RAFAEL AFONSO BARBOSA

Códigos de avaliação a partir de uma perspectiva de códigos de variedades afins

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2013

RAFAEL AFONSO BARBOSA

Códigos de avaliação a partir de uma perspectiva de códigos de variedades afins

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Álgebra.

Orientador: Prof. Dr. Cícero Fernades de Carvalho.

UBERLÂNDIA - MG
2013

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU , MG, Brasil

B238c 2013

Barbosa, Rafael Afonso, 1987-
Códigos de avaliação a partir de uma perspectiva de códigos de variedades afins / Rafael Afonso Barbosa. - 2013.
42 p. : il.

Orientador: Cícero Fernandes de Carvalho.

Dissertação (mestrado) – Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Inclui bibliografia.

1. Matemática - Teses. 2. Códigos de Goppa - Teses. 3. Bases de Gröbner - Teses. 3. Variedades algébricas - Teses. I. Carvalho, Cícero Fernandes de. II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III.Título.

CDU: 51

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 152
Campus Santa Mônica, Uberlândia - MG, CEP 38400-902

ALUNO: Rafael Afonso Barbosa.

NÚMERO DE MATRÍCULA: 11112MAT003.

ÁREA DE CONCENTRAÇÃO: Matemática.

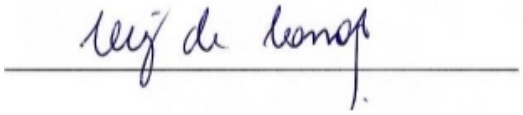
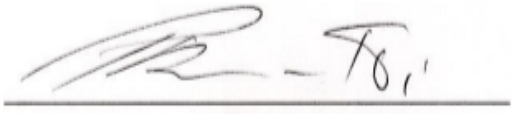
LINHA DE PESQUISA: Álgebra.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Códigos de avaliação a partir de uma perspectiva de códigos de variedades afins.

ORIENTADOR: Prof. Dr. Cícero Fernandes de Carvalho.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 08 de março de 2013, às 14h00min, pela seguinte Banca Examinadora:

NOME	**ASSINATURA**
Prof. Dr. Cícero Fernandes de Carvalho UFU - Universidade Federal de Uberlândia	
Prof. Dr. Paulo Roberto Brumatti UNICAMP - Universidade Estadual de Campinas	
Prof. Dr. Guilherme Chaud Tizziotti UFU - Universidade Federal de Uberlândia	

Uberlândia-MG, 08 de março de 2013.

Dedicatória

A minha família, noiva e amigos que de muitas formas me incentivaram e ajudaram para que fosse possível a concretização deste trabalho. Ao meu orientador, por sua dedicação, competência e profissionalismo.

Agradecimentos

Agradeço à Universidade Federal de Uberlândia pela oportunidade que me foi oferecida, a todos os meus professores pelo conhecimento compartilhado, ao meu orientador, Prof. Dr. Cícero Carvalho, pelos comentários sempre visando o meu amadurecimento, pela paciência e pela oportunidade de aprender com um excelente matemático. Agradeço a minha noiva, Mariana, que de forma especial sempre me deu força e coragem, me apoiando nos momentos de dificuldades.

BARBOSA, R. A. *Códigos de avaliação a partir de uma perspectiva de códigos de variedades afins* 2013. (42) p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Códigos de avaliação (também chamados códigos de domínio de ordem) são tradicionalmente apresentados como códigos de Goppa de um ponto generalizados. Na presente dissertação, vamos estudar um novo ponto de vista sobre códigos de avaliação, introduzindo-os como bons exemplos particulares de códigos de variedades afins. Nosso estudo inclui uma reformulação dos métodos usuais para estimar as distâncias mínimas de códigos de avaliação no conjunto dos códigos de variedades afins. Finalmente descrevemos a conexão com a teoria dos códigos geométricos Goppa de um ponto.

Palavras-chave: (Variedades afins, Códigos de Goppa, Bases de Gröbner).

BARBOSA, R. A. *Evaluation Codes from an Affine Variety Codes Perspective* 2013. (42 p.) p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

Evaluation codes (also called order domain codes) are traditionally introduced as generalized one point geometric Goppa codes. In the present dissertation we will give a new point of view on evaluation codes by introducing them instead as particular nice examples of affine variety codes. Our study includes a reformulation of the usual methods to estimate the minimum distances of evaluation codes into the setting of affine variety codes. Finally we describe the connection to the theory of one point geometric Goppa codes.

Keywords: (Affine variety, Goppa codes, Gröbner basis).

Sumário

Introdução

Ao longo dos anos a teoria dos códigos de Goppa tem produzido muitos resultados interessantes. Algumas desvantages é que os códigos são frequentemente descritos teoricamente e que as matrizes geradoras concretas e matrizes checagem de paridade são frequentementes não apresentadas. Como uma tentativa para simplificar a descrição de códigos geométricos de Goppa de um ponto e dar suporte para uma fácil generalização de tais códigos para objetos com dimensões maiores que curvas, Hoholdt, Vanlint e Pelikan fundaram a teoria de domínios de ordem em [10]. Os códigos definidos a partir de domínios de ordem são frequentemente chamados de códigos de avaliação ou códigos de domínios de ordem. A distância mínima e a grande maioria dos pesos generalizados de Hamming de códigos de avaliação podem ser encontrados aplicando uma de duas cotas que dependem apenas de uma teoria relativamente simples.

Apesar dos códigos de avaliação terem suas origens em estudos de códigos geométricos de Goppa neste trabalho nós vamos estudar como virar as coisas de cabeça para baixo e introduzi-los como bons exemplos particulares da teoria dos códigos de variedades afins. Isto adiciona uma nova perspectiva para a teoria dos códigos de avaliação bem como para a teoria dos códigos de variedades afins.

Rafael Afonso Barbosa
Uberlândia-MG, 08 de março de 2013.

Capítulo 1

Códigos de variedades afins

Códigos de variedades afins foram introduzidos por Fitzgerald e Lax em [6]. Seja $\mathbb{F}_q$ um corpo finito com q elementos e $\mathbb{F}_q[X_1, \cdots, X_m]$ o anel de plinômios com coeficientes em $\mathbb{F}_q$. A definição de códigos precisa de um ideal $I \subseteq \mathbb{F}_q[X_1, \cdots, X_m]$ a partir do qual nós começamos definindo

$$I_q = I + \langle X_1^q - X_1, \cdots, X_m^q - X_m \rangle \tag{1.1}$$

$$R_q = \mathbb{F}_q[X_1, \cdots, X_m]/I_q = \{F + I_q \mid F \in \mathbb{F}_q[X_1, \cdots, X_m]\} \tag{1.2}$$

onde $F + I_q = \overline{F}$ é a classe determinada por F.

Seja

$$V = \{P_1, \cdots, P_n\} = \mathcal{V}_{\mathbb{F}_q}(I_q) = \mathcal{V}_{\overline{\mathbb{F}}_q}(I_q)$$

sendo o conjunto dos pontos de $\mathbb{F}_q^m$ que anulam todos os polinômios de I_q. A última igualdade é devido ao fato de que os elementos de $\overline{\mathbb{F}_q}$ que são raízes de $X_i^q - X_i,\ i = 1, \cdots, n$, são os elementos de $\mathbb{F}_q$. Aqui, $\overline{k}$ significa o fecho algébrico do corpo k e $P_i \neq P_j$ para $i \neq j$. Definimos uma aplicação $\mathbb{F}_q$-linear $ev : R_q \to \mathbb{F}_q^n$ por

$$ev(F + I_q) = (F(P_1), \cdots, F(P_n)).$$

Nós vamos chamar esta aplicação de aplicação avaliação. Escrevendo $P_j = (P_j^{(1)}, \cdots, P_j^{(m)})$ para $j = 1, \cdots, n$. Definimos para cada $i = 1, \cdots, n$ o polinômio

$$G_i = \left(\prod_{s=1,\cdots,m} \prod_{j=1,\cdots,n; P_j^{(s)} \neq P_i^{(s)}} (X_s - P_j^{(s)}) \right)$$

temos então que $G_i(P_i) \neq 0$, pois $G_i(P_i)$ é o produto de fatores $P_i^{(s)} - P_j^{(s)}$, todos diferentes de zero já que estamos considerando apenas os $P_j^{(s)} \neq P_i^{(s)}$. Por outro lado, $G_i(P_j) = 0,\ \forall i \neq j$. De fato, como $P_i \neq P_j,\ \forall i \neq j$, temos $P_j^{(r)} \neq P_i^{(r)}$, para algum $1 \leq r \leq m$, então o fator $X_r - P_j^{(r)}$ aparece em G_i. Portanto,

$$ev\left(G_i + I_q\right)$$

é diferente de zero na i-ésima entrada, enquanto que todas as outras entradas são iguais a zero. Assim, $\dfrac{G_i}{G_i(P_i)} + I_q \in R_q$ e

$$ev\left(\frac{G_i}{G_i(P_i)} + I_q\right) = e_i$$

onde e_i é o vetor da base canônica de $\mathbb{F}_q^n$ que tem 1 na i-ésima entrada e 0 nas demais. Consequentemente, a aplicação ev é sobrejetiva. Nossa próxima prova é de que ev é também injetiva. Para isso nós primeiro recordamos de [2, Pro. 8.14] que se J é um ideal em um anel polinomial $k[X_1, \cdots, X_m]$ onde k é perfeito e J contém um polinômio de uma variável livre de quadrados em cada variável então J é um ideal radical. Isto torna I_q radical, pois como todo corpo finito é perfeito,

$\mathbb{F}_q$ é perfeito, e $X_i^q - X_i$ é livre de quadrados para todo $i = 1, \cdots, n$. Em seguida nós recordamos que o Teorema dos zeros de Hilbert forte [3, Th. 6, Sec. 4.2] diz que se $J \subseteq k[X_1, \cdots, X_m]$ é radical então o ideal anulador da variedade $\mathcal{V}_{\bar{k}}(J)$ é o próprio J. Logo, $I(\mathcal{V}_{\overline{\mathbb{F}}_q}(I_q)) = \sqrt{I_q} = I_q$. Como $V = \mathcal{V}_{\mathbb{F}_q}(I_q) = \mathcal{V}_{\overline{\mathbb{F}}_q}(I_q)$ temos $I(\mathcal{V}_{\mathbb{F}_q}(I_q)) = I_q$, assim se $\overline{F} \in Ker(ev)$ temos que $\overline{F} \in R_q$ com $ev(\overline{F}) = 0$, daí $(F(P_1), \cdots, F(P_n)) = (0, \cdots, 0)$, então F zera em todos os pontos de V. Segue que, $F \in I(V) = I_q$ e $\overline{F} = \overline{0}$. Portanto, $Ker(ev) = \{\overline{0}\}$. Consequentemente a aplicação ev é injetiva. Nós acabamos de mostrar que ev é um isomorfismo de espaços vetorias. Podemos definir agora os códigos de varidade afim.

Definição 1.1 *Seja I_q e R_q como definido anteriormente e assuma que L é um $\mathbb{F}_q$-subespaço vetorial de R_q. Definimos o código de varidade afim $C(I, L) = ev(L)$, e o código de varidade afim $C(I, L)^\perp$ como sendo o complemento ortogonal de $C(I, L)$ com respeito ao produto interno usual de $\mathbb{F}_q^n$. Isto é,*

$$C(I, L)^\perp = \{c \mid c.ev(F + I_q) = 0, \forall F + I_q \in L\}$$

onde $f.h$ denota o produto interno de f e h.

Capítulo 2

Algumas ferramentas da teoria das bases de Gröbner

Nesta seção nós apresentamos algumas ferramentas da teoria das bases de Gröbner que serão muito úteis na construção de códigos de variedades afins. Tais ferramentas irão também nos ajudar a estimar os parâmetros dos códigos. Nós começamos recordando o conceito de pegada.

Definição 2.1 *Seja $J \subseteq k[X_1, \cdots, X_m]$ um ideal e seja $\prec$ uma ordenação monomial fixada. Denote por $\mathcal{M}(X_1, \cdots, X_m)$ os monômios nas variáveis $X_1, \cdots, X_m$. A pegada de J com respeito a $\prec$ é o conjunto*

$$\Delta_{\prec}(J) = \{M \in \mathcal{M}(X_1, \cdots, X_m) \mid M \text{ não é o monômio líder de nenhum polinômio em } J\}$$

Dado um cojunto de geradores para o ideal J pode não ser óbvio a primeira vista qual é a pegada. Entretanto, todo ideal polinômial possui um tipo particular de conjuto de geradores a partir do qual a pegada pode ser facilmente determinada. Estas são as bases de Gröbner.

Definição 2.2 *Seja $J \subseteq k[X_1, \cdots, X_m]$ um ideal e $\prec$ uma ordenação monomial. Um subconjunto finito $\mathcal{G}$ de J é chamado de base de Gröbner (com respeito a $\prec$) se para cada polinômio $P(X_1, \cdots, X_m) \in J$ existe um $G \in \mathcal{G}$ tal que o monômio líder de G divide o monômio líder de P.*

Um dos resultados mais importantes na teoria das base de Gröbner é que uma base de Gröbner $\mathcal{G}$ para J é de fato uma base para J. Dada uma base para J nós podemos extendê-la para uma base de Gröbner aplicando o algoritmo de Buchberger. Consequentemente, existe um método para detectar a pegada $\Delta_{\prec}(J)$.

O próximo par de resultados explica nosso interesse na pegada de [3, Prop. 4, sec. 5.3] nós temos a proposição abaixo.

Proposição 2.1 *Considerando a notação como na definição 2.1. O conjunto*

$$\{M + J \mid M \in \Delta_{\prec}(J)\} \tag{2.1}$$

constitui uma base $k[X_1, \cdots, X_m]/J$ como espaço vetorial

Demonstração. Ao longo deste capítulo vamos fazer uso extensivamento do algoritmo da divisão para polinômios multivariáveis [3, sec 2.3]. Dada uma ordem monomial, um polinômio H e uma lista ordenada de polinômios $(G_1, \cdots, G_r)$ o algoritmo calcula o resto H módulo $(G_1, \cdots, G_r)$. Este resto é escrito H rem $(G_1, \cdots, G_r)$. Quando $\mathcal{G} = \{G_1, \cdots, G_r\}$ constitui uma base de Gröbner (para o ideal $\langle G_1, \cdots, G_r \rangle$) o resto não depende da forma como nós ordenamos os elementos da lista $(G_1, \cdots, G_r)$ e portanto neste caso nós vamos simplesmente dizer resto de H módulo $\mathcal{G}$. Nós observamos que para escrever um elemento $H + J \in k[X_1, \cdots, X_m]/J$ como uma combinação linear dos elementos de $\{M + J \mid M \in \Delta_{\prec}(J)\}$ nós precisamos somente achar o resto de H módulo a base de Gröbner $\mathcal{G}$. De

fato, do algoritmo da divisão temos que $H = g + r$ com $g \in J$ e $r = 0$ ou $r = \alpha_1 M_1 + \cdots + \alpha_s M_s$ é uma combinação com coeficientes em k, de monômios que não são divisíveis pelo monômio líder de nenhum dos $G_i's$. Isto é, $M_1, \cdots, M_s \in \Delta_\prec(J)$. Como $\mathcal{G}$ é base de Gröbner r é único. Então $\overline{H} = \overline{0}$ ou $\overline{H} = \alpha_1\overline{M_1} + \cdots \alpha s\overline{M_s}$. Portanto, H é combinação linear de termos em (2.1). Mostremos agora a independência linear. Seja $\alpha_1\overline{M_1} + \cdots + \alpha_t\overline{M_t} = \overline{0}$ uma combinação linear nula de termos em (2.1). Daí, $\overline{\alpha_1 M_1 + \cdots + \alpha_t M_t} = \overline{0}$. Logo, $M = \alpha_1 M_1 + \cdots + \alpha_t M_t \in J$, então o resto da divisão de M por $\mathcal{G}$ é 0. Por outro lado, como os $M_i's \in \Delta_\prec(J)$ eles vão para o resto quando aplicamos o algoritmo da divisão em M e $\mathcal{G}$. Assim, temos a igualdade polinomial $\alpha_1 M_1 + \cdots + \alpha_t M_t = 0$. Portanto, $\alpha_i = 0$, $\forall i = 1, \cdots, t$. ■

Como uma consequência da proposição 2.1 e da definição da base de Gröbner, H rem $\mathcal{G}$ é o mesmo não importa qual a base de Gröbner é escolhida para J enquanto $\prec$ é fixa. De fato, seja $\mathcal{G}_1$ e $\mathcal{G}_2$ bases de Gröbner distintas de J. Como vimos na demonstração da proposição anterior $\overline{H} = \overline{r_1}$ e $\overline{H} = \overline{r_2}$ onde $r_1 = H\ rem\ \mathcal{G}_1$ e $r_2 = H\ rem\ \mathcal{G}_2$. Daí, $\overline{r_1} = \overline{r_2}$ e $\overline{r_1 - r_2} = \overline{0}$. Logo, $r_1 - r_2 \in J$. Pela definição de base de Gröbner existe um polinômio $G_1 \in \mathcal{G}_1$ tal que $lm(G_1) \mid lm(r_1 - r_2)$. Agora, pelo algoritmo da divisão nenhum monômio de r_1 é divisível por $lm(G_1)$, então se $r_1 - r_2 \neq 0$ necessariamente temos que $lm(r_1 - r_2)$ é um monômio de r_2. Por outro lado, como $\mathcal{G}_2$ também é base de Gröbner, temos que existe $G_2 \in \mathcal{G}_2$ tal que $lm(G_2) \mid lm(r_1 - r_2)$. Absurdo, pois novamente pelo algoritmo da divisão nenhum monômio de r_2 é divisível por $lm(G_2)$. Portanto, $r_1 - r_2 = 0$ e $r_1 = r_2$.

Aplicando a teoria acima para o caso $R_q = \mathbb{F}_q[X_1, \cdots, X_m]/I_q$ nós vemos que para cada escolha fixa de $\prec$ a proposição 2.1 nos dá uma base $\{M + I_q \mid M \in \Delta_\prec(I_q)\}$ para R_q. Se $\{B_1 + I_q, \cdots, B_{dim(L)} + I_q\}$ é uma base para um subespaço $L \subseteq R_q$ nós podemos, portanto, sem perda de generalidade, assumir que $Supp(B_1), \cdots, Supp(B_{dim(L)}) \subseteq \Delta_\prec(I_q)$. Onde, $Supp(F) = \{M \mid M\ é\ monômio\ de\ F\}$ significa suporte de F. De fato, seja $\mathcal{G}$ uma base de Gröbner de I_q. Se $Supp(B_i) \nsubseteq \Delta_\prec(I_q)$ para algum $i = 1, \cdots, dim(L)$, então existe um monômio M de B_i que é monômio líder de algum polinômio em I_q. Portanto, M é divisível pelo monômio líder de algum polinômio $g \in \mathcal{G}$. Logo, podemos dividir B_i por $\mathcal{G}$,

$$B_i = \alpha g + r\ e\ \overline{B_i} = \overline{r}$$

com $Supp(r) \subseteq \Delta_\prec(I_q)$. Portanto, basta trocar B_i por r. Uma vez que a variedade $\mathcal{V}_{\mathbb{F}_q}(I_q) = \{P_1, \cdots, P_n\}$ é encontrada nós podemos então facilmente especificar a matriz geradora para $C(I, L)$, bem como especificar facilmente a matriz checagem de paridade para $C(I, L)^\perp$. O comprimento do código é

$$n = \#\mathcal{V}_{\mathbb{F}_q}(I_q) = \#\mathcal{V}_{\mathbb{F}_q}(I) = \#\Delta_\prec(I_q)$$

Onde a última igualdade vem do fato de ev ser um isomorfismo, $dim(R_q) = n$, e pela proposição 2.1 $dim(R_q) = \#\Delta_\prec(I_q)$. Novamente, ev é isomorfimo, então a dimensão de $C(I, L)$ é $dim(L)$ enquanto que a dimensão de $C(I, L)^\perp$ é igual a $n - dim(L)$. O que resta é estimar a distância mínima dos códigos. Isto será feito na seção 3 e seção 4 abaixo. Na seção 3 nós vamos precisar de um corolário da Proposição 2.1. Isto é uma incidência da mais geral cota da pegada [4, Cor. 2.5, Sec 4.2]

Corolário 2.1 *Seja $F_1, \cdots, F_s \in \mathbb{F}_q[X_1, \cdots, X_m]$. O número de zeros comuns de $F_1, \cdots, F_s$ sobre $\mathbb{F}_q$ é $\#\Delta_\prec(\langle F_1, \cdots, F_s, X_1^q - X_1, \cdots, X_m^q - X_m\rangle)$(Aqui $\prec$ é uma ordem monomial qualquer).*

Demonstração. Defina $I = \langle F_1, \cdots, F_s \rangle$, assim

$$I_q = I + \langle X_1^q - X_1, \cdots, X_m^q - X_m \rangle \;=\; \langle F_1, \cdots, F_s, X_1^q - X_1, \cdots, X_m^q - X_m \rangle \,.$$

Seja $n = \#\mathcal{V}_{\mathbb{F}_q}(I_q)$ o número de zeros comuns. Como explicado na seção anterior, R_q é isomorfo a $\mathbb{F}_q^n$ como espaço vetorial sobre $\mathbb{F}_q$ sob o isomorfismo ev. Pela Proposição 2.1 a dimensão de R_q é $\#\Delta_\prec(I_q)$, o que conclui a prova. ■

Capítulo 3

Uma cota para distância mínima de $C(I, L)$

Nós agora estimamos a distância mínima de $C(I, L)$. A cota que apresentamos pode ser vista como uma interpretação da cota em [1,Th.8]. Seja $\prec$ e $I \subseteq \mathbb{F}_q[X_1, \cdots, X_m]$ fixos e considere um subespaço $L \subseteq R_q$.

Definição 3.1 *Uma base* $\{B_1 + I_q, \cdots, B_{dim(L)} + I_q\}$ *para o subespaço* $L \subseteq R_q$ *onde* $Supp(B_i) \subseteq \Delta_\prec(I_q)$ *para* $i = 1, \cdots, dim(L)$ *e* $lm(B_1) \prec \cdots \prec lm(B_{dim(L)})$ *é dita ser bem comportada com respeito a* $\prec$. *Aqui* $lm(F)$ *significa o monômio lider de* F.

Usando eliminação Gaussiana qualquer base de L pode ser transformada em uma base da forma acima. Isto é, se $\{B_1 + I_q, \cdots, B_{dim(L)} + I_q\}$ é base de L, quando escalonamos a matriz $dim(L) \times m$, formada pelos coeficientes de cada B_i na linha i, encontramos uma nova matriz $dim(L) \times m$ tal que o conjunto dos polinômios formados pelos coeficientes de cada linha i ainda é uma base de L e não contêm monômios de mesmo grau.

Para $\prec$ fixa, a sequência $(lm(B_1), \cdots, lm(B_{dim(L)}))$ é a mesma para todas as escolhas de bases bem comportadas de L. De fato, sejam

$$\{B_1 + I_q, \cdots, B_{dim(L)} + I_q\} \text{ e } \left\{B_1' + I_q, \cdots, B_{dim(L)}' + I_q\right\}$$

bases distintas e bem comportadas de L. Como $\overline{B_i} \in L, \forall i = 1, \cdots, dim(L)$ temos que para cada i existem $\lambda_1^i, \cdots, \lambda_{dim(L)}^i \in \mathbb{F}_q$ tais que $\overline{B}_i = \lambda_1^i \overline{B_1'} + \cdots + \lambda_{dim(L)}^i \overline{B_{dim(L)}'}$. Então $lm(B_i) = lm(B_j')$, $\forall i, j = 1, \cdots, dim(L)$, segue que o conjunto $\{lm(B_i) \mid i = 1, \cdots, dim(L)\}$ é igual ao conjunto $\{lm(B_j') \mid j = 1, \cdots, dim(L)\}$. Logo, como $\prec$ é fixa temos que a sequência $(lm(B_1), \cdots, lm(B_{dim(L)}))$ é igual a a sequência $(lm(B_1'), \cdots, lm(B_{dim(L)}'))$. Portanto, a definição abaixo faz sentido.

Definição 3.2 *Seja* L *um subespaço de* R_q *e defina*

$$\square_\prec(L) = \{lm(B_1), \cdots, lm(B_{dim(L)})\}$$

onde $\{B_1 + I_q, \cdots, B_{dim(L)+I_q}\}$ *é qualquer base bem comportada de* L *com respeito a* $\prec$.

Definição 3.3 *Seja* $\mathcal{G}$ *uma base de Gröbner para* I_q *com respeito a* $\prec$. *Um par de monômios ordenados* (M_1, M_2), $M_1, M_2 \in \Delta_\prec(I_q)$ *é bem comportado em uma direção* (OWB) *se* $\forall H$ *com* $Supp(H) \subseteq \Delta_\prec(I_q)$ *e* $lm(H) = M_1$ *tem-se*

$$lm(M_1 M_2 \; rem \; \mathcal{G}) = lm(H M_2 \; rem \; \mathcal{G}).$$

Como já mencionamos, F rem $\mathcal{G} = F$ rem $\mathcal{G}'$ se $\mathcal{G}$ e $\mathcal{G}'$ são base de Gröbner para I_q com respeito a mesma ordenação. Portanto, a definição de OWB é independente de qual base de Gröbner nós consideramos, enquanto $\prec$ é fixa.

Teorema 3.1 *Seja $\prec$ fixa. Para cada $P \in \square_{\prec}(L)$ defina*

$$S(P) = \{K \in \Delta_{\prec}(I_q) \mid \exists N \in \Delta_{\prec}(I_q) \text{ de tal modo que (P,N) é OWB e } lm(PN \ rem \ \mathcal{G}) = K\}.$$

A distância mínima de $C(I, L)$ é pelo menos

$$min\{\#S(P) \mid P \in \square_{\prec}(L)\}.$$

Demonstração. Seja $\vec{c} \in C(I, L)$ e $\mathcal{B} = \left\{B_1 + I_q, \cdots, B_{dim(L)} + I_q\right\}$ uma base bem comportada de L. Então existe um $\overline{F} \in L$ tal que $\vec{c} = ev(\overline{F})$, com $\overline{F}$ combinação linear dos elementos de $\mathcal{B}$. Segue da definição de base bem comportada que $Supp(F) \subseteq \Delta_{\prec}(I_q)$ e da definição do $\square_{\prec}(L)$ que $lm(F) = P \in \square_{\prec}(L)$, pois $lm(F)$ é o monômio líder de algum elemento de $\mathcal{B}$. Pelo corolário 2.1 o número de zeros comuns de $I_q + \langle F\rangle$ é $\#\Delta_{\prec}(I_q + \langle F\rangle)$. Sabemos que os zeros de I_q são $\{P_1, \cdots, P_n\} = \mathcal{V}_{\mathbb{F}_q}(I_q)$, então os zeros comuns de $I_q + \langle F\rangle$ são os $P_i's \in \mathcal{V}_{\mathbb{F}_q}(I_q)$ que zeram F. Portanto, $\#\Delta_{\prec}(I_q + \langle F\rangle) = \#\{P_i \in \mathcal{V}_{\mathbb{F}_q}(I_q) \mid F(P_i) = 0\}$. Como $\vec{c} = (F(P_1), \cdots, F(P_n))$ tem n coordenadas, das quais $\#\Delta_{\prec}(I_q + \langle F\rangle)$ são zero, temos que o peso de Hamming de $\vec{c}$ é igual a $n - \#\Delta_{\prec}(I_q + \langle F\rangle)$. Vamos então olhar mais de perto $\Delta_{\prec}(I_q + \langle F\rangle)$. Se $N, K \in \Delta_{\prec}(I_q)$ satisfaz que (P, N) é OWB e $lm(PN \ rem \ \mathcal{G}) = K$ então

$$K \in \Delta_{\prec}(I_q) \setminus \Delta_{\prec}(I_q + \langle F\rangle).$$

De fato, sabemos que $Supp(F) \subseteq \Delta_{\prec}(I_q)$ e $lm(F) = P$, como (P, N) é OWB segue que $lm(FN \ rem \ \mathcal{G}) = lm(PN \ rem \ \mathcal{G}) = K$. Aplicando o algoritmo da divisão em FN e $\mathcal{G}$ temos $FN = Q + FN \ rem \ \mathcal{G}$, com $Q \in I_q$. Assim, claramente $FN \ rem \ \mathcal{G} = FN - Q \in I_q + \langle F\rangle$. Logo, $FN \ rem \ \mathcal{G}$ é um polinômio de $I_q + \langle F\rangle$ com $lm(FN \ rem \ \mathcal{G}) = K$. Portanto, $K \notin \Delta_{\prec}(I_q + \langle F\rangle)$. Consequentemente,

$$\begin{aligned}\#\Delta_{\prec}(I_q + \langle F\rangle) \leq \#\Delta_{\prec}(I_q) - \#\{K \in \Delta_{\prec}(I_q) \mid \exists N \in \Delta_{\prec}(I_q) \\ \text{de tal modo que (P,N) é OWB e } lm(PN \ rem \ \mathcal{G}) = K\}\end{aligned} \tag{3.1}$$

Como $n = \#\Delta_{\prec}(I_q)$, temos

$$\begin{aligned}\#\Delta_{\prec}(I_q + \langle F\rangle) \leq n - \#\{K \in \Delta_{\prec}(I_q) \mid \exists N \in \Delta_{\prec}(I_q) \\ \text{de tal modo que (P,N) é OWB e } lm(PN \ rem \ \mathcal{G}) = K\}\end{aligned} \tag{3.2}$$

equivalentemente,

$$\begin{aligned}n - \#\Delta_{\prec}(I_q + \langle F\rangle) \geq \#\{K \in \Delta_{\prec}(I_q) \mid \exists N \in \Delta_{\prec}(I_q) \\ \text{de tal modo que (P,N) é OWB e } lm(PN \ rem \ \mathcal{G}) = K\}\end{aligned} \tag{3.3}$$

Mas $w(\vec{c}) = n - \#\Delta_{\prec}(I_q + \langle F\rangle)$, então

$$\begin{aligned}w(\vec{c}) \geq \#\{K \in \Delta_{\prec}(I_q) \mid \exists N \in \Delta_{\prec}(I_q) \text{ de tal modo que} \\ \text{(P,N) é OWB e } lm(PN \ rem \ \mathcal{G}) = K\}.\end{aligned} \tag{3.4}$$

Portanto o peso de Hamming de $\vec{c}$ é pelo menos

$$\#\{K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q) \text{ de tal modo que (P,N) é OWB e } lm(PN \ rem \ \mathcal{G}) = K\}$$

■

É claro que é possível aplicar o teorema 3.1 para diferentes escolhas de $\prec$ para ver qual delas dá a estimativa mais precisa. O corolário seguinte se aplica facilmente para qualquer código de variedade afim. Esta cota também pode ser aplicada para diferentes escolhas de $\prec$ para obter a estimativa mais precisa.

Corolário 3.1 *Seja $\prec$ fixa. A ditância mínima de $C(I, L)$ é pelo menos*

$$min\left\{\#\left\{K \in \Delta_\prec(I_q) \mid P \text{ divide } K\right\} \mid P \in \square_\prec(L)\right\}. \tag{3.5}$$

Demonstração. Sejam K, P como acima. Observe que $\frac{K}{P} \in \Delta_\prec(I_q)$, pois se $\frac{K}{P} \notin \Delta_\prec(I_q)$ então $\frac{K}{P}$ seria o monômio líder de algum polinômio $Q \in I_q$, isto é, $lm(Q) = \frac{K}{P}$. Claramente, $lm(QP) = K$. Assim, $QP \in I_q$ e $lm(QP) = K$. Portanto $K \notin \Delta_\prec(I_q)$. O que é absurdo. Para ver que $(P, \frac{K}{P})$ é OWB tome H sendo um polinômio com $lm(H) = P$ e $Supp(H) \subseteq \Delta_\prec(I_q)$. Claramente, o monômio lider de $H\frac{K}{P}$ é igual a K. O algoritmo da divisão quando aplicado em $H\frac{K}{P}$ e $\mathcal{G}$, começa movendo K para o resto. Isto é devido a $K \in \Delta_\prec(I_q)$. Quando nós executamos o algoritmo da divisão todos os outros termos A de $H\frac{K}{P}$ são movidos para o resto, e são substituídos por polinômios S de tal modo que $lm(S) \prec lm(A)$ acontece, ou são substituídos com 0. Assim,

$$lm\left(H\frac{K}{P} \ rem \ \mathcal{G}\right) = K = lm(P\frac{K}{P} \ rem \ \mathcal{G})$$

Portanto,

$$\{K \in \Delta_\prec(I_q) \mid P \text{ divide } K\} \subseteq \{K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q) \text{ de tal modo que (P,N) é OWB e } lm(PN \ rem \ \mathcal{G}) = K\}, \ \forall P \in \square_\prec(L)$$

então

$$\#\{K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q) \text{ de tal modo que (P,N) é OWB e } lm(PN \ rem \ \mathcal{G}) = K\} \geq \#\left\{K \in \Delta_\prec(I_q) \mid P \text{ divide } K\right\}, \ \forall P \in \square_\prec(L)$$

.

Logo, o teorema 3.1 garante que a distância mínima de $C(I, L)$ é pelo menos

$$min\left\{\#\left\{K \in \Delta_\prec(I_q) \mid P \text{ divide } K\right\} \mid P \in \square_\prec(L)\right\}$$

■

Observação 3.1 *É possível modificar o teorema 3.1 e o corolário 3.1 para lidar também com pesos generalizados de Hamming. Para o caso do teorema 3.1 isto corresponde a interpretação de cota em [1, Th. 10].*

Exemplo 3.1 *Seja* $I = \langle 0 \rangle \subseteq \mathbb{F}_q[X_1, \cdots, X_m]$. *Então*

$$\mathcal{G} = \{X_1^q - X_1, \cdots, X_m^q - X_m\},$$

é fácil ver que $\mathcal{G}$ *é uma base de Gröbner para* I_q *(independente da ordenação* $\prec$ *escolhida). Consequetemente*

$$\Delta_\prec(I_q) = \left\{X_1^{i_1} \cdots X_m^{i_m} \mid 0 \leq i_1 < q, \cdots, 0 \leq i_m < q\right\}$$

e pela proposição 2.1 temos que

$$\left\{X_1^{i_1} \cdots X_1^{i_m} + I_q \mid 0 \leq i_1 < q, \cdots, 0 \leq i_m < q\right\}$$

é base para $R_q = \mathbb{F}_q[X_1, \cdots, X_m]/I_q$ *como espaço vetorial sobre* $\mathbb{F}_q$. *Segue o código de variedade afim correspondente é de comprimento* $n = \#\Delta_\prec(I_q) = q^m$. *Seja* s *um inteiro* $0 \leq s \leq m(q-1)$. *Se nós escolhemos* L *sendo o espaço vetorial gerado pelos elementos da base* $X_1^{i_1} \cdots X_m^{i_m} + I_q$ *com* $i_1 + \cdots + i_m \leq s$ *então nós temos*

$$L = \{F(X_1, \cdots, X_m) + I_q \mid grau(F) \leq s\} \tag{3.6}$$

Aqui, $grau(F)$ *siginifica o grau total de* F. *Observe que,*

$$\square_\prec(L) = \left\{X_1^{i_1} \cdots X_m^{i_m} \mid 0 \leq i_q < q, \cdots, 0 \leq i_m < q, i_1 + \cdots + i_m \leq s\right\}.$$

De fato, $\mathcal{B} = \left\{X_1^{i_1} \cdots X_m^{i_m} \mid 0 \leq i_q < q, \cdots, 0 \leq i_m < q, i_1 + \cdots + i_m \leq s\right\}$ *gera* L *por definição, é subconjunto de um conjunto LI , a base de* R_q, *portanto LI e pelo mesmo fato não possui dois elementos iguais, logo* $lm(B_1) \prec \cdots \prec lm(B_{dim(L)})$, *onde os* $B_i's$ *são os elementos de* $\mathcal{B}$. *O código* $C(I, L)$ *é conhecido como código generalizado de Reed-Muller* $RM_q(s, m)$, *e o corolário 3.1 nos diz que a distância mínima de* $RM_q(s, m)$ *é pelo menos*

$$min\left\{\#\left\{K \in \Delta_\prec(I_q) \mid P \; divide \; K\right\} \mid P \in \square_\prec(L)\right\}$$

isto é,

$$min\left\{\#\left\{X_1^{j_1} \cdots X_m^{j_m} \in \Delta_\prec(I_q) \mid X_1^{i_1} \cdots X_m^{i_m} \; divide \; X_1^{j_1} \cdots X_m^{j_m}\right\} \mid X_1^{i_1} \cdots X_m^{i_m} \in \square_\prec(L)\right\}$$

mas

$$\#\left\{X_1^{j_1} \cdots X_m^{j_m} \in \Delta_\prec(I_q) \mid X_1^{i_1} \cdots X_m^{i_m} \; divide \; X_1^{j_1} \cdots X_m^{j_m}\right\} = (q - i_1)...(q - i_m)$$

logo, a distância mínima de $RM_q(s, m)$ *é*

$$min\left\{(q - i_1)...(q - i_m) \mid 0 \leq i_q < q, \cdots, 0 \leq i_m < q, i_1 + \cdots + i_m \leq s\right\} \tag{3.7}$$

Escrevendo $s = a(q-1) + b$ *com* $a, b \in \mathbb{N}_0$ *e* $0 \leq b < q - 1$ *o número em (3.7) é igual a* $(q-b)q^{m-a-1}$, *fato demonstrado em [16, Lem. 1] . Agora, fazendo* $\mathbb{F}_q = \{\alpha_1, \cdots, \alpha_q\}$ *e definindo*

$$F = (X_1^{q-1} - 1)...(X_a^{q-1} - 1)(X_{a+1} - \alpha_1)...(X_{a+1} - \alpha_b)$$

nós vemos que $ev(F + I_q) \in C(I, L)$ *é de peso de Hamming igual a* $(q-b)q^{m-a-1}$. *De fato, os pontos de* $\mathbb{F}_q^m$ *que não zeram* F *são os pontos que contém* 0 *nas primeiras* a*'s coordenadas, para a coordenada* $a + 1$ *temos* $q - b$ *possibilidades, já que se* $\alpha_1, \cdots, \alpha_b$ *aparecerem nesta coordenada zerariam* F *e nas outras* $m - (a + 1)$ *coordenadas podemos ter qualquer valor, ou seja, temos* q *possibilidades. Usando o princípio de contagem encontramos* $(q-b)q^{m-a-1}$ *pontos de* $\mathbb{F}_q^m$ *que não zeram* F. *Portanto, o peso de Hamming de* $ev(F + I_q) \in C(I, L)$ *é igual a* $(q-b)q^{m-a-1}$. *Por isso, o corolário 3.1 produz o valor correto da distância mínima dos códigos generalizados de Reed-Muller.*

É interessante observar que a distância mínima dos códigos generalizados de Reed-Muller foi originalmente estabelecida usando métodos mais complicados e totalmente diferentes [12]. Se o objetivo é produzir códigos com bons parâmetros então existe uma escolha melhor de L do que (3.6), a saber

$$L = Span_{\mathbb{F}_q}\left\{X_1^{i_1}\cdots X_m^{i_m} \mid 0 \leq i_1 < q, \cdots, 0 \leq i_m < q, (q-i_1)...(q-i_m) \geq \delta\right\} \tag{3.8}$$

O corolário 3.1 nos diz que o código $C(I, L)$ correspondente é de distância mínima pelo menos δ e é o maior código de distância mínima prescrita pelo menos δ. Se realmente existem $i_1, \cdots, i_m$ com $(q-i_1)...(q-i_m) = \delta$, então, como acima, nós podemos detectar uma palavra-código de distância mínima δ e nós concluímos que o corolário 3.1 produz a real distância mínima neste caso. Os códigos $C(I, L)$ correspondentes para (3.8) são chamados códigos Massey Costello Justesen [13], [11] e são exemplos de melhorias dos códigos generalizados de Reed-Muller.

Capítulo 4

A cota Feng Rao para $C(I,L)^{\perp}$

Nesta seção nós reformulamos a cota Feng Rao no contexto dos códigos de variedades afins.

Teorema 4.1 *Seja $\prec$ fixa. Para cada $K \in \Delta_{\prec}(I_q) \setminus \square_{\prec}(L)$ defina*

$$S^{\perp}(K) = \{P \in \Delta_{\prec}(I_q) \mid \exists N \in \Delta_{\prec}(I_q) \text{ de tal modo que (P,N) é OWB e } lm(PN \ rem \ \mathcal{G}) = K\}.$$

A distância mínima de $C(I,L)^{\perp}$ é pelo menos

$$min\{\#S^{\perp}(K) \mid K \in \Delta_{\prec}(I_q) \setminus \square_{\prec}(L)\}. \tag{4.1}$$

Demonstração. Seja $\{B_1 + I_q, \cdots, B_{dim(L)} + I_q\}$ uma base bem comportada para L. Considere $\vec{c} \in C(I,L)^{\perp} \setminus \vec{0}$. Ou seja, $\vec{c}$ satisfaz $\vec{c}.ev(B_i + I_q) = 0$ para $i = 1, \cdots, dim(L)$, mas

$$\vec{c}.ev(K + I_q) \neq 0 \tag{4.2}$$

para algum $K \in \Delta_{\prec}(I_q)$. De fato, supondo que $\forall k \in \Delta_{\prec}(I_q)$ o produto $\vec{c}.ev(K + I_q) = 0$, temos que $\vec{c}.(R_q) = 0$ pois os elementos da $\Delta_{\prec}(I_q)$ formam uma base para R_q. Como ev é isomorfismo entre R_q e $\mathbb{F}_q^n$, existe $\overline{F} \in R_q$ tal que $ev(F + I_q) = \vec{c}$. Segue que $ev(F + I_q).\vec{c} = 0$, ou seja, $\vec{c}.\vec{c} = 0$. Logo, $\vec{c} = \vec{0}$. Absurdo. Seja $K \in \Delta_{\prec}(I_q)$ sendo o menor possível com respeito a $\prec$ tal que (4.2) aconteça. A existência deste menor elemento é garantida pelo fato da $\Delta_{\prec}(I_q)$ ser finita e $\prec$ ser uma ordem total. Se $K \in \square_{\prec}(L)$, podemos supor sem perda de generalidade que K é o monômio líder de algum B_i com $i = i, \cdots, dim(L)$. Sabemos então que $Supp(B_i) \subseteq \Delta_{\prec}(I_q)$ e $lm(B_i) = K$. Como K é o menor monômio da pegada tal que $\vec{c}.ev(K + I_q) \neq 0$ temos que $\vec{c}.ev(M + I_q) = 0$, onde M é qualquer monômio de B_i diferente de K. A linearidade de ev garante que $\vec{c}.ev(B_i + I_q) = \vec{c}.ev(K + I_q)$. O que é uma contradição já que $\vec{c}.ev(B_i + I_q) = 0$ e $\vec{c}.ev(K + I_q) \neq 0$. Portanto, $K \notin \square_{\prec}(L)$. Considere pares OWB $(P_1, N_1), \cdots, (P_\delta, N_\delta)$ onde $P_1, N_1, \cdots, P_\delta, N_\delta \in \Delta_{\prec}(I_q)$, $P_1 \prec \cdots \prec P_\delta$ e $lm(P_i N_i \ rem \ \mathcal{G}) = K$ para $i = 1, \cdots, \delta$. A minimalidade de K e a propriedade OWB de (P_i, N_i) garante que

$$\vec{c}.ev\left((\sum_{t=1,\cdots,i;\ a_i \neq 0} a_t P_t) N_i \ rem \ \mathcal{G} + I_q \right) \neq 0 \tag{4.3}$$

ocorre para qualquer $i \in \{1, \cdots, \delta\}$. De fato, seja $H = (\sum_{t=1,\cdots,i;\ a_i \neq 0} a_t P_t)$ com $i \in \{1, \cdots, \delta\}$. Claramente, $Supp(H) \subseteq \Delta_{\prec}(I_q)$ e $lm(H) = P_i$. Como (P_i, N_i) é OWB temos $lm(HN_i \ rem \ \mathcal{G}) = lm(P_i N_i \ rem \ \mathcal{G}) = K$. Do algoritmo da divisão temos que $Supp(HN_i \ rem \ \mathcal{G}) \subseteq \Delta_{\prec}(I_q)$, pelo argumento anterior,

$$\vec{c}.ev(HN_i \ rem \ \mathcal{G} + I_q) = \vec{c}.ev(K + I_q) \neq 0.$$

Seja $*$ o produto coordenada a coordenada sobre $\mathbb{F}_q^n$ dado por

$$(a_1, \cdots, a_n) * (b_1, \cdots, b_n) = (a_1 b_1, \cdots, a_n b_n)$$

Como

$$(\sum_{t=1,\cdots,i;\ a_i\neq 0} a_tP_t)N_i \ rem\ \mathcal{G} + I_q = (\sum_{t=1,\cdots,i;\ a_i\neq 0} a_tP_t)N_i + I_q$$

concluímos de (4.3) que

$$\vec{c} * ev\left((\sum_{t=1,\cdots,i;\ a_i\neq 0} a_tP_t) + I_q\right) \neq \vec{0}$$

para qualquer $i \in 1,\cdots,\delta$. Portanto, $\vec{c} * \vec{e} \neq \vec{0}$ para todo

$$\vec{e} \in \left\{ ev\left((\sum_{t=1}^{\delta} a_tP_t) + I_q\right) \mid a_1,\cdots,a_\delta \in \mathbb{F}_q, a_i \text{ não todos iguais a } 0 \right\}. \tag{4.4}$$

O espaço constituído de (4.4) e $(0,\cdots,0)$ é de dimensão δ. De fato, o conjunto formado pelos δ polinômios $\sum_{t=1}^{\delta} a_tP_t + I_q$ com $a_1,\cdots,a_\delta \in \mathbb{F}_q, a_i$ não todos iguais a 0 é LI, basta observar que $P_1 \prec \cdots \prec P_\delta$, e ev é isomorfismo. Portanto, $\vec{c}$ é tal que o produto $*$ de $\vec{c}$ por um espaço de dimensão δ é diferente de 0, logo o peso de Hamming de $\vec{c}$ tem que ser pelo menos δ. ■

É claro que é possível aplicar o teorema 4.1 para diferentes escolhas de $\prec$ para ver qual da a estimativa mais precisa.

Corolário 4.1 *A distância mínima de $C(I,L)^\perp$ é pelo menos*

$$min\left\{\#\left\{P \in \Delta_\prec(I_q) \mid P \text{ divide } K\right\} \mid K \in \Delta_\prec(I_q) \setminus \square_\prec(L)\right\}$$

Demonstração. Veja a prova do corolário 3.1. ■

Observação 4.1 *É possível modificar o teorema 4.1 e corolário 4.1 para lidar também com pesos generalizados de Hamming. Para o caso do teorema 4.1 isto corresponde a interpretação da última parte de [9, Th. 1]*

Exemplo 4.1 *Isto é uma continução do exemplo 3.1. É bem conhecido que o código dual de códigos generalizados de Reed-Muller é novamente um código generalizado de Reed-Muller. Mais precisamente,*

$$RM_q(s,m) = RM_q((q-1)m-1-s,m)^\perp$$

[5, Th. 2.21]. Aplicando o corolário 4.1 para $RM_q((q-1)m-1-s,m)^\perp$ nós vemos que a distância mínima de $RM_q(s,m)$ é pelo menos

$$min\left\{(i_1+1)...(i_m+1) \mid 0 \leq i_q < q,\cdots,0 \leq i_m < q, i_1+\cdots+i_m \geq (q-1)m-s\right\}. \tag{4.5}$$

De fato, do exemplo 3.1 segue que

$$\Delta_\prec(I_q) = \left\{X_1^{i_1}\cdots X_m^{i_m} \mid 0 \leq i_1 < q,\cdots,0 \leq i_m < q\right\}$$

$$\square_\prec(L) = \left\{X_1^{i_1}\cdots X_m^{i_m} \mid 0 \leq i_q < q,\cdots,0 \leq i_m < q, i_1+\cdots+i_m \leq (q-1)m-1-s\right\}.$$

Assim, para $X_1^{i_1}\cdots X_m^{i_m} \in \Delta_\prec(I_q) \setminus \square_\prec(L)$ temos $0 \leq i_q < q,\cdots,0 \leq i_m < q$ e $i_1+\cdots+i_m > (q-1)m-1-s$, equivalentemente, $0 \leq i_q < q,\cdots,0 \leq i_m < q$ e $i_1+\cdots+i_m \geq (q-1)m-s$. Para concluir basta observar que

$$\#\{X_1^{j_1}\cdots X_m^{j_m} \in \Delta_\prec(I_q) \mid X_1^{j_1}\cdots X_m^{j_m} \text{ divide } X_1^{i_1}\cdots X_m^{i_m}\} = (i_1+1)\cdots(i_m+1).$$

Escrevendo novamente $s = a(q-1)+b$ com $0 \leq b < q-1$ (4.5) torna-se igual a $(q-b)q^{m-a-1}$ que no exemplo 3.1 vimos ser igual ao valor da distância mínima verdadeira dos códigos generalizados de Reed-Muller.

Se o objetivo é produzir códigos $C(I,L)^{\perp}$ com bons parâmetros então escolher L como

$$L = Span_{\mathbb{F}_q}\left\{X_1^{i_1}\cdots X_m^{i_m} \mid 0 \leq i_1 < q, \cdots, 0 \leq i_m < q, (i_1+1)...(i_m+1) < q^m - s\right\} \tag{4.6}$$

seria a melhor opção. Os códigos $C(I,L)^{\perp}$ correspondentes a (4.6) são chamados códigos hiperbólicos e denotados $Hyp_q(s,m)$ [7, Def. 6].

Capítulo 5

Usando ordens grau-ponderadas

Nesta seção nós consideramos dois exemplos onde a ordem é a ordem grau-lexicográfica com peso.

Definição 5.1 *Seja $w(X_1), \cdots, w(X_m) \in \mathbb{N}$ e defina o peso de $X_1^{i_1} \cdots X_m^{i_m}$ como o número $w(X_1^{i_1} \cdots X_m^{i_m}) = i_1 w(X_1) + \cdots + i_m w(X_m)$. A ordem grau-lexicográfica com peso em $\mathcal{M}(X_1, \cdots, X_m)$ é uma ordenação com*

$$X_1^{i_1} \cdots X_m^{i_m} \prec X_1^{j_1} \cdots X_m^{j_m} \text{ se } w(X_1^{i_1} \cdots X_m^{i_m}) < w(X_1^{j_1} \cdots X_m^{j_m})$$
$$\text{ou } w(X_1^{i_1} \cdots X_m^{i_m}) = w(X_1^{j_1} \cdots X_m^{j_m}) \text{ e } X_1^{i_1} \cdots X_m^{i_m} \prec_{lex} X_1^{j_1} \cdots X_m^{j_m}.$$

Aqui, $\prec_{lex}$ é a ordem lexicográfica com $X_m \prec_{lex} \cdots \prec_{lex} X_1$.

Uma das qualidades da ordem grau-lexicográfica com peso é o lema seguinte.

Lema 5.1 *Considere a ordem grau-lexicográfica com peso dada pela definição 5.1 . Se H tem exatamente um monômio de maior peso w' em seu suporte e G tem exatamente dois monômios de maior peso em seu suporte então H rem G tem exatamente um monômio de maior peso em seu suporte e este peso é w'.*

Demonstração. Sejam $H = H' + \lambda_\alpha X^\alpha$, $w(H') < w(H)$, $lm(H) = X^\alpha$ e $G = G' + \mu_1 M_1 + \mu_2 M_2$, $w(G') < w(M_1) = w(M_2)$, $M_1 \prec_{lex} M_2$. Executando o primeiro passo da divisão de H por G temos

$$H = G\mu M + R.$$

Equivalentemente, $R = H - G\mu M$. É claro que $w(MG) \leq w(H)$. Se $w(MG) < w(H)$, então $R = (H' - \mu MG) + \lambda_\alpha X^\alpha$ e $w(H' - \mu MG) < w(H)$, já que $w(H') < w(H)$. Como $w(H) = w(X^\alpha)$, segue que $w(H' - \mu MG) < w(X^\alpha)$. Portanto, $w(R) = w(H)$ e X^α é o único monômio de maior peso no suporte de R. Supondo agora $w(MG) = w(H)$, temos que o termo líder de μMG será $\mu\mu_2 MM_2$. Como $\lambda_\alpha X^\alpha$ é o único termo de H com peso $w(MG)$ necessariamente $\lambda_\alpha X^\alpha = \mu\mu_2 MM_2$. Portanto, $R = (H' - \mu MG') - \mu\mu_1 MM_1$. Mas $w(MG) = w(MM_1)$ e $w(H) = w(X^\alpha)$, logo $w(MM_1) = w(X^\alpha)$. Como $w(G') < w(M_1)$ temos que $w(MG') < w(MM_1)$, e por construção $w(H') < w(H) = w(MM_1)$. Assim, $w(H' - \mu MG') < w(\mu\mu_1 MM_1)$ e $w(R) = w(MM_1)$. Portanto, $w(R) = w(H)$ e MM_1 é o único monômio de maior grau no suporte de R. Então em cada passo da divisão de H por G temos que o resto parcial tem um único monômio de maior peso, e este peso é w'. Logo, H *rem* G terá um único monômio de maior peso, e este peso será w' ■

Exemplo 5.1 *Considere os ideais*

$$I = \left\langle X^3Y + Y^3 + X \right\rangle \subseteq \mathbb{F}_8[X, Y]$$

$$I_q = I + \left\langle X^8 + X, Y^8 + Y \right\rangle \subseteq \mathbb{F}_8[X, Y]$$

Seja $\prec$ a ordem grau-lexicográfica com peso definida pela configuração $w(X) = 2, w(Y) = 3$ e interpretando X como X_1 e Y como X_2. Claramente, $\mathcal{B} = \left\{X^3Y + Y^3 + X\right\}$ é uma base de Gröbner para

I. Como $lm(X^3Y + Y^3 + X) = X^3Y$ *e* X^iY^j *não é divisível por* X^3Y *quando* $0 \leq i < 3$ *e* $j \in \mathbb{N}$ *ou* $i \geq 3$ *e* $j = 0$ *temos*

$$\Delta_\prec(I) = \left\{X^iY^j \mid \text{ se } i \geq 3 \text{ então } j = 0\right\}.$$

Usando o algoritmo de Buchberger encontramos a seguinte base de Gröbner para I_q

$$\mathcal{G} = \{X^3Y + Y^3 + X,\ X^8 + X,\ XY^5 + X^5 + X^2Y^2 + Y,\ Y^7 + X^7\}$$

e, portanto,

$$\begin{aligned}\Delta_\prec(I_q) = \{&1, X, Y, X^2, XY, Y^2, X^3, XY^2, X^4, Y^3, X^2Y^2,\\ &X^5, XY^3, Y^4, X^6, X^2Y^3, XY^4, X^7, Y^5, X^2Y^4, Y^6\}\end{aligned} \tag{5.1}$$

com pesos correspondentes

$$\{0, 2, 3, 4, 5, 6, 6, 7, 8, 8, 9, 10, 10, 11, 12, 12, 13, 14, 14, 15, 16, 18\}.$$

Os elementos em (5.1) estão listados em ordem crescente com respeito a $\prec$*. Usando o Lema 5.1 e alguns outros resultados nós podemos detectar um total 166 pares OWB úteis, e um pouco mais que nós não usaremos. Ilustramos o método utilizado para verificar a propriedade OWB considerando alguns poucos pares OWB. Primeiro para vermos que* (X^3, X) *é OWB precisamos mostrar que* $lm(HX\ rem\ \mathcal{G}) = lm(X^3X\ rem\ \mathcal{G}), \forall\ H$ *com* $Supp(H) \subseteq \Delta_\prec(I_q)$ *e* $lm(H) = X^3$*. Observe que um polinômio* H *satisfazendo tais condições é da forma* $a_1 + a_2X + a_3Y + a_4X^2 + a_5XY + a_6Y^2 + X^3$*, temos*

$$lm((a_1 + a_2X + a_3Y + a_4X^2 + a_5XY + a_6Y^2 + X^3)X\ rem\ \mathcal{G}) = X^4 \tag{5.2}$$

não importa quem são $a_1, \cdots, a_6$*. Isto é porque* $X^3X = X^4 \in \Delta_\prec(I_q)$ *e, portanto,* X^4 *é movido para o resto na divisão por* $\mathcal{G}$*. A prova que* (X^3, X) *é OWB está completa. Para ver que* (XY, X^2) *é OWB nós não podemos aplicar o mesmo argumento já que* $XYX^2 = X^3Y \notin \Delta_\prec(I_q)$*. Seja* H *com* $Supp(H) \subseteq \Delta_\prec(I_q)$ *e* $lm(H) = XY$*, então* H *é da forma*

$$a_1 + a_2X + a_3Y + a_4X^2 + XY.$$

Vamos mostrar que $lm(HX^2\ rem\ \mathcal{G}) = lm(XYX^2\ rem\ \mathcal{G})$*. Temos*

$$w(1.X^2), w(X.X^2), w(Y.X^2), w(X^2.X^2)\ <\ w(XY.X^2) = 9,$$

isto é, existe um único monômio de maoir peso em $(a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2$ *e este peso é* 9*. Como* $X^3Y + Y^3 + X$ *tem extamente dois monômios de maior peso em seu suporte o Lema 5.1 nos diz que o monômio*

$$lm((a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2\ rem\ \mathcal{B})$$

é também de peso 9. Existe um único monômio em $\Delta_\prec(I)$ *com peso* 9*, a saber,* Y^3*. Como* $\mathcal{B} \subseteq \mathcal{G}$ *e* Y^3 *também pertence a* $\Delta_\prec(I_q)$ *nós concluímos que*

$$lm((a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2\ rem\ \mathcal{G}) = Y^3$$

não importa quem são $a_1, \cdots, a_4$*. Como* X^3Y *tem um único monômio de maior peso e este peso é* 9*, pelo mesmo argumento anterior* $lm(X^3Y\ rem\ \mathcal{G}) = Y^3$*. Consequentemente,* (XY, X^2) *é OWB. Finalmente, para ver que* (XY, X^2Y) *é OWB considere* H *tal que* $Supp(H) \subseteq \Delta_\prec(I_q)$ *e* $lm(H) = XY$*, novamente* H *é da forma*

$$a_1 + a_2X + a_3Y + a_4X^2 + XY.$$

Vamos mostrar que $lm(HX^2Y\ rem\ \mathcal{G}) = lm(XYX^2Y\ rem\ \mathcal{G})$*. Começamos reconhecendo do Lema 5.1 que o peso de*

$$lm((a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2Y\ rem\ \mathcal{B})$$

é igual $w(XY.X^2Y) = 12$. *Contudo, agora existem duas possibilidades* X^6 *e* Y^4 *de monômios líderes já que os dois são de peso 12 e pertencem a* $\Delta_\prec(I)$. *Quando executamos a divisão de* $(a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2Y$ *por* $\mathcal{B}$ *vemos que*

$$lm((a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2Y \; rem \; \mathcal{B}) = Y^4.$$

Como Y^4 *pertence a* $\Delta_\prec(I_q)$ *concluímos que*

$$lm((a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2Y \; rem \; \mathcal{G}) = Y^4.$$

Agora, X^3Y^2 *tem um único monômio de maior peso e este peso é* 12, *repetindo o argumento temos que* $lm(X^3Y^2 \; rem \; \mathcal{G}) = Y^4$. *Portanto,* (XY, X^2Y) *é OWB.*
Observe que para fixos P *e* K *pode existir mais de uma escolha de* N *tal que* (P, N) *é OWB e* $lm(PN \; rem \; \mathcal{G}) = K$. *Como um exemplo, ambos* (XY, Y^2) *e* (XY, X^3) *são OWB e satisfazem*

$$lm(XY.Y^2 \; rem \; \mathcal{G}) = lm(XY.X^3 \; rem \; \mathcal{G}) = XY^3.$$

De fato, como $XY^3 \in \Delta_\prec(I_q)$ *temos* $lm(XY^3 \; rem \; \mathcal{G}) = XY^3$. *Observe agora que* X^4Y *tem um único monômio de maior peso e este peso é* 11, *pelo Lema 5.1 temos que o peso de*

$$lm(X^4Y \; rem \; \mathcal{B})$$

é igual a 11. *Existe um único monômio em* $\Delta_\prec(I)$ *de peso* 11, *a saber,* XY^3. *Como* $XY^3 \in \Delta_\prec(I_q)$ *temos*

$$lm(X^4Y \; rem \; \mathcal{G}) = XY^3.$$

Para a propriedade OWB, seja H *tal que* $Supp(H) \subseteq \Delta_\prec(I_q)$ *e* $lm(H) = XY$, *então* H *é da forma*

$$a_1 + a_2X + a_3Y + a_4X^2 + XY.$$

Temos

$$lm((a_1 + a_2X + a_3Y + a_4X^2 + XY)Y^2 \; rem \; \mathcal{G}) = XY^3$$

não importa quem são $a_1, \cdots, a_4$. *Pois* $XY^3 \in \Delta_\prec(I_q)$ *e, portanto,* XY^3 *é movido para o resto na divisão por* $\mathcal{G}$. *A prova que* (XY, XY^3) *é OWB está completa. Para o caso de* (XY, X^3) *basta observar que* $(a_1 + a_2X + a_3Y + a_4X^2 + XY)X^3$ *tem um único monômio de maior peso e este peso é* 11. *Pelo Lema 5.1 temos que o peso de*

$$lm((a_1 + a_2X + a_3Y + a_4X^2 + XY)X^3 \; rem \; \mathcal{B})$$

é igual a 11. *Sabemos que* XY^3 *é o único monômio em* $\Delta_\prec(I)$ *de peso* 11 *e* $XY^3 \in \Delta_\prec(I_q)$, *portanto*

$$lm((a_1 + a_2X + a_3Y + a_4X^2 + XY)X^3 \; rem \; \mathcal{G}) = XY^3.$$

Na tabela 1 *listamos algumas informações sobres os pares OWB. Por* $\bar{\sigma}(P)$ *denotamos o número de detectados* $K \in \Delta_\prec(I_q)$ *tal que existe um* $N \in \Delta_\prec(I_q)$ *com* (P, N) *OWB e* $lm(PN \; rem \; \mathcal{G}) = K$. *Por* $\bar{\mu}(K)$ *denotamos o número de detectados* $P \in \Delta_\prec(I_q)$ *tal que existe um* $N \in \Delta_\prec(I_q)$ *com* (P, N) *OWB e* $lm(PN \; rem \; \mathcal{G}) = K$.

Tabela 1 Informações sobre pares OWB

M	1	X	Y	X^2	XY	Y^2	X^3	X^2Y	XY^2	X^4	Y^3
$\bar{\sigma}(M)$	22	19	14	16	12	11	5	10	9	4	8
$\bar{\mu}(M)$	1	2	2	3	4	3	4	6	6	5	8

M	X^2Y^2	X^5	XY^3	Y^4	X^6	X^2Y^3	XY^4	X^7Y	Y^5	X^2Y^4	Y^6
$\bar{\sigma}(M)$	7	3	6	5	2	4	3	1	2	2	1
$\bar{\mu}(M)$	9	6	10	11	7	12	13	8	14	15	17

Para a construção do código $C(I,L)$ escolhemos L como sendo gerado por $(M+I_q)'s$ com $M \in \Delta_\prec(I_q)$ e $\bar{\sigma}(M) \geq \delta$. Pelo Teorema 3.1 isto nos dá códigos de maior dimensão possível com distância mínima prescrita pelo menos δ. Para construção de $C(I,L)^\perp$ escolhemos L como sendo gerado por $(M+I_q)'s$ com $M \in \Delta_\prec(I_q)$ e $\bar{\mu}(M) < \delta$. Pelo Teorema 4.1 isto nos dá códigos de maior dimensão possível com distância mínima prescrita pelo menos δ. O comprimento desses códigos é igual a $n = \#\Delta_\prec(I_q)$. De 5.1 temos, portanto, $n = 22$. Na tabela 2 listamos os parâmetros $[k,\delta]$ que podem ser realizados a partir do Teorema 3.1 e Teorema 4.1. Portanto, k é a dimensão e δ é a distância mínima prescrita.

Tabela 2 Parâmetros dos códigos

$C(I,L)$	$[1,22]$	$[2,19]$	$[3,16]$	$[4,14]$	$[5,12]$	$[6,11]$
	$[7,10]$	$[8,9]$	$[9,8]$	$[10,7]$	$[11,6]$	$[13,5]$
	$[15,4]$	$[17,3]$	$[20,2]$	$[22,1]$		
$C(I,L)^\perp$	$[1,17]$	$[2,15]$	$[3,14]$	$[4,13]$	$[5,12]$	$[6,11]$
	$[7,10]$	$[8,9]$	$[10,8]$	$[11,7]$	$[14,6]$	$[15,5]$
	$[17,4]$	$[19,3]$	$[21,2]$			

Concluímos que embora a cota no Teorema 3.1 baseia-se na mesma noção que a cota no Teorema 4.1 as duas cotas podem, às vezes, produzir resultados completamentes diferentes.

No exemplo 5.1 foi trabalhoso detectar quais pares são OWB. Isto é devido ao fato que na $\Delta_\prec(I)$ bem como na $\Delta_\prec(I_q)$ haviam monômios distintos de mesmo peso. No próximo exemplo não há dois monômios diferentes na $\Delta_\prec(I)$ como o mesmo peso. Como consequência torna-se muito fácil encontrar pares OWB.

Exemplo 5.2 *Considere os ideais*

$$I = \left\langle X^4 - Y^3 - Y \right\rangle \subseteq \mathbb{F}_9[X,Y]$$

$$I_q = \left\langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \right\rangle \subseteq \mathbb{F}_9[X,Y].$$

Seja $\prec$ a ordem grau-lexicográfica com peso dada por $w(X) = 3$, $w(Y) = 4$ e interpretando X como X_2 e Y como X_1. Claramente,

$$\mathcal{B} = \{X^4 - Y^3 - Y\}$$

é uma base de Gröbner para I e aplicando o algoritmo de Buchberger nós encontramos que

$$\mathcal{G} = \{X^4 - Y^3 - Y, X^9 - X\}$$

é uma base de Gröbner para I_q. Consequentemente,

$$\begin{aligned} \Delta_\prec(I) &= \{X^iY^j \mid 0 \leq i, 0 \leq j < 3\} \\ \Delta_\prec(I_q) &= \{X^iY^j \mid 0 \leq i < 9, 0 \leq j < 3\}. \end{aligned} \tag{5.3}$$

A aplicação $w : \Delta_\prec(I) \to \langle 3,4\rangle$, dada por $x(X^iY^j) = 3i + 4j$ é uma bijeção. Aqui, $\langle 3,4\rangle$ significa o semigrupo gerado por 3 e 4. De fato, sejam X^iY^j e $X^\alpha Y^\beta \in \Delta_\prec(I)$ com $X^iY^j \neq X^\alpha Y^\beta$, isto é, $i - \alpha \neq 0$ ou $\beta - j \neq 0$. Se $w(X^iY^j) = w(X^\alpha Y^\beta)$, então $3i + 4j = 3\alpha + 4\beta$ o que equivale $3(i-\alpha) = 4(\beta - j)$. Como 3 não divide 4, 3 tem que dividir $\beta - j$. Mas $\beta - j < 3$ pois $0 \leq j < 3$ e $0 \leq \beta < 0$ então a única é $\beta - j = 0$. Assim, $3(i-\alpha) = 0$ o que implica $i - \alpha = 0$. Absurdo. Logo, w é injetora. Considere agora $3i + 4j \in \langle 3,4\rangle$. Se $0 \leq j < 3$ então $X^iY^j \in \Delta_\prec(I)$ e $w(X^iY^j) = 3i + 4j$. Agora, se $j \geq 3$ então podemos escrever $j = 3q + r$ onde $0 \leq r < 3$. Portanto $X^{i+4q}Y^r \in \Delta_\prec(I)$ e $w(X^{i+4q}Y^r) = 3(i+4q) + 4r = 3i + 4(3q + r) = 3i + 4j$. Logo, w é sobrejetora. Consequentemente, nós podemos identificar qualquer monômio $M \in \Delta_\prec(I)$ unicamente por seu peso. Considere um polinômio F com $Supp(F) \subseteq \Delta_\prec(I_q)$ e escreva $P = lm(F)$. Seja $N \in \Delta_\prec(I_q)$ arbitrário. Como $Supp(F) \subseteq \Delta_\prec(I_q)$ e $\Delta_\prec(I_q) \subseteq \Delta_\prec(I)$ segue $Supp(F) \subseteq \Delta_\prec(I)$, portanto F não tem dois monômios

distintos de mesmo peso. Pelo Lema 5.1 o monômio lider de FN rem $\mathcal{B}$ é o monômio único $K \in \Delta_\prec(I)$ de peso iqual a $w(PN) = w(P) + w(N)$. Se $K \in \Delta_\prec(I_q)$ então (P, N) é OWB. Portanto, dado $P, N \in \Delta_\prec(I_q)$ então (P, N) é OWB se $w(P) + w(N) \in w(\Delta_\prec(I_q))$. Agora nós mostraremos que se $K \in \Delta_\prec(I_q)$ e (P, N) satisfaz $w(P)+w(N) = w(K)$ então $P, N \in \Delta_\prec(I_q)$. Isto, em particular, implica que (P, N) é OWB. Suponha por contradição que $P \notin \Delta_\prec(I_q)$. Pela definição de pegada existe um polinômio $H \in I_q$ tendo P como monômio líder. Como $P \in \Delta_\prec(I)$ podemos sem perda de generalidade assumir que H é resto módulo $\mathcal{B}$. Isto é, nós podemos assumir que $Supp(H) \subseteq \Delta_\prec(I)$. De $H \in I_q$ nós concluímos que

$$HN \text{ rem } \mathcal{B} \in I_q. \tag{5.4}$$

Por outro lado, a suposição $Supp(H) \subseteq \Delta_\prec(I)$ combinada com o Lema 5.1 implica que

$$lm(HN \text{ rem } \mathcal{B}) = K.$$

Aqui nós usamos novamente o fato não há dois monômios distintos na $\Delta_\prec(I)$ com o mesmo peso. Mas K, por suposição, esta na $\Delta_\prec(I_q)$ e portanto (5.4) não pode ser verdade. Chegamos a uma contradição. Supor $N \notin \Delta_\prec(I_q)$ levaria a uma contradição similar. As observações acima implicam que para detectar pares OWB é suficiente o estudo dos pesos. Para este propósito defina

$$\Gamma = w(\Delta_\prec(I)) = \langle 3, 4 \rangle$$

para $\lambda \in w(\Delta_\prec(I_q))$ seja

$$\sigma(\lambda) = \#\{\eta \in w(\Delta_\prec(I_q)) \mid \eta - \lambda \in \Gamma\}$$

e para $\lambda \in \Gamma$ tome

$$\mu(\lambda) = \#\{\alpha \in \Gamma \mid \lambda - \alpha \in \Gamma\}.$$

Mostramos acima que se $P \in \Delta_\prec(I_q)$ então existem diferentes pares de elementos $K_1, \cdots, K_{\sigma(w(P))} \in \Delta_\prec(I_q)$ e elementos correspondentes $N_1, \cdots, N_{\sigma(w(P))} \in \Delta_\prec(I_q)$ tais que para $i = 1, \cdots, \sigma(w(p))$ o par (P, N_i) é OWB com $lm(PN_i \text{ rem } \mathcal{G}) = K_i$. Similarmente, se $K \in \Delta_\prec(I_q)$ então existem diferentes pares de elementos $P_1, \cdots, P_{\mu(w(K))} \in \Delta_\prec(I_q)$ e elementos correspondentes $N_1, \cdots, N_{\mu(w(K))} \in \Delta_\prec(I_q)$ tais que para $i = 1, \cdots, \sigma(w(p))$ o par (P_i, N_i) é OWB com $lm(P_iN_i \text{ rem } \mathcal{G}) = K$. Na Tabela 3 listamos $\sigma(w)$ e $\mu(w)$ para todo $w \in \Delta_\prec(I_q)$.

Tabela 3

w	0	3	4	6	7	8	9	10	11
$\sigma(w)$	27	24	23	21	20	19	18	17	16
$\mu(w)$	1	2	2	3	4	3	4	6	6
w	12	13	14	15	16	17	18	19	20
$\sigma(w)$	15	14	13	12	11	10	9	8	7
$\mu(w)$	7	8	9	10	11	12	13	14	15
w	21	22	23	24	25	26	28	29	32
$\sigma(w)$	6	6	4	3	4	3	2	2	1
$\mu(w)$	16	17	18	19	20	21	23	24	27

Com a finalidade de contruir códigos definimos abaixo os subespaços de $R_q = \mathbb{F}_9[X, Y]/I_q$

$$L_1 = Span_{\mathbb{F}_9}\{M + I_q \mid M \in \Delta_\prec(I_q), w(M) \leq s\}$$

$$L_2 = Span_{\mathbb{F}_9}\{M + I_q \mid M \in \Delta_\prec(I_q), \sigma(w(M)) \geq \delta\}$$

$$L_3 = Span_{\mathbb{F}_9}\{M + I_q \mid M \in \Delta_\prec(I_q), \mu(w(M)) < \delta\}$$

O código de variedade afim correspondente são todos de comprimento $n = \#\Delta_\prec(I_q) = 27$. Do Teorema 3.1 a distância mínima de $C(I, L_2)$ é pelo menos δ e do Teorema 4.1 a distância mínima de $C(I, L_3)^\perp$ é

também pelo menos δ*. Os códigos* $C(I, L_2)$ *e* $C(I, L_3)^{\perp}$ *são os maiores códigos com distância mínima prescrita* δ *com respeito ao Teorema 3.1 e ao Teorema 4.1. Aplicando o Teorema 3.1 e o Teorema 4.1 aos códigos* $C(I, L_1)$ *e* $C(I, L_1)^{\perp}$*, respectivamente, temos cotas inferiores das distâncias mínimas. Como um exemplo, escolhendo* $s = 23$ *o código* $C(I, L_1)$ *é de dimensão* 21 *e distância mínima pelo menos* 4*. Escolhendo* $\delta = 4$ *o código* $C(I, L_2)$ *é de dimensão* 22 *e também de distância mínima pelo menos* 4*. Como um outro exemplo, escolhendo* $s = 7$ *o código* $C(I, L_1)^{\perp}$ *é de dimensão* 22 *e distância mínima pelo menos* 3*. Escolhendo* $\delta = 4$ *o código* $C(I, L_3)^{\perp}$ *é também de dimensão* 22 *mas é distância mínima pelo menos* 4*.*

Capítulo 6

As condições de domínios de ordem

No capítulo anterior nós demonstramos que a ordem grau-lexicográfica com peso pode, às vezes, ser muito útil quando procuramos pares OWB. Em particular, a tarefa de encontrar pares OWB foi bastante simples no Exemplo 5.2 devido ao fato de que em $\Delta_{\prec}(I)$ não haviam monômios distintos de mesmo peso e devido ao fato de que o polinômio gerador de I possuia exatamente dois monômios de maior peso em seu suporte. Neste capítulo generalizamos a construção no Exemplo 5.2. Todas as provas serão generalizações simples dos argumentos do Exemplo 5.2, portanto faremos apenas algumas delas. Começamos pela generalização do conceito de ordem grau-lexicográfica com peso.

Definição 6.1 *Seja $w(X_1), \cdots, w(X_m) \in \mathbb{N}_0^r$ e assuma $\prec_{\mathbb{N}_0^r}$ uma ordenação monomial em $\mathbb{N}_0^r$. Extenda w para uma função monomial sobre $\mathcal{M}(X_1, \cdots, X_m)$ por*

$$w(X_1^{i_1} \cdots X_m^{i_m}) = i_1 w(X_1) + \cdots + i_m w(X_m).$$

Tome $\prec_{\mathcal{M}}$ sendo uma ordenação monomial em $\mathcal{M}(X_1, \cdots, X_m)$. A ordem grau-ponderada generalizada definida sobre $w(X_1), \cdots, w(X_m)$, $\prec_{\mathbb{N}_0^r}$ e $\prec_{\mathcal{M}}$ é a ordem $\prec_w$ dada por

$$X_1^{i_1} \cdots X_m^{i_m} \prec_w X_1^{j_1} \cdots X_m^{j_m}$$

se

$$w(X_1^{i_1} \cdots X_m^{i_m}) \prec_{\mathbb{N}_0^r} w(X_1^{j_1} \cdots X_m^{j_m})$$

ou, se

$$w(X_1^{i_1} \cdots X_m^{i_m}) = w(X_1^{j_1} \cdots X_m^{j_m}) \text{ e } X_1^{i_1} \cdots X_m^{i_m} \prec_{\mathcal{M}} X_1^{j_1} \cdots X_m^{j_m}.$$

O grau-ponderado de um polinômio F é $wdeg(F) = w(lm(F))$.

Agora apresentamos as condições de domínios de ordem, as quais desempenham um papel central no presente capítulo.

Definição 6.2 *Considere um ideal $I \subseteq k[X_1, \cdots, X_m]$, onde k é um corpo. Seja $\prec_w$ a ordem grau-ponderada generalizada dada pela Definição 6.1. Assuma que I possui uma base de Gröbner $\mathcal{B}$, tal que qualquer $G \in \mathcal{B}$ tem exatamente dois monômios de maior peso e que não exista monômios distintos de mesmo peso em $\Delta_{\prec}(I)$. Neste caso, dizemos que I e $\prec_w$ satisfazem as condições de domínios de ordem.*

O lema abaixo é uma generalização do Lema 5.1.

Lema 6.1 *Sejam I, $\prec_w$ e $\mathcal{B}$ como na Definição 6.2. Tome F um polinômio com exatamente um monômio de maior peso. Então $w(lm(F)) = w(lm(F \text{ rem } \mathcal{B}))$. Em particular, $w(lm(F)) = w(lm(F \text{ rem } \mathcal{B}))$ para todo F com $Supp(F) \subseteq \Delta_{\prec_w}(I)$.*

Demonstração. Basta observar que o resultado de cada etapa da divisão de F por $\mathcal{B}$ é um polinômio F' que, pelo Lema 5.1, tem um único monômio de maior peso e este peso é $w(lm(F))$. ∎

A proposição seguinte é uma generalização de resultados similares do Exemplo 5.2.

Proposição 6.1 *Assuma $I \subseteq \mathbb{F}_q[X_1, \cdots, X_m]$ e $\prec_w$ satisfazendo as condições de domínios de ordem. Considere $I_q = I + \langle X_1^q - X_1, \cdots, X_m^q - X_m \rangle$. Um par (P, N) onde $P, N \in \Delta_{\prec_w}(I_q)$ é OWB se $w(P) + w(N) \in w(\Delta_{\prec_w}(I_q))$. Se $K \in \Delta_{\prec_w}(I_q)$ e $P, N \in \Delta_{\prec_w}(I)$ satisfazem $w(P) + w(N) = w(K)$, então $P, N \in \Delta_{\prec_w}(I_q)$, e (P, N) é OWB.*

Demonstração. Sejam $\mathcal{B}$ e $\mathcal{G}$ bases de Gröbner de I e I_q respectivamente. Sabemos que $I \subseteq I_q$ e $\Delta_{\prec_w}(I_q) \subseteq \Delta_{\prec_w}(I)$. Tome $(P, N) \in \Delta_{\prec_w}(I_q)$ e $w(PN) = w(P) + w(N) \in w(\Delta_{\prec_w}(I_q))$. Seja H tal que $Supp(H) \subseteq \Delta_{\prec_w}(I_q)$ e $lm(H) = P$, temos que mostrar que $lm(PN \ rem \ \mathcal{G}) = lm(HN \ rem \ \mathcal{G})$. Observe que PN é um polinômio com um único monômio de maior peso. Pelo Lema 6.1, $w(PN) = w(lm(PN)) = w(lm(PN \ rem \ \mathcal{B}))$. Então, $lm(PN \ rem \ \mathcal{B}) \in \Delta_{\prec_w}(I)$ e $w(lm(PN \ rem \ \mathcal{B})) = w(P) + w(N) \in w(\Delta_{\prec_w}(I_q))$. Portanto, $lm(PN \ rem \ \mathcal{B}) \in \Delta_{\prec_w}(I_q)$ e $lm(PN \ rem \ \mathcal{B}) = lm(PN \ rem \ \mathcal{G})$. Por outro lado, com $Supp(H) \subseteq \Delta_{\prec_w}(I_q)$ segue que H não possui monômios distintos de mesmo peso. Então, claramente, HN não possui monômios distintos de mesmo peso e $lm(HN) = PN$. Npvamente pelo Lema 6.1, $w(lm(HN)) = w(lm(HN \ rem \ \mathcal{B}))$. Mas $w(lm(HN)) = w(PN) = w(P) + w(N)$, assim $lm(HN \ rem \ \mathcal{B} \in \Delta_{\prec_w}(I)$ e $w(lm(HN \ rem \ \mathcal{B})) = w(P) + w(N) \in \Delta_{\prec_w}(I_q)$. Portanto, $lm(HN \ rem \ \mathcal{B}) \in \Delta_{\prec_w}(I_q)$ e $lm(HN \ rem \ B) = lm(HN \ rem \ \mathcal{G})$. Assim, $lm(PN \ rem \ \mathcal{G})$ e $lm(HN \ rem \ \mathcal{G})$ estão na pegada de I_q e possuem o mesmo peso. Logo, $lm(PN \ rem \ \mathcal{G}) = lm(HN \ rem \ \mathcal{G})$. Para a segunda afirmação, considere $K \in \Delta_{\prec_w}(I_q)$ e $P, N \in \Delta_{\prec_w}(I)$. Se $w(K) = w(P) + w(N)$, como $w(K) \in w(\Delta_{\prec_w}(I_q))$ pelo que fizemos acima (P, N) é OWB. Suponha por absurdo que $P \notin \Delta_{\prec_w}(I_q)$. Então existe um polinômio $H \in I_q$ tal que $lm(H) = P$. Como $P \in \Delta_{\prec_w}(I)$, podemos assumir que H é resto módulo $\mathcal{B}$, isto é, $Supp(H) \subseteq \Delta_{\prec_w}(I)$. Pelo algoritmo da divisão,

$$HN = Q + HN \ rem \ \mathcal{G}$$

como $H \in I_q$ temos $HN \in I_q$ e por definição $Q \in I_q$, então $HN \ rem \ \mathcal{G} \in I_q$. Por outro lado, como $Supp(H) \subseteq \Delta_{\prec_w}(I_q)$ o Lema 6.1 garante que $lm(HN \ rem \ \mathcal{B}) = K$. Daí, $lm(HN \ rem \ \mathcal{G}) = K$. O que é absurdo, pois $HN \ rem \ \mathcal{G} \in I_q$ e $K \in \Delta_{\prec_w}(I_q)$. O caso $N \notin \Delta_{\prec_w}(I_q)$ é análogo. ■

Definição 6.3 *Assuma I e $\prec_w$ satisfazendo as condições de domínios de ordem. Seja $\Gamma = w(\Delta_{\prec_w}(I))$ e defina para todo $\lambda \in w(\Delta_{\prec_w}(I_q))$*

$$\sigma(\lambda) = \#\left\{\eta \in w(\Delta_{\prec_w}(I_q)) \mid \eta - \lambda \in \Gamma\right\}$$

e para todo $\lambda \in \Gamma$

$$\mu(\lambda) = \#\left\{\alpha \in \Gamma \mid \lambda - \alpha \in \Gamma\right\}.$$

Aplicando o Teorema 3.1 e o Teorema 4.1 em combinação com a Proposição 6.1 temos o seguinte teorema.

Teorema 6.1 *Assuma I e $\prec_w$ satisfazendo as condições de domínios de ordem. Seja L um subespaço de $R_q = \mathbb{F}_q[X_1, \cdots, X_m]/I_q$ tal que*

$$\{B_1 + I_q, \cdots, B_{dim(L)} + I_q\}$$

é uma base bem comportada de L. A distância mínima de $C(I, L)$ é pelo menos

$$min\{\sigma(w(lm(B_1))), \cdots, \sigma(w(lm(B_{dim(L)})))\}.$$

A distância mínima de $C(I, L)^{\perp}$ é pelo menos

$$\begin{aligned} &min\{\mu(w(M)) \mid M \in \Delta_{\prec_w}(I_q) \setminus \{lm(B_1), \cdots, lm(B_{dim(L)})\} \\ &\quad \geq min\{\mu(\lambda) \mid \lambda \in \Gamma \setminus \{w(B_1), \cdots, w(B_{dim(L)})\}. \end{aligned}$$

Considere as escolhas abaixo de L. Seja $\vec{s} \in \mathbb{N}_0^r$ e $\delta \in \mathbb{N}$.

$$L_1 = Span_{\mathbb{F}_q}\{M + I_q \mid M \in \Delta_{\prec_w}(I_q), w(M) \preceq_{\mathbb{N}_0^r} \vec{s}\} \tag{6.1}$$

$$L_2 = Span_{\mathbb{F}_q}\{M + I_q \mid M \in \Delta_{\prec_w}(I_q), \sigma(w(M)) \geq \delta\} \tag{6.2}$$

$$L_3 = Span_{\mathbb{F}_q}\{M + I_q \mid M \in \Delta_{\prec_w}(I_q), \mu(w(M)) < \delta\}. \tag{6.3}$$

O Teorema 6.1 nos diz que a distância mínima de $C(I, L_2)$ e $C(I, L_3)^\perp$ é pelo menos δ. Por construção $C(I, L_2)$ e $C(I, L_3)$ são os maiores códigos com distância mínima prescrita δ. No capítulo 9 veremos que os pesos são sempre numéricos, isto é, sempre temos $\vec{s} = s$, onde s é um inteiro, então a distância mínima de $C(I, L_1)$ é pelo menos $n - s$. Aqui, $n = \#\Delta_{\prec_w}(I_q)$. Da mesma forma, vamos derivar no capítulo 9 uma expressão simples para uma cota inferior da distância mínima de $C(I, L_1)^\perp$ sempre que os pesos são numéricos.

Exemplo 6.1 *Isto é uma continuação do Exemplo 3.1 e do Exemplo 4.1. Escolha os pesos* $w(X_1) = (1, 0, \cdots, 0)$, $w(X_2) = (0, 1, 0, \cdots, 0), \cdots,$ $w(X_m) = (0, \cdots, 0, 1) \in \mathbb{N}_0^m$. *Seja* $\prec_{\mathbb{N}_0^m}$ *a ordem graduada em* $\mathbb{N}_0^m$ *com* $(1, 0, \cdots, 0) \prec_{\mathbb{N}_0^m} \cdots \prec_{\mathbb{N}_0^m} (0, \cdots, 0, 1)$. *Seja agora* $\prec_{\mathcal{M}}$ *uma ordenação monomial qualquer em* $\mathcal{M}(X_1, \cdots, X_m)$. *Usando a convenção de que o conjunto vazio é uma base de Gröbner para o ideal* $I = \langle 0 \rangle \subseteq \mathbb{F}_q[X_1, \cdots, X_m]$, *vemos que* $\varnothing$ *é uma base de Gröbner para* I *que não tem nenhum polinômio com o número de monômios líderes diferente de* 2. *Claramente* $\Delta_{\prec_{\mathcal{M}}}(I) = \mathcal{M}(X_1, \cdots, X_m)$, *observe agora que se* $X_1^{i_1} \cdots X_m^{i_m}$ *é diferente de* $X_1^{j_1} \cdots X_m^{j_m}$, *então para algum* $r \in \{1, \cdots, m\}$ *tem-se* $i_r \neq j_r$. *Portanto,* $w(X_1^{i_1} \cdots X_m^{i_m}) = (i_1, \cdots, i_m) \neq (j_1, \cdots, j_m) = w(X_1^{j_1} \cdots X_m^{j_m})$. *Logo,* $\Delta_{\prec_{\mathcal{M}}}(I)$ *não possui monômios distintos de mesmo peso. Concluímos que* I *e* $\prec_{\mathcal{M}}$ *satisfazem as condições de domínios de ordem. O código* $C(I, L_1)$ *com* $\vec{s} = (0, \cdots, s)$ *é o código generalizado de Reed-Muller* $RM_q(s, m)$. *Da mesma forma, os códigos* $C(I, L_2)$ *e* $C(I, L_3)^\perp$ *são melhoramentos dos códigos generalizados de Reed-Muller considerados nos Exemplos 3.1 e 4.1.*

Dados I e $\prec_w$ tais que as condições de domínios de ordem são satisfeitas, podemos querer construir códigos pela avaliação de um subconjunto $U \subsetneq \mathcal{V}_{\mathbb{F}_q}(I)$. A observação abaixo trata desta situação

Observação 6.1 *Assuma que o par* I *e* $\prec_w$ *satisfazem as condições de domínios de ordem. Seja* $U \subseteq \mathcal{V}_{\mathbb{F}_q}(I)$. *Todo conjunto finito de pontos é uma variedade e , mais ainda, existem polinômios* $H_1, \cdots, H_r$ *tais que o ideal anulador de* U *é igual*

$$I_U = I_q + \langle H_1, \cdots, H_r \rangle$$

As estimativas de distância mínima de $C(I, L)$ *e* $C(I, L)^\perp$ *ainda valem se estes códigos são feitos pela avaliação em* U *em vez de na variedade inteira* $\mathcal{V}_{\mathbb{F}_q}(I)$. *Tudo que precisamos fazer é substituir* I_q *por* I_U *na Definição 3.1, Definição 3.2, Proposição 6.1, Definição 6.3 e Teorema 6.1.*

Capítulo 7

Funções peso e domínios de ordem

O conceito de função ordem foi introduzido por Hoholdt et al. em [10]. Seu objetivo foi simplificar o tratamento de códigos geométricos de Goppa de um ponto e fornecer uma linguagem para facilitar a generalização de códigos geometricos de Goppa de um ponto para objetos de dimensão maior, como por exemplo curvas. O conceito foi ainda desenvolvido em [15] e [8]. Aqui, descrevemos algumas terminologias de [8].

Definição 7.1 *Sejam R uma k-álgebra e Γ um subsemigrupo de $\mathbb{N}_0^r$ para algum r. Seja $\prec$ uma ordenação monomial em $\mathbb{N}_0^r$. Uma aplicação sobrejetiva $\rho : R \to \Gamma_{-\infty} = \Gamma \cup \{-\infty\}$ que satisfaz as seis condições abaixo é chamada de função peso*

(W.0) $\rho(f) = -\infty$ se, e somente se, $f = 0$
(W.1) $\rho(af) = \rho(f)$ $\forall a \in \mathbb{F}_q$ diferente de zero
(W.2) $\rho(f + g) \preceq max\{\rho(f), \rho(g)\}$ e a igualdade ocorre quando $\rho(f) \prec \rho(g)$
(W.3) Se $\rho(f) \prec \rho(g)$ e $h \neq 0$ então $\rho(fh) \prec \rho(gh)$
(W.4) Se f e g são diferentes de zero e $\rho(f) = \rho(g)$, então existe um $a \in \mathbb{F}_q$ não nulo tal que $\rho(f - ag) \prec \rho(g)$
(W.5) Se f e g são diferentes de zero, então $\rho(fg) = \rho(f) + \rho(g)$.

Uma k-álgebra com uma função peso é chamada domínio de ordem e Γ é chamado semigrupo de valores de ρ.

De [8] Th. 9.1 e Th. 10.4 sabemos que se o semigrupo de valores Γ é finitamente gerado, então pode ser descrito na linguagem da teoria de bases de Gröbner. Nós temos o seguinte resultado que conecta a Definição 7.1 com a teoria do capítulo anterior.

Teorema 7.1 *Sejam $\prec_w$ a ordenação grau-ponderada generalizada em $\mathcal{M}(X_1, \cdots, X_m)$ e $I \subseteq k[X_1, \cdots, X_m]$ um ideal. Se I e $\prec_w$ satisfazem as condições de domínio de ordem (Definição 6.2) então $R = k[X_1, \cdots, X_m]/I$ é um domínio de ordem com uma função peso definida como segue: Dado $f \in k[X_1, \cdots, X_m]/I$ não nulo, escreva $f = F + I$ onde $Supp(F) \subseteq \Delta_{\prec_w}(I)$. Temos $\rho(f) = wdeg(F)$ e $\rho(0) = -\infty$.*
Qualquer função peso com um semigrupo de valores Γ finitamente gerado pode ser descrita como acima.

Demonstração. Vamos mostrar somente a primeira parte do teorema. Em relação a última parte indicamos a prova em [8, pág. 379, Corolário 5.7]. Assuma que I e $\prec_w$ satisfazem as condições de domínios de ordem. As propriedades (W.0), (W.1) e (W.2) são obviamente satisfeitas. Dados $f = F_1 + I$ e $g = F_2 + I$ com $Supp(F_1) \subseteq \Delta_{\prec_w}(I)$ e $Supp(F_2) \subseteq \Delta_{\prec_w}(I)$. Se $\rho(f) = \rho(g)$ então $wdeg(F_1) = wdeg(F_2)$, isto é, $w(lm(F_1)) = w(lm(F_2))$ e consequentemente $lm(F_1) = lm(F_2)$. Seja b o coeficiente 1íder de F_1 e c o coeficiente líder de F_2. Se escolhermos $a = b/c$, temos que $\rho(f - ag) = wdeg(F_1 - aF_2) \prec wdeg(F_2) = \rho(g)$. Logo o resultado de (W.4) acontece. Observe agora que $fg = F_1F_2 + I$ e $wdeg(F_1F_2) = w(lm(F_1F_2)) = w(lm(F_1)) + w(lm(F_2)) = \rho(f) + \rho(g)$. O

$Supp(F_1F_2)$ pode não estar na pegada de I, mas claramente F_1F_2 tem um único monômio de maior grau. Pelo Lema 6.1 temos $wdeg(F_1F_2) = wdeg(F_1F_2\ rem\ \mathcal{G})$. Chamando $F = F_1F_2\ rem\ \mathcal{G}$ temos que $fg = F + I$ e $\rho(fg) = wdeg(F) = wdeg(F_1F_2) = \rho(f) + \rho(g)$. A propriedade (W.5) está demonstrada. Finalmente, (W.3) é uma consequência de (W.5)(portanto, (W.3) não é necessária na definição de função peso). ■

Como mencionado anteriormente, os ideais e a ordenação monomial considerados nos Exemplos 5.2 e 6.1 satisfazem as condições de domínios de ordem. Portanto, pelo Teorema 7.1 os anéis quociente correspondentes são domínios de ordem e os pesos correspondem as funções peso do Teorema 7.1.

Capítulo 8

Códigos de domínios de ordem

Nós agora descrevemos os códigos relacionados com domínios de ordem. Vamos precisar de duas definições.

Definição 8.1 *Seja R uma $\mathbb{F}_q$-álgebra. Uma aplicação sobrejetiva $\varphi : R \to \mathbb{F}_q^n$ é chamada morfismo de $\mathbb{F}_q$-álgebras se φ é $\mathbb{F}_q$-linear e se*

$$\varphi(fg) = \varphi(f) * \varphi(g)$$

para todo $f, g \in R$ (Aqui, $*$ significa o produto coordenada a coordenada definido no Capítulo 4).

Definição 8.2 *Seja $\rho : R \to \Gamma \cup \{-\infty\}$ uma função peso. Um conjunto*

$$\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$$

é dito uma base bem comportada para R.

É claro que todo domínio de ordem possui uma base bem comportada. Lembre que nós na Definição 3.1 introduzimos o conceito de base bem comportada para $L \subseteq R_q$. O conceito de base bem comportada para um domínio de ordem R como definimos acima não é o mesmo. Entretanto, os dois conceitos estão intimamentes relacionados.

Proposição 8.1 *Assuma R um domínio de ordem sobre k. Se $\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$ é uma base bem comportada para R, então é uma base para R como um espaço vetorial sobre k.*

Demonstração. Seja $\{f_{\alpha_1}, f_{\alpha_2}, \cdots, f_{\alpha_m}\} \subset \{f_\alpha \mid \alpha \in \Gamma\}$ com $\alpha_1 < \alpha_2 < \cdots < \alpha_m$. Considere a $\mathbb{F}_q-$combinação linear $a_1 f_{\alpha_1} + \cdots + a_m f_{\alpha_m} = 0$. Aplicando a função ρ temos que $\rho(a_1 f_{\alpha_1} + \cdots + a_m f_{\alpha_m}) = \rho(0) = -\infty$, mas como $f_{\alpha_1}, \cdots, f_{\alpha_m}$ são distintos temos que $\rho(a_1 f_{\alpha_1} + \cdots + a_m f_{\alpha_m}) = max\{\rho(a_1 f_{\alpha_1}), \cdots, \rho(a_m f_{\alpha_m})\} = \rho(a_j f_{\alpha_j})$ para algum j. Logo, $\rho(a_j f_{\alpha_j}) = -\infty \Rightarrow a_j = 0$. Logo, temos que $a_i = 0$ para $i = 1, \cdots, m$, e portanto $\{f_{\alpha_1}, f_{\alpha_2}, \cdots, f_{\alpha_m}\}$ é linearmente independente. Agora seja $f \neq 0 \in R$, logo existe $f_{\alpha_1} \in \{f_\alpha \mid \alpha \in \Gamma\}$ tal que $\rho(f_{\alpha_1}) = \rho(f)$. Por (W.4) existe $a_1 \neq 0 \in \mathbb{F}_q$ tal que $\rho(f - a f_{\alpha_1}) < \rho(f_{\alpha_1})$. Se $\rho(f - a_1 f_{\alpha_1}) = -\infty$ acabou. Caso contrário, existe $f_{\alpha_2} \in \{f_\alpha \mid \alpha \in \Gamma\}$ tal que $\rho(f_{\alpha_2}) = \rho(f - a_1 f_{\alpha_1})$, mas por (W.4) existe $a_2 \neq 0 \in \mathbb{F}_q$ tal que $\rho((f - a_1 f_{\alpha_1}) - a_2 f_{\alpha_2}) < \rho(f_{\alpha_2})$. Se $\rho(f - a_1 f_{\alpha_2} - a_2 f_{\alpha_2}) = -\infty$ acabou. Caso contrário, repetimos este processo novamente. Agora note que a sequência:

$$(\alpha) := \alpha_1 > \alpha_2 > \alpha_3 > \cdots$$

é uma sequência (não necessariamente infinita) estritamente decrescente de elementos de $\Gamma \subseteq \mathbb{N}_0^r$. Como $\prec$ é uma ordem monomial sobre $\mathbb{N}_0^r$, logo $\prec$ é uma boa ordem sobre $\mathbb{N}_0^r$, então segue que a sequência (α) eventualmente termina, isto é; existe $m \in \mathbb{N}$ tal que $(\alpha) = \alpha_1 > \alpha_2 > \cdots > \alpha_m$. Logo, após repetirmos este processo m vezes, obtemos:

$$\rho(f - a_1 f_{\alpha_1} - a_2 f_{\alpha_2} - \cdots - a_m f_{\alpha_m}) = -\infty$$

o que nos diz que $f = a_1 f_{\alpha_1} + \cdots + a_m f_{\alpha_m}$. Para o caso geral veja [8, Th. Pro. 3.2 e Def. 3.1]. ■

Observação 8.1 *Sejam duas bases bem comportadas* $\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$ *e* $\{g_\lambda \mid \rho(g_\lambda) = \lambda, \lambda \in \Gamma\}$*, então* $\forall \eta \in \Gamma$, g_η *é uma combinação linear de elementos de* $\{f_\lambda \mid \lambda \preceq \eta\}$ *e o coeficiente de* f_η *na nesta expreção é diferente de zero.*

Segue da Observação 8.1 que não tem importância na próxima definição qual base bem comportada é considerada.

Definição 8.3 *Seja* R *um domínio de ordem sobre* $\mathbb{F}_q$ *com função peso* $\rho : R \to \Gamma \cup \{-\infty\}$ *e* $\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$ *uma base bem comportada. Seja* $\varphi : R \to \mathbb{F}_q^n$ *um morfismo como na Definição 8.1. Defina* $\alpha(1) = 0$*. Para* $i = 2, \cdots, n$ *defina recursivamente* $\alpha(i)$ *como o menor elemento de* Γ *que é maior do que* $\alpha(1), \cdots, \alpha(i-1)$ *e satisfaz*

$$\varphi(f_{\alpha(i)}) \notin Span_{\mathbb{F}_q}\{\varphi(f_\lambda) \mid \lambda \prec_{\mathbb{N}_0^r} \alpha(i)\}.$$

Escreva $\Delta(R, \rho, \varphi) = \{\alpha(1), \cdots, \alpha(n)\}$.

Definição 8.4 *Para* $\lambda \in \Delta(R, \rho, \varphi)$ *defina*

$$\sigma(\lambda) = \#\{\gamma \in \Delta(R, \rho, \varphi) \mid \gamma - \lambda \in \Gamma\}.$$

Para $\lambda \in \Gamma$ *defina*

$$\mu(\lambda) = \#\{\alpha \in \Gamma \mid \lambda - \alpha \in \Gamma\}.$$

Agora podemos definir os códigos.

Definição 8.5 *Seja* R *um domínio de ordem sobre* $\mathbb{F}_q$ *e* φ *um morfismo como na Definição 8.1. Considere uma base bem comportada fixa* $\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$*. Para* $\lambda \in \Gamma$ *e* $\delta \in \mathbb{N}$ *considere os códigos*
$E(\lambda) = Span_{\mathbb{F}_q}\{\varphi(f_\eta) \mid \eta \preceq_{\mathbb{N}_0^r} \lambda\}$
$\tilde{E}(\delta) = Span_{\mathbb{F}_q}\{\varphi(f_\eta) \mid \eta \in \Delta(R, \rho, \varphi) \text{ e } \sigma(\eta) \geq \delta\}$
$C(\lambda) = \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c}.\varphi(f_\eta) = 0, \forall \eta \text{ com } \eta \preceq_{\mathbb{N}_0^r} \lambda\}$
$\tilde{C}(\delta) = \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c}.\varphi(f_\eta) = 0, \forall \eta \in \Delta(R, \rho, \varphi) \text{ com } \mu(\eta) < \delta\}$.

Observação 8.2 *Da Observação 8.1 concluímos que a escolha da base bem comportada não é importante na definição dos códigos* $E(\lambda)$ *e* $C(\lambda)$.

De [10, Th.4.13 e Pro. 4.23] e [2. Th. 33] temos o seguinte teorema. O resultado relativo e $C(\lambda)$ e $\tilde{C}(\delta)$ é conhecido como cota ordem.

Teorema 8.1 *A ditância mínima de* $E(\lambda)$ *é pelo menos*

$$min\{\sigma(\eta) \mid \eta \preceq_{\mathbb{N}_0^r} \lambda\} \tag{8.1}$$

e a distância mínima de $C(\lambda)$ *é pelo menos*

$$min\{\mu(\eta) \mid \lambda \prec_{\mathbb{N}_0^r} \eta \text{ e } \eta \in \Delta(R, \rho, \varphi)\} \geq min\{\mu(\eta) \mid \lambda \prec_{\mathbb{N}_0^r}\}. \tag{8.2}$$

As distâncias mínimas de $\tilde{E}(\delta)$ *e* $\tilde{C}(\delta)$ *são pelo menos* δ.

Lembre do Teorama 7.1 que se Γ é um semigrupo de valores finitamente gerado então o correspondente domínio de ordem R pode ser descrito como um anel quociente. Mostraremos agora que para tais domínios de ordem o Teorema 8.1 é uma consequência direta da teoria desenvolvida na Seção 6. Começamos com a seguinte caracterização de φ.

Proposição 8.2 *Seja $\varphi : R = \mathbb{F}_q[X_1, \cdots, X_m]/I \to \mathbb{F}_q^n$ um morfismo como na Definição 8.1. Então existe um conjunto*

$$U = \{P_1, \cdots, P_n\} \subseteq \mathcal{V}_{\mathbb{F}_q}(I)$$

tal que $\varphi(F + I) = (F(P_1), \cdots, F(P_n))$, para todo $F + I \in R$. Os $P_i's$ são diferentes dois a dois.

Demonstração. Seja $\pi_i : \mathbb{F}_q^n \to \mathbb{F}_q$ a aplicação de projeção na i-ésima coordenada, isto é, $\pi_i(a_1, a_2, \cdots, a_n) = a_i$. Como φ é uma aplicação $\mathbb{F}_q$-linear sobrejetora, então para cada $i = 1, \cdots, n$ a aplicação $\varphi_i : \mathbb{F}_q[X_1, \cdots, X_m]/I \to \mathbb{F}_q$ definida por $\varphi_i(F + I) = \pi_i(\varphi(F + I))$ é $\mathbb{F}_q$-linear e sobrejetora, além disso essas aplicações são todas distintas. Seja $a = (a_1, a_2, \cdots, a_n) \in \mathbb{F}_q^n$ tal que $\varphi(1 + I) = a$, e sejam $b = (b_1, b_2, \cdots, b_n) \in \mathbb{F}_q^n$ com $b_i \neq 0$ para todo $i = 1, \cdots, n$ e $F + I \in \mathbb{F}_q[X_1, \cdots, X_m]/I$ tal que $\varphi(F + I) = b$. Veja que $\varphi(F + I) = \varphi((1 + I)(F + I)) = \varphi(1 + I) * \varphi(F + I) = (a_1b_1, \cdots, a_nb_n) = (b_1, \cdots, b_n)$, assim $\varphi(1 + I) = (1, 1, \cdots, 1)$, logo φ é um homomorfismo de anéis. E como φ é $\mathbb{F}_q$-linear segue que $\varphi(c + I) = (c, c, \cdots, c)$ para todo $c \in \mathbb{F}_q$. Assim, cada φ_i é um homomorfismo com $\varphi_i(c + I) = c$ para todo $c \in \mathbb{F}_q$. Sejam

$$\begin{gathered} P_1 = (P_1^{(1)}, P_1^{(2)}, \cdots, P_1^{(m)}) \in \mathbb{F}_q^m \\ P_2 = (P_2^{(1)}, P_2^{(2)}, \cdots, P_2^{(m)}) \in \mathbb{F}_q^m \\ \vdots \\ P_n = (P_n^{(1)}, P_n^{(2)}, \cdots, P_n^{(m)}) \in \mathbb{F}_q^m \end{gathered}$$

tais que

$$\begin{gathered} P_1^{(1)} = \varphi_1(X_1 + I), P_1^{(2)} = \varphi_1(X_2 + I), \cdots, P_1^{(m)} = \varphi_1(X_m + I) \\ P_2^{(1)} = \varphi_2(X_1 + I), P_1^{(2)} = \varphi_2(X_2 + I), \cdots, P_2^{(m)} = \varphi_2(X_m + I) \\ \vdots \\ P_n^{(1)} = \varphi_n(X_1 + I), P_n^{(2)} = \varphi_n(X_2 + I), \cdots, P_n^{(m)} = \varphi_n(X_m + I) \end{gathered}$$

Seja $\prec$ uma ordem monomial sobre o conjunto de todos os monômios em $X_1, \cdots, X_m$. Temos que o conjunto $\{M + I | M \in \Delta_\prec(I)\}$ é uma base para $\mathbb{F}_q[X_1, \cdots, X_m]/I$ como $\mathbb{F}_q$-espaço vetorial. Seja $M = X_1^{\alpha_1}X_2^{\alpha_2} \cdots X_m^{\alpha_m} \in \Delta_\prec(I)$, e seja $G = cM$, onde $c \in \mathbb{F}_q$. Logo

$$\begin{gathered} G(P_i) = G((P_i^{(1)}, P_i^{(2)}, \cdots, P_i^{(m)})) = c(P_i^{(1)})^{\alpha_1}(P_i^{(2)})^{\alpha_2} \cdots (P_i^{(m)})^{\alpha_m} = \\ \varphi_i(c + I)\varphi_i(X_1^{\alpha_1} + I)\varphi_i(X_2^{\alpha_2} + I) \cdots \varphi_i(X_m^{\alpha_m} + I) = \varphi_i(cX_1^{\alpha_1}X_2^{\alpha_2} \cdots X_m^{\alpha_m} + I) = \varphi_i(cM + I). \end{gathered}$$

Assim, $\varphi_1(cM + I) = cM(P_i)$ para todo $M \in \Delta_\prec(I)$, $c \in \mathbb{F}_q$ e $i = 1, \cdots, n$. Como qualquer $f \in \mathbb{F}_q[X_1, \cdots, X^m]/I$ pode ser escrito como $f = F + I$ onde $F \in span\mathbb{F}_q\{M | M \in \Delta_\prec(I)\}$ e φ_i é $\mathbb{F}_q$-linear, segue que $\varphi_i(F + I) = F(P_i)$ para todo $i = 1, \cdots, n$. Assim, $\varphi(F + I) = (F(P_1), F(P_2), \cdots, F(P_n))$. Agora, vamos mostrar que $P_i \in \mathcal{V}_{\mathbb{F}_q}(I)$ para todo $i = 1, \cdots, n$. Para todo $F(X_1, \cdots, X_m) \in I$ temos que $\varphi(F(X_1, \cdots, X_m) + I) = \varphi(0 + I) = (0, 0, \cdots, 0) = (F(P_1), \cdots, F(P_n))$. Logo $F(P_1) = F(P_2) = \cdots = F(P_n) = 0$ para todo $F \in I$, assim $P_1, P_2, \cdots, P_n \in \mathcal{V}_{\mathbb{F}_q}(I)$. ■

Aplicando a Proposição 8.2 para domínios de ordem com semigrupo de valores finitamente gerado vemos que os códigos na Definição 8.5 são do tipo coberto pela Observação 6.1 da Seção 6. Em vez de lidar com o caso geral $U \subseteq \mathcal{V}_{\mathbb{F}_q}(I)$ vamos seguir concentrados na situação $U = \mathcal{V}_{\mathbb{F}_q}(I)$. Podemos facilmente generalizar nossos resultados, substituindo como na Observação 6.1, I_q por I_U. Nossa mais importante observação é que

$$\Delta(R, \rho, \varphi) = w(\Delta_{\prec_w}(I_q)). \tag{8.3}$$

Para mostrar (8.3) começamos notando que, por construção $\Delta(R,\rho,\varphi)$ tem cardinalidade n e como $\Delta_{\prec_w}(I_q)$ é base para $\mathbb{F}_q^n$ e não tem monômios distintos de mesmo peso, $w(\Delta_{\prec_w}(I_q))$ também tem cardinalidade n. Portanto, basta mostrar que

$$\Delta(R,\rho,\varphi) \subseteq w(\Delta_{\prec_w}(I_q))$$

Claramente, $\alpha(1) = 0 \in w(\Delta_{\prec_w}(I_q))$ já que toda pegada não vazia contém 1. Suponha por contradição que $\alpha(i) \notin w(\Delta_{\prec_w}(I_q))$ para algum $2 \leq i \leq n$. Seja $f_{\alpha(i)} = F + I,\ w(lm(F)) = \alpha(i)$. Seja $\mathcal{G}$ uma base de Gröbner para I_q, então $F\ rem\ \mathcal{G}$ é tal que $Supp(F\ rem\ \mathcal{G}) \subseteq \Delta_{\prec_w}(I_q)$ e $F - F\ rem\ \mathcal{G} \in I_q$. Como $\mathcal{V}_{\mathbb{F}_q}(I_q) = \mathcal{V}_{\mathbb{F}_q}(I)$ temos $\varphi(F - F\ rem\ \mathcal{G} + I) = 0$. Daí,

$$\varphi(f_{\alpha(i)}) = \varphi(F+I) = \varphi(F - (F - F\ rem\ \mathcal{G} + I)) = \varphi(F\ rem\ \mathcal{G} + I) \tag{8.4}$$

A própria definição de base de Gröbner garante que $lm(F\ rem\ \mathcal{G}) \in \Delta_{\prec_w}(I_q)$. Portanto, $lm(F\ rem\ \mathcal{G}) \prec_w lm(F)$. Mas, por (8.4) e pela Definição 8.3, $\alpha(i) \notin \Delta(R,\rho,\varphi)$. O que é uma contradição. Logo, (8.3) acontece. Com (8.3) nas mãos nós estabelecemos as seguintes conexões: $E(\lambda)$ e $C(\lambda)$ são iguais a $C(I,L_1)$ e $C(I,L_1)^{\perp}$, respectivamente, com L_1 como em (6.1). $\tilde{E}(\delta)$ é igual a $C(I,L_2)$, L_2 como em (6.2), e $\tilde{C}(\delta)$ é igual a $C(I,L_3)^{\perp}$ e L_3 como em (6.3). Concluímos que as cotas no Teorema 8.1 das distâncias mínimas de $E(\lambda)$, $\tilde{E}(\delta)$, $C(\lambda)$ e $\tilde{C}(\delta)$ são consequências do Teorema 6.1.

Capítulo 9

Códigos geométricos de Goppa de um ponto

Uma das razões mais importantes para introduzir os domínios de ordem em [10] foi para se ter uma fácil descrição dos códigos geométricos de Goppa de um ponto e também para se ter uma maneira fácil de generalizar a construção dos códigos geométricos de Goppa de um ponto para estruturas algébricas de maior grau de transcendência. Aprensentando nesta dissertação as coisas na ordem reversa do que normalmente é feito, chegamos, finalmente, aos códigos geométricos de Goppa de um ponto.

Seja $\mathcal{P}$ um lugar racional no corpo de funções algébricas $\mathbb{F}$ de uma variável com corpo de constantes $\mathbb{F}_q$. Seja $\mathcal{V}_\mathcal{P}$ a valorização correspondente a $\mathcal{P}$. Considere a estrutura algébrica

$$R = \cup_{m=0}^{\infty} \mathcal{L}(m\mathcal{P}). \tag{9.1}$$

Defina $\rho = -\mathcal{V}_\mathcal{P}$ temos $\rho(R) = \Gamma \cup \{-\infty\}$ onde $\Gamma \subseteq \mathbb{N}_0$ é conhecido como semigrupo de Weierstrass correspondente a ρ. Por verificação a aplicação $\rho : R \to \Gamma \cup \{-\infty\}$ satisfaz as seis condições na Definição 7.1 e, mais ainda, é uma função peso.
Infelizmente, não é, em geral, uma tarefa fácil determinar a estrutura R acima e, portanto, muitas vezes é difícil encontrar a descrição anel quociente de R garantida pelo Teorema 7.1. Observe, que uma tal descrição foi dada no Exemplo 5.2 no caso da curva Hermetiana sobre $\mathbb{F}_9$.
Os códigos geométricos de Goppa provenientes da estrutura (9.1) são conhecidos como códigos geométricos de Goppa de um ponto. Nós agora explicamos a conexão entre estes códigos e os códigos de variedades afins da Seção 6. Seja $\mathcal{Q}_1, \cdots, \mathcal{Q}_n$ lugares racionais, diferentes dois a dois, e diferentes de $\mathcal{P}$. A aplicação $\varphi : R \to \mathbb{F}_q^n,\ \varphi(f) = (f(\mathcal{Q}_1), \cdots, f(\mathcal{Q}_n))$ é um morfismo como na Definição 8.1. Portanto, da Proposição 8.2 os lugares racionais $\mathcal{Q}_1, \cdots, \mathcal{Q}_n$ correspondem a n diferentes pontos afins $P_1, \cdots, P_n$ em $\mathcal{V}(I_q)$ e $\varphi(F + I) = (F(P_1), \cdots, F(P_n))$. Temos

$$C_\mathcal{L}(\mathcal{Q}_1 + \cdots + \mathcal{Q}_n, \lambda\mathcal{P}) = C(I, L)$$

e

$$C_\Omega(\mathcal{Q}_1 + \cdots + \mathcal{Q}_n, \lambda\mathcal{P}) = C(I, L)^\perp$$

onde

$$L = \{f \in R \mid \rho(f) \leq \lambda\}.$$

As cotas de Goppa da geometria algébrica podem ser aplicadas ao caso dos códigos geométricos de Goppa de um ponto.

Teorema 9.1 *Seja $\mathcal{P}$ um lugar racional como acima e seja R o domínio de ordem correspondente como em (9.1). A distância mínima de $E(\lambda)$ é pelo menos*

$$n - \lambda. \tag{9.2}$$

A distância mínima de $C(\lambda_t)$ é pelo menos

$$t + 1 - g. \tag{9.3}$$

Agora vamos mostrar que as cotas do Teorema 9.1 podem ser vistas como uma concequência do Teorema 8.1. Precisaremos do seguinte lema técnico de [10, Lem. 5.15 e Th. 5.24].

Lema 9.1 *Seja* $\Gamma = \{\lambda_1, \lambda_2, \cdots\}$ *com* $\lambda_1 < \lambda_2 < \cdots$ *um semigrupo em* $\mathbb{N}_0$ *com um número finito de lacunas. Defina*

$$g(i) = \#\{\lambda \in \mathbb{N}_0 \setminus \Gamma \mid \lambda < \lambda_i\}.$$

Para qualquer λ_i *temos* $\#(\Gamma \setminus (\lambda_i + \Gamma)) = \lambda_i$ *e* $\mu(\lambda_i) = i - g(i) + D(i)$ *onde*

$$D(i) = \{(x, y) \mid x, y \in \mathbb{N}_0 \setminus \Gamma \text{ e } x + y = \lambda_i\}.$$

Aqui, $\lambda + \Gamma$ *significa* $\{\lambda + \lambda_1, \lambda + \lambda_2, \cdots\}$.

Teorema 9.2 *Para o caso dos códigos geométricos de Goppa de um ponto a cota em (8.1) é sempre pelo menos tão boa quanto (e às vezes melhor que) a cota em (9.2). Analogamente, a cota em (8.2) é sempre pelo menos tão boa quanto (e às vezes melhor que) a cota em (9.3).*

Demonstração. Para provar a primeira afirmação precisamos considerar números $\lambda_i \in \Delta(R, \rho, \varphi),\ \lambda_i \leq s$. Temos $\sigma(\lambda_i) = \#(\Delta(R, \rho, \varphi) \cap (\lambda_i + \Gamma))$. Da primeira parte do Lema 9.1 vemos que o número de elementos de $\Delta(R, \rho, \varphi)$ que não estão em $\lambda_i + \Gamma$ é, no máximo, λ_i. Portanto, $\sigma(\lambda_i) \geq n - \lambda_i$ com a igualdade acontecendo somente quando $\Gamma \setminus (\lambda_i + \Gamma) \subseteq \Delta(R, \rho, \varphi)$. Concluímos que $min\{\sigma(\lambda_i) \mid \lambda_i \in \Delta(R, \rho, \varphi),\ \lambda_i \leq s\} \geq n - s$. Como consequência da última afirmação temos

$$min\{\mu(\eta) \mid \eta \in \Gamma \text{ e } \lambda_t < \eta\} = min\{i - g(i) + \#D(i) \mid t < i\} \geq t + 1 - g$$

com a igualdade acontecendo se, e somente se, $\lambda_{t+1} = \lambda_t + 1,\ g(t+1) = g$ e $\#D(t+1) = 0$. ∎

Ter mostrado que as cotas do Teorema 8.1 das distâncias mínimas dos códigos $E(\lambda)$ e $C(\lambda)$ são pelo menos tão boas quanto as cotas de Goppa, no caso de R ser da forma em (9.1), torna evidente que se pode considerar a códigos $\tilde{E}(\delta)$ e $\tilde{C}(\delta)$ de (9.1) como códigos geométricos de Goppa de um ponto melhorados.
Foi mostrado em [14, Th. 1] que todas as funções peso numéricas (isto é, funções peso com pesos em $\mathbb{N}_0$) são também da forma (9.1) ou é uma sub-álgebra de tal estrutura. Mudando para semigrupos que não são numéricos as estruturas relacionadas não são mais curvas, mas são de dimensão mais elevadas [8, Sec. 11]. Os códigos relacionados podem ser vistos como generalizações de códigos geométricos de Goppa de um ponto.

Referências Bibliográficas

[1] H. E. Andersen and O. Geil, Evaluation codes from order domains theory, Finite fields and their applications, 14, (2008), pp. 92 123.

[2] T. Becker and V. Weipsfenning, "Gröbner Bases: A Computational aproach to Commutative Algebra,"Springer Velarg, Berlin, (1993)

[3] D. Cox, J. Little and D. O'Shea, "Ideals, Varieties and Algorithms, 2nd ed.,"Springer, Berlim, (1997).

[4] D. Cox, J. Little and D. O'Shea, "Using Algebraic Geometry,"Springer, Berlim, (1998).

[5] P. Delsarte, J. M. Goethals and F. J. Mac Williams, On generalized Reed-Muller codes and their relatives, Information and control, 16, (1970), 403 442.

[6] J. Fitzgerald and R. F. Lax, Decoding Affine Variety Codes Using Gröbner bases, Designs, Codes and Cryptography, 13, 2, (1998), pp. 147 158.

[7] O. Geil and T. Hoholdt, On Hyperbolic Codes, Proc. of AAECC-14, Lecture Notes in Comput. Sci. 2227, Springer, Berlim, (2001), pp. 159 171.

[8] O. Geil and R. Pellikaan, On the Structure of Order Domains, Finite Fields and their Applications, 8, (2002), pp. 369 396.

[9] O. Geil and C. Thommesen, On the Feng Rao Bound for generalized Hamming Weights, Proc. of AECC-16, Lecture Notes in Comput. Sci. 3857, Springer, Berlin, (2006), pp. 295 306.

[10] T. Hoholdt, J van Lint and R. Pellikaan, "Algebraic Geometry Codes", Chapter 10 in Hanbook of Coding Theory (V.S. Pless and W.C. Huffman, eds.), vol.1, Elsevier, Amsterdam, (1998), pp. 871 961.

[11] G. Kabatiansky, Two Generalizations of Product Codes, Proc. of academy of Science USSR, Cybernetics and theory of Regulation, 232, vol. 6, (1997), pp. 1227 1280 (in Russian).

[12] T. Kasami, S.Lin, and W. Peterson, New generalizations of the Reed Muller Codes. I. Primitive Codes, IEEE Transactions on Informations Theory, 14, (1968), pp. 189 199.

[13] J. Massey, D. J. Costello and J. Justesen, Polynomial Weights and Code Constructions, IEEE Trans. Inf. Theory, 19, (1973), pp. 101 110.

[14] R. Matsumoto, Miura's Generalization of One Point AG Codes is Equivalent to Hoholdt, van Lint and Pellikaan's Generalization, IEICE Trans. Fundamentals, E82 A, no. 10 (1969), 2007 2010.

[15] M. E. O'Sullivan, New Codes for the Berlekamp Massey Sakata algorithm, Finite Fields and Their Applications, 7, 2001, pp. 293 317.

[16] O. Geil, On the Second Weight of Generalized Reed-Muller Codes, Department of Mathematical Science, Aalborg University.

[17] O. Geil, Evaluation Codes from an Affine Variety Code Perspective, World Scientific Review, Volume-9in x 6in, (2008).