois $h_{26} \in M_{(6,11)}$. Por simetria, $h_{16,7}$ não é fracamente bem comportado e $M_{(11,6)}$ não é extrema para h_{26}. Segundo,

$$M_{(8,9)} = \begin{pmatrix} xy^7 & x^3y^4 \\ x^3y^4 & x^5y \end{pmatrix} = \begin{pmatrix} h_{26} & h_{27} \\ h_{27} & x^5y \end{pmatrix}.$$

Observe que $M_{(8,9)} = M_{(6,11)}$. Assim, nem $h_{10,12} \in M_{(8,9)}$ nem $h_{12,10} \in M_{(9,8)}$ são fracamente bem comportados. Além disso, nem $M_{(8,9)}$ nem $M_{(9,8)}$ são extremas para h_{26}. Portanto, $N_{26} = \widetilde{N}_{26} = A_{26} = 16$.

Para $h_{28} = x^2y^6$ temos $S_{28} = \{x^2y^6, x^6\}$, com $B_{28} = 22$ e $D_{28} = 21$. Como $x^6 <_t h_{29}$, pelo Corolário 2.36 segue que $\widetilde{N}_{28} = A_{28} = B_{28}$. Vemos que $h_{12,12} = x^6$ não é bem comportado, uma vez que $h_{11,11} = h_{28}$. Deste modo, $N_{28} = D_{28} = 21$.

Para $h_{30} = x^2y^7$ temos $S_{30} = \{x^2y^7, x^6y\}$, com $B_{30} = 26$ e $D_{30} = 24$. Como $x^6y <_t h_{31}$ sabemos, pelo Corolário 2.36, que $\widetilde{N}_{30} = A_{30} = B_{30}$. Por outro lado, $h_{12,16}$ e $h_{16,12}$ não são bem comportados, pois $h_{11,15} = h_{15,11} = h_{30}$. Assim, $N_{30} = D_{30} = 24$.

Para $h_{31} = x^3y^6$ e $h_{32} = x^3y^7$ temos que $S_{31} = \{x^3y^6, x^7\}$ e $S_{32} = \{x^3y^7, x^7y\}$, com $B_{31} = D_{31} = 28$ e $B_{32} = D_{32} = 32$. Consequentemente, $N_{31} = \widetilde{N}_{31} = A_{31} = 28$ e $N_{32} = \widetilde{N}_{32} = A_{32} = 32$.

Resumimos as observações acima na Tabela 3.2.

h_r	1	y	x	y^2	xy	y^3	x^2	xy^2
N_r	1	2	2	3	4	4	3	6
$\widetilde{N}_r$	1	2	2	3	4	4	3	6
A_r	1	2	2	3	4	4	3	6
B_r	1	2	2	3	4	4	3	6
h_r	y^4	x^2y	xy^3	x^3	y^5	x^2y^2	xy^4	x^3y
N_r	5	6	8	4	6	9	10	8
$\widetilde{N}_r$	5	6	8	4	6	9	10	8
A_r	5	6	8	4	6	9	10	8
B_r	5	6	8	4	6	9	10	8
h_r	y^6	x^2y^3	xy^5	x^3y^2	y^7	x^2y^4	xy^6	x^3y^3
N_r	7	12	12	12	8	15	14	16
$\widetilde{N}_r$	7	12	12	12	8	15	14	16
A_r	9	12	12	12	12	15	14	16
B_r	10	12	12	12	14	15	16	16
h_r	x^2y^5	xy^7	x^3y^4	x^2y^6	x^3y^5	x^2y^7	x^3y^6	x^3y^7
N_r	18	16	20	21	24	24	28	32
$\widetilde{N}_r$	18	16	20	22	24	26	28	32
A_r	18	16	20	22	24	26	28	32
B_r	18	20	20	22	24	26	28	32

Tabela 3.2: Comparação de N_r, $\widetilde{N}_r$, A_r e B_r para cada $h_r \in H$.

A fim de criar códigos com parâmetros relativamente bons, seguiremos a construção de Feng-Rao de códigos geométricos de Goppa melhorados, dada em [6].

Construção: Dado uma distância mínima designada δ, seja $\{1, \ldots, r, v_1, \ldots, v_l\}$ o subconjunto de um conjunto $\{1, \ldots, n\}$ tal que

1. para $1 \leq v \leq r$, $N_v < \delta$ e $N_{r+1} \geq \delta$;

2. para $r+1 < u \leq n$, se $N_u < \delta$, então $u \in \{v_1, \ldots, v_l\}$.

Deste modo, um $[n, n-r-l, \geq \delta]$ é um código linear definido por H como uma matriz teste de paridade e dito um *código geométrico de Goppa melhorado*. Note que este código é o mesmo dado na Definição 2.3. Esta construção também é válida quando utilizamos os números $\widetilde{N}_r$, A_r e B_r no lugar de N_r.

Suponha que desejamos um código com distância designada δ, isto é, queremos que $C^{\perp}(I, L)$ tenha distância mínima pelo menos δ. Por exemplo, suponha que $\delta = 12$. Se usarmos os números N ou $\widetilde{N}$ como um guia veremos que $C^{\perp}(I, L)$, onde $L = L(\underline{17}, 21)$, tem distância mínima pelo menos 12. Em outras palavras, o maior código que pode ser construído para esta família usando δ_{WFR} ou δ_{FR} como nossa cota inferior para a distância mínima é um $[32, 14, \geq 12]$-código. Por outro lado, se usarmos a cota indicativa, então vemos que $L = L(\underline{17})$ produz um $[32, 15]$-código com a melhor distância mínima conhecida (cf [2]). De fato, para qualquer δ tal que $8 \leq \delta \leq 12$, os números indicativos produzem um código com uma dimensão maior que a do código produzido pelos números $\widetilde{N}$ (veja a Tabela 3.3), nesse sentido, dizemos que aquele código é melhor do que este, ou seja, dados códigos com o mesmo comprimento e a mesma distância mínima, o código que tiver dimensão maior será o melhor código.

	$\widetilde{N}_r$		A_r	
δ	L	$C^{\perp}(I, L)$	L	$C^{\perp}(I, L)$
8	$L(\underline{10}, 12, 13, 17)$	[32,19,8]	$L(\underline{10}, 12, 13)$	[32,20,8]
9	$L(\underline{13}, 16, 17, 21)$	[32,16,9]	$L(\underline{13}, 16)$	[32,18,9]
10	$L(\underline{14}, 16, 17, 21)$	[32,15,10]	$L(\underline{14}, 16, 17)$	[32,16,10]
11	$L(\underline{17}, 21)$	[32,14,12]	$L(\underline{17})$	[32,15,12]
12	$L(\underline{17}, 21)$	[32,14,12]	$L(\underline{17})$	[32,15,12]

Tabela 3.3: Comparação de códigos produzidos por $\widetilde{N}_r$ e A_r para $8 \leq \delta \leq 12$.

Por fim, vale mencionar que esta família produz diversos códigos bons. Por

exemplo, quando $\delta \in \{3, 4, 6, 12\}$, o correspondente $[32, k]$-código tem a melhor distância mínima conhecida. Veja a Tabela 3.4.

	$N_r = \widetilde{N}_r$		A_r	
δ	L	$C^{\perp}(I, L)$	L	$C^{\perp}(I, L)$
3	$L(\underline{3})$	[32,29,3]	$L(\underline{3})$	[32,29,3]
4	$L(\underline{4}, 7)$	[32,27,4]	$L(\underline{4}, 7)$	[32,27,4]
6	$L(\underline{7}, 9, 12)$	[32,23,6]	$L(\underline{7}, 9, 12)$	[32,23,6]
12	$L(\underline{17}, 21)$	[32,14,12]	$L(\underline{17})$	[32,15,12]

Tabela 3.4: Comparação de códigos produzidos por $\widetilde{N}_r$ e A_r para $\delta \in \{3, 4, 6, 12\}$.

3.3 Uma família de códigos para superfícies não singulares

Seja $\mathcal{F}$ o conjunto de polinômios especificado por $\mathcal{F} = \{f(x) + g(y) + h(z) : f,\ g\ e\ h\ são\ (\mathbb{F}_4, \mathbb{F}_2) - polinômios\ com\ gr(f) = gr(h) = 3\ e\ gr(g) = 2\}$. Pela descrição de $f(x)$, $g(y)$ e $h(z)$ dada em $\mathcal{F}$, podemos escrever $f(x) = a_0 + a_1x + a_1^2x^2 + x^3$, com $a_0 \in \mathbb{F}_2$ e $a_1 \in \mathbb{F}_4$, $g(y) = b_0 + b_1y + b_1^2y^2$, com $b_0 \in \mathbb{F}_2$ e $b_1 \in \mathbb{F}_4^*$, e $h(z) = c_0 + c_1z + c_1^2z^2 + z^3$, com $c_0 \in \mathbb{F}_2$ e $c_1 \in \mathbb{F}_4$. Deste modo, temos, por $f(x)$, 8 polinômios, por $g(y)$, 6 polinômios e, por $h(z)$, 8 polinômios, resultando, por combinação, que a família $\mathcal{F}$ tem 96 membros.

Afirmamos que todo $(\mathbb{F}_4, \mathbb{F}_2)$-polinômio quadrático tem 2 raízes distintas sobre $\mathbb{F}_4$. De fato, seja $g(x)$ um $(\mathbb{F}_4, \mathbb{F}_2)$-polinômio quadrático, então $g(x) = a_0 + a_1x + a_1^2x^2$, com $a_0 \in \mathbb{F}_2$ e $a_1 \in \mathbb{F}_4^*$.

Tomando $a_0 = 1$ temos que $x = 0$ não é solução de $g(x)$, assim, pelo Teorema de König-Rados, o número de soluções de $g(x)$ é $N = 3 - r$, onde r é o posto da matriz

$$A = \begin{pmatrix} 1 & a_1 & a_1^2 \\ a_1 & a_1^2 & 1 \\ a_1^2 & 1 & a_1 \end{pmatrix}.$$

Escalonando A obtemos a matriz

$$A^{'} = \begin{pmatrix} 1 & a_1 & a_1^2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

que implica que $r = 1$, logo, $N = 2$.

Tomando $a_0 = 0$ podemos escrever $g(x)$ na forma $g(x) = x(a_1 + a_1^2 x) = xk(x)$. Claramente, $x = 0$ é uma solução de $g(x)$. As demais soluções de $g(x)$ são as soluções de $k(x) = a_1 + a_1^2 x$. Note que $x = 0$ não é solução de $k(x)$, uma vez que $a_1 \neq 0$. Deste modo, o número de soluções de $g(x)$ é $N = N^{'} + 1$, onde $N^{'}$ é o número de soluções de $k(x)$ e, pelo Teorema de König-Rados, $N^{'} = 3 - r$, com r igual o posto da matriz

$$B = \begin{pmatrix} a_1 & a_1^2 & 0 \\ a_1^2 & 0 & a_1 \\ 0 & a_1 & a_1^2 \end{pmatrix}.$$

Escalonando B obtemos

$$B^{'} = \begin{pmatrix} 1 & 0 & a_1^2 \\ 0 & 1 & a_1 \\ 0 & 0 & 0 \end{pmatrix},$$

que implica que $r = 2$, logo, $N^{'} = 1$ e $N = 2$. Portanto, em ambos os casos, temos $N = 2$.

Agora, cada membro de nossa família tem 32 raízes em $\mathbb{F}_4^3$, pois para cada $a, b \in \mathbb{F}_4$, $f(a) + g(y) + h(b)$ é um $(\mathbb{F}_4, \mathbb{F}_2)$-polinômio, assim, $f(a) + g(y) + h(b) = 0$ tem 32 raízes, uma vez que $g(y)$ tem 2 raízes distintas e temos 4 escolhas diferentes tanto para a como para b.

Escolha $t \in \mathcal{F}$ e seja $I = \langle t \rangle$. Ponha $w(x) = 2$, $w(y) = 3$ e $w(z) = 2$. Assim, os monômios x^3, y^2 e z^3 têm peso máximo dentre todos os monômios no suporte de t. Observe que $t \in I_4$, com $lm(t) = x^3$ e $t_1 = xt - (x^4 - x) \in I_4$, com $lm(t_1) = xy^2$.

Como um resultado,

$$\Delta(I_4) = \{x^a y^b z^c : 0 \leq a \leq 2 \text{ e } 0 \leq b, c \leq 3; \text{ se } a \neq 0, \text{ então } b \leq 1\}.$$

A sequência H é:

$$H = \{1, z, x, y, z^2, xz, x^2, yz, xy, z^3, y^2, xz^2, x^2z, yz^2, xyz, x^2y, y^2z, xz^3, x^2z^2, yz^3, y^3, xyz^2, x^2yz, y^2z^2, x^2z^3, y^3z, xyz^3, x^2yz^2, y^2z^3, y^3z^2, x^2yz^3, y^3z^3\}$$

e cada um de seus elementos pode ser relacionado na seguinte tabela:

PESO	MONÔMIOS
0	$h_1 = 1$
2	$h_2 = z,\ h_3 = x$
3	$h_4 = y$
4	$h_5 = z^2,\ h_6 = xz,\ h_7 = x^2$
5	$h_8 = yz,\ h_9 = xy$
6	$h_{10} = z^3,\ h_{11} = y^2,\ h_{12} = xz^2,\ h_{13} = x^2z$
7	$h_{14} = yz^2,\ h_{15} = xyz,\ h_{16} = x^2y$
8	$h_{17} = y^2z,\ h_{18} = xz^3,\ h_{19} = x^2z^2$
9	$h_{20} = yz^3,\ h_{21} = y^3,\ h_{22} = xyz^2,\ h_{23} = x^2yz$
10	$h_{24} = y^2z^2,\ h_{25} = x^2z^3$
11	$h_{26} = y^3z,\ h_{27} = xyz^3,\ h_{28} = x^2yz^2$
12	$h_{29} = y^2z^3$
13	$h_{30} = y^3z^2,\ h_{31} = x^2yz^3$
15	$h_{32} = y^3z^3$

Tabela 3.5: Elementos de H e seus respectivos pesos.

Note que muitos $h_r \in H$ satisfazem $|S_r| = 1$, neste caso, pelo Corolário 2.38, $B_r = D_r$. Existem 12 monômios em H que têm conjunto de consistência não trivial. São eles: $h_{11} = y^2$, $h_{17} = y^2z$, $h_{18} = xz^3$, $h_{21} = y^3$, $h_{24} = y^2z^2$, $h_{25} = x^2z^3$, $h_{26} = y^3z$, $h_{27} = xyz^3$, $h_{29} = y^2z^3$, $h_{30} = y^3z^2$, $h_{31} = x^2yz^3$ e $h_{32} = y^3z^3$. Examinemos individualmente cada um desses monômios juntamente com seus números associados N_r, $\widetilde{N}_r$, A_r e B_r. Pelo Lema 2.21, precisamos somente examinar os $h_{i,j}$ tais que $h_{i,j} \sim h_r$, mas $h_{i,j} \neq h_r$.

Para $h_{11} = y^2$ temos $S_{11} = \{y^2, x^3\}$, com

$$\mathcal{B}_{11} = \{(1,11),(4,4),(11,1)\} \cup \{(3,7),(7,3)\}.$$

Podemos ver que para cada $(u,v) \in \mathcal{B}_{11}$, $h_{u,v}$ se encontra em uma submatriz diferente das demais. Pela Observação 2.48, obtemos $A_{11} = B_{11} = 5$. Por outro lado, $h_{3,7}$ e $h_{7,3}$ não são fracamente bem comportados, pois $h_{3,6} = h_{6,3} = h_{13}$. Portanto, $N_{11} = \widetilde{N}_{11} = 3$.

Para $h_{17} = y^2z$ temos $S_{17} = \{y^2z, x^3z\}$, com

$$\mathcal{B}_{17} = \{(1,17),(2,11),(4,8),(8,4),(11,2),(17,1)\} \cup \{(3,13),(6,7),(7,6),(13,3)\}.$$

Examinemos as duas submatrizes $M_{(2,6)}$ e $M_{(4,4)}$. Primeiro,

$$M_{(2,6)} = \begin{pmatrix} z^4 & y^2z & xz^3 & x^2z^2 \\ xz^3 & xy^2 & x^2z^2 & x^3z \end{pmatrix} = \begin{pmatrix} z^4 & h_{17} & h_{18} & h_{19} \\ h_{18} & xy^2 & h_{19} & x^3z \end{pmatrix}.$$

Note que $h_{3,13} = x^3z \in M_{(2,6)}$ não é fracamente bem comportado, pois $h_{3,12} = h_{19}$. Além disso, $M_{(2,6)}$ não é extrema para h_{17}, visto que $h_{17} \in M_{(2,6)}$. Por simetria, $h_{13,3}$ não é fracamente bem comportado e $M_{(6,2)}$ naõ é extrema para h_{17}. Segundo,

$$M_{(4,4)} = \begin{pmatrix} z^4 & xz^3 & x^2z^2 \\ xz^3 & x^2z^2 & x^3z \\ x^2z^2 & x^3z & x^4 \end{pmatrix} = \begin{pmatrix} z^4 & h_{18} & h_{19} \\ h_{18} & h_{19} & x^3z \\ h_{19} & x^3z & x^4 \end{pmatrix}.$$

Observe que nem $h_{6,7}$ nem $h_{7,6}$ são fracamente bem comportados, pois $h_{6,6} = h_{19}$. Assim, $M_{(4,4)}$ é extrema para h_{17}. Deste modo, $N_{17} = \widetilde{N}_{17} = 6$, $A_{17} = 7$ e $B_{17} = 10$.

Para $h_{18} = xz^3$ temos $S_{18} = \{xz^3, xy^2\}$, com

$$\mathcal{B}_{18} = \{(1,18),(2,12),(3,10),(5,6),(6,5),(10,3),(12,2),(18,1)\} \cup \{(4,9),(9,4)\}.$$

Como $xy^2 <_t h_{19}$ sabemos, pelo Corolário 2.36, que $\widetilde{N}_{18} = A_{18} = B_{18} = 10$. Analisando $h_{4,9}$ e $h_{9,4}$ vemos que eles são bem comportados. Deste modo, $N_{18} = 10$.

Para $h_{21} = y^3$ temos $S_{21} = \{y^3, x^3y\}$, com

$$\mathcal{B}_{21} = \{(1,21),(4,11),(11,4),(21,1)\} \cup \{(3,16),(7,9),(9,7),(16,3)\}.$$

Observe que para cada $(u,v) \in \mathcal{B}_{21}$ temos que $h_{u,v}$ se encontra em uma submatriz distinta das outras. Deste modo, pela Observação 2.48, $A_{21} = B_{21} = 8$. Os monômios $h_{3,16}$, $h_{7,9}$, $h_{9,7}$ e $h_{16,3}$ não são bem comportados, pois $h_{2,16} = h_{16,2} = h_{6,9} = h_{9,6} = h_{23}$. Deste modo, $N_{21} = \widetilde{N}_{21} = 4$.

Para $h_{24} = y^2z^2$ temos $S_{24} = \{y^2z^2, x^3z^2\}$, com

$$\begin{aligned}\mathcal{B}_{24} = \ & \{(1,24),(2,17),(4,14),(5,11),(8,8),(11,5),(14,4),(17,2),(24,1)\} \\ & \cup\{(3,19),(6,13),(7,12),(12,7),(13,6),(19,3)\}.\end{aligned}$$

Considere as duas submatrizes $M_{(2,8)}$ e $M_{(4,6)}$. Primeiro,

$$M_{(2,8)} = \begin{pmatrix} y^2z^2 & xz^4 & x^2z^3 \\ xy^2z & x^2z^3 & x^3z^2 \end{pmatrix} = \begin{pmatrix} h_{24} & xz^4 & h_{25} \\ xy^2z & h_{25} & x^3z^2 \end{pmatrix}.$$

Note que $h_{3,19} = x^3z^2 \in M_{(2,8)}$ não é fracamente bem comportado, visto que $h_{3,18} = h_{25}$. Além disso, $M_{(2,8)}$ não é extrema para h_{24}, pois $h_{24} \in M_{(2,8)}$. Por simetria, $h_{19,3}$ não é fracamente bem comportado e $M_{(2,8)}$ não é extrema para h_{24}. Segundo,

$$M_{(4,6)} = \begin{pmatrix} z^5 & y^2z^2 & xz^4 & x^2z^3 \\ xz^4 & xy^2z & x^2z^3 & x^3z^2 \\ x^2z^3 & x^2y^2 & x^3z^2 & x^4z \end{pmatrix} = \begin{pmatrix} z^5 & h_{24} & xz^4 & h_{25} \\ xz^4 & xy^2z & h_{25} & x^3z^2 \\ h_{25} & x^2y^2 & x^3z^2 & x^4z \end{pmatrix}.$$

Podemos ver que nem $h_{6,13}$ nem $h_{7,12}$ são fracamente bem comportados, pois $h_{6,12} = h_{25}$. Além disso, $M_{(4,6)}$ não é extrema para h_{24}, pois $h_{24} \in M_{(4,6)}$. Por simetria, $h_{13,6}$ e $h_{12,7}$ não são fracamente bem comportados e $M_{(4,6)}$ não é extrema para h_{24}. Logo, $N_{24} = \widetilde{N}_{24} = A_{24} = 9$ e $B_{24} = 15$.

Para $h_{25} = x^2z^3$ temos $S_{25} = \{x^2z^3, x^2y^2\}$, com $B_{25} = 15$ e $D_{25} = 12$. Como $x^2y^2 <_t h_{26}$, sabemos, pelo Corolário 2.36, que $\widetilde{N}_{25} = A_{25} = B_{25}$. Analisando $h_{4,16}$, $h_{16,4}$ e $h_{9,9}$ vemos que eles são bem comportados, assim, $N_{25} = 15$.

Para $h_{26} = y^3z$ temos $S_{26} = \{y^3z, x^3yz\}$, com

$$\begin{aligned}\mathcal{B}_{26} = \ & \{(1,26),(2,21),(4,17),(8,11),(11,8),(17,4),(21,2),(26,1)\} \\ & \cup\{(3,23),(6,16),(7,15),(9,13),(13,9),(15,7),(16,6),(23,3)\}.\end{aligned}$$

Examinemos as três submatrizes $M_{(2,9)}$, $M_{(4,7)}$ e $M_{(5,6)}$. Primeiro,

$$M_{(2,9)} = \begin{pmatrix} yz^4 & y^3z & xyz^3 & x^2yz^2 \\ xyz^3 & xy^3 & x^2yz^2 & x^3yz \end{pmatrix} = \begin{pmatrix} yz^4 & h_{26} & h_{27} & h_{28} \\ h_{27} & xy^3 & h_{28} & x^3yz \end{pmatrix}.$$

Note que $h_{3,23} = x^3yz \in M_{(2,9)}$ não é fracamente bem comportado, pois $h_{3,22} = h_{28}$, e que $M_{(2,9)}$ não é extrema para h_{26}, uma vez que $h_{26} \in M_{(2,9)}$. Por simetria, $h_{23,3}$ não é fracamente bem comportado e $M_{(9,2)}$ não é extrema para h_{26}. Segundo,

$$M_{(4,7)} = \begin{pmatrix} yz^4 & xyz^3 & x^2yz^2 \\ xyz^3 & x^2yz^2 & x^3yz \\ x^2yz^2 & x^3yz & x^4y \end{pmatrix} = \begin{pmatrix} yz^4 & h_{27} & h_{28} \\ h_{27} & h_{28} & x^3yz \\ h_{28} & x^3yz & x^4y \end{pmatrix}.$$

Observe que nem $h_{6,16}$ nem $h_{7,15}$ são fracamente bem comportados, pois $h_{6,15} = h_{28}$. Consequentemente, $h_{16,6}$ e $h_{15,7}$ não são fracamente bem comportados. Portanto, $M_{(4,7)}$ e $M_{(7,4)}$ são extremas para h_{26}. Terceiro,

$$M_{(5,6)} = \begin{pmatrix} yz^4 & y^3z & xyz^3 & x^2yz^2 \\ xyz^3 & xy^3 & x^2yz^2 & x^3yz \end{pmatrix} = \begin{pmatrix} yz^4 & h_{26} & h_{27} & h_{28} \\ h_{27} & xy^3 & h_{28} & x^3yz \end{pmatrix}.$$

Veja que $M_{(5,6)} = M_{(2,9)}$. Assim, nem $h_{9,13} \in M_{(5,6)}$ nem $h_{13,9} \in M_{(6,5)}$ são fracamente bem comportados, pois $h_{9,12} = h_{28}$. Além disso, nem $M_{(5,6)}$ nem $M_{(6,5)}$ são extremas para h_{26}. Logo, $N_{26} = \widetilde{N}_{26} = 8$, $A_{26} = 10$ e $B_{26} = 16$.

Para $h_{27} = xyz^3$ temos $S_{27} = \{xyz^3, xy^3\}$, com $B_{27} = D_{27} = 16$. Deste modo, $N_{27} = \widetilde{N}_{27} = A_{27} = 16$.

Para $h_{29} = y^2z^3$ temos $S_{29} = \{y^2z^3, x^3z^3\}$, com $B_{29} = 20$ e $D_{29} = 12$. Visto que $x^3z^3 <_t h_{30}$, sabemos, pelo Corolário 2.36, que $\widetilde{N}_{29} = A_{29} = B_{29}$. Note que os monômios $h_{7,22}$, $h_{9,19}$, $h_{6,23}$ e $h_{13,15}$ não são bem comportados, pois $h_{6,22} = h_{8,19} = h_{12,15} = h_{31}$. Por simetria, $h_{22,7}$, $h_{19,9}$, $h_{23,6}$ e $h_{15,13}$ não são bem comportados. Portanto, $N_{29} = D_{29}$.

Para $h_{30} = y^3z^2$ temos $S_{30} = \{y^3z^2, x^3yz^2\}$, com $B_{30} = 24$ e $D_{30} = 12$. Note que para $h_{u,v} = x^3yz^2$, com $(u, v) \in \mathcal{B}_{30}$ e $u \leq v$, temos que $h_{u,v}$ está em uma das

submatrizes $M_{(2,11)}$, $M_{(4,9)}$, $M_{(5,8)}$ ou $M_{(6,7)}$. Além disso,

$$M_{(2,11)} = \begin{pmatrix} y^3z^2 & xyz^4 & x^2yz^3 \\ xy^3z & x^2yz^3 & x^3yz^2 \end{pmatrix} = \begin{pmatrix} h_{30} & xyz^4 & h_{31} \\ xy^3z & h_{31} & x^3yz^2 \end{pmatrix},$$

$$M_{(4,9)} = \begin{pmatrix} yz^5 & y^3z^2 & xyz^4 & x^2yz^3 \\ xyz^4 & xy^3z & x^2yz^3 & x^3yz^2 \\ x^2yz^3 & x^2y^3 & x^3yz^2 & x^4yz \end{pmatrix} = \begin{pmatrix} yz^5 & h_{30} & xyz^4 & h_{31} \\ xyz^4 & xy^3z & h_{31} & x^3yz^2 \\ h_{31} & x^2y^3 & x^3yz^2 & x^4yz \end{pmatrix},$$

$M_{(5,8)} = M_{(2,11)}$ e $M_{(6,7)} = M_{(4,9)}^t = M_{(9,4)}$. Vemos que cada $h_{u,v} = x^3yz^2$, com $(u,v) \in \mathcal{B}_{30}$, não é fracamente bem comportado, visto que $h_{u-1,v} = h_{31}$ ou $h_{u,v-1} = h_{31}$. Assim, nenhuma submatriz é extrema para h_{30}. Logo, $N_{30} = \widetilde{N}_{30} = A_{30} = D_{30}$.

Para $h_{31} = x^2yz^3$ temos $S_{31} = \{x^2yz^3, x^2y^3\}$, com $B_{31} = D_{31} = 24$. Assim, $N_{31} = \widetilde{N}_{31} = A_{31} = 24$.

Para $h_{32} = y^3z^3$ temos $S_{32} = \{y^3z^3, x^3yz^3\}$, com $B_{32} = 32$ e $D_{32} = 16$. Pelo Corolário 2.36 sabemos que $\widetilde{N}_{32} = A_{32} = B_{32}$. Note que os monômios $h_{3,31}$, $h_{9,25}$, $h_{7,27}$, $h_{6,28}, h_{16,18}, h_{15,19}, h_{12,23}$ e $h_{13,22}$ não são bem comportados, uma vez que $h_{2,30} = h_{8,24} = h_{5,26} = h_{14,17} = h_{11,20} = h_{32}$. Deste modo, $N_{32} = 16$.

Resumimos as observações acima na Tabela 3.6.

h_r	1	z	x	y	z^2	xz	x^2	yz
N_r	1	2	2	2	3	4	3	4
$\widetilde{N}_r$	1	2	2	2	3	4	3	4
A_r	1	2	2	2	3	4	3	4
B_r	1	2	2	2	3	4	3	4
h_r	xy	z^3	y^2	xz^2	x^2z	yz^2	xyz	x^2y
N_r	4	4	3	6	6	6	8	6
$\widetilde{N}_r$	4	4	3	6	6	6	8	6
A_r	4	4	5	6	6	6	8	6
B_r	4	4	5	6	6	6	8	6
h_r	y^2z	xz^3	x^2z^2	yz^3	y^3	xyz^2	x^2yz	y^2z^2
N_r	6	10	9	8	4	12	12	9
$\widetilde{N}_r$	6	10	9	8	4	12	12	9
A_r	7	10	9	8	8	12	12	9
B_r	10	10	9	8	8	12	12	15
h_r	x^2z^3	y^3z	xyz^3	x^2yz^2	y^2z^3	y^3z^2	x^2yz^3	y^3z^3
N_r	15	8	16	18	12	12	24	16
$\widetilde{N}_r$	15	8	16	18	20	12	24	32
A_r	15	10	16	18	20	12	24	32
B_r	15	16	16	18	20	24	24	32

Tabela 3.6: Comparação de N_r, $\widetilde{N}_r$, A_r e B_r para cada $h_r \in H$.

Para esta família mostraremos que a estimativa indicativa forte, δ_{A^+}, é uma cota inferior melhor para a distância mínima de $C^{\perp}(I, L)$. Observe que $A_r \neq B_r$ somente para $r = 17$, 24, 26 e 30. Usando o método mencionado na Observação 2.59, mostraremos que para estes quatro casos temos

$$\sum_{(a,b)\in\mathcal{P}_r} posto[S_c]_{(a,b)} \geq B_r,$$

com c satisfazendo $s_r(c) \neq 0$ e $s_v(c) = 0$ para todo $v < r$. Assim, pela Observação 2.59, podemos substituir δ_A por δ_{A^+} no Teorema 2.58.

Suponha $s_{17}(c) \neq 0$ e $s_v(c) = 0$ para todo $v < 17$. Examinando as submatrizes $M_{(2,6)}$ e $M_{(4,4)}$ vemos que cada uma contém duas entradas consistentes com h_{17} cujos índices estão em $\mathcal{B}_{17}$. Assim, pela demonstração do Teorema 2.57, é suficiente mostrar que *posto* $[S_c]_{(2,6)} \geq 2$ e *posto* $[S_c]_{(4,4)} \geq 2$. Para simplificar a notação, denote $s_i(c)$ por s_i e $s_{i,j}(c)$ por $s_{i,j}$. Como $z^4 \in L(\underline{2})$ e $x^3z \in S_{17}$, de $M_{(2,6)}$ obtemos

$$[S_c]_{(2,6)} = \begin{pmatrix} 0 & * & s_{18} & s_{19} \\ s_{18} & s_{3,11} & s_{19} & * \end{pmatrix},$$

onde $*$ indica uma entrada não nula conhecida. Note que para quaisquer valores de s_{18} e s_{19} temos *posto* $[S_c]_{(2,6)} = 2$. Visto que $x^4 \in L(\underline{3})$, obtemos de $M_{(4,4)}$ que

$$[S_c]_{(4,4)} = \begin{pmatrix} 0 & s_{18} & s_{19} \\ s_{18} & s_{19} & * \\ s_{19} & * & 0 \end{pmatrix}.$$

Claramente, as duas últimas linhas são linearmente independentes e *posto* $[S_c]_{(4,4)} \geq 2$. As demais submatrizes $M_{(a,b)} \in \mathcal{C}_{17}$ (ver Definição 2.45) são $M_{(0,8)}$, $M_{(3,5)}$ (as quais contêm somente uma linha) e suas transpostas, assim, *posto* $[S_c]_{(0,8)} =$ *posto* $[S_c]_{(3,5)} = 1$. Portanto,

$$\sum_{(a,b)\in\mathcal{P}_{17}} \textit{posto}\ [S_c]_{(a,b)} \geq 10 = B_{17}.$$

Suponha $s_{24}(c) \neq 0$ e $s_v(c) = 0$ para todo $v < 24$. Examinando $M_{(2,8)}$ e $M_{(4,6)}$ vemos que elas contêm, respectivamente, duas e três entradas consitentes com h_{24} cujos índices estão em $\mathcal{B}_{24}$, com isso, é suficiente mostrar que *posto* $[S_c]_{(2,8)} \geq 2$ e *posto* $[S_c]_{(4,6)} \geq 3$. Como $xz^4 \in L(\underline{6})$ e $x^3z^2 \in S_{24}$, vemos, por $M_{(2,8)}$ que

$$[S_c]_{(2,8)} = \begin{pmatrix} * & 0 & s_{25} \\ s_{3,17} & s_{25} & * \end{pmatrix}.$$

Para quaisquer valores de s_{25} vemos facilmente que *posto* $[S_c]_{(2,8)} = 2$. Como $z^5 \in L(\underline{5})$ e $x^4z \in L(\underline{6})$, de $M_{(4,6)}$ temos

$$[S_c]_{(4,6)} = \begin{pmatrix} 0 & * & 0 & s_{25} \\ 0 & s_{6,11} & s_{25} & * \\ s_{25} & s_{7,11} & * & 0 \end{pmatrix}.$$

Para quaisquer valores de s_{25} temos *posto* $[S_c]_{(4,6)} = 3$. As demais submatrizes $M_{(a,b)} \in \mathcal{C}_{24}$ são $M_{(0,10)}$, $M_{(3,7)}$ (as quais contêm somente uma linha), $M_{(5,5)}$ (de ordem 2×2) e suas transpostas. Logo, *posto* $[S_c]_{(0,10)} =$ *posto* $[S_c]_{(3,7)} = 1$ e *posto* $[S_c]_{(5,5)} \geq 1$. Portanto,

$$\sum_{(a,b)\in\mathcal{P}_{24}} \textit{posto}\ [S_c]_{(a,b)} \geq 15 = B_{24}.$$

Suponha $s_{26}(c) \neq 0$ e $s_v(c) = 0$ para todo $v < 26$. Examinando $M_{(2,9)}$ e $M_{(4,7)}$, vemos que é suficiente mostrar que *posto* $[S_c]_{(2,9)} \geq 2$ e *posto* $[S_c]_{(4,7)} \geq 2$. Visto que $yz^4 \in L(\underline{8})$ e $x^3yz \in S_{26}$, vemos, por $M_{(2,9)}$, que

$$[S_c]_{(2,9)} = \begin{pmatrix} 0 & * & s_{27} & s_{28} \\ s_{27} & s_{3,21} & s_{28} & * \end{pmatrix},$$

logo *posto* $[S_c]_{(2,9)} = 2$. Como $x^4y \in L(\underline{9})$, de $M_{(4,7)}$ obtemos

$$[S_c]_{(4,7)} = \begin{pmatrix} 0 & s_{27} & s_{28} \\ s_{27} & s_{28} & * \\ s_{28} & * & 0 \end{pmatrix},$$

assim, *posto* $[S_c]_{(4,7)} \geq 2$. As demais submatrizes $M_{(a,b)} \in \mathcal{C}_{26}$ são $M_{(0,11)}$, $M_{(3,8)}$ (as quais contêm somente uma linha), $M_{(5,6)} = M_{(2,9)}$ e suas transpostas. Assim, *posto* $[S_c]_{(0,11)} =$ *posto* $[S_c]_{(3,8)} = 1$ e *posto* $[S_c]_{(5,6)} = 2$. Portanto,

$$\sum_{(a,b)\in\mathcal{P}_{26}} \textit{posto}\ [S_c]_{(a,b)} \geq 16 = B_{26}.$$

Suponha $s_{30}(c) \neq 0$ e $s_v(c) = 0$ para todo $v < 30$. Analisando $M_{(2,11)}$ e $M_{(4,9)}$, vemos que é suficiente mostrar que *posto* $[S_c]_{(2,11)} \geq 2$ e *posto* $[S_c]_{(4,9)} \geq 3$. Uma vez

que $xyz^4 \in L(\underline{15})$ e $x^3yz^2 \in S_{30}$, de $M_{(2,11)}$ temos que

$$[S_c]_{(2,11)} = \begin{pmatrix} * & 0 & s_{31} \\ s_{3,26} & s_{31} & * \end{pmatrix},$$

logo, *posto* $[S_c]_{(2,11)} = 2$. Como $yz^5 \in L(\underline{14})$ e $x^4yz \in L(\underline{15})$, obtemos de $M_{(4,9)}$ que

$$[S_c]_{(4,9)} = \begin{pmatrix} 0 & * & 0 & s_{31} \\ 0 & s_{6,21} & s_{31} & * \\ s_{31} & s_{7,21} & * & 0 \end{pmatrix},$$

assim, *posto* $[S_c]_{(4,9)} = 3$. As demais submatrizes $M_{(a,b)} \in \mathcal{C}_{30}$ são $M_{(0,13)}$, $M_{(3,10)}$ (as quais contêm somente uma linha), $M_{(5,8)} = M_{(2,11)}$, $M_{(6,7)} = M_{(4,9)}^t$ e suas transpostas. Logo, *posto* $[S_c]_{(0,13)} =$ *posto* $[S_c]_{(3,10)} = 1$, *posto* $[S_c]_{(5,8)} = 2$ e *posto* $[S_c]_{(6,7)} = 3$. Portanto,

$$\sum_{(a,b)\in\mathcal{P}_{30}} \textit{posto}\ [S_c]_{(a,b)} = 24 = B_{30}.$$

Esta família ajuda a ver as diferenças entre as quatro cotas da distância mínima. Pela Tabela 3.6, constatamos que para quaisquer duas das quatro cotas, existe uma ampla classe de distâncias mínimas designadas para as quais a estimativa indicativa forte pode garantir um código grande. De fato, para cada par de cotas existe pelo menos dois valores de δ para os quais a diferença na dimensão é pelo menos 2.

Exemplo 3.4. Suponha que desejamos um código com distância mínima designada $\delta = 15$. Usando δ_{FR} como a cota inferior, vemos, pelos números N, que o maior código $C^{\perp}(I, L)$ que pode ser construído é quando $L = L(\underline{24}, 26, 29, 30)$, a saber, um $[32, 5, \geq 15]$-código. Por outro lado, se usamos δ_{WFR} ou δ_A, então, para $L = L(\underline{24}, 26, 30)$, obtemos um $[32, 6, \geq 15]$-código. Além disso, note que a estimativa indicativa forte, δ_{A^+}, assegura que, para $L = L(\underline{23})$, temos um $[32, 9, \geq 15]$-código, que pode corrigir 7 erros.

3.4 Outra família de códigos para superfícies não singulares

Seja $\mathcal{F}$ a família de polinômios em $\mathbb{F}_4[x,y,z]$ dada por $\mathcal{F} = \{\beta x^2 z + \beta^2 x z^2 + f(x) + g(y) + h(z) : \beta \in \mathbb{F}_4^* \text{ e } f, g \text{ e } h \text{ são } (\mathbb{F}_4, \mathbb{F}_2) - \textit{polinômios com } gr(g) = 2,\ gr(f) \leq 2 \textit{ e } gr(h) \leq 3\}$. A família $\mathcal{F}$ contém 576 membros, cada um com 32 raízes em $\mathbb{F}_4^3$.

Escolha um $t \in \mathcal{F}$ e seja $I = \langle t \rangle$. Suponha que queremos designar pesos para as variáveis tal que somente x^2z e y^2 tenham peso máximo dentre os monômios no suporte de t. Note que $t \in I_4$, com $lm(t) = x^2z$, $t_1 = x^2t - z(x^4 - x) \in I_4$, com $lm(t_1) = x^2y^2$ e $t_2 = z^3t - x^2(z^4 - z) \in I_4$, com $lm(t_2) = y^2z^3$. Como um resultado,

$$\begin{aligned}\Delta(I_4) = \ & \{x^a y^b z^c : 0 \leq a,b,c \leq 3;\ \textit{se } a \geq 2,\ \textit{então } b \leq 1 \textit{ e } c = 0;\\ & \textit{se } b \geq 2,\ \textit{então } c \neq 3\}.\end{aligned}$$

Observe que para cada monômio em $\Delta(I_4)$, seu correspondente conjunto de consitência é fixo, isto é, o conjunto de consistência é independente da posição do monômio na sequência H. Para obtermos os números indicaticos tão grandes quanto possíveis, o Corolário 2.37 sugere que designemos os pesos (se possível) tais que a sequência W seja estritamente crescente.

Uma tal possibilidade é tomarmos $w(x) = 8$, $w(y) = 9$ e $w(z) = 2$. Então a sequência H é

$$\begin{aligned}H = \ & \{1, z, z^2, z^3, x, y, xz, yz, xz^2, yz^2, xz^3, yz^3, x^2, xy, y^2, xyz, y^2z, xyz^2, y^2z^2,\\ & xyz^3, x^3, x^2y, xy^2, y^3, xy^2z, y^3z, xy^2z^2, y^3z^2, x^3y, xy^3, xy^3z, xy^3z^2\}\end{aligned}$$

e a sequência

$$\begin{aligned}W = \ & \{0, 2, 4, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20,\\ & 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 33, 35, 37, 39\}\end{aligned}$$

é estritamente crescente. Portanto, $A_r = B_r$ e obtemos a Tabela 3.7:

h_r	1	z	z^2	z^3	x	y	xz	yz
A_r	1	2	3	4	2	2	4	4
h_r	xz^2	yz^2	xz^3	yz^3	x^2	xy	y^2	xyz
A_r	6	6	8	8	3	4	7	8
h_r	y^2z	xyz^2	y^2z^2	xyz^3	x^3	x^2y	xy^2	y^3
A_r	11	12	15	16	4	6	10	12
h_r	xy^2z	y^3z	xy^2z^2	y^3z^2	x^3y	xy^3	xy^3z	xy^3z^2
A_r	16	18	22	24	8	16	24	32

Tabela 3.7: Números indicativos para cada $h_r \in H$.

Exemplo 3.5. Para uma distância mínima designada $\delta = 7$, podemos ver que $C^{\perp}(I, L)$, onde $L = L(\underline{10}, 13, 14, 21, 22)$, é um $[32, 18, \geq 7]$-código que pode corrigir 3 erros.

Apêndice A

Alguns resultados de Miura

Feng e Rao apresentaram um eficiente algoritmo de decodificação para códigos algébricos geométricos, indicando que pode-se aumentar a dimensão desses códigos sem diminuir sua capacidade de correção de erros. Tal construção é dita *código geométrico de Goppa melhorado*. Miura observou que os resultados de Feng e Rao podem ser obtidos usando somente álgebra linear. Logo abaixo seguem alguns desses resultados de Miura.

Seja $\omega = \{w_1, \ldots, w_n\}$ uma base de $\mathbb{F}_q^n$. Para $i = 1, \ldots, n$, seja $\mathcal{W}(\underline{i})$ o subespaço linear de $\mathbb{F}_q^n$ gerado por $\{w_1, \ldots, w_i\}$, com $\mathcal{W}(\underline{0}) = \{0\}$ e $\mathcal{W}(\underline{-1}) = \emptyset$. Para $a, b \in \mathbb{F}_q^n$, $ab \in \mathbb{F}_q^n$ denota o produto coordenada a coordenada de n-uplas de $\mathbb{F}_q^n$.

Definição A.1. Um par (w_i, w_j) é dito *bem comportado em relação a* ω se $w_i w_j \in \mathcal{W}(\underline{r})\backslash\mathcal{W}(\underline{r-1})$ para algum r e $w_u w_v \in \mathcal{W}(\underline{r-1})$ para todo $1 \leq u \leq i$, $1 \leq v \leq j$ e $(u, v) \neq (i, j)$.

Um par (w_i, w_j) é dito *fracamente bem comportado em relação a* ω se $w_i w_j \in \mathcal{W}(\underline{r})\backslash\mathcal{W}(\underline{r-1})$ para algum r e $w_u w_j \in \mathcal{W}(\underline{r-1})$ para todo $1 \leq u < i$ e $w_i w_v \in \mathcal{W}(\underline{r-1})$ para todo $1 \leq v < j$.

Definição A.2. Para $r = 1, \ldots, n$, definimos

$$N_r = |\{(w_i, w_j) : (w_i, w_j) \textit{ é bem comportado e } w_i w_j \in \mathcal{W}(\underline{r})\backslash\mathcal{W}(\underline{r-1})\}|$$

e

$$\tilde{N}_r = |\{(w_i, w_j) : (w_i, w_j) \text{ é } fracamente\ bem\ comportado \text{ e } w_i w_j \in \mathcal{W}(\underline{r})\backslash\mathcal{W}(\underline{r-1})\}|.$$

Denotemos por $\mathcal{W}$ um subconjunto próprio de $\omega = \{w_1, \ldots, w_n\}$. Seja $C(\mathcal{W})^{\perp}$ o código dual do código linear gerado pelos elementos de $\mathcal{W}$, $C(\mathcal{W})$.

Definição A.3. Defina

$$\delta_{FR}(\mathcal{W}) := min\{N_r : w_r \notin \mathcal{W}\}$$

e

$$\delta_{WFR}(\mathcal{W}) := min\{\tilde{N}_r : w_r \notin \mathcal{W}\}.$$

Facilmente podemos ver que $\delta_{FR} \leq \delta_{WFR}$, pois bem comportado implica fracamente bem comportado.

Proposição A.4. *A distância mínima de $C(\mathcal{W})^{\perp}$ é maior ou igual a δ_{WFR}.*

Demonstração: Para $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, definimos a matriz

$$S(y) = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \begin{pmatrix} y_1 & & \\ & \ddots & \\ & & y_n \end{pmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}^t$$

Então o peso de y é igual ao posto de $S(y)$ e a entrada (i, j) de $S(y)$ é igual a $< y, w_i w_j >$, onde $<,>$ denota o produto interno usual de $\mathbb{F}_q^n$.

Suponha que $< y, w_1 >= \cdots =< y, w_{r-1} >= 0$ e $< y, w_r > \neq 0$ para algum inteiro positivo r. Se (w_i, w_j) é fracamente bem comportado e $w_i w_j \in \mathcal{W}(\underline{r})\backslash\mathcal{W}(\underline{r-1})$, então a entrada (i, j) de $S(y)$ é diferente de zero, porque $w_i w_j$ é uma combinação linear de $w_1, \ldots, w_r$ e o coeficiente de w_r é não nulo. As entradas (u, j) e (i, v) são nulas para todo $1 \leq u < i$ e $1 \leq v < j$, pois $w_u w_j$ e $w_i w_v$ são combinações lineares de $w_1, \ldots, w_{r-1}$. O número de (w_i, w_j) fracamente bem comportado tal que $w_i w_j \in \mathcal{W}(\underline{r})\backslash\mathcal{W}(\underline{r-1})\}$ é $\tilde{N}_r$. Deste modo, o peso de y (= posto de $S(y)$) é maior ou igual a $\tilde{N}_r$.

Além disso, suponha que y seja uma palavra não nula do código $C(\mathcal{W})^{\perp}$. Então $w_r \notin \mathcal{W}$, o que completa a prova. □

Conclusão

O presente trabalho teve como finalidade apresentar melhoras das cotas de Feng-Rao e de Miura para a distância mínima de códigos definidos sobre uma variedade afim. Para isso estruturamos o texto como a seguir.

No Capítulo 1 apresentamos alguns requisitos para o bom entendimento da dissertação. Definimos códigos lineares e uma classe desses códigos que é a dos códigos cíclicos, bem como uma subclasse destes que são os códigos de Goppa, de onde originou os códigos geométricos de Goppa melhorados descritos no Capítulo 2.

Já no Capítulo 2 definimos códigos sobre uma variedades afim, que são os códigos geométricos de Goppa melhorados, mostramos a cota de Feng-Rao (δ_{FR}), que é uma cota para a distância mínima de tais códigos, depois mostramos uma melhora desta cota, a cota de Miura também dita cota fraca de Feng-Rao (δ_{WFR}) e por fim provamos que a cota indicativa (δ_A) é uma melhora para esta cota e que, quando possível ela pode ser substituída pela estimativa indicativa forte (δ_{A^+}) que, sendo assim, para alguns casos, é uma melhora da cota indicativa.

No último capítulo, o Capítulo 3, descrevemos famílias de códigos para as quais se aplicam as cotas descritas no Capítulo 2 e verificamos através de exemplos que os códigos que têm as melhoras das cotas como cota para a distância mínima são melhores, ou seja, são códigos com mesmo comprimento e mesma distância mínima, porém com dimensão maior, consequentemente, temos um código com mais palavras e satisfazendo os mesmos requisitos.

Com o estudo feito sobre códigos definidos sobre uma variedade afim verificamos que, apesar das cotas já existentes para a distância mínima desses códigos, ainda há

possibilidade de melhorá-lhas e que muito ainda há para ser feito dentro da teoria dos códigos corretores de erros.

Referências Bibliográficas

[1] R. C. Bose and Ray-Chaudhuri, On a class of error-correcting binary group codes, Inform. Control 3 (1960) 68-79.

[2] Code Tables: Bounds on the parameters of various types of codes, database at www.rz.uni-karlsruhe.de/∼kg11/codetables/BKLC/index.html.

[3] D. Eisenbud, Comutative Algebra with a View Toward Algebraic Geometry. Graduate texts in Mathematics, Springer, 1999.

[4] E. R. Fávaro, A. A. de Andrade, Códigos Alternantes e de Goppa, II Jornada de Iniciação Científica. Ibilce-Unesp, São José do Rio Preto, SP.

[5] G. -L. Feng, T. R. N. Rao, Decoding algebraic-geometric codes up to the designed minimum distance, IEEE Trans. Inform. Theory 39 (1993) 37-45.

[6] G. -L. Feng, T. R. N. Rao, Improved geometric goppa codes, Part I: basic theory, IEEE Trans. Inform. Theory 41 (1995) 1678-1693.

[7] V. D. Goppa, A new class of linear error-correcting codes, Probl. Peredach. Inform. 6(3) (1970) 24-30.

[8] D. Gorenstein and N. Zierler, A class of cyclic linear error-correcting codes in p^m symbols, J. Soc. Ind. App. Math. 9 (1961) 107-214.

[9] Griesmer Bound for Linear Codes over Finite Fields, database at www.geocities.com/mars39.geo/griesmer.htm.

[10] A. Hefez, e Maria Lúcia T. Villela, Códigos Corretores de Erros. 1ª edição, Série de Computação e Matemática. IMPA, 2002.

[11] A. Hocquenghem, Codes correcteurs d'erreurs, Chiffres 2 (1959) 147-156.

[12] M. S. Kolluru, G. L. Feng, T. R. N. Rao, Construction of Improved Geometric Goppa Codes from Klein Curves and Kein - like Curves, AAECC 10 (2000) 433-464.

[13] R. Lidl, H. Niederreiter, Encyclopedia of Mathematics and its applications vol 20, Finite Fields. Cambridge, 2003.

[14] S. Ling, C. Xing, Coding Theory, A First Course. Cambridge University Press, 2004.

[15] F. J. Mac Willians, N. J. A. Sloane, The Theory of Error-Correcting, Vol. 16. North-Holland Mathematical Library, 1998.

[16] R. Matsumoto, S. Miura, On the Feng-Rao bound for the $\mathcal{L}$-construction of algebraic geometry codes, IEICE Trans. E83-A (2000) 923-926.

[17] A. M. de Mesquita, Teoria dos Códigos Corretores de Erros, Monografia de Especialização em Matemática. UFG, Goiânia, 2005.

[18] S. Miura, Ph.D. thesis, Univ. Tokyo, May 1997 (Japanese).

[19] S. Miura, Linear codes on affine algebraic varieties, IEICE Trans. J81-A, 10 (1998) 1386-1397 (Japanese).

[20] L. Rédei, Lacunary polynomials over finite fields. North-Holland, Amsterdam, 1973.

[21] I. S. Reed, G. Solomon, Polynomial codes over certain finite fields, SIAM Journal of Applied Math, vol 8. Philadelphia, PA (1960) 300-304.

[22] G. Salazar, D. Dunn, S. B. Graham, An improviment of the Feng-Rao bound on minimum distance, ELSEVIER, Finite Fields and Their Applications 12 (2006) 313-335.

[23] C. E. Shannon, A mathematical theory of communication, Bell Syst. Tech Journal, vol 27 (1948) 379-423, 623-656.

[24] J. H. van Lint, Introduction to Coding Theory, 2^{nd} edition. Springer-Verlag, 1992.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo