DANILO ADRIAN MARQUES

O estudo de pesos generalizados de Hamming através de equações polinomiais

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2010

DANILO ADRIAN MARQUES

O estudo de pesos generalizados de Hamming através de equações polinomiais

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: Geometria Algébrica e Geometria Diferencial.

Orientador: Prof. Dr. Cícero Fernandes de Carvalho.

UBERLÂNDIA - MG
2010

Dados Internacionais de Catalogação na Publicação (CIP)

M357e Marques, Danilo Adrian, 1985-
O estudo de pesos generalizados de Hamming através de equações polinomiais [manuscrito] / Danilo Adrian Marques. - 2010.
82 f.

Orientador: Cícero Fernandes de Carvalho.

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

1. Geometria algébrica - Teses. 2. Geometria diferencial - Teses. I. Carvalho, Cícero Fernandes de. II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III. Título.

CDU: 514.16

Elaborado pelo Sistema de Bibliotecas da UFU / Setor de Catalogação e Classificação

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: DANILO ADRIAN MARQUES.

NÚMERO DE MATRÍCULA: 93804.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica e Geometria Diferencial.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: O estudo de pesos generalizados de Hamming através de equações polinomiais.

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 25 de fevereiro de 2010, às 15h00min, 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. Victor Gonzalo Lopez Neumann UFU - Universidade Federal de Uberlândia	

Uberlândia-MG, 25 de fevereiro de 2010.

Dedicatória

Dedico primeiramente a Deus, pois sem Ele eu não teria chegado até aqui. Dedico aos meus pais Antônio e Nilce e minha namorada Cláudia Helena que em momentos de fraqueza, sempre me deram força, amor, carinho e apoio para continuar. E, aos meus familiares e amigos, que sempre acreditaram em mim e nunca duvidaram da minha capacidade.
Obrigado a todos pois, sem vocês, não alcançaria esse sucesso.

Agradecimentos

Gostaria de agradecer a agência CAPES pelo fornecimento da bolsa de pesquisa ao longo da Pós-Graduação; ao meu orientador, Cícero Fernandes de Carvalho pelos ensinamentos dados e aos professores Paulo Roberto Brumatti e Victor Gonzalo Lopez Neumann por terem aceito o convite para fazerem parte da minha banca.

MARQUES, D. A. *O estudo de pesos generalizados de Hamming através de equações polinomiais.* 2010. 82 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho estudamos os pesos generalizados de Hamming de alguns códigos de avaliação definidos sobre variedades, utilizando a resolução de sistemas de equações polinomiais e também a chamada Cota da Pegada.

Palavras-chave: Cota da Pegada, Pesos Generalizados de Hamming, Hierarquia de Pesos, Duais de Códigos de Avaliação.

MARQUES, D. A. *The study of generalized Hamming weights through polynomial equations.* 2010. 82 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work, we study the generalized Hamming weights of some codes defined over varieties, using the solutions of systems of polynomial equations and also the so-called Footprint Bound.

Keywords: Footprint Bound, Generalized Hamming Weights , Weights Hierarchy, Duals of Evaluation Codes.

Sumário

Introdução

Essa dissertação trata do estudo dos pesos generalizados de Hamming para certos códigos lineares em que é conhecida a sua matriz checagem de paridade. Para este estudo vamos utilizar a cota da pegada e os resultados provados por Geil em [2].
Este trabalho está dividido em três capítulos, sendo que no primeiro, veremos conceitos e resultados relacionados à anéis de polinômios que serão aplicados para estimar o tamanho de certas variedades, dentre estes conceitos estão ordem de monômios e algoritmo da divisão em $K[X_1, \ldots, X_n]$, a cota da pegada e a resultante entre dois polinômios em $K[X_1, \ldots, X_n]$.
No segundo capítulo, veremos conceitos e alguns resultados relacionados a teoria de códigos, como o que são os pesos generalizados de Hamming e a cota de Singleton generalizada.
No último capítulo, fazemos a ligação entre os pesos generalizados de Hamming e o tamanho de certas variedades. Neste capítulo, apresentaremos resultados relacionados aos pesos generalizados de Hamming e duais de códigos de avaliação sobre uma variedade.
Na última seção deste capítulo, estimamos os pesos generalizados de Hamming para alguns códigos (no primeiro caso dos códigos de Klein melhorados, calculamos estes pesos) e também obtemos uma cota inferior para estes pesos no caso de códigos construídos através de pegadas.
O primeiro capítulo está baseado em resultados de [1], o segundo em resultados encontrados em [4] e [3], e o último capítulo foi baseado em [2].

DANILO ADRIAN MARQUES
Uberlândia-MG, 25 de fevereiro de 2010.

Capítulo 1

Divisão em Anéis de Polinômios

1.1 Conceitos Preliminares

Vamos trabalhar com o anel de polinômios $K[X_1, \ldots, X_n]$.

Definição 1.1.1 *Um monômio em $X_1, \ldots, X_n$ é um produto da forma*

$$X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdot \ldots \cdot X_n^{\alpha_n},$$

onde todos os expoentes $\alpha_1, \ldots, \alpha_n$ são inteiros não-negativos. O grau total deste monômio é a soma

$$\alpha_1 + \cdots + \alpha_n.$$

Observação 1.1.2
Podemos simplificar a notação para monômios como a seguir:
Seja $\alpha = (\alpha_1, \ldots, \alpha_n)$ uma n-upla de inteiros não-negativos. Então definimos:

$$X^\alpha := X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdot \ldots \cdot X_n^{\alpha_n}.$$

Definição 1.1.3 *Seja n um inteiro positivo. Chamamos de $\mathbb{N}_0^n$ o conjunto:*

$$\mathbb{N}_0^n := \{(\alpha_1, \ldots, \alpha_n) : \alpha_1, \ldots, \alpha_n \text{ são inteiros não-negativos}\}.$$

Observação 1.1.4 *Temos que a observação 1.1.2 estabelece uma correspondência bijetiva entre monômios em $K[X_1, \ldots, X_n]$ e o conjunto $\mathbb{N}_0^n$. Além disso, qualquer ordem $>$ sobre o espaço $\mathbb{N}_0^n$ nos dará uma ordem sobre monômios: se $\alpha > \beta$, de acordo com esta ordem, também diremos que $X^\alpha > X^\beta$.*

Definição 1.1.5 *Um subconjunto $I \subset K[X_1, \ldots, X_n]$ é um ideal se satisfaz as seguintes condições:*

i) $0 \in I$.

ii) Se $f, g \in I$, *então* $f + g \in I$.

iii) Se $f \in I$ *e* $h \in K[X_1, \ldots, X_n]$, *então* $hf \in I$.

Definição 1.1.6 *Sejam $f_1, \ldots, f_s$ polinômios em $K[X_1, \ldots, X_n]$. Chamamos de ideal gerado por $f_1, \ldots, f_s$ o conjunto:*

$$\langle f_1, \ldots, f_s \rangle := \left\{ \sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in K[X_1, \ldots, X_n] \right\}.$$

1.2 Ordens Sobre Monômios

Examinando em detalhes o algoritmo da divisão em $K[X]$ e o escalonamento para sistemas de equações lineares (ou matrizes), veremos que uma noção de ordem de termos é um ingrediente chave em ambos (embora isto não seja freqüentemente enfatizado). Por exemplo, dividindo $f(X) = X^5 - 3X^2 + 1$ por $g(X) = X^2 - 4X + 7$ pelo método padrão, faríamos o seguinte:

i) escreveríamos os termos do polinômio em ordem decrescente de grau de X;

ii) no primeiro passo, o termo líder (o termo de maior grau) em f é:

$$X^5 = X^3 \cdot X^2 = X^3 \cdot (\text{termo líder em } g).$$

Então, subtraímos $X^3 \cdot g(X)$ de f para cancelar o termo líder, obtendo $4X^4 - 7X^3 - 3X^2 + 1$;

iii) então, repetiríamos o mesmo processo sobre $f(X) - X^3 \cdot g(X)$, etc. até obtermos um polinômio de grau menor que 2.

Logo, para o algoritmo da divisão sobre polinômios de uma variável, lidamos com a ordem de grau sobre monômios de uma variável:

$$\ldots > X^{m+1} > X^m > \ldots > X^2 > X > 1. \tag{1.1}$$

Similarmente, nas equações lineares, isto é expressado pela ordem das variáveis $X_1, \ldots, X_n$ como a seguir:

$$X_1 > X_2 > \ldots > X_n. \tag{1.2}$$

Escrevemos os termos nas nossas equações em ordem decrescente. Além disso, num sistema na forma escalonada (onde a primeira entrada não nula de cada linha é 1, e todas as outras entradas na coluna contendo um líder 1 são zero) as equações são listadas com seus termos líderes em ordem decrescente.

Da evidência acima, podemos imaginar que uma componente muito importante de alguma extensão da divisão e escalonamento para polinômios arbitrários em várias variáveis seja uma ordem de termos em polinômios em $K[X_1, \ldots, X_n]$. Aqui, discutiremos as propriedades desejáveis que as ordens poderiam ter, e construiremos vários exemplos diferentes que satisfarão nossas necessidades. Cada uma destas ordens será usada em diferentes contextos.

Definição 1.2.1 *Uma ordem monomial em $K[X_1, \ldots, X_n]$ é qualquer relação $>$ sobre $\mathbb{N}_0^n$ (equivalentemente, uma relação no conjunto dos monômios X^α, $\alpha \in \mathbb{N}_0^n$), satisfazendo:*

i) A relação $>$ é uma ordem total (ou linear) sobre $\mathbb{N}_0^n$, isto é, para todo par α, $\beta \in \mathbb{N}_0^n$, exatamente uma das três condições é verdadeira:

$$\alpha > \beta \quad ou \quad \alpha = \beta \quad ou \quad \alpha < \beta;$$

ii) Se $\alpha > \beta$ e $\gamma \in \mathbb{N}_0^n$, então $\alpha + \gamma > \beta + \gamma$;

iii) $>$ *é uma boa ordenação sobre* $\mathbb{N}_0^n$*. Isto significa que todo subconjunto não vazio de* $\mathbb{N}_0^n$ *tem um elemento mínimo em relação a* $>$*.*

Dada uma tal relação $>$ *sobre* $\mathbb{N}_0^n$*, escrevemos* $X^\alpha > X^\beta$ *se, e somente se,* $\alpha > \beta$*.*

O Lema a seguir nos ajudará a entender o que a condição da boa ordenação significa.

Lema 1.2.2 *Uma relação de ordem* $>$ *sobre* $\mathbb{N}_0^n$ *é uma boa ordenação se, e somente se, toda seqüência estritamente decrescente em* $\mathbb{N}_0^n$

$$\alpha_1 > \alpha_2 > \alpha_3 > \dots$$

é finita.

Demonstração:
Provaremos a contra-positiva: A relação $>$ não é uma boa ordenação se, e somente se, existe uma seqüência infinita estritamente decrescente em $\mathbb{N}_0^n$.

($\Rightarrow$) Se $>$ não é uma boa ordenação, então algum subconjunto não vazio $S \subset \mathbb{N}_0^n$ não possui elemento mínimo. Seja $\alpha_1 \in S$. Já que α_1 não é o elemento mínimo, podemos encontrar $\alpha_2 \in S$ tal que $\alpha_1 > \alpha_2$ em S. Então α_2 também não é o elemento mínimo, logo existe $\alpha_3 \in S$ tal que $\alpha_1 > \alpha_2 > \alpha_3$ em S. Continuando este processo, conseguimos uma seqüência infinita estritamente decrescente: $\alpha_1 > \alpha_2 > \alpha_3 > \dots$.
($\Leftarrow$) Dada uma seqüência infinita estritamente decrescente, $\alpha_1 > \alpha_2 > \alpha_3 > \dots$, temos que o conjunto $\{\alpha_1, \alpha_2, \alpha_3, \dots\}$ é um subconjunto não-vazio $S \subset \mathbb{N}_0^n$ que não possui elemento mínimo, e então $>$ não é uma boa ordenação. □

Esse lema será usado para mostrar que vários algoritmos terminam, pois alguns de seus termos são estritamente decrescentes (com respeito a uma determinada ordem fixada) em cada passo do algoritmo.
Como um exemplo simples de uma ordem de monômios, vemos que a ordem numérica usual

$$\dots > m+1 > m > \dots > 3 > 2 > 1 > 0$$

nos elementos de $\mathbb{N}_0$ satisfaz as três condições da Definição 1.2.1. Então, a ordenação grau (1.1) sobre monômios em $K[X]$ é uma ordem de monômios.
Nosso primeiro exemplo de uma ordem sobre n-uplas será a ordem lexicográfica (ou ordem lex, abreviadamente).

Definição 1.2.3 (Ordem Lexicográfica) *Sejam* $\alpha = (\alpha_1, \dots, \alpha_n)$*,* $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}_0^n$*. Dizemos que* $\alpha >_{lex} \beta$ *se no vetor diferença* $\alpha - \beta \in \mathbb{Z}^n$ *a primeira entrada não-nula a partir da esquerda é positiva. Escrevemos* $X^\alpha >_{lex} X^\beta$ *se* $\alpha >_{lex} \beta$*.*

Exemplo 1.2.4 *i)* $(1,2,0) >_{lex} (0,3,4)$ *já que* $\alpha - \beta = (1,-1,-4)$*;*

ii) $(3,2,4) >_{lex} (3,2,1)$ *já que* $\alpha - \beta = (0,0,3)$*;*

iii) As variáveis $X_1, \dots, X_n$ *foram ordenadas de maneira usual pela ordem lex, pois:*

$$X_1 := X^{(1,0,\dots,0)},\ X_2 := X^{(0,1,0,\dots,0)}, \dots,\ X_n := X^{(0,0,\dots,1)}$$

e como

$$(1,0,\ldots,0) >_{lex} (0,1,0,\ldots,0) >_{lex} \ldots >_{lex} (0,0,\ldots,1)\,,$$

temos que

$$X_1 >_{lex} X_2 >_{lex} \ldots >_{lex} X_n.$$

A ordem Lex é análoga a ordem de palavras usadas em dicionários (por isso o nome). Assim podemos ter em vista as entradas das n-uplas $\alpha \in \mathbb{N}_0^n$ como análogo das letras numa palavra, que são ordenadas alfabeticamente por $a > b > \ldots > y > z$.

É importante dar-se conta que existem várias ordens lex, dependendo de como as variáveis são ordenadas. Até agora, temos usado a ordem lex com $X_1 > X_2 > \ldots > X_n$. Mas dada alguma ordem das variáveis $X_1, X_2, \ldots, X_n$, existe uma ordem lex correspondente. Por exemplo, se as variáveis são X e Y, temos então uma primeira ordem lex com $X > Y$ e uma segunda com $Y > X$. No caso geral de n variáveis, existem $n!$ ordens lex. No que segue, a frase "ordem lex"sempre se refere para a primeira com $X_1 > X_2 > \ldots > X_n$, a menos que explicitada de outra forma. E na prática, quando trabalhamos com polinômios em duas ou três variáveis, chamamos as variáveis de X, Y e Z ao invés de X_1, X_2 e X_3.

Observe que na ordem lex, independentemente do grau total, uma variável é maior que qualquer monômio envolvendo variáveis menores, por exemplo, utilizando a ordem lex com $X > Y > Z$, temos $X >_{lex} Y^5Z^3$. Para alguns propósitos, podemos querer levar em consideração também o grau total dos monômios e ordenar monômios de maior grau primeiro. Nossa primeira forma de se fazer isso, é a ordem lexicográfica graduada (ou ordem grlex).

Definição 1.2.5 (Ordem Grau-lex) *Seja $\alpha, \beta \in \mathbb{N}_0^n$. Dizemos que $\alpha >_{grlex} \beta$ se:*

$$|\alpha| := \sum_{i=1}^{n} \alpha_i \; > |\beta| := \sum_{i=1}^{n} \beta_i$$

ou

$$|\alpha| = |\beta| \;\; e \; \alpha >_{lex} \beta.$$

Assim temos que, a ordem grlex primeiro ordena pelo grau total e, caso os monômios possuam o mesmo grau total, "desempata" pela ordem lex.

Exemplo 1.2.6 *i)* $(1,2,3) >_{grlex} (3,2,0)$ *já que* $|(1,2,3)| = 6 > 5 = |(3,2,0)|$*;*

ii) $(1,2,4) >_{grlex} (1,1,5)$ *já que* $|(1,2,4)| = |(1,1,5)|$ *e* $(1,2,4) >_{lex} (1,1,5)$*;*

iii) As variáveis são ordenadas de acordo com a ordem lex, pois:

$$|\,(1,0,\ldots,0)\,| = |\,(0,1,0,\ldots,0)\,| = \ldots = |\,(0,0,\ldots,1)\,| = 1.$$

Como no caso da ordem lex, existem $n!$ ordens grlex sobre n variáveis, dependendo de como as variáveis são ordenadas.

Mais adiante, definiremos uma ordem que usaremos bastante, a ordem grau-ponderada lexicográfica (ver página 35).

1.3 Ordenando Polinômios

Se $f = \sum_\alpha a_\alpha X^\alpha$ é um polinômio em $K[X_1, \ldots, X_n]$ então dada uma ordem monomial $>$ podemos ordenar os monômios de f sem ambigüidades com respeito a $>$.

Exemplo 1.3.1 *Seja* $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2 \in K[X, Y, Z]$

a) Na ordem lex, f *fica ordenado em ordem decrescente da seguinte forma:*

$$f = -5X^3 + 7X^2Z^2 + 4XY^2Z + 4Z^2.$$

b) Na ordem grlex, temos:

$$f = 7X^2Z^2 + 4XY^2Z - 5X^3 + 4Z^2.$$

Usaremos a seguinte terminologia:

Definição 1.3.2 *Sejam* $f = \sum_\alpha a_\alpha X^\alpha$ *um polinômio não nulo em* $K[X_1, \ldots, X_n]$ *e* $>$ *uma ordem monomial.*

i) O multi-grau de f *é:*

$$\text{multigr}(f) = \max\{\alpha \in \mathbb{N}_0^n : a_\alpha \neq 0\} \text{ (o máximo é dado com respeito a } >).$$

ii) O coeficiente líder de f *é:*

$$CL(f) = a_{mutigr(f)} \in K.$$

iii) O monômio líder de f *é:*

$$ML(f) = X^{\text{multigr}(f)}.$$

iv) O termo líder de f *é:*

$$TL(f) = CL(f) \cdot ML(f) = a_{mutigr(f)} \cdot X^{\text{multigr}(f)}.$$

Exemplo 1.3.3 *Seja* $f = -5X^3 + 7X^2Z^2 + 4XY^2Z + 4Z^2$ *ordenado pela ordem lex. Então:*

$$\begin{aligned} \text{multigr}(f) &= (3, 0, 0) \\ CL(f) &= -5 \\ ML(f) &= X^3 \\ TL(f) &= -5X^3 \end{aligned}$$

Não é difícil provar o seguinte resultado.

Lema 1.3.4 *Sejam* $f, g \in K[X_1, \ldots, X_n]$ *polinômios não-nulos. Então:*

i) $\text{multigr}(f.g) = \text{multigr}(f) + \text{multigr}(g)$

ii) Se $f + g \neq 0$, *então* $\text{multigr}(f + g) \leq \max(\text{multigr}(f), \text{multigr}(g))$.

Se, além disso, $\text{multigr}(f) \neq \text{multigr}(g)$, *então a igualdade ocorre.*

1.4 Algoritmo da Divisão em $K[X_1, \ldots, X_n]$

Vamos formular um algoritmo de divisão para polinômios em $K[X_1, \ldots, X_n]$ que estende o conhecido algoritmo para $K[X]$. No caso geral, a meta é dividir $f \in K[X_1, \ldots, X_n]$ por $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ com resto "pequeno". Como veremos, isto significa expressar f na forma:

$$f = a_1 f_1 + \ldots + a_s f_s + r$$

onde os "quocientes" $a_1, \ldots, a_s$ e o resto r estão em $K[X_1, \ldots, X_n]$. Alguns cuidados serão necessários para caracterizar o resto e neste momento usaremos as ordens de monômios introduzidas.

A idéia básica do algoritmo é a mesma do caso de uma variável: queremos cancelar o termo líder de f (com respeito a ordem de monômios escolhida) pela multiplicação de algum f_i por um monômio apropriado e subtraí-lo de f. Então esse monômio torna-se um termo correspondente a_i. Ao invés de escrever o algoritmo no caso geral, primeiro trabalharemos com alguns exemplos para ver o que é envolvido.

Exemplo 1.4.1 *Primeiro dividiremos $f = XY^2 + 1$ por $f_1 = XY + 1$ e $f_2 = Y + 1$ usando a ordem lex com $X > Y$. Queremos empregar o mesmo esquema para divisão de polinômios de uma variável, a diferença sendo, que agora existem vários divisores e quocientes.*

$$\begin{array}{ll} XY^2 + 1 & |\underline{\ XY + 1;\ Y + 1} \end{array}$$

Os termos líderes $TL(f_1) = XY$ e $TL(f_2) = Y$ ambos dividem o termo líder $TL(f) = XY^2$. Já que f_1 é listado primeiro, usaremos ele. Dividindo XY^2 por XY, temos Y e então subtraímos Yf_1 de f.

$$\begin{array}{ll} XY^2 + 1 & |\underline{XY + 1;\ Y + 1} \\ \underline{-XY^2 - Y\ \ } & \quad Y\ ; \\ -Y + 1 & \end{array}$$

Agora repetimos o mesmo processo sobre $-Y + 1$. Dessa vez usaremos f_2 já que $TL(f_1) = XY$ não divide $TL(-Y + 1) = -Y$. Assim obtemos:

$$\begin{array}{ll} XY^2 + 1 & |\underline{XY + 1;\ Y + 1} \\ \underline{-XY^2 - Y\ \ } & \quad Y\ ;\ (-1) \\ -Y + 1 & \\ \underline{\ \ Y + 1\ \ } & \\ 2 & \end{array}$$

Já que $TL(f_1)$ e $TL(f_2)$ não dividem 2, o resto é $r = 2$ e concluímos a divisão. Então, temos escrito $f = XY^2 + 1$ na forma:

$$XY^2 + 1 = Y(XY + 1) + (-1)(Y + 1) + 2$$

Exemplo 1.4.2 *Neste exemplo, encontraremos uma sutileza inesperada que pode ocorrer quando se trabalha com polinômios de mais de uma variável. Vamos dividir $f = X^2Y + XY^2 + Y^2$ por $f_1 = XY - 1$ e $f_2 = Y^2 - 1$. Como no exemplo anterior, usaremos a ordem lex com $X > Y$.*

$$\begin{array}{ll} X^2Y + XY^2 + Y^2 & |\underline{XY - 1;\ Y^2 - 1} \\ \underline{-X^2Y + X\ \ \ \ \ \ } & \quad X + Y\ ; \\ XY^2 + X + Y^2 & \\ \underline{-XY^2 + Y\ \ \ \ } & \\ X + Y^2 + Y & \end{array}$$

Observe que nem $TL(f_1) = XY$ *nem* $TL(f_2) = Y^2$ *dividem* $TL(X + Y^2 + Y) = X$. *Entretanto,* $X + Y^2 + Y$ *não é um resto adequado já que* $TL(f_2)$ *divide* Y^2 *(ou seja, ainda podemos fazer uma divisão). Então, se movermos* X *para o resto, podemos continuar dividindo.*

Observação 1.4.3 *Este é um problema que nunca acontece no caso de uma variável: uma vez que o termo líder do divisor não divide mais o termo líder do dividendo intermediário (neste caso, o polinômio chamado de dividendo intermediário é* $X + Y^2 + Y$*), o algoritmo termina.*

Para executar essa idéia, criamos uma coluna de resto r*, do lado esquerdo do dividendo, onde colocamos os termos que pertencem ao resto. E então continuamos dividindo até o dividendo intermediário seja zero. O próximo passo é mover* X *para a coluna do resto (como indicado pela seta):*

$$\begin{array}{rc} \underline{r} & X^2Y + XY^2 + Y^2 \\ & \underline{-X^2Y + X} \\ & XY^2 + X + Y^2 \\ & \underline{-XY^2 + Y} \\ X & \longleftarrow \quad X + Y^2 + Y \\ & \overline{Y^2 + Y} \end{array} \qquad \begin{array}{c} |\underline{XY - 1;\ Y^2 - 1} \\ X + Y\ ; \end{array}$$

Agora continuamos dividindo. Se podemos dividir pelo $TL(f_1)$ *ou* $TL(f_2)$*, procedemos como usualmente e, se nenhum divide, movemos o termo líder do dividendo intermediário para a coluna do resto. Aqui está o resto da divisão:*

$$\begin{array}{rc} \underline{r} & X^2Y + XY^2 + Y^2 \\ & \underline{-X^2Y + X} \\ & XY^2 + X + Y^2 \\ & \underline{-XY^2 + Y} \\ X & \longleftarrow \quad X + Y^2 + Y \\ & \overline{Y^2 + Y} \\ & \underline{-Y^2 + 1} \\ X + Y & \longleftarrow \quad Y + 1 \\ & \overline{\longleftarrow \quad 1} \\ X + Y + 1 & \overline{0} \end{array} \qquad \begin{array}{c} |\underline{XY - 1;\ Y^2 - 1} \\ X + Y\ ;\ 1 \end{array}$$

Então, o resto é $X + Y + 1$*, e obtemos:*

$$X^2Y + XY^2 + Y^2 = (X + Y)(XY - 1) + 1\left(Y^2 - 1\right) + X + Y + 1. \tag{1.3}$$

Observe que o resto é uma soma de monômios, *nenhum dos quais é divisível pelos termos líderes* $TL(f_1)$ ou $TL(f_2)$.

O exemplo acima é uma ilustração bastante completa de como o algoritmo da divisão funciona. Este exemplo nos mostra também uma propriedade que queremos que o resto tenha: nenhum dos seus termos podem ser divisíveis pelos termos líderes dos polinômios que estão dividindo.

Podemos agora enunciar a forma geral do algoritmo da divisão.

Teorema 1.4.4 (Algoritmo da Divisão em $K[X_1, \ldots, X_n]$**)** *Fixe uma ordem de monômios* $>$ *sobre* $\mathbb{N}_0^n$ *e seja* $F = (f_1, \ldots, f_s)$ *uma s-upla ordenada de polinômios em* $K[X_1, \ldots, X_n]$*. Então todo* $f \in K[X_1, \ldots, X_n]$ *pode ser escrito como:*

$$f = a_1 f_1 + \ldots + a_s f_s + r$$

onde a_i, $r \in K[X_1, \ldots, X_n]$ *e,* $r = 0$ *ou* r *é uma combinação linear, com coeficientes em* K*, de monômios, nenhum dos quais é divisível por nenhum dos* $TL(f_1), \ldots, TL(f_s)$*. Chamaremos* r *de um resto de* f *na divisão por* F*. Além disso, se* $a_i f_i \neq 0$*, então temos:*

$$\text{multigr}(f) \geq \text{multigr}(a_i f_i).$$

Demonstração: A demonstração consiste em mostrar que o algoritmo abaixo

$Input : f_1, \ldots, f_s, f$
$Output : a_1, \ldots, a_s, r$
$a_1 := 0, \ldots, a_s := 0, r := 0$
$p := f$
$While\ p \neq 0\ Do$
    $i := 1$
    $divisaoocorreu := false$
    $While\ i \leq s\ and\ divisaoocorreu = false\ Do$
        $If\ TL(f_i)\ divides\ TL(p)\ Then$
            $a_i := a_i + TL(p)\ /\ TL(f_i)$
            $p := p - (TL(p)/TL(f_i))\, f_i$
            $divisaoocorreu = true$
        $Else$
            $i := i + 1$
    $If\ divisaoocorreu = false\ Then$
        $r := r + TL(p)$
        $p := p - TL(p)$

determina os coeficientes $a_1, \ldots, a_s$ e r como no enunciado e termina após um número finito de passos. O leitor interessado pode ver a demonstração completa em [1], página 62.

□

Infelizmente, esse algoritmo não possui as mesmas propriedades agradáveis da versão de uma variável.

Uma propriedade importante do algoritmo da divisão em $K[X]$ é que o resto é unicamente determinado. Para ver como isto pode falhar quando existe mais de uma variável considere o seguinte exemplo:

Exemplo 1.4.5 *Vamos dividir* $f = X^2Y + XY^2 + Y^2$ *por* $f_1 = Y^2 - 1$ *e* $f_2 = XY - 1$*. Usaremos a ordem lex com* $X > Y$*. Este é o mesmo exemplo 1.4.2, exceto que mudamos a ordem dos divisores.*

$$\begin{array}{lll}
\underline{r} & X^2Y + XY^2 + Y^2 & |\underline{Y^2 - 1;\ XY - 1} \\
 & -X^2Y + X & X + 1\ ;\ X \\
 & \hline XY^2 + X + Y^2 & \\
 & -XY^2 + X & \\
 & \hline \longleftarrow\quad 2X + Y^2 & \\
2X & \hline Y^2 & \\
 & -Y^2 + 1 & \\
 & \hline \longleftarrow\quad 1 & \\
2X + 1 & \hline 0 &
\end{array}$$

Isto mostra que:

$$X^2Y + XY^2 + Y^2 = (X+1)\left(Y^2-1\right) + X\left(XY-1\right) + 2X + 1. \tag{1.4}$$

Comparando esta equação com a equação (1.3), vemos que os restos são diferentes.

Isto mostra que o resto não é único apenas pela exigência que nenhum dos seus termos sejam divisíveis pelos $TL(f_1), \ldots, TL(f_s)$, ou seja, para cada ordem $F = (f_1, \ldots, f_s)$, existe um resto na divisão de f por F.

1.5 Ideais de Monômios e o Lema de Dickson

Definição 1.5.1 *Um ideal $I \subset K[X_1, \ldots, X_n]$ é um ideal de monômios se existe um subconjunto $A \subset \mathbb{N}_0^n$ (possivelmente infinito) tal que I é o conjunto de todos os polinômios que são combinações lineares finitas da forma $\sum_{\alpha \in A} h_\alpha X^\alpha$, onde $h_\alpha \in K[X_1, \ldots, X_n]$. Neste caso, escrevemos $I = \langle X^\alpha : \alpha \in A \rangle$ e dizemos que o ideal I é gerado por $X^\alpha, \alpha \in A$.*

Exemplo 1.5.2 *O conjunto $I = \langle X^4Y^2, X^3Y^4, X^2Y^5 \rangle$ é um exemplo de um ideal de monômios onde $A = \{(4,2), (3,4), (2,5)\}$.*

Lema 1.5.3 *Seja $I = \langle X^\alpha : \alpha \in A \rangle$ um ideal de monômios. Então um monômio X^β pertence a I se, e somente se, X^β é divisível por X^α para algum $\alpha \in A$.*

Demonstração:
($\Rightarrow$) Se $X^\beta \in I$, então $X^\beta = \sum_{i=1}^{s} h_i X^{\alpha_i}$, onde $h_i \in K[X_1, \ldots, X_n]$ e $\alpha_i \in A$. Se expandimos cada h_i como uma combinação linear de monômios, temos que todo termo do lado direito da equação é divisível por algum X^{α_i}. Então, o lado esquerdo, que é o monômio X^β, possui a mesma propriedade.

($\Leftarrow$) Se X^β é um múltiplo de X^α para algum $\alpha \in A$, então $X^\beta \in I$ pela definição de ideal. □

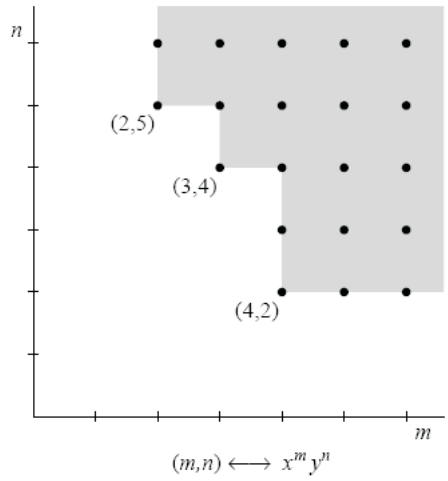
Observe que X^β é divisível por X^α exatamente quando $X^\beta = X^\alpha \cdot X^\gamma$ para algum $\gamma \in \mathbb{N}_0^n$, o que é equivalente a $\beta = \alpha + \gamma$. Então, o conjunto

$$\alpha + \mathbb{N}_0^n := \{\alpha + \gamma : \gamma \in \mathbb{N}_0^n\}$$

consiste dos expoentes de todos os monômios divisíveis por X^α. Esta observação e o Lema 1.2.2 nos permite desenhar uma ilustração dos monômios de um ideal de monômios dado. Por exemplo, se $I = \langle X^4Y^2, X^3Y^4, X^2Y^5 \rangle$, então os expoentes dos monômios em I formam o conjunto

$$((4,2) + \mathbb{N}_0^2) \cup ((3,4) + \mathbb{N}_0^2) \cup ((2,5) + \mathbb{N}_0^2).$$

Podemos visualizar este conjunto como a união de pontos com coordenadas inteiras não-negativas no primeiro quadrante do plano.



Mostraremos a seguir que se um polinômio f dado pertence a um ideal de monômios, ele pode ser determinado apenas pela inspeção dos monômios de f.

Lema 1.5.4 *Seja I um ideal de monômios, e seja $f \in K[X_1, \ldots, X_n]$. Então as seguintes condições são equivalentes:*

i) $f \in I$;

ii) *Todo termo de f está em I;*

iii) *f é uma combinação K-linear de monômios em I.*

Demonstração:
As implicações $(iii) \Rightarrow (ii) \Rightarrow (i)$ são triviais.

$\vdash (i) \Rightarrow (iii)$

Se $f \in I$ então $f = \sum_{i=1}^{s} h_i X^{\alpha_i}$ com $h_i \in K[X_1, \ldots, X_n]$ e $\alpha_i \in A$.
Se expandimos h_i como uma combinação de monômios, temos:

$$f = \sum_{i=1}^{s} \left(\sum_{\beta} a_\beta X^\beta \right) X^{\alpha_i} = \sum_{\beta} a_\beta \sum_{i=1}^{s} X^{\beta+\alpha_i}$$

onde $a_\beta \in K$. Como $X^{\beta+\alpha_i}$ é divisível por X^{α_i}, pelo Lema 1.5.3, temos que $X^{\beta+\alpha_i} \in I$. Logo, f é uma combinação K-linear de monômios em I. □

Uma conseqüência imediata da parte (iii) do lema é que o ideal de monômio é unicamente determinado por seus monômios. Então, temos o seguinte corolário:

Corolário 1.5.5 *Dois ideais de monômios são iguais se, e somente se, eles contém os mesmos monômios.*

O principal resultado desta seção é que todos os ideais de monômios de $K[X_1, \ldots, X_n]$ são finitamente gerados.

Teorema 1.5.6 (Lema de Dickson) *Um ideal de monômios $I = \langle X^\alpha : \alpha \in A \rangle \subset K[X_1, \ldots, X_n]$ pode ser escrito sobre a forma $I = \langle X^{\alpha_1}, \ldots, X^{\alpha_s} \rangle$, onde $\alpha_1, \ldots, \alpha_s \in A$. Em particular, I tem uma base finita.*

Demonstração: Ver demonstração em [1] na página 69.

□

Utilizando o Lema de Dickson vamos provar o seguinte fato importante sobre ordens de monômios em $K[X_1, \ldots, X_n]$.

Corolário 1.5.7 *Seja $>$ uma relação sobre $\mathbb{N}_0^n$ satisfazendo:*

i) $>$ é uma ordem total sobre $\mathbb{N}_0^n$;

ii) se $\alpha > \beta$ e $\gamma \in \mathbb{N}_0^n$ então $\alpha + \gamma > \beta + \gamma$

Então $>$ é uma boa ordenação se, e somente se, $\alpha \geq 0$ para todo $\alpha \in \mathbb{N}_0^n$.

Demonstração:
($\Rightarrow$) Assumindo que $>$ é uma boa ordenação, seja α_0 o elemento mínimo de $\mathbb{N}_0^n$. É suficiente mostrar que $\alpha_0 \geq 0$.

Suponha, por absurdo, que $0 > \alpha_0$. Então pela hipótese (ii), podemos somar α_0 em ambos os lados da equação obtendo $\alpha_0 > 2\alpha_0$, o que é um absurdo, já que α_0 é o elemento mínimo de $\mathbb{N}_0^n$.

($\Leftarrow$) Assumindo $\alpha \geq 0$ para todo $\alpha \in \mathbb{N}_0^n$, seja $A \subset \mathbb{N}_0^n$ não-vazio. Precisamos mostrar que A tem um elemento mínimo. Já que $I = \langle X^\alpha : \alpha \in A \rangle$ é um ideal de monômios, pelo Lema de Dickson temos que existem $\alpha_1, \ldots, \alpha_s \in A$ tal que $I = \langle X^{\alpha_1}, \ldots, X^{\alpha_s} \rangle$. Reordenando, se necessário, podemos assumir que $\alpha_1 < \alpha_2 < \ldots < \alpha_s$.

Afirmação 1.5.8 *: α_1 é o elemento mínimo de A*

Demonstração: (Afirmação)

Para provar isto, seja $\alpha \in A$. Então, $X^\alpha \in I = \langle X^{\alpha_1}, \ldots, X^{\alpha_s} \rangle$ e, pelo Lema 1.5.3, X^α é divisível por algum X^{α_i}. Isto diz que $\alpha = \alpha_i + \gamma$ para algum $\gamma \in \mathbb{N}_0^n$. Então $\gamma \geq 0$ e a hipótese (ii) implica que:

$$\alpha = \alpha_i + \gamma \geq \alpha_i + 0 = \alpha_i \geq \alpha_1.$$

Então, α_1 é o elemento mínimo de A □
E assim, termina a prova. □

Como um resultado desse corolário, a definição de ordem monomial dada na Definição 1.2.1 pode ser simplificada. Podemos substituir a condição (iii) pela condição mais simples, $\alpha \geq 0$ para todo $\alpha \in \mathbb{N}_0^n$. Isto facilita a verificação de que uma ordem dada é uma ordem monomial.

1.6 O Teorema da Base de Hilbert e Variedades Algébricas

Definição 1.6.1 *Seja $I \subset K[X_1, \ldots, X_n]$ um ideal diferente de $\{0\}$.*

i) Denotamos por $TL(I)$ o conjunto dos termos líderes dos elementos de I. Ou seja,

$$TL(I) := \{cX^\alpha : existe \quad f \in I \quad com \quad TL(f) = cX^\alpha\}.$$

ii) Denotamos por $\langle TL(I)\rangle$ *o ideal gerado pelos elementos de* $TL(I)$.

Já vimos que os termos líderes têm um importante papel no algoritmo da divisão. Com isso, surge uma sutileza que deve ser mencionada: dado um conjunto gerador finito para I, digamos $I = \langle f_1, \ldots, f_s\rangle$, temos que $\langle TL(f_1), \ldots, TL(f_s)\rangle$ e $\langle TL(I)\rangle$ podem ser ideais diferentes. É verdade, pela definição, que $TL(f_i) \in TL(I) \subset \langle TL(I)\rangle$ o que implica $\langle TL(f_1), \ldots, TL(f_s)\rangle \subset \langle TL(I)\rangle$. Entretanto, $\langle TL(I)\rangle$ pode ser estritamente maior. Para ver isto, considere o exemplo a seguir.

Exemplo 1.6.2 *Sejam* $I = \langle f_1, f_2\rangle$, *onde* $f_1 = X^3 - 2XY$ *e* $f_2 = X^2Y - 2Y^2 + X$ *e a ordem grlex sobre monômios em* $K[X, Y]$. *Então,* $X \cdot (X^2Y - 2Y^2 + X) - Y(X^3 - 2XY) = X^2$ *e* $X^2 \in I$. *Logo,* $X^2 = TL(X^2) \in \langle TL(I)\rangle$. *Entretanto,* $X^2 \in I$ *não é divisível por* $TL(f_1) = X^3$ *ou* $TL(f_2) = X^2Y$, *logo,* X^2 *não pertence* $\langle TL(f_1), TL(f_2)\rangle$ *pelo Lema 1.5.3.*

Agora mostraremos que $\langle TL(I)\rangle$ é um ideal de monômios e isto nos permitirá aplicar os resultados anteriores. Em particular, seguirá que $\langle TL(I)\rangle$ é gerado por um número finito de termos líderes.

Proposição 1.6.3 *Seja* $I \subset K[X_1, \ldots, X_n]$ *um ideal.*

i) O conjunto $\langle TL(I)\rangle$ *é um ideal de monômios.*

ii) Existem $g_1, \ldots, g_t \in I$ *tal que* $\langle TL(I)\rangle = \langle TL(g_1), \ldots, TL(g_t)\rangle$.

Demonstração:

i) O monômio líder $ML(g)$ dos elementos $g \in I - \{0\}$ gera o ideal de monômios $\langle ML(g) : g \in I - \{0\}\rangle$. Já que $ML(g)$ e $TL(g)$ diferem apenas por uma constante não-nula, pelo Corolário 1.5.5 temos que $\langle ML(g) : g \in I - \{0\}\rangle = \langle TL(g) : g \in I - \{0\}\rangle = \langle TL(I)\rangle$, pois possuem os mesmos monômios. Então, $\langle TL(I)\rangle$ é um ideal de monômios.

ii) Já que $\langle TL(I)\rangle$ é gerado pelos monômios $ML(g)$ para $g \in I - \{0\}$, o Lema de Dickson garante que $\langle TL(I)\rangle = \langle ML(g_1), \ldots, ML(g_t)\rangle$ para finitos $g_1, \ldots, g_t \in I$. Já que $ML(g_i)$ difere de $TL(g_i)$ apenas por uma constante não nula, novamente pelo Corolário 1.5.5, temos que $\langle TL(I)\rangle = \langle ML(g_1), \ldots, ML(g_t)\rangle = \langle TL(g_1), \ldots, TL(g_t)\rangle$ e isto completa a prova.

□

Agora, podemos usar a Proposição 1.6.3 e o Algoritmo da Divisão para provar a existência de um conjunto gerador finito para todo ideal de polinômios. Seja $I \subset K[X_1, \ldots, X_n]$ um ideal qualquer e considere o ideal associado $\langle TL(I)\rangle$ como na Definição 1.6.1. Como sempre, selecionamos uma ordem monomial particular para usar no algoritmo da divisão e na computação dos termos líderes.

Teorema 1.6.4 (Teorema da Base de Hilbert) *Todo ideal* $I \subset K[X_1, \ldots, X_n]$ *tem um conjunto gerador finito. Isto, é,* $I = \langle g_1, \ldots, g_t\rangle$ *para algum* $g_1, \ldots, g_t \in I$.

Demonstração:

Se $I = \{0\}$, tomamos nosso conjunto gerador como $\{0\}$, que certamente é finito.

Se I contém algum polinômio não-nulo, então um conjunto gerador $g_1, \ldots, g_t$ para I pode ser construído como a seguir. Pela Proposição 1.6.3, existem $g_1, \ldots, g_t \in I$ tal que $\langle TL(I)\rangle = \langle TL(g_1), \ldots, TL(g_t)\rangle$. Afirmamos que $I = \langle g_1, \ldots, g_t\rangle$.

É claro que $\langle g_1, \ldots, g_t \rangle \subset I$, já que cada $g_i \in I$. Por outro lado, seja $f \in I$ um polinômio qualquer. Aplicando o algoritmo da divisão para dividir f por $\langle g_1, \ldots, g_t \rangle$ chegamos numa expressão da forma:

$$f = a_1 g_1 + \ldots + a_t g_t + r$$

onde nenhum termo de r é divisível por nenhum dos $TL(g_1), \ldots, TL(g_t)$. Afirmamos que $r = 0$.

Para ver isto, observe que:

$$r = f - a_1 g_1 + \ldots + a_t g_t \in I.$$

Se $r \neq 0$, então $TL(r) \in \langle TL(I) \rangle = \langle TL(g_1), \ldots, TL(g_t) \rangle$, e pelo Lema 1.5.3, segue que $TL(r)$ deve ser divisível por algum $TL(g_i)$. Isto contradiz o fato dele ser o resto e, conseqüentemente, r tem que ser zero.

Então,

$$f = a_1 g_1 + \ldots + a_t g_t + 0 \in \langle TL(g_1), \ldots, TL(g_t) \rangle$$

o que mostra que $I \subset \langle g_1, \ldots, g_t \rangle$ e, portanto, $I = \langle g_1, \ldots, g_t \rangle$. □

A base $\{g_1, \ldots, g_t\}$ usada na prova do Teorema 1.6.4 tem a propriedade especial $\langle TL(I) \rangle = \langle TL(g_1), \ldots, TL(g_t) \rangle$. Como nem todas as bases possuem essa propriedade, como vimos no Exemplo 1.4.2, às essas bases daremos o seguinte nome.

Definição 1.6.5 *Fixe uma ordem de monômios. Um subconjunto finito $G = \{g_1, \ldots, g_t\}$ de um ideal I é dito ser uma base de Groebner (ou base padrão) se*

$$\langle TL(g_1), \ldots, TL(g_t) \rangle = \langle TL(I) \rangle.$$

Equivalentemente, um conjunto $\{g_1, \ldots, g_t\} \subset I$ é uma base de Groebner para I se, e somente se, o termo líder de qualquer elemento de I é divisível por um dos $TL(g_i)$.

De fato,

($\Rightarrow$) Trivial.

($\Leftarrow$) Sabemos que $\langle TL(g_1), \ldots, TL(g_t) \rangle \subset \langle TL(I) \rangle$.

Seja $f \in I$. Então $TL(f) \in \langle TL(I) \rangle$. Como o termo líder de qualquer elemento de I é divisível por um dos $TL(g_i)$, $i = 1, ..., t$, temos que $TL(f) = a_i TL(g_i)$, para algum i, ou seja, $TL(f) = a_1 TL(g_1) + ... + a_t TL(g_t)$, onde $a_i \neq 0$ para algum i e $a_s = 0$ para $s \neq i$. Logo, $\langle TL(I) \rangle \subset \langle TL(g_1), \ldots, TL(g_t) \rangle$. Assim, $\langle TL(g_1), \ldots, TL(g_t) \rangle = \langle TL(I) \rangle$, ou seja, $\{g_1, \ldots, g_t\} \subset I$ é uma base de Groebner para I.

A prova do Teorema 1.6.4 também estabelece o seguinte resultado.

Corolário 1.6.6 *Fixe uma ordem monomial. Então todo ideal $I \subset K[X_1, \ldots, X_n]$ diferente de $\{0\}$ tem uma base de Groebner. Além disso, qualquer base de Groebner para um ideal I é uma base de I.*

Demonstração:

Dado um ideal não-nulo, o conjunto $G = \{g_1, \ldots, g_t\}$ construído na prova do Teorema 1.6.4 é uma base de Groebner pela definição. Para segunda afirmação, observe que se $\langle TL(I) \rangle = \langle TL(g_1), \ldots, TL(g_t) \rangle$, então o argumento dado no Teorema 1.6.4 mostra que $I = \langle g_1, \ldots, g_t \rangle$, e então G é uma base para I. □

Definição 1.6.7 *Seja K um corpo e sejam $f_1, \ldots, f_s$ polinômios em $K[X_1, \ldots, X_n]$. Chamamos de variedade algébrica, ou simplesmente variedade, definida por $f_1, \ldots, f_s$ o seguinte conjunto:*

$$V(f_1, \ldots, f_s) := \{(a_1, \ldots, a_n) \in K^n : f_i(a_1, \ldots, a_n) = 0, \textit{para todo } 1 \leq i \leq s\}.$$

Pelo Teorema das Bases de Hilbert, faz sentido falar na variedade definida por um ideal $I \subset K[X_1, \ldots, X_n]$.

Definição 1.6.8 *Seja $I \subset K[X_1, \ldots, X_n]$ um ideal. Denotamos por $V(I)$ o conjunto*

$$V(I) := \{(a_1, \ldots, a_n) \in K^n : f(a_1, \ldots, a_n) = 0 \textit{ para todo } f \in I\}.$$

Ainda que um ideal I não-nulo sempre contenha infinitos polinômios diferentes, o conjunto $V(I)$ ainda pode ser definido por um conjunto finito de equações polinomiais.

Proposição 1.6.9 *Temos que $V(I)$ é uma variedade. Em particular, se $I = \langle f_1, \ldots, f_s \rangle$, então $V(I) = V(f_1, \ldots, f_s)$.*

Demonstração:
Pelo Teorema das Bases de Hilbert, $I = \langle f_1, \ldots, f_s \rangle$ para algum conjunto gerador finito. Afirmamos que $V(I) = V(f_1, \ldots, f_s)$.

Primeiramente, já que $f_i \in I$ e $f(a_1, \ldots, a_n) = 0$ para todo $f \in I$, temos que $f_i(a_1, \ldots, a_n) = 0$ e então $V(I) \subset V(f_1, \ldots, f_s)$.

Por outro lado, seja $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$ e seja $f \in I$. Já que $I = \langle f_1, \ldots, f_s \rangle$, podemos escrever

$$f = \sum_{i=1}^{s} h_i f_i$$

para alguns $h_i \in K[X_1, \ldots, X_n]$.
Então:

$$f(a_1, \ldots, a_n) = \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) = \sum_{i=1}^{s} h_i(a_1, \ldots, a_n).0 = 0.$$

Então, $V(f_1, \ldots, f_s) \subset V(I)$.

Portanto, $V(I) = V(f_1, \ldots, f_s)$, como queríamos provar. □

No último capítulo estudaremos variedades definidas sobre corpos finitos e relacionaremos sua cardinalidade ao estudo de certos parâmetros de códigos.

1.7 Propriedades das Bases de Groebner

Como mostrado na Seção 1.6, todo ideal não-nulo $I \subset K[X_1, \ldots, X_n]$ tem uma base de Groebner. Nesta seção, estudaremos as propriedades das Bases de Groebner e aprenderemos como detectar quando uma base dada é de Groebner. Começaremos mostrando que o comportamento indesejável do algoritmo da divisão em $K[X_1, \ldots, X_n]$ que observamos em alguns exemplos não ocorre quando dividimos por elementos da base de Groebner.

Primeiramente provaremos que o resto é unicamente determinado quando dividimos por uma base de Groebner.

Proposição 1.7.1 *Sejam $G = \{g_1, \ldots, g_t\}$ uma base de Groebner para um ideal $I \subset K[X_1, \ldots, X_n]$ e $f \in K[X_1, \ldots, X_n]$. Então existe um único $r \in K[X_1, \ldots, X_n]$ com as seguintes propriedades:*

i) Nenhum termo de r é divisível por algum $TL(g_1), \ldots, TL(g_t)$.

ii) Existe $g \in I$ tal que $f = g + r$.

Em particular, r é o resto da divisão de f por G, independente de como os elementos de G são listados quando usado o algoritmo da divisão.

Demonstração:

i) O algoritmo da divisão fornece $f = a_1 g_1 + \ldots + a_t g_t + r$, onde nenhum termo de r é divisível por nenhum dos $TL(g_1), \ldots, TL(g_t)$.

ii) Seja $g = a_1 g_1 + \ldots + a_t g_t \in I$. Temos que $r = f - g \in K[X_1, \ldots, X_n]$ e então isso prova a existência de r.

Para provar a unicidade, suponha que $f = g + r = g' + r'$ satisfazendo (i) e (ii). Então, $r - r' = g' - g \in I$.

Se $r \neq r'$, então $TL(r - r') \in \langle TL(I) \rangle = \langle TL(g_1), \ldots, TL(g_t) \rangle$, pois G é uma base de Groebner. Pelo Lema 1.5.3, segue que $TL(r - r')$ é divisível por algum $TL(g_i)$, o que é um absurdo, já que nenhum termo de r ou r' é divisível por algum $TL(g_1), \ldots, TL(g_t)$. Então temos que:

$$r - r' = 0 \Rightarrow r = r'$$

$$r - r' = g' - g \Rightarrow g' - g = 0 \Rightarrow g = g'.$$

Logo, temos provada a unicidade de r. □

O resto r é chamado "a forma normal de f". Embora o resto r seja único, mesmo para uma base de Groebner, os "quocientes" a_i produzidos pelo algoritmo da divisão $f = a_1 g_1 + \ldots + a_t g_t + r$ podem mudar se listarmos os geradores numa ordem diferente.

Como um corolário, temos o seguinte critério para quando um polinômio está em um ideal.

Corolário 1.7.2 *Sejam $G = \{g_1, \ldots, g_t\}$ uma base de Groebner para um ideal $I \subset K[X_1, \ldots, X_n]$ e $f \in K[X_1, \ldots, X_n]$. Então $f \in I$ se, e somente se, o resto na divisão de f por G é zero.*

Demonstração:

Se o resto é zero, já observamos que $f \in I$. Por outro lado, dado $f \in I$, então $f = f + 0$ satisfaz as duas condições da Proposição 1.7.1. Assim segue que 0 é o resto da divisão de f por G. □

Usaremos as seguintes notações para o resto.

Definição 1.7.3 *Denotaremos por* $\overline{f}^F$ *o resto da divisão de* f *pela s-upla ordenada* $F = (f_1, \ldots, f_t)$. *Se* F *é uma base de Groebner para* $\langle f_1, \ldots, f_t \rangle$, *então podemos considerar* F *como um conjunto (sem nenhuma ordem particular) pela Proposição 1.7.1.*

Por exemplo, com $F = (X^2Y - Y^2, X^4Y^2 - Y^2) \subset K[X, Y]$ e usando a ordem lex temos:

$$\overline{X^5Y}^F = XY^3$$

já que o algoritmo da divisão produz:

$$X^5Y = (X^3 + XY)(X^2Y - Y^2) + (0)(X^4Y^2 - Y^2) + XY^3.$$

A seguir, discutiremos como distinguir se um dado conjunto gerador de um ideal é ou não uma base de Groebner. A "obstrução" para $\{f_1, \ldots, f_s\}$ ser uma base de Groebner é a possível ocorrência de combinações polinomiais dos f_i's, cujo termos líderes não estejam no ideal gerado pelos $TL(f_i)$'s. Uma possibilidade que pode ocorrer é se os termos líderes na combinação conveniente

$$aX^\alpha f_i - bX^\beta f_j$$

se cancelam, deixando somente termos menores. Por outro lado, $aX^\alpha f_i - bX^\beta f_j \in I$, logo seu termo líder está em $\langle TL(I) \rangle$. Para estudar esse fenômeno de cancelamento, introduziremos as seguintes combinações especiais.

Definição 1.7.4 *Sejam* $f, g \in K[X_1, \ldots, X_n]$ *polinômios não-nulos.*

i) Se $\text{multigr}(f) = \alpha$ *e* $\text{multigr}(g) = \beta$, *com* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *e* $\beta = (\beta_1, \ldots, \beta_n)$, *então seja* $\gamma = (\gamma_1, \ldots, \gamma_n)$, *onde* $\gamma_i = \max(\alpha_i, \beta_i)$ *para cada* i. *Chamamos* X^γ *o mínimo múltiplo comum de* $ML(f)$ *e* $ML(g)$ *e denotamos por* $X^\gamma = MMC(ML(f), ML(g))$

ii) O S-polinômio de f *e* g *é a combinação:*

$$S(f, g) = \frac{X^\gamma}{TL(f)} f - \frac{X^\gamma}{TL(g)} g.$$

Exemplo 1.7.5 *Sejam* $f = X^3Y^2 - X^2Y^3 + X$, $g = 3X^4Y + Y^2 \in K[X, Y]$ *com a ordem grlex.*

Temos $\text{multigr}(f) = (3, 2)$ *e* $\text{multigr}(g) = (4, 1)$. *Logo,* $\gamma = (4, 2)$ *e*

$$S(f, g) = \frac{X^4Y^2}{X^3Y^2} f - \frac{X^4Y^2}{3X^4Y} g = Xf - \frac{1}{3} Yg = -X^3Y^3 - \frac{1}{3} Y^3 + X^2.$$

Um S-polinômio $S(f, g)$ é definido para produzir o cancelamento dos termos líderes. De fato, o seguinte lema mostrará que todo cancelamento de termos líderes entre polinômios de mesmo multi-grau resulta deste tipo de cancelamento.

Lema 1.7.6 *Suponha que exista uma soma* $f = \sum_{i=1}^s c_i f_i$, *onde* $c_i \in K$ *e* $\text{multigr}(f_i) = \delta \in \mathbb{N}_0^n$ *para todo* i. *Se* $\text{multigr}\left(\sum_{i=1}^s c_i f_i\right) < \delta$, *então* $\sum_{i=1}^s c_i f_i$ *é uma combinação linear, com coeficientes em* K, *de S-polinômios* $S(f_j, f_k)$ *para* $1 \leq j, k \leq s$. *Além disso, cada* $S(f_j, f_k)$ *têm multi-grau menor que* δ.

Demonstração:
Ver demonstração em [1] na página 81.

□

Quando $f_1, \ldots, f_t$ satisfaz as hipóteses do Lema 1.7.6, temos uma equação da forma:

$$\sum_{i=1}^{s} c_i f_i = \sum_{j,k} c_{j,k} S(f_j, f_k).$$

Considerando onde o cancelamento ocorre; na soma da esquerda, cada parcela $c_i f_i$ tem multi-grau δ, então, o cancelamento ocorre somente depois de somá-los. Entretanto, na soma da direita, cada parcela $c_{j,k} S(f_j, f_k)$ tem multi-grau menor que δ e, então, o cancelamento já ocorreu. Intuitivamente, isto significa que todo cancelamento vem de S-polinômios.

Usando S-polinômios e o Lema 1.7.6, podemos provar o seguinte critério de Buchberger, para quando uma base de um ideal é uma base de Groebner.

Teorema 1.7.7 *Seja I um ideal polinomial. Então uma base $G = \{g_1, \ldots, g_t\}$ para I é uma base de Groebner para I se, e somente se, para todo par $i \neq j$, o resto na divisão de $S(g_i, g_j)$ por G (listada em alguma ordem) é zero.*

Demonstração:
Ver demonstração em, [1] na página 82.

□

O Teorema 1.7.7 é chamado "Critério S-par de Buchberger"e é um resultado chave sobre as Bases de Groebner. Vimos que as Bases de Groebner tem várias propriedades agradáveis, mas é difícil determinar se uma base é de Groebner. Entretanto, usando o Critério S-par, torna-se agora, mais fácil mostrar quando a base dada é uma base de Groebner. Além disso, mostraremos que o Critério S-par também conduz a um algoritmo para computar bases de Groebner.

Exemplo 1.7.8 *Considere o ideal $I = \langle Y - X^2, Z - X^3 \rangle$ da cúbica torcida em $\mathbb{R}^3$. Afirmamos que $G = \{Y - X^2, Z - X^3\}$ é uma base de Groebner para a ordem lex com $Y > Z > X$.*

Para provar isto, considere o S-polinômio:

$$S(Y - X^2, Z - X^3) = \frac{YZ}{Y}.(Y - X^2) - \frac{YZ}{Z}.(Z - X^3) = YX^3 - ZX^2.$$

Usando o algoritmo da divisão, temos:

$$YX^3 - ZX^2 = (X^3).(Y - X^2) + (-X^2).(Z - X^3) + 0$$

de forma que $\overline{S(Y - X^2, Z - X^3)}^G = 0$.

Então pelo Teorema 1.7.7, G é uma base de Groebner de I.

Exemplo 1.7.9 *Temos que $T = \{Y - X^2, Z - X^3\}$ não é uma base de Groebner para $I = \langle Y - X^2, Z - xX^3 \rangle$ com a ordem lex $X > Y > Z$.*

Considere o S-polinômio:

$$S(-X^2 + Y, -X^3 + Z) = \frac{X^3YZ}{-X^2}.(-X^2 + Y) - \frac{X^3YZ}{-X^3}.(-X^3 + Z) = -XY^2Z + YZ^2.$$

Usando o algoritmo da divisão, temos:

$$-XY^2Z + YZ^2 = (0).(-X^2 + Y) + (0).(-X^3 + Z) - XY^2Z + YZ^2.$$

Como $\overline{S(-X^2+Y, -X^3+Z)}^T \neq 0$ *temos pelo Teorema 1.7.7, que* T *não é uma base de Groebner de* I*.*

1.8 A Cota da Pegada

Definição 1.8.1 *Seja* $>$ *uma dada ordem de monômios em* $K[X_1, \ldots, X_m]$ *. A pegada de* I *com respeito a* $>$ *é:*

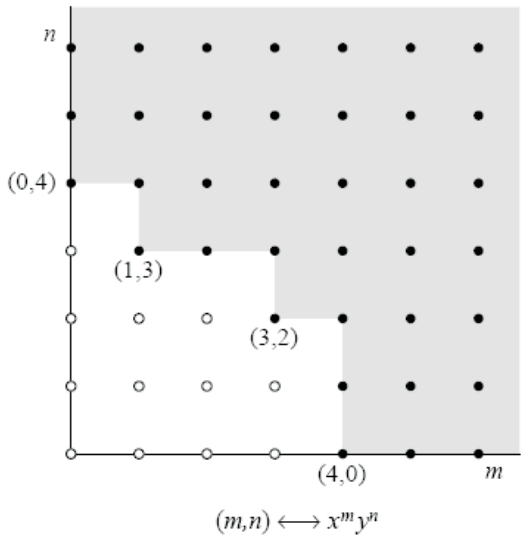
$$\Delta_>(I) := \{M \text{ um monômio em } K[X_1, \ldots, X_m] : \\ M \text{ não é um monômio líder de qualquer polinômio em } I\}.$$

Quando a ordem de monômios é clara para o contexto, usamos abreviadamente $\Delta(I)$. Variando a ordem de monômios, em geral, muda-se a pegada. Entretanto, quando o tamanho (de uma delas) é finita, esta será finita independente da escolha de $>$, isto é uma conseqüência da Proposição 1.8.4 adiante.

Exemplo 1.8.2 *Considere o ideal* $I = \langle X^3Y^2 - Y, X^4 - Y^2, XY^3 - X^2, Y^4 - XY\rangle \in \mathbb{R}[X, Y]$ *e a ordem grau-lex. Como na Seção 1.5, podemos desenhar um diagrama em* $\mathbb{N}_0^2$ *para representar os expoentes dos monômios de* $\langle TL(I)\rangle = \langle X^3Y^2, X^4, XY^3, Y^4\rangle$*. Os elementos de*

$$((3,2) + \mathbb{N}_0^2) \cup ((4,0) + \mathbb{N}_0^2) \cup ((1,3) + \mathbb{N}_0^2) \cup ((0,4) + \mathbb{N}_0^2)$$

representam os expoentes dos monômios em $\langle TL(I)\rangle$*. Assim, podemos representar os monômios em* $\langle TL(I)\rangle$ *por pontos com coordenadas inteiras não-negativas na região sombreada em* $\mathbb{N}_0^2$ *como a seguir:*



E assim, temos que os elementos da pegada são os pontos que estão na região não-sombreada, ou seja,

$$\Delta(I) := \{1, X, X^2, X^3, Y, XY, X^2Y, X^3Y, Y^2, XY^2, X^2Y^2, X^3Y^2\}.$$

Proposição 1.8.3 *Fixe uma ordem de monômios $>$ sobre $K[X_1,\ldots,X_m]$ e seja $I \subseteq K[X_1,\ldots,X_m]$ um ideal.*

i) Todo $f \in K[X_1,\ldots,X_m]$ é congruente módulo I a um único polinômio r que é uma combinação K-linear de monômios em $\Delta_>(I)$;

ii) Os elementos de $\Delta_>(I)$ são linearmente independentes módulo I, isto é, se $\sum_\alpha c_\alpha X^\alpha \equiv 0$ mod I, onde $X^\alpha \in \Delta_>(I)$ e $c_\alpha \in K$ para todo α, então $c_\alpha = 0$ para todo α.

Demonstração:

i) Seja G uma base de Groebner para I e seja $f \in K[X_1,\ldots,X_m]$. Pelo algoritmo da divisão, o resto $r = \overline{f}^G$ satisfaz $f = q + r$, onde $q \in I$. Então $f - r = q \in I$ e temos, $f \equiv r \ mod \ I$. O algoritmo da divisão também diz que r é uma combinação K-linear de monômios $X^\alpha \in \Delta_>(I)$. A unicidade de r segue da Proposição 1.7.1.

ii) Seja G uma base de Groebner para I. Então se $\sum_\alpha c_\alpha X^\alpha \equiv 0 \ mod \ I$ temos $\sum_\alpha c_\alpha X^\alpha \in I$ e logo $\overline{\sum_\alpha c_\alpha X^\alpha}^G = 0$.

Como $X^\alpha \in \Delta_>(I)$, $\forall \alpha$, temos que:

$$\overline{\sum_\alpha c_\alpha X^\alpha}^G = \sum_\alpha c_\alpha X^\alpha.$$

Assim, de $\sum_\alpha c_\alpha X^\alpha = 0$, vem que $c_\alpha = 0$, para todo α.

□

Proposição 1.8.4 *Seja $I \subseteq K[X_1,\ldots,X_m]$ um ideal. Então $K[X_1,\ldots,X_m]/I$ é isomorfo ao K-espaço vetorial $S = Span\{\Delta_>(I)\}$.*

Demonstração: Pela Proposição 1.8.3, a aplicação $\Phi : K[X_1,\ldots,X_m]/I \to S$ definida por $\Phi([f]) = \overline{f}^G$ define uma correspondência 1 a 1 entre as classes em $K[X_1,\ldots,X_m]/I$ e os elementos de S. Então, resta provar que Φ preserva as operações do espaço vetorial. Considere a operação soma em $K[X_1,\ldots,X_m]/I$, ou seja, $[f]+[g] = [f+g]$, para $[f],[g] \in K[X_1,\ldots,X_m]/I$.

Como $[f],[g]$ são elementos de $K[X_1,\ldots,X_m]/I$ então, pela Proposição 1.8.3, podemos padronizar nosso polinômio representativo pela computação dos restos com respeito a base de Groebner G para I. Como temos $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$, então se $\overline{f}^G = \sum_\alpha c_\alpha X^\alpha$ e $\overline{g}^G = \sum_\alpha d_\alpha X^\alpha$ (onde a soma é sobre α com $X^\alpha \in \Delta_>(I)$), então:

$$\overline{f+g}^G = \sum_\alpha (c_\alpha + d_\alpha) X^\alpha.$$

Concluímos assim, que com a representação padrão, a operação de soma em $K[X_1,\ldots,X_m]/I$ é a mesma da soma vetorial no K-espaço vetorial S.

Além disso, se $a \in K$, segue que $\overline{af}^G = \sum_\alpha a c_\alpha X^\alpha$, mostrando assim que a multiplicação por a em $K[X_1,\ldots,X_m]/I$ é a mesma da multiplicação por escalar em S. Isto mostra que a aplicação Φ é linear e, logo é um isomorfismo.

□

Observe que se $\sharp(\Delta_>(I)) < \infty$ então, das Proposições 1.8.3 e 1.8.4 segue que

$$dim K[X_1,\ldots,X_m]/I = \sharp(\Delta_>(I)).$$

Definição 1.8.5 *Seja $V \subset K^m$ uma variedade. Então:*

$$I(V) := \{f \in K[X_1, \ldots, X_m] : f(a_1, \ldots, a_m) = 0 \text{ para todo } (a_1, \ldots, a_m) \in V\}.$$

O seguinte teorema é conhecido como a *Cota da Pegada*.

Teorema 1.8.6 *Sejam K um corpo e $J \subseteq K[X_1, \ldots, X_m]$ um ideal. Se $\Delta_>(J)$ é finito então $\sharp(V_K(J)) \leq \sharp(\Delta_>(J))$.*

Demonstração:

Primeiro mostraremos que dados pontos distintos $P_1, \ldots, P_r \in K^m$, existe um polinômio $f_1 \in K[X_1, \ldots, X_m]$ com $f_1(P_1) = 1$ e $f_1(P_2) = \ldots = f_1(P_r) = 0$. Para provar isto, observe se $A \neq B \in K^m$, então eles tem que se diferenciar em alguma coordenada, digamos a j-ésima, e assim $g = \frac{X_j - B_j}{A_j - B_j}$ satisfaz $g(A) = 1$, $g(B) = 0$. Se aplicarmos esta observação para cada par P_1, P_i com $P_1 \neq P_i$, $i \geq 2$, temos polinômios g_i tal que $g_i(P_1) = 1$ e $g_i(P_i) = 0$ para $i \geq 2$. Então $f_1 = g_2 \cdot g_3 \cdots g_r$ tem a propriedade desejada.

Neste argumento que acabamos de dar, não existe nada em especial com P_1. Se aplicarmos o mesmo argumento com cada P_i, $i \geq 1$, teremos polinômios $f_1, \ldots, f_r$ tal que $f_i(P_i) = 1$ e $f_i(P_j) = 0$ para $i \neq j$.

Agora, podemos provar o Teorema.

Suponha que $V_K = \{P_1, \ldots, P_r\}$, onde os P_i's são distintos. Então temos $f_1, \ldots, f_r$ como acima, ou seja, $f_i(P_i) = 1$ e $f_i(P_j) = 0$ para $i \neq j$. Se provarmos que $[f_1], \ldots, [f_r] \in K[X_1, \ldots, X_m]/J$ são linearmente independentes, então

$$r \leq dim(K[X_1, \ldots, X_m]/J) = \sharp(\Delta_>(J)) \tag{1.5}$$

segue e o teorema está provado.

Para provar a independência linear, suponha que $\sum_{i=1}^{r} a_i[f_i] = 0$ em $K[X_1, \ldots, X_m]/J$, onde $a_i \in K$. Voltando em $K[X_1, \ldots, X_m]$, isto significa que se $g = \sum_{i=1}^{r} a_i f_i \in I$, então g se anula em todos os pontos de $V_K = \{P_1, \ldots, P_r\}$.

Então, para $1 \leq j \leq r$, temos:

$$0 = g(P_j) = \sum_{i=1}^{r} a_i f_i(P_j) = 0 + a_j f_j(P_j) = a_j$$

e a independência linear segue.

□

Observação 1.8.7 *De acordo com [1, Proposição 8, página 232] a igualdade ocorre se, e somente se, K é um corpo algebricamente fechado e I é um ideal radical (isto é, se $f^m \in I$ para algum inteiro $m \geq 1$ implica que $f \in I$).*

1.9 Resultante de Dois Polinômios

Definição 1.9.1 *Sejam $f, g \in K[X_1, \ldots, X_n]$ de grau positivo em X_1. Então podemos escrever*

$$\begin{aligned} f &= a_0 X_1^l - \cdots - a_l, \text{ com } a_0 \neq 0 \\ g &= b_0 X_1^m - \cdots - b_m, \text{ com } b_0 \neq 0 \end{aligned} \tag{1.6}$$

onde $a_i, b_j \in K[X_2, \ldots, X_n]$, para todo $i = 0, \ldots, l$ e $j = 0, \ldots, m$. Definimos a resultante de f e g com respeito a X_1 e denotamos por $Res(f, g, X_1)$, como sendo o determinante

$$Res(f,g,X_1) := \begin{vmatrix} a_0 & \cdots & a_l & & & \\ & a_0 & \cdots & a_l & & \\ & & \ddots & & \ddots & \\ & & & a_0 & \cdots & a_l \\ b_0 & \cdots & b_m & & & \\ & b_0 & \cdots & b_m & & \\ & & \ddots & & \ddots & \\ & & & b_0 & \cdots & b_m \end{vmatrix}$$

onde os espaços vazios são zeros, os coeficientes a_i's, $i = 0, \ldots, l$, ocupam m linhas e os coeficientes b_j's, $j = 0, \ldots, m$, ocupam l linhas.

Proposição 1.9.2 *Sejam $f, g \in K[X_1, \ldots, X_n]$ de grau positivo em X_1.*

Então $Res(f, g, X_1) = 0$ se, e somente se, f e g têm um fator comum em $K[X_1, \ldots, X_n]$ que tem grau positivo em X_1.

Demonstração: A prova encontra-se em [1], página 158. □

Corolário 1.9.3 *Seja $\overline{K}$ o fecho algébrico do corpo K. Se $f, g \in \overline{K}[X]$, então $Res(f, g, X) = 0$ se, e somente se, f e g têm uma mesma raiz em $\overline{K}$.*

Demonstração:

($\Rightarrow$) Como $Res(f, g, X) = 0$, pela Proposição 1.9.2, temos que f, g possuem um fator comum e como $\overline{K}$ é algebricamente fechado, então possuem um fator comum de grau 1. Assim, podemos escrever $f = (aX + b)f_1$ e $g = (aX + b)g_1$, onde $f_1, g_1 \in \overline{K}[X]$. Assim, $-b/a$ é raiz de f e g.

($\Leftarrow$) Seja α a raiz em comum de f e g. Assim, temos que $f = (X - \alpha)f_1$ e $g = (X - \alpha)g_1$, onde $f_1, g_1 \in \overline{K}[X]$ e, logo, f, g possuem um fator comum, o que implica , pela Proposição 1.9.2, que $Res(f, g, X) = 0$. □

Proposição 1.9.4 *Sejam $f, g \in \overline{K}[X_1, \ldots, X_n]$, tais que:*

$$f = a_0 X_1^l - \cdots - a_l, \text{ com } a_0 \neq 0$$
$$g = b_0 X_1^m - \cdots - b_m, \text{ com } b_0 \neq 0$$

onde $a_i, b_j \in K[X_2, \ldots, X_n]$, para todo $i = 0, \ldots, l$ e $j = 0, \ldots, m$.

Se $Res(f, g, X_1) \in \overline{K}[X_2, \ldots, X_n]$ se anula em $(c_2, \ldots, c_n) \in \overline{K}^{n-1}$, então

i) a_0 ou b_0 se anula em $(c_2, \ldots, c_n)$, ou

ii) existe $c_1 \in \overline{K}$ tal que f e g se anulam em $(c_1, \ldots, c_n) \in \overline{K}^n$.

Demonstração: Primeiro introduziremos algumas notações para simplificar a prova. Sejam $\mathbf{c} = (c_2, \ldots, c_n)$ e $f(X_1, \mathbf{c}) = f(X_1, c_2, \ldots, c_n)$. É suficiente provar que $f(X_1, \mathbf{c})$ e $g(X_1, \mathbf{c})$ têm uma mesma raiz quando $a_0(\mathbf{c})$ e $b_0(\mathbf{c})$ são ambos não-nulos. Para provar isto, escreva

$$\begin{aligned} f(X_1, \mathbf{c}) &= a_0(\mathbf{c})X_1^l - \cdots - a_l(\mathbf{c}), \text{ com } a_0(\mathbf{c}) \neq 0 \\ g(X_1, \mathbf{c}) &= b_0(\mathbf{c})X_1^m - \cdots - b_m(\mathbf{c}), \text{ com } b_0(\mathbf{c}) \neq 0. \end{aligned} \tag{1.7}$$

Por hipótese, $h := Res(f, g, X_1)$ se anula em $\mathbf{c}$. Então

$$0 = h(\mathbf{c}) = Res(f(X_1, \mathbf{c}), g(X_1, \mathbf{c}), X_1).$$

Então, do Corolário 1.9.3, temos que $f(X_1, \mathbf{c})$ e $g(X_1, \mathbf{c})$ tem uma mesma raiz e a proposição está provada.

□

No último capítulo utilizaremos a teoria de resultantes para estimar o número de soluções para alguns sistemas de equações polinomiais.

Capítulo 2

Códigos Lineares

2.1 Introdução aos Códigos Lineares

Definição 2.1.1 *Denotamos por $\mathbb{F}_q$ o corpo finito com q elementos.*

Consideraremos o espaço vetorial n-dimensional $\mathbb{F}_q^n$, cujo os elementos são n-uplas $a = (a_1, a_2, ..., a_n)$ com $a_i \in \mathbb{F}_q$, para todo $i = 1, \ldots, n$.

Definição 2.1.2 *Seja A um conjunto. Denotamos por $\sharp(A)$ o número de elementos do conjunto A.*

Definição 2.1.3 *Uma métrica num conjunto A é uma função $d : A \times A \to \mathbb{R}$ que associa a cada par de pontos $x, y \in A$ um número real $d(x, y)$, chamado a distância do ponto x ao ponto y, de tal modo que:*

1) $d(x, x) = 0$.

2) $d(x, y) > 0$ *se* $x \neq y$.

3) $d(x, y) = d(y, x)$.

4) $d(x, z) \leq d(x, y) + d(y, z)$ *quaisquer que sejam* $x, y, z \in A$.

Definição 2.1.4 *Seja $a = (a_1, a_2, ..., a_n)$, $b = (b_1, b_2, ..., b_n) \in \mathbb{F}_q^n$. A função $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N}_0$ definida por*

$$d(a, b) := \sharp(\{i : a_i \neq b_i\})$$

é chamada de distância de Hamming sobre $\mathbb{F}_q^n$.

A distância de Hamming é uma métrica sobre $\mathbb{F}_q^n$.

Definição 2.1.5 *O peso de um elemento $a \in \mathbb{F}_q^n$ é definido como:*

$$\omega(a) := d(a, 0) = \sharp(\{i : a_i \neq 0\}) = n - \sharp(\{i : a_i = 0\}).$$

Definição 2.1.6 *Um código linear C (sobre o alfabeto $\mathbb{F}_q$) é um subespaço vetorial de $\mathbb{F}_q^n$, onde os elementos de C são chamados de palavras do código. Chamamos de n o comprimento de C e $dim C$ (como $\mathbb{F}_q$-espaço vetorial) a dimensão de C. Um código $[n, k]$ é um código de comprimento n e de dimensão k.*

Neste trabalho tratamos apenas de códigos lineares, chamados a partir de agora somente de códigos.

Definição 2.1.7 *A distância (de Hamming) mínima $d(C)$ de um código $C \neq 0$ é definida como:*

$$d(C) := min\{d(a,b)|\ a,b \in C\ e\ a \neq b\}.$$

Como C é um espaço vetorial temos $d(a,b) = d(a-b,0) = \omega(a-b)$ e logo a distância mínima é igual a:

$$d(C) := min\{\omega(c)|\ c \in C\ e\ c \neq 0\}.$$

Um código $[n,k]$ com distância mínima d é dito ser um código $[n,k,d]$.

Definição 2.1.8 *A distribuição de peso de um código $[n,k]$ é a $(n+1)$-upla $(A_0,...,A_n) \in \mathbb{N}_0^{n+1}$ dada por:*

$$A_i := \sharp(\{c \in C; \omega(c) = i\}).$$

Evidentemente $A_0 = 1$ e $A_i = 0$ para $1 \leq i \leq d(C) - 1$.

Definição 2.1.9 *O polinômio*

$$W_C(X) := \sum_{i=0}^{n} A_i X^i \in \mathbb{Z}[X]$$

é chamado de polinômio enumerador de peso do código C.

Definição 2.1.10 *Para um código C com distância mínima $d = d(C)$, definimos $t := [\frac{d-1}{2}]$ (onde $[x]$ denota a parte inteira do número real x, isto é, $x = [x] + \varepsilon$ com $[x] \in \mathbb{Z}$ e $0 \leq \varepsilon < 1$). Então C é chamado corretor de t-erros.*

Lema 2.1.11 *Se $u \in \mathbb{F}_q^n$ e $d(u,c) \leq t$ para algum $c \in C$ então c é a única palavra do código com $d(u,c) \leq t$.*

Demonstração:
Suponha que existam $c_1, c_2 \in C, c_1 \neq c_2$, tal que $d(u,c_1) \leq t$ e $d(u,c_2) \leq t$. Assim,

$$d(c_1,c_2) \leq d(u,c_1) + d(u,c_2) \leq t + t = 2t \leq d - 1$$

o que é um absurdo, pois contraria o fato de d ser a distância mínima de C. Logo, c é única palavra do código com $d(u,c) \leq t$.

□

Definição 2.1.12 *Seja C um código $[n,k]$ sobre $\mathbb{F}_q$. Uma matriz geradora de C é uma matriz $k \times n$ onde as linhas formam uma base para C.*

Definição 2.1.13 *O produto interno canônico de $\mathbb{F}_q^n$ é definido por:*

$$\langle a,b \rangle := \sum_{i=1}^{n} a_i b_i$$

para $a = (a_1,...,a_n)$, $b = (b_1,...,b_n) \in \mathbb{F}_q^n$.

Definição 2.1.14 *Se $C \subseteq \mathbb{F}_q^n$ é um código, então*

$$C^{\perp} := \{u \in \mathbb{F}_q^n |\ \langle u, c\rangle = 0, \text{ para todo } c \in C\}$$

é chamado o dual de C. C é chamado auto-dual (respectivamente, auto-ortogonal) se $C = C^{\perp}$ (respectivamente, $C \subseteq C^{\perp}$).

A álgebra linear diz que o dual de um código $[n, k]$ é um código $[n, n-k]$ e $(C^{\perp})^{\perp} = C$.

Definição 2.1.15 *Uma matriz geradora H de $C^{\perp}$ é dita ser uma matriz de checagem de paridade para C. Claramente uma matriz de checagem de paridade de um código C é uma matriz H de ordem $(n-k) \times n$ e posto $n-k$, e temos*

$$C = \{u \in \mathbb{F}_q^n |\ Hu^t = 0\}$$

(onde u^t, a transposta de u, é um vetor coluna). Então a matriz de checagem de paridade verifica quando um vetor $u \in \mathbb{F}_q^n$ é uma palavra do código ou não.

2.2 Cota de Singleton Generalizada

Um dos problemas básicos em teorias de códigos é construir, sobre um alfabeto $\mathbb{F}_q$ fixado, códigos cuja dimensão e a distância mínima são grandes em comparação com seu comprimento. Entretanto, existem algumas restrições: se a dimensão de um código é grande (com respeito ao seu comprimento) então sua distância mínima é pequena. A cota mais simples é a seguinte:

Proposição 2.2.1 (Cota de Singleton)*: Para um código C, $[n, k, d]$, segue que:*

$$k + d \leq n + 1.$$

Demonstração:
Considere o subespaço linear $W \subseteq \mathbb{F}_q^n$ dado por

$$W := \{(a_1, ..., a_n) \in \mathbb{F}_q^n |\ a_i = 0 \text{ para todo } i \geq d\}.$$

Qualquer $a \in W$ tem peso menor ou igual a $d-1$ e C tem peso maior ou igual a d. Assim, segue que, $W \cap C = 0$. Como $dimW = d-1$, obtemos:

$$k + (d-1) = dimC + dimW = dim(C+W) + dim(C \cap W) = dim(C+W) \leq n$$

ou seja,

$$k + d \leq n + 1.$$

□

Códigos com $k + d = n + 1$ são, num certo sentido, ótimos. Tal códigos são chamados de códigos MDS (códigos de distância máxima separáveis).

Definição 2.2.2 *Dado $U \subseteq \mathbb{F}_q^n$ define-se o suporte de U como:*

$$Supp(U) := \{i |\ \exists u \in U \text{ com a } i\text{-ésima entrada não-nula}\}.$$

Definição 2.2.3 *Considere um código C de dimensão k. Para $h = 1, \ldots, k$, o h-ésimo peso generalizado de Hamming é definido por:*

$$d_h := min\{\sharp(Supp(U))|\ U \text{é um sub-código de } C \text{ de dimensão } h\}.$$

O conjunto $\{d_1, \ldots, d_k\}$ é chamado hierarquia de pesos para C.

Teorema 2.2.4 (Monotonicidade) *Seja C um código $[n, k]$ com $k > 0$. Então:*

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

Demonstração: Seja D um sub-código de C tal que $\sharp(Supp(D)) = d_r$ e $dim(D) = r$. Sejam ainda $i \in Supp(D)$ e $D_i := \{x \in D : x_i = 0\}$. É claro que $D_i \subsetneq D$. Assim, existe $y \in D \backslash D_i$. Note que fazendo $y = (y_1, \ldots, y_n)$, temos que $y_i \neq 0$. Mostremos agora que $D = D_i \oplus \langle y \rangle$.

De fato,

se $x := (x_1, \ldots, x_n) \in D$, então existe $\lambda \in \mathbb{F}_q$ tal que $x_i = \lambda y_i$. Assim, $x = (x - \lambda y) + \lambda y$ com $(x - \lambda y) \in D_i$ e $\lambda y \in \langle y \rangle$. Além disso, se $x \in D_i \cap \langle y \rangle$, então $x_i = 0$ e existe $\lambda \in \mathbb{F}_n^q$ tal que $x = \lambda y$. Assim, $0 = x_i = \lambda y_i$ com $y_i \neq 0$. Logo, $\lambda = 0$ e, portanto, $x = 0$, ou seja, $D_i \cap \langle y \rangle = \{0\}$. Segue então, que $D = D_i \oplus \langle y \rangle$.

Então, temos que, $dim(D_i) = dim(D) - 1$. Daí,

$$d_{r-1}(C) \leq \sharp(Supp(D_i)) = \sharp(Supp(D)) - 1 = d_r(C) - 1 < d_r(C).$$

Falta mostrar que $d_1(C) \geq 1$ e $d_k(C) \leq n$. Mas, se D é um sub-código de C de dimensão um, $D \neq \{0\}$, logo existe $x \in D$ tal que $x \neq 0$, isto é, $Supp(D) \neq 0$, ou ainda, $\sharp(Supp(D)) \geq 1$. Assim, como D foi tomado arbitrariamente, $d_1(C) \geq 1$. Como os elementos de C têm no máximo n coordenadas, $\sharp(Supp(C)) \leq n$. Daí, $d_k(C) \leq \sharp(Supp(C)) \leq n$. □

Corolário 2.2.5 *Sejam C um código $[n, k]$, $r \in \{1, \ldots, k\}$ e $t \in \{0, \ldots, k - r\}$. Então:*

$$d_r(C) + t \leq d_{r+t}(C).$$

Demonstração: Utilizaremos indução sobre t. Fixado $r \in \{1, \ldots, k\}$, é claro que $d_r(C) + 0 \leq d_{r+0}(C)$. Suponha que $d_r(C) + t \leq d_{r+t}(C)$ com $t \in \{0, \ldots, k - r - 1\}$. Pelo Teorema 2.2.4, temos $d_{r+t}(C) \leq d_{r+t+1}(C)$. Assim, $d_{r+t+1}(C) \geq d_{r+t}(C) + 1 \geq d_r(C) + t + 1$.
□

Corolário 2.2.6 (Cota de Singleton Generalizada) *Sejam C um código $[n, k]$ e $r \in \{1, \ldots, k\}$. Então*

$$d_r(C) \leq n - k + r.$$

Demonstração:
Basta tomar $t = k - r$ no Corolário 2.2.5. Assim, de $d_r(C) + k - r \leq d_{r+(k-r)}(C)$ e $d_k(C) \leq n$ segue que:

$$d_r(C) \leq d_k(C) - k + r \leq n - k + r.$$

□

Capítulo 3

A Cota da Pegada e Pesos Generalizados de Hamming

3.1 Resultados Sobre Pesos Generalizados

Dada uma matriz checagem de paridade $H := [h_1, \ldots, h_r]^T$, ou seja, as linhas da matriz H são os r vetores $h_1, \ldots, h_r$, defina

$$[h_i] := \left\{ h_i + \sum_{j=1}^{i-1} \alpha_j h_j |\ \alpha_j \in \mathbb{F}_q \right\}$$

para $i = 1, \ldots, r$.

$$D_{\left\{[h_{i_1}],\ldots,[h_{i_s}]\right\}} := max\left\{ n - \sharp\left(Supp(\{h'_{i_1}, \ldots, h'_{i_s}\})\right) | h'_{i_t} \in [h_{i_t}], t = 1, \ldots, s \right\}$$

para $1 \leq i_1 < \ldots < i_s \leq r$.

$$D_s := max\left\{ D_{\left\{[h_{i_1}],\ldots,[h_{i_s}]\right\}} | 1 \leq i_1 < \ldots < i_s \leq r \right\}$$

para $s = 1, \ldots, r$.

Existe uma importante relação entre os números D_s e os pesos generalizados de Hamming para os códigos com matriz checagem de paridade H. Para explicar esta relação necessitamos da seguinte proposição.

Proposição 3.1.1 *Seja C um código com matriz checagem de paridade H. Então d_h é o h-ésimo peso generalizado de Hamming se, e somente se, d_h é o maior número tal que qualquer $d_h - 1$ colunas de H constituem uma matriz de posto maior ou igual a $d_h - h$.*

Demonstração: A demonstração encontra-se em [5, Proposition 2.4] □

A relação mencionada acima é:

Teorema 3.1.2 *Seja C um código de comprimento n com matriz checagem de paridade $H := [h_1, \ldots, h_r]^T$ (não necessariamente de posto máximo). Para qualquer $d^* \leq r + h$, $h \leq k, d^* \leq n$ as seguintes equivalências são verdadeiras.*

i) $d_h \geq d^* \Leftrightarrow D_{r-d^*+h+1} \leq d^* - 2$

ii) $d_h \leq d^* \Leftrightarrow D_{r-d^*+h} \geq d^*$

Demonstração:

i) ($\Leftarrow$) Como C é um código de comprimento n e H possui r linhas temos que H é uma matriz $r \times n$ e assim podemos representar H por:

$$H := \begin{bmatrix} h_{11} & h_{12} & h_{13} & \cdots & h_{1n} \\ h_{21} & h_{22} & h_{23} & \cdots & h_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ h_{r1} & h_{r2} & h_{r3} & \cdots & h_{rn} \end{bmatrix},$$

ou seja, as linhas de H são dadas por $h_i := (h_{i1}, \ldots, h_{in})$ para todo $i = 1, \ldots, r$.

Assuma $d_h < d^*$. Pela Proposição 3.1.1 existe uma sub-matriz de H, $r \times (d^* - 1)$,

$$M := \begin{bmatrix} h_{1j_1} & h_{1j_2} & h_{1j_3} & \cdots & h_{1j_{d^*-1}} \\ h_{2j_1} & h_{2j_2} & h_{2j_3} & \cdots & h_{2j_{d^*-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ h_{rj_1} & h_{rj_2} & h_{rj_3} & \cdots & h_{rj_{d^*-1}} \end{bmatrix},$$

cuja as linhas de M são dadas por $m_i := (h_{ij_1}, \ldots, h_{ij_{d^*-1}})$ para todo $i = 1, \ldots, r$, de posto no máximo $d^* - h - 1$.

Assim, existem no mínimo $t := r - (d^* - h - 1)$ linhas m_{i_l}, $l = 1, \ldots, t$, tais que $m_{i_l} = \sum_{k=1}^{i_l - 1} \alpha_k m_k$, para todo $l = 1, \ldots, t$ (onde $\alpha_k \in \mathbb{F}_q$ para todo $k = 1, \ldots, i_l - 1$), ou seja, $h_{i_l j_s} = \sum_{k=1}^{i_l - 1} \alpha_k h_{k j_s}$, para todo $l = 1, \ldots, t$ e $s = 1, \ldots, d^* - 1$.

Logo, quando fazemos $h_{i_l} - \sum_{k=1}^{i_l - 1} \alpha_k h_k$ temos que as posições $j_1, \ldots, j_{d^*-1}$ se anulam, pois, $h_{i_l j_s} - \sum_{k=1}^{i_l - 1} \alpha_k h_{k j_s} = 0$, para todo $l = 1, \ldots, t$ e $s = 1, \ldots, d^* - 1$.

Assim, $h_i - \sum_{k=1}^{i-1} \alpha_k h_k \in [h_i]$ possui no mínimo $d^* - 1$ zeros sempre que $i = i_l$, $l \in \{1, \ldots, t\}$, o que leva a $\sharp(Supp(\{h'_{\sigma_1}, \ldots, h'_{\sigma_t}\})) \leq n - (d^* - 1)$ para $h'_{\sigma_\eta} \in [h_{\sigma_\eta}]$, $\eta = 1, \ldots, t$ e $1 \leq \sigma_1 < \ldots < \sigma_s \leq r$.

Logo, $n - \sharp(Supp(\{h'_{\sigma_1}, \ldots, h'_{\sigma_t}\})) \geq d^* - 1$ implica $max\{n - \sharp(Supp(\{h'_{\sigma_1}, \ldots, h'_{\sigma_t}\}))\} \geq d^* - 1$, ou seja, $D_{\{[h_{\sigma_1}], \ldots, [h_{\sigma_t}]\}} \geq d^* - 1$ e, portanto, $D_{r - d^* + h + 1} \geq d^* - 1$, o que é contra nossa hipótese.
Portanto $d_h \geq d^*$.

($\Rightarrow$) Suponha por absurdo que $D_t \geq d^* - 1$, onde $t = r - (d^* - h - 1)$, ou seja, existem $h'_{i_1}, \ldots, h'_{i_t}$ com $h'_{i_k} \in [h_{i_k}], k = 1, \ldots, t$, tal que $n - \sharp(Supp(\{h'_{i_1}, \ldots, h'_{i_t}\})) \geq d^* - 1$ o que implica $\sharp(Supp(\{h'_{i_1}, \ldots, h'_{i_t}\})) \leq n - (d^* - 1)$, ou seja, $h'_{i_j} = h_{i_j} - \sum_{l=1}^{i_j - 1} \alpha_l h_l$ possuem no mínimo $d^* - 1$ zeros para todo $j = \{1, \ldots, t\}$.
Assim, existe uma sub-matriz M, $r \times (d^* - 1)$, de posto no máximo $r - t = r - (r - d^* + h + 1) = d^* - h - 1$ e, pela Proposição 3.1.1, temos que $d_h \neq d^*$.

Provemos agora que, $d_h < d^*$.
Suponha, por absurdo, que $d_h > d^*$. Fazendo $u := d_h - d^*$, considere a sub-matriz M', como sendo a matriz M aumentada de u colunas e, portanto, de tamanho $r \times (d^* - 1 + u)$,

ou seja, $r \times (d_h - 1)$.
Pela Proposição 3.1.1, temos que M' é uma matriz de posto no mínimo $d_h - h$.
Por outro lado, temos que M' possui posto no máximo igual a posto de M mais posto de U, onde U é uma matriz $r \times u$, cujas colunas são as colunas que não fazem parte de M.
Assim,

$$postoM' \leq r - t + u = d^* - h - 1 + u = d_h - h - 1$$

contradizendo a Proposição 3.1.1.
Logo, $d_h < d^*$.
E assim, temos que $D_t \leq d^* - 1$.

ii) ($\Rightarrow$) Assuma que $D_{r-d^*+h} < d^*$, ou seja, $D_{r-d^*+h} \leq d^* - 1$. Então,

$$D_{r-d^*+h} = D_{r-(d^*+1)+h+1} \leq d^* - 1 = (d^* + 1) - 2$$

E, por (i), temos $d_h \geq d^* + 1$, o que é um absurdo.
Logo, $D_{r-d^*+h} \geq d^*$.

($\Leftarrow$) Assuma $d_h \geq d^* + 1$. Por (i) temos $D_{r-(d^*+1)+h+1} \leq (d^* + 1) - 2 = d^* - 1$, o que é um absurdo.
Logo, $d_h \leq d^*$.

□

3.2 Duais de Códigos de Avaliação Sobre uma Variedade

Seja $V = \{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q^m$ uma variedade, digamos, $V = V_{\mathbb{F}_q}(I)$, onde

$$I = \langle G_1(X_1, \ldots, X_m), \ldots, G_g(X_1, \ldots, X_m) \rangle \subseteq \mathbb{F}_q[X_1, \ldots, X_m].$$

Considere a função

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{F}_q[X_1, \ldots, X_m] & \rightarrow & \mathbb{F}_q^n \\ F & \mapsto & (F(P_1), \ldots, F(P_n)). \end{array} \right.$$

Sejam $F_1, \ldots, F_r \in \mathbb{F}_q[X_1, \ldots, X_m]$ e seja $f_i := \varphi(F_i)$, $i = 1, \ldots, r$.

O código cuja matriz *geradora* é da forma $H := [f_1, \ldots, f_r]^T$ é chamado de código de avaliação sobre a variedade V. O código cuja matriz *checagem de paridade* é da forma $H := [f_1, \ldots, f_r]^T$ é chamado de dual de um código de avaliação sobre V. Estes são os códigos que vamos estudar. Seja $H := [f_1, \ldots, f_r]^T$. Definimos:

$$[F_i] := \left\{ F_i + \sum_{j=1}^{i-1} \alpha_j F_j | \alpha_j \in \mathbb{F}_q \right\}$$

para $i = 1, \ldots, r$.

$$\begin{aligned} D_{\{[F_{i_1}], \ldots, [F_{i_s}]\}} &:= max \left\{ \sharp\{P_j \in V | F'_{i_1}(P_j) = \ldots = F'_{i_s}(P_j) = 0\}; \text{ onde } F'_{i_t} \in [F_{i_t}],\ t = 1, \ldots, s \right\} \\ &= max \left\{ \sharp\{Q \in \mathbb{F}_q^m | F'_{i_1}(Q) = \ldots = F'_{i_s}(Q) = G_1(Q) = \ldots = G_g(Q) = 0\}; \text{ onde} \right. \\ &\qquad \left. F'_{i_t} \in [F_{i_t}],\ t = 1, \ldots, s \right\} \end{aligned}$$

para $1 \leq i_1 < \ldots < i_s \leq r$.

Observação 3.2.1 *A igualdade vem do fato que como* $\{G_1, \ldots, G_g\}$ *gera o ideal então*

$$G_i(Q) = 0, \forall i \Leftrightarrow Q \in V.$$

Usando a definição de $D_{\{[h_{i_1}],\ldots,[h_{i_s}]\}}$ e $D_{\{[F_{i_1}],\ldots,[F_{i_s}]\}}$ temos que

$$D_{\{[f_{i_1}],\ldots,[f_{i_s}]\}} = D_{\{[F_{i_1}],\ldots,[F_{i_s}]\}}$$

e em particular, temos:

$$D_s := max\left\{D_{\{[F_{i_1}],\ldots,[F_{i_s}]\}} | i \leq i_1 < \ldots < i_s \leq r\right\} \text{ para } s = 1, \ldots, r.$$

Pelo Teorema 3.1.2, o problema de estimar o peso generalizado de Hamming é traduzido para o problema de estimar o número de soluções comuns para um certo conjunto de equações polinomiais, ou, em outras palavras, para estimar o tamanho de certas variedades.
Poderia-se pensar que a igualdade em $D_{r-d^*+h+1} \leq d^* - 2$ implicaria $d_h = d^*$. O seguinte exemplo mostra que isto não é o caso.

Exemplo 3.2.2 *Sejam* $V := \mathbb{F}_2^2 = \{(0,0); (1,0); (0,1); (1,1)\}$ *e* φ *como na Seção 3.2, onde o anel de polinômios agora é* $\mathbb{F}_q[X, Y]$. *Considere o código sobre* $\mathbb{F}_2$ *com matriz checagem de paridade*

$$H = [\varphi(1), \varphi(X), \varphi(Y)]^T = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Como $dimV = 4$ *e* $dimC^\perp = 3$ *temos que* $dimC = dimV - dimC^\perp = 4 - 3 = 1$ *logo* $h = 1$. *Temos:*

$$[1] = \{1\};$$

$$[X] = \{X; X + 1\};$$

$$[Y] = \{Y; Y + 1; Y + X; Y + X + 1\}.$$

Assim,

- $D_3 = 0$, *pois* $D_{\{[1],[X],[Y]\}} = 0$;
- $D_{\{[1],*\}} = 0$ *e* $D_{\{[X],[Y]\}} = 1 \Rightarrow D_2 = max\{0, 1\} = 1$;
- $D_{\{[1]\}} = 0$, $D_{\{[X]\}} = 2$ *e* $D_{\{[Y]\}} = 2 \Rightarrow D_1 = max\{0, 2\} = 2$.

Pelo Teorema 3.1.2, temos que:

$$D_{r-d^*+h+1} \leq d^* - 2 \Rightarrow D_{3-d^*+1+1} \leq d^* - 2 \Rightarrow D_{5-d^*} \leq d^* - 2.$$

Assim, se $d^* = 2 \Rightarrow D_3 \leq 0$, *porém, como* $d = 4$, *temos* $d \neq d^*$.

3.3 Estimando o Número de Zeros Comuns - Estudos de Casos

No que se segue, vamos querer estimar o número de soluções comuns em $\mathbb{F}_q^m$ de um conjunto de equações

$$E : \begin{cases} F_1(X_1, \ldots, X_m) = 0 \\ \vdots \\ F_s(X_1, \ldots, X_m) = 0 \end{cases} \tag{3.1}$$

onde $F_i(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ para todo $i = 1, \ldots, s$. Equivalentemente, queremos estimar a cardinalidade da variedade $V \subset \mathbb{F}_q^m$ definida pelo ideal

$$J = \langle F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m) \rangle;$$

usando o Teorema 1.8.6, temos que $\#(V(J)) \leq \#(\Delta_>(J))$.

Definição 3.3.1 *Seja E qualquer conjunto de equações da forma (3.1). Dada uma ordem de monômios $>$ sobre $\mathbb{F}_q[X_1, \ldots, X_m]$, definimos o ideal*

$$I_{lead} := \langle ML(F_1), \ldots, ML(F_s) \rangle.$$

Lema 3.3.2 $\Delta_>(I) \subseteq \Delta_>(I_{lead})$

Demonstração: Para provar isto, utilizaremos o fato que se $A \subseteq B \subseteq C$ então $B^c \subseteq A^c$, onde A, B e C são conjuntos e A^c, B^c são os complementares de A, B, respectivamente, com relação a C.

Sejam

$$A := \{M : M \text{ é um monômio líder de um polinômio em } I\}$$

e

$$B := \{M : M \text{ é um monômio líder de um polinômio em } I_{lead}\}$$

Observe que $\Delta_>(I) = A^c$ e $\Delta_>(I_{lead}) = B^c$. Assim provando que $B \subseteq A$ temos nossa afirmação provada. Provemos então que $B \subseteq A$.

Seja $f = f_1 \cdot ML(F_1) + \ldots + f_s \cdot ML(F_s) \in I_{lead}$. Temos que $ML(f) \in B$ é obtido por $t_1 \cdot ML(F_1) + \ldots + t_s \cdot ML(F_s)$, onde t_i é um termo de f_i, $i = 1, \ldots, s$.

Seja também, $g = t_1 \cdot F_1 + \ldots + t_s \cdot F_s \in I$. Temos que $ML(g) \in A$ é dado por $t_1 \cdot ML(F_1) + \ldots + t_s \cdot ML(F_s)$, pois $t_1 \cdot ML(F_1) + \ldots + t_s \cdot ML(F_s) \neq 0$ (já que é monômio líder de f e $ML(t_i \cdot F_i) = t_i \cdot ML(F_i)$, para todo $i = 1, \ldots, s$), ou seja, $ML(f) = ML(g) \in A$ e, assim $B \subseteq A$.

E assim, $\Delta_>(I) \subseteq \Delta_>(I_{lead})$.

□

Assim, usando a afirmação anterior temos que o número de soluções para (3.1) é no máximo $\sharp(\Delta_>(I_{lead}))$, ou seja, $\sharp(\Delta_>(I_{lead}))$ é uma cota para o número de soluções de (3.1). Observe que I_{lead} depende apenas da escolha da representação de I e da escolha da ordem de monômios.

Proposição 3.3.3 *Sejam i_s e j_s números naturais, $s = 1, 2, \ldots, n$, onde*

$$i_1 > i_2 > \ldots > i_n = 0 \text{ e } 0 = j_1 < j_2 < \ldots < j_n.$$

Seja K um corpo e considere os polinômios

$$\begin{aligned}
G_1(X,Y) =& F_{10}(Y)X^{i_1} + F_{11}(Y)X^{i_1-1} + \ldots + F_{1i_1}(Y)\\
G_2(X,Y) =& F_{20}(Y)X^{i_2} + F_{21}(Y)X^{i_2-1} + \ldots + F_{2i_2}(Y)\\
&\vdots\\
G_n(X,Y) =& F_{n0}(Y)X^{i_n} + F_{n1}(Y)X^{i_n-1} + \ldots + F_{ni_n}(Y)
\end{aligned}$$

em $K[X,Y]$, onde F_{i0} é um polinômio de grau $j_i, i = 1,\ldots,n$. O conjunto de equações

$$G_1(X,Y) = G_2(X,Y) = \ldots = G_n(X,Y) = 0$$

tem no máximo

$$j_2(i_1 - i_2) + j_3(i_2 - i_3) + \ldots + j_n i_{n-1}$$

soluções.

Demonstração: Considere a ordem lexicográfica $>_{lex}$ com $X >_{lex} Y$.

O monômio líder de G_s, $s = 1,\ldots,n$, é $ML(G_s) = X^{i_s}Y^{j_s}$. Em particular, $ML(G_1) = X^{i_1}$ e $ML(G_n) = Y^{j_n}$. Defina

$$I := \langle G_1(X,Y), \ldots, G_n(X,Y)\rangle \subseteq K[X,Y]$$

e assim temos que:

$$I_{lead} = \langle X^{i_1}, X^{i_2}Y^{j_2}, \ldots, X^{i_{n-1}}Y^{j_{n-1}}, Y^{j_n}\rangle.$$

Logo,

$$\Delta_>(I_{lead}) = \{X^iY^j | \text{ para todo } s = 1,\ldots,n \text{ vale } i < i_s \text{ ou } j < j_s\}.$$

Logo,

$$\begin{aligned}
\sharp(\Delta_>(I_{lead})) =& i_1 j_n - (i_1 - i_2)(j_n - j_2) - (i_2 - i_3)(j_n - j_3) - \cdots - (i_{n-2} - i_{n-1})(j_n - j_{n-1})\\
=& j_2(i_1 - i_2) + j_3(i_2 - i_3) + \ldots + j_n i_{n-1}.
\end{aligned}$$

□

Proposição 3.3.4 *Considere*

$$\begin{aligned}
G_1(X,Y,Z) =& X^{i_1} + F_{11}(Y,Z)X^{i_1-1} + \ldots + F_{1i_1}(Y,Z)\\
G_2(X,Y,Z) =& Y^{j_2} + F_{21}(Z)Y^{j_2-1} + \ldots + F_{2j_2}(Z)\\
G_3(X,Y,Z) =& Z^{k_3} + F_{31}Z^{k_3-1} + \ldots + F_{3k_3}\\
H_4(X,Y,Z) =& F_{40}(Y,Z)X^{i_4} + F_{41}(Y,Z)X^{i_4-1} + \ldots + F_{4i_4}(Y,Z)
\end{aligned}$$

Seja $Y^{j_4}Z^{k_4}$ o monômio líder de $F_{40}(Y,Z)$ com respeito a ordem lexicográfica onde $X >_{lex} Y >_{lex} Z$. O número de soluções do conjunto de equações

$$G_1(X,Y,Z) = G_2(X,Y,Z) = G_3(X,Y,Z) = H_4(X,Y,Z) = 0$$

é no máximo

$$i_1 \cdot j_2 \cdot k_3 - (i_1 - i_4)(j_2 - j_4)(k_3 - k_4)$$

quando $i_1 > i_4$, $j_2 > j_4$, $k_3 > k_4$ e é no máximo igual a $i_1 \cdot j_2 \cdot k_3$, caso contrário.

Demonstração:
Seja $I = \langle G_1(X,Y,Z), G_2(X,Y,Z), G_3(X,Y,Z), H_4(X,Y,Z)\rangle$. Usando a ordem de monômios da proposição, temos:

$$I_{lead} = \langle X^{i_1}, Y^{j_2}, Z^{k_3}, X^{i_4}Y^{j_4}Z^{k_4}\rangle.$$

Assim, temos quatro casos a analisar.

1) Se $i_1 \leq i_4$.

   Assim, temos que I_{lead} se reduz à $I_{lead} = \langle X^{i_1}, Y^{j_2}, Z^{k_3}\rangle$, já que $X^{i_4}Y^{j_4}Z^{k_4}$ é múltiplo de X^{i_1}.
   Logo, temos que

$$\Delta_>(I_{lead}) = \{X^iY^jZ^k |\ i < i_1 \text{ e } j < j_2 \text{ e } k < k_3\}$$

   e então

$$\sharp(\Delta_>(I_{lead})) = i_1 \cdot j_2 \cdot k_3.$$

2) Se $j_2 \leq j_4$.

   Assim, temos que I_{lead} se reduz à $I_{lead} = \langle X^{i_1}, Y^{j_2}, Z^{k_3}\rangle$, já que $X^{i_4}Y^{j_4}Z^{k_4}$ é múltiplo de Y^{j_2}.
   Logo, temos que

$$\Delta_>(I_{lead}) = \{X^iY^jZ^k |\ i < i_1 \text{ e } j < j_2 \text{ e } k < k_3\}$$

   e então

$$\sharp(\Delta_>(I_{lead})) = i_1 \cdot j_2 \cdot k_3.$$

3) Se $k_3 \leq k_4$.

   Assim, temos que I_{lead} se reduz à $I_{lead} = \langle X^{i_1}, Y^{j_2}, Z^{k_3}\rangle$, já que $X^{i_4}Y^{j_4}Z^{k_4}$ é múltiplo de Z^{k_3}.
   Logo, temos que

$$\Delta_>(I_{lead}) = \{X^iY^jZ^k |\ i < i_1 \text{ e } j < j_2 \text{ e } k < k_3\}$$

   e então

$$\sharp(\Delta_>(I_{lead})) = i_1 \cdot j_2 \cdot k_3.$$

4) Se $i_1 > i_4$, $j_2 > j_4$ e $k_3 > k_4$.

   Definindo $j_1 = k_1 = i_2 = k_2 = i_3 = j_3 = 0$ temos

$$\Delta_>(I_{lead}) = \{X^iY^jZ^k |\ \text{para todo } s = 1, \ldots, 4 \text{ vale } i < i_s \text{ ou } j < j_s \text{ ou } k < k_s\}$$

   Assim,

$$\sharp(\Delta_>(I_{lead})) = i_1 \cdot j_2 \cdot k_3 - (i_1 - i_4)(j_2 - j_4)(k_3 - k_4).$$

□

Definição 3.3.5 *Dado um monômio $M = X_1^{\alpha_1} \cdot \ldots \cdot X_m^{\alpha_m} \in K[X_1, \ldots, X_m]$, o grau-ponderado de M (com pesos $\omega(X_i) := a_i \in \mathbb{R}_+, \forall i = 1, \ldots, m$) é*

$$gr_p(M) := a_1\alpha_1 + \ldots + a_m\alpha_m.$$

Uma função ordem grau-ponderada lexicográfica é aquela dada por:

$$M > N \iff gr_p(M) > gr_p(N)$$

ou

$$M >_{lex} N \text{ se } gr_p(M) = gr_p(N)$$

Proposição 3.3.6 *Defina uma função grau-ponderada em* $K[X,Y]$ *dada pelos pesos* $\omega(X) = b$ *e* $\omega(Y) = a$. *Considere*

$$\begin{aligned} F(X,Y) =& X^a + \alpha Y^b + F'(X,Y) \\ G(X,Y) =& X^iY^j + G'(X,Y) \end{aligned}$$

onde α *é não-nulo,* $a, b > 0$, $\omega(F') < ab$ *e* $\omega(G') < bi + aj$. *O conjunto de equações* $F(X,Y) = G(X,Y) = 0$ *têm no máximo* $bi + aj$ *soluções.*

Demonstração:

Considere a ordem grau-ponderada lexicográfica sobre $K[X,Y]$, dada pela função grau-ponderada da proposição combinada com a ordem lexicográfica $Y >_{lex} X$. Como, $\omega(X^a) = ba$, $\omega(Y^b) = ab$, $\omega(F') < ab$ e $Y >_{lex} X$, temos que $ML(F) = Y^b$. Além disso, também temos $\omega(X^iY^j) = bi + aj$ e $\omega(G') < bi + aj$, logo $ML(G) = X^iY^j$. Vamos mostrar que podemos tomar $j < b$.

Se $j \geq b$ então escrevemos

$$\begin{aligned} X^iY^j =& X^iY^{j-b}Y^b \\ =& X^iY^{j-b}(\alpha^{-1}F(X,Y) - \alpha^{-1}X^a - \alpha^{-1}F'(X,Y)) \\ =& \alpha^{-1}X^iY^{j-b}F(X,Y) - \alpha^{-1}X^{i+a}Y^{j-b} - \alpha^{-1}X^iY^{j-b}F'(X,Y). \end{aligned}$$

Assim,

$$\begin{aligned} G(X,Y) =& X^iY^j + G'(X,Y) \\ =& \alpha^{-1}X^iY^{j-b}F(X,Y) - \alpha^{-1}X^{i+a}Y^{j-b} - \alpha^{-1}X^iY^{j-b}F'(X,Y) + G'(X,Y). \end{aligned}$$

Tomando

$$\begin{aligned} \overline{G_1}(X,Y) :=& -\alpha(-\alpha^{-1}X^{i+a}Y^{j-b} - \alpha^{-1}X^iY^{j-b}F'(X,Y) + G'(X,Y)) \\ =& X^{i+a}Y^{j-b} + X^iY^{j-b}F'(X,Y) - \alpha G'(X,Y) \\ =& X^{i+a}Y^{j-b} + \overline{G_1}'(X,Y) \end{aligned}$$

temos que $G(X,Y) = \alpha^{-1}X^iY^{j-b}F(X,Y) - \alpha^{-1}\overline{G_1}(X,Y)$, logo é claro que $\langle F, G\rangle = \langle F, \overline{G_1}\rangle$, e portanto $V(\langle F, G\rangle) = V(\langle F, \overline{G_1}\rangle)$. Temos também que

$$ML(\overline{G_1}) = X^{i+a}Y^{j-b}, \quad \omega(X^{i+a}Y^{j-b}) = bi + aj = \omega(X^iY^j) \text{ e } \omega(\overline{G_1}') < bi + aj.$$

De fato:

$$\omega(X^{i+a}Y^{j-b}) = b(i+a) + a(j-b) = bi + aj \quad ,$$

$$\omega(X^iY^{j-b}F'(X,Y)) < bi + a(j-b) + ab = bi + aj \qquad \text{e}$$

$$\omega(-\alpha G'(X,Y)) < bi + aj.$$

Se $j - b < b$, acabamos. Caso contrário, repetimos o processo. Vamos então supor que $\overline{G}(X,Y) := X^iY^j + \overline{G}'(X,Y)$ com $j < b$.

Observamos agora que um outro polinômio que pertence ao ideal I é

$$\begin{aligned} H(X,Y) :=& \alpha S(F,\overline{G}) \\ =& \alpha(\frac{X^iY^b}{\alpha Y^b}F - \frac{X^iY^b}{X^iY^j}\overline{G}) \\ =& X^i(X^a + \alpha Y^b + F') - \alpha Y^{b-j}(X^iY^j + \overline{G}') \\ =& X^{i+a} + X^iF' - \alpha Y^{b-j}\overline{G}' \end{aligned}$$

com monômio líder X^{i+a}, já que,

$$\omega(X^{i+a}) = bi + ab \quad , \quad \omega(X^iF') < bi + ab \quad \text{e} \quad \omega(Y^{b-j}\overline{G}') < a(b-j) + bi + aj = bi + ab.$$

Assim, utilizando o fato que $I := \langle F, G\rangle = \langle F, \overline{G}\rangle$ e definindo $I_* := \langle Y^b, X^iY^j, X^{i+a}\rangle$ temos que

$$\Delta(I) \subseteq \Delta(I_*) := \{X^\alpha Y^\beta | \alpha < a + i,\ \beta < b;\ \alpha < i \text{ ou } \beta < j\}$$

e

$$\sharp(\Delta(I_*)) = (a+i)b - (a+i-i)(b-j) = \omega(X^iY^j) = bi + aj.$$

E assim, temos que o conjunto de equações possui no máximo $\omega(X^iY^j) = bi + aj$ soluções. □

Corolário 3.3.7 *Defina uma função grau-ponderada por $\omega(X) = c$ e $\omega(Y) = a + b$. Considere*

$$\begin{aligned} F(X,Y) =& X^iY^j + \alpha X^a + F'(X,Y) \\ G(X,Y) =& X^{i+b}Y^j + \beta Y^c + G'(X,Y) \end{aligned}$$

onde α, β são não-nulos, $ci + (a+b)j > ac > \omega(F')$ e $\omega(G') < ac + bc$. O conjunto de equações $F(X,Y) = G(X,Y) = 0$ têm no máximo $(a+b)j + ci$ soluções.

Demonstração:

A partir do S-polinômio $S(F,G)$ definimos

$$\begin{aligned}
H(X,Y) :=& \frac{1}{\alpha} S(F,G) \\
=& \frac{1}{\alpha}\left(\frac{X^{i+b}Y^j}{X^iY^j}F - \frac{X^{i+b}Y^j}{X^{i+b}Y^j}G\right) \\
=& \frac{1}{\alpha}(X^bF(X,Y) - G(X,Y)) \\
=& \frac{1}{\alpha}(X^b(X^iY^j + \alpha X^a + F'(X,Y)) - (X^{i+b}Y^j + \beta Y^c + G'(X,Y))) \\
=& \frac{1}{\alpha}(X^{i+b}Y^j + \alpha X^{a+b} + X^bF' - X^{i+b}Y^j - \beta Y^c - G'(X,Y)) \\
=& X^{a+b} + \frac{1}{\alpha}X^bF' - \frac{\beta}{\alpha}Y^c - \frac{1}{\alpha}G'(X,Y) \\
=& X^{a+b} - \frac{\beta}{\alpha}Y^c + H'(X,Y) \\
=& X^{a+b} - mY^c + H'(X,Y)
\end{aligned}$$

onde $m \neq 0$, pois $\alpha, \beta \neq 0$ e $\omega(H') < \omega(X^{a+b}) = \omega(Y^c)$.

Agora, se (x,y) é solução de $F(X,Y) = G(X,Y) = 0$ então (x,y) é solução de $H(X,Y) = F(X,Y) = 0$.

De fato,

Seja (x,y) solução de $F(X,Y) = G(X,Y) = 0$ então $F(x,y) = G(x,y) = 0$. Como, $H(X,Y) = \frac{1}{\alpha}(X^bF(X,Y) - G(X,Y))$, temos que:

$$H(x,y) = \frac{1}{\alpha}(x^bF(x,y) - G(x,y)) = \frac{1}{\alpha}(x^b \cdot 0 - 0) = 0.$$

Logo, considerando o conjunto de equações $H(X,Y) = F(X,Y) = 0$ e aplicando o Proposição 3.3.6 onde $a = a+b$, $b = c$, $i = i$ e $j = j$, temos que existem no máximo $bi + aj = ci + (a+b)j$ soluções. Logo, $F(X,Y) = G(X,Y) = 0$ tem no máximo $bi + aj = ci + (a+b)j$ soluções.

□

Corolário 3.3.8 *Defina uma função grau-ponderada como na Proposição 3.3.6. Considere*

$$\begin{aligned}
F(X,Y) =& X^a + \alpha Y^b + F'(X,Y) \\
G(X,Y) =& X^iY^j + G'(X,Y)
\end{aligned}$$

onde α é não-nulo, $a,b > 0$, $j \leq b$, $\omega(G') < bi + aj$, $\omega(F') \leq ab$ e qualquer monômio em F' de peso ab não é X^a, Y^b nem X^sY^t onde $t < j$. O conjunto de equações $F(X,Y) = G(X,Y) = 0$ têm no máximo $bi + aj$ soluções.

Demonstração:

A partir do S-polinômio $S(F,G)$ definimos

$$\begin{aligned}
H(F,G) :=& \alpha S(F,G) \\
=& \alpha\left(\frac{X^iY^b}{\alpha Y^b}F - \frac{X^iY^b}{X^iY^j}G\right) \\
=& X^iF - \alpha Y^{b-j}G \\
=& X^i(X^a + \alpha Y^b + F') - \alpha Y^{b-j}(X^iY^j + G') \\
=& X^{i+a} + \alpha X^iY^b + X^iF' - \alpha X^iY^b - \alpha Y^{b-j}G' \\
=& X^{i+a} + X^iF' - \alpha Y^{b-j}G'
\end{aligned}$$

onde $\omega(X^{i+a}) = bi + ab$, $\omega(X^iF') \leq bi + ab$ e $\omega(Y^{b-j}G') < bi + ab$.

Observe que, em princípio, não podemos determinar qual é o monômio líder de H, já que $\omega(X^iF') \leq bi + ab$. Provemos que se os monômios de F' com peso ab não são X^a, Y^b nem X^sY^t onde $t < j$ temos que $ML(H) = X^{i+a}$.

De fato, como qualquer polinômio em F' de peso ab não é X^a, Y^b nem X^sY^t onde $t < j$, temos que os monômios de F' são da seguinte forma: X^mY^l com $l \neq 0$, $m \neq 0$, $l \geq j$ e, sem perda de generalidade, podemos assumir, l como sendo a maior potência de Y nessas condições.

Temos que

$$X^mY^l = X^{m-i}Y^{l-j}X^iY^j$$

e assim, reduzindo H módulo G, temos:

$$\begin{aligned} H - cX^{m-i}Y^{l-j}G =& \alpha S - (cX^mY^l + cX^{m-i}Y^{l-j}G') \\ =& X^{i+a} + X^iF' - \alpha Y^{b-j}G' - cX^mY^l - cX^{m-i}Y^{l-j}G' \end{aligned}$$

onde c é uma constante que elimine o termo X^mY^l de F' ao se fazer a diferença $X^iF' - cX^mY^l$. Caso ainda possua mais termos da forma $X^{m'}Y^{l'}$, efetuamos novamente redução de H módulo G, até eliminarmos todos esses termos. Esse processo é finito, devido ao fato que consideramos l como sendo a maior potência de Y que satisfaz as condições acima.

Assim, após eliminarmos todos os termos da forma X^mY^l, temos que H, possui monômio líder igual a X^{i+a} e o resultado segue pelo final da demonstração da Proposição 3.3.6.

□

Proposição 3.3.9 *Defina uma função grau-ponderada sobre $K[X, Y, Z]$ por $\omega(X) = b^2$, $\omega(Y) = ab$ e $\omega(Z) = a^2$. Considere*

$$\begin{aligned} G_1(X, Y, Z) =& X^a + \alpha Y^b + G_1'(X, Y, Z) \\ G_2(X, Y, Z) =& Y^a + \beta Z^b + G_2'(X, Y, Z) \\ G_3(X, Y, Z) =& X^iY^jZ^k + G_3'(X, Y, Z) \end{aligned}$$

onde α, β são não-nulos e onde $\omega(G_1') < ab^2$, $\omega(G_2') < a^2b$ e $\omega(G_3') < ib^2 + jab + ka^2$. O conjunto de equações

$$G_1(X, Y, Z) = G_2(X, Y, Z) = G_3(X, Y, Z) = 0$$

tem no máximo $\omega(G_3') = ib^2 + jab + ka^2$ soluções.

Demonstração:

Considere a ordem grau-ponderada lexicográfica sobre $K[X, Y, Z]$ dada pela função grau-ponderada em combinação com a ordem lexicográfica $X >_{lex} Y >_{lex} Z$. Assumiremos sem perda de generalidade que $a \geq b$ (caso contrário, basta substituir X por Z e Z por X, que voltamos para o caso em que o expoente de X é maior que o expoente de Y em G_1 e o expoente de Y é maior que o expoente de Z em G_2). Agora G_3 pode ser reduzido módulo $\{G_1, G_2\}$ para um polinômio com monômio líder $X^iY^jZ^k$, onde i, $j < a$.

De fato,

Antes de provar isto necessitamos da seguinte observação

Observação 3.3.10 *Calcular as raízes do conjunto de equações*

$$G_1(X, Y, Z) = G_2(X, Y, Z) = G_3(X, Y, Z) = 0$$

é equivalente a calcular as raízes do ideal $\langle G_1, G_2, G_3\rangle$. *Por outro lado, pelo algoritmo da divisão temos que* $G_3 = a_1G_1 + a_2G_2 + r$ *com* $a_1, a_2, r \in K[X, Y, Z]$. *Observe que* $\langle G_1, G_2, G_3\rangle \subseteq \langle G_1, G_2, r\rangle$, *pois* $G_3 = a_1G_1 + a_2G_2 + r$ *e* $\langle G_1, G_2, r\rangle \subseteq \langle G_1, G_2, G_3\rangle$, *pois* $r = G_3 - a_1G_1 - a_2G_2$ *e, portanto temos* $\langle G_1, G_2, G_3\rangle = \langle G_1, G_2, r\rangle$. *Assim, calcular as raízes do conjunto de equações* $G_1(X, Y, Z) = G_2(X, Y, Z) = G_3(X, Y, Z) = 0$ *é equivalente a calcular as raízes do ideal* $\langle G_1, G_2, r\rangle$.

Agora, voltemos a nossa demonstração. Se $i < a$ e $j < a$ não temos nada a fazer. Se $i < a$ e $j \geq a$ vamos direto para o passo 2. Se $i \geq a$, então vamos para o Passo 1.

Passo 1:

Da primeira equação, temos que $X^a = G_1 - \alpha Y^b - G_1'$ e substituindo em G_3 obtemos:

$$\begin{aligned} G_3 =& X^iY^jZ^k + G_3' \\ =& X^{i-a}X^aY^jZ^k + G_3' \\ =& X^{i-a}(G_1 - \alpha Y^b - G_1')Y^jZ^k + G_3' \\ =& X^{i-a}Y^jZ^kG_1 - \alpha X^{i-a}Y^{b+j}Z^k - X^{i-a}Y^jZ^kG_1' + G_3' \\ =& X^{i-a}Y^jZ^kG_1 + 0G_2 - \alpha X^{i-a}Y^{b+j}Z^k - X^{i-a}Y^jZ^kG_1' + G_3' \end{aligned}$$

e utilizando a observação acima, onde $r = -\alpha X^{i-a}Y^{b+j}Z^k - X^{i-a}Y^jZ^kG_1' + G_3'$, podemos trocar G_3 por r. Temos que $\omega(r) = \omega(G_3)$, porém, a potência $\widetilde{i}$ de X no $ML(r)$ (neste caso, $\widetilde{i} = i - a$) é menor que a potência de X no $ML(G_3)$, ou seja, $\widetilde{i} < i$ e a potência de Y no $ML(r)$ (neste caso, $\widetilde{j} = b + j$) é maior que a potência de Y no $ML(G_3)$, ou seja, $\widetilde{j} > j$. E agora, se $\widetilde{i} < a$ vamos para o Passo 2, caso contrário voltamos para o Passo 1 e repetimos o processo até obtermos um $\widetilde{i} < a$.

Agora, se temos $\widetilde{j} < a$, concluímos a demonstração, caso contrário, segue o Passo 2.

Passo 2:

Por uma questão de simplicidade, suponha que ao se fazer o Passo 1, apenas uma vez, obtemos $\widetilde{i} = i - a < a$ e $\widetilde{j} = b + j > a$.

Da segunda equação, temos que $Y^a = G_2 - \beta Z^b - G_2'$ e substituindo em r obtemos:

$$\begin{aligned} r =& -\alpha X^{\widetilde{i}}Y^{\widetilde{j}}Z^k - X^{\widetilde{i}}Y^{\widetilde{j}-b}Z^kG_1' + G_3' \\ =& -\alpha X^{\widetilde{i}}Y^{\widetilde{j}-a}Y^aZ^k - X^{\widetilde{i}}Y^{\widetilde{j}-b-a}Y^aZ^kG_1' + G_3' \\ =& -\alpha X^{\widetilde{i}}Y^{\widetilde{j}-a}(G_2 - \beta Z^b - G_2')Z^k - X^{\widetilde{i}}Y^{\widetilde{j}-b-a}(G_2 - \beta Z^b - G_2')Z^kG_1' + G_3' \\ =& -\alpha X^{\widetilde{i}}Y^{\widetilde{j}-a}Z^kG_2 + \alpha\beta X^{\widetilde{i}}Y^{\widetilde{j}-a}Z^{b+k} + \alpha X^{\widetilde{i}}Y^{\widetilde{j}-a}Z^kG_2' - X^{\widetilde{i}}Y^{\widetilde{j}-b-a}Z^kG_1'G_2 \\ &+\beta X^{\widetilde{i}}Y^{\widetilde{j}-b-a}Z^{k+b}G_1' + X^{\widetilde{i}}Y^{\widetilde{j}-b-a}Z^kG_1'G_2' + G_3' \\ =& 0G_1 + (-\alpha X^{\widetilde{i}}Y^{\widetilde{j}-a}Z^k - X^{\widetilde{i}}Y^{\widetilde{j}-b-a}Z^kG_1')G_2 + \alpha\beta X^{\widetilde{i}}Y^{\widetilde{j}-a}Z^{b+k} + \alpha X^{\widetilde{i}}Y^{\widetilde{j}-a}Z^kG_2' \\ &+\beta X^{\widetilde{i}}Y^{\widetilde{j}-b-a}Z^{k+b}G_1' + X^{\widetilde{i}}Y^{\widetilde{j}-b-a}Z^kG_1'G_2' + G_3'. \end{aligned}$$

Novamente, pela observação 3.3.10 podemos trocar r por

$$\widetilde{r} := \alpha\beta X^{\widetilde{i}}Y^{\widetilde{j}-a}Z^{b+k} + \alpha X^{\widetilde{i}}Y^{\widetilde{j}-a}Z^kG_2' + \beta X^{\widetilde{i}}Y^{\widetilde{j}-b-a}Z^{k+b}G_1' + X^{\widetilde{i}}Y^{\widetilde{j}-b-a}Z^kG_1'G_2' + G_3'.$$

Assim, continuamos o Passo 2 até obtermos um polinômio que no monômio líder tenha a potência de Y menor que a. Observe que quando estamos fazendo o Passo 2, a potência de X, no monômio líder, não se altera e, portanto, conseguimos assim, um polinômio com $\widetilde{i}, \widetilde{j} < a$. Observe também que $\omega(\widetilde{r}) = \omega(G_3)$.

Para facilitar a notação, assumiremos, sem perda de generalidade, que G_3 é da forma como no enunciado, com $i, j < a$.

Assim, existem 2 casos a considerar:

Caso 1: $a < b + j$.

Seja o S-polinômio

$$\begin{aligned} S(G_1, G_3) =& \frac{X^a Y^j Z^k}{X^a} G_1 - \frac{X^a Y^j Z^k}{X^i Y^j Z^k} G_3 \\ =& Y^j Z^k G_1 - X^{a-i} G_3 \\ =& X^a Y^j Z^k + \alpha Y^{b+j} Z^k + Y^j Z^k G_1' - X^a Y^j Z^k - X^{a-i} G_3' \\ =& \alpha Y^{b+j} Z^k + Y^j Z^k G_1' - X^{a-i} G_3'. \end{aligned}$$

Como $\omega(Y^{b+j}Z^k) = ab^2 + abj + a^2k$, $\omega(Y^j Z^k G_1') < ab^2 + abj + a^2k$ e $\omega(X^{a-i} G_3') < ab^2 + abj + a^2k$, temos que $ML(S(G_1, G_3)) = Y^{b+j}Z^k$.

Reduzindo $S(G_1, G_3)$ módulo G_2, obtemos:

$$G_4 = -\alpha\beta Y^{b+j-a} Z^{k+b} + Y^j Z^k G_1' - \alpha Y^{b+j-a} Z^k G_2' - X^{a-i} G_3'$$

com $ML(G_4) = Y^{b+j-a} Z^{k+b}$.

De fato,

Dividindo-se $\alpha Y^{b+j} Z^k + Y^j Z^k G_1' - X^{a-i} G_3'$ por $Y^a + \beta Z^b + G_2'$, obtemos quociente $\alpha Y^{b+j-a} Z^k$ e resto $-\alpha\beta Y^{b+j-a} Z^{k+b} + Y^j Z^k G_1' - \alpha Y^{b+j-a} Z^k G_2' - X^{a-i} G_3'$, ou seja,

$$S(G_1, G_3) \equiv -\alpha\beta Y^{b+j-a} Z^{k+b} + Y^j Z^k G_1' - \alpha Y^{b+j-a} Z^k G_2' - X^{a-i} G_3' \ (mod\ G_2).$$

Portanto, tomando $G_4 := -\alpha\beta Y^{b+j-a} Z^{k+b} + Y^j Z^k G_1' - \alpha Y^{b+j-a} Z^k G_2' - X^{a-i} G_3'$, temos

$$\omega(Y^{b+j-a} Z^{k+b}) = ab^2 + abj + a^2k,$$

$$\omega(Y^j Z^k G_1') < ab^2 + abj + a^2k,$$

$$\omega(Y^{b+j-a} Z^k G_2') < ab^2 + abj + a^2k \text{ e}$$

$$\omega(X^{a-i} G_3') < ab^2 + abj + a^2k,$$

o que implica $ML(G_4) = Y^{b+j-a} Z^{k+b}$.

Além disso, sejam

$$\begin{aligned} G_5 :=& S(G_2, G_4) \\ =& \frac{Y^a Z^{k+b}}{Y^a} G_2 - \frac{Y^a Z^{k+b}}{-\alpha\beta Y^{b+j-a} Z^{k+b}} G_4 \\ =& Z^{k+b} G_2 + \frac{Y^{2a-b-j}}{\alpha\beta} G_3 \\ =& Y^a Z^{k+b} + \beta Z^{2b+k} + Z^{k+b} G_2' - Y^a Z^{k+b} + \frac{Y^{2a-b} Z^k G_1'}{\alpha\beta} - \frac{Y^a Z^k G_2'}{\beta} - \frac{X^{a-i} Y^{2a-b-j} G_3'}{\alpha\beta} \\ =& \beta Z^{2b+k} + \frac{Y^{2a-b} Z^k G_1'}{\alpha\beta} + Z^{k+b} G_2' - \frac{Y^a Z^k G_2'}{\beta} - \frac{X^{a-i} Y^{2a-b-j} G_3'}{\alpha\beta} \end{aligned}$$

onde, $\omega(Z^{2b+k}) = 2a^2b + a^2k$, $\omega(Y^{2a-b}Z^kG_1') < 2a^2b + a^2k$, $\omega(Z^{k+b}G_2') < 2a^2b + a^2k$, $\omega(Y^aZ^kG_2') < 2a^2b + a^2k$ e $\omega(X^{a-i}Y^{2a-b-j}G_3') < 2a^2b + a^2k$, ou seja, $ML(G_5) = Z^{2b+k}$; e

$$\begin{aligned} G_6 :=& S(G_2, G_3) \\ =& \frac{X^iY^aZ^k}{Y^a}G_2 - \frac{X^iY^aZ^k}{X^iY^jZ^k}G_3 \\ =& X^iZ^kG_2 - Y^{a-j}G_3 \\ =& X^iY^aZ^k + \beta X^iZ^{k+b} + X^iZ^kG_2' - X^iY^aZ^k - Y^{a-j}G_3' \\ =& \beta X^iZ^{k+b} + X^iZ^kG_2' - Y^{a-j}G_3' \end{aligned}$$

onde, $\omega(X^iZ^{k+b}) = b^2i + a^2k + a^2b$, $\omega(X^iZ^kG_2') < b^2i + a^2k + a^2b$ e $\omega(Y^{a-j}G_3') < b^2i + a^2k + a^2b$, ou seja, $ML(G_6) = X^iZ^{k+b}$.

Observação 3.3.11 *Para o cálculo de G_5 temos que*

$$MMC(ML(G_2), ML(G_4)) = Y^aZ^{k+b},$$

pelo fato de $b \leq a$ e $j < a$, o que implica $b + j < 2a$, ou seja, $b + j - a < a$.

Assim, detectamos os seguintes monômios líderes em $\langle G_1, G_2, G_3\rangle$,

$$\{X^a, Y^a, Z^{2b+k}, Y^{b+j-a}Z^{k+b}, X^iZ^{k+b}, X^iY^jZ^k\}.$$

Agora, definindo

$$I_* := \langle X^a, Y^a, Z^{2b+k}, Y^{b+j-a}Z^{k+b}, X^iZ^{k+b}, X^iY^jZ^k\rangle$$

temos

$$\begin{aligned} \sharp(\Delta(I_*)) =& \ a \cdot a \cdot (2b+k) - i \cdot (a-b-j+a) \cdot (2b+k-b-k) \\ & - j \cdot (a-i) \cdot (2b+k-b-k) - (a-i) \cdot (a-j) \cdot (2b+k-k) \\ =& \ a^2k + b^2i + jab \end{aligned}$$

e de $\Delta(I) \subseteq \Delta(I_*)$ vem que existem no máximo $a^2k + b^2i + jab$ soluções.

Caso 2: $a \geq b + j$

Temos os seguintes S-polinômios:

$$G_4 := S(G_1, G_3) = \alpha Y^{b+j}Z^k + Y^jZ^kG_1' - X^{a-i}G_3'$$

com $ML(S(G_1, G_3)) = Y^{b+j}Z^k$ e,

$$\begin{aligned}
G_5 :=& S(G_2, G_4) \\
=& \frac{Y^a Z^k}{Y^a} G_2 - \frac{Y^a Z^k}{\alpha Y^{b+j} Z^k} G_4 \\
=& Z^k G_2 - \frac{Y^{a-j-b}}{\alpha} G_4 \\
=& Y^a Z^k + \beta Z^{k+b} + Z^k G_2' - Y^a Z^k - \frac{Y^{a-b} Z^k G_1'}{\alpha} + \frac{X^{a-i} Y^{a-b-j} G_3'}{\alpha} \\
=& \beta Z^{k+b} + Z^k G_2' - \frac{Y^{a-b} Z^k G_1'}{\alpha} + \frac{X^{a-i} Y^{a-b-j} G_3'}{\alpha}
\end{aligned}$$

onde $\omega(Z^{k+b}) = a^2k + a^2b$, $\omega(Z^k G_2') < a^2k + a^2b$, $\omega(Y^{a-b} Z^k G_1') < a^2k + a^2b$ e $\omega(X^{a-i} Y^{a-b-j} G_3')$, ou seja, $ML(G_5) = Z^{k+b}$.

Agora, detectamos os seguintes monômios líderes em $\langle G_1, G_2, G_3 \rangle$,

$$\{X^a, Y^a, Z^{b+k}, Y^{b+j} Z^k, X^i Y^j Z^k\}.$$

Agora, definindo

$$I_* := \langle X^a, Y^a, Z^{b+k}, Y^{b+j} Z^k, X^i Y^j Z^k \rangle$$

temos

$$\begin{aligned}
\sharp(\Delta(I_*)) =& a \cdot a \cdot (b+k) - i \cdot (a-j-b) \cdot (b+k-k) - (a-i) \cdot (a-j) \cdot (b+k-k) \\
=& a^2k + b^2 i + jab = \omega(G_3)
\end{aligned}$$

e de $\Delta(I) \subseteq \Delta(I_*)$ vem que existem no máximo $a^2k + b^2 i + jab$ soluções.

□

Proposição 3.3.12 *Considere*

$$\begin{aligned}
F(X, Y) =& Y + \alpha X + \beta \\
G(X, Y) =& G_1(X, Y) + G_2(X, Y)
\end{aligned}$$

onde G_1 é irredutível e homogêneo de multi-grau m maior ou igual a 1, e onde G_2 é de multi-grau menor que m. O conjunto de equações $F(X, Y) = G(X, Y) = 0$ tem no máximo m soluções.

Demonstração:

Seja $H(X) := G(X, -\alpha X - \beta)$; temos que $H(X)$ é um polinômio de grau no máximo m. Se $H(X)$ não é o polinômio nulo então temos que $H(X)$ tem no máximo m soluções e nossa proposição segue. Resta mostrar então que $H(X)$ não pode ser o polinômio nulo.

O coeficiente para X^m em $H(X)$ é $G_1(1, -\alpha)$. De fato,

seja $G_1 = \alpha_m X^m + \alpha_{m-1} X^{m-1} Y + \ldots + \alpha_2 X^2 Y^{m-2} + \alpha_1 X^1 Y^{m-1} + \alpha_0 Y^m$. Assim:

$$\begin{aligned} H(X) =& G(X, -\alpha X - \beta) \\ =& G_1(X, -\alpha X - \beta) + G_2(X, -\alpha X - \beta) \\ =& \alpha_m X^m + \alpha_{m-1} X^{m-1}(-\alpha X - \beta) + \ldots + \alpha_2 X^2 (-\alpha X - \beta)^{m-2} + \\ &+ \alpha_1 X^1 (-\alpha X - \beta)^{m-1} + \alpha_0 (-\alpha X - \beta)^m + G_2(X, -\alpha X - \beta) \\ =& (\alpha_m - \alpha\alpha_{m-1} + \alpha^2 \alpha_{m-2} + \ldots + (-1)^m \alpha^m \alpha_0) X^m + \ldots \\ =& G_1(1, -\alpha) X^m + \ldots \end{aligned}$$

Observe que $G_2(X, Y)$ não influencia no coeficiente de X^m, já que o multi-grau dele é menor que m.

Assim, se $G_1(1, -\alpha) = 0$, temos que α é raiz do polinômio $G_1(1, T)$, logo podemos escrever $G_1(1, T) = (T + \alpha)P(T)$ nos dando

$$G_1(X, Y) = X^m G_1(X, Y/X) = (Y + \alpha)P'(X, Y)$$

o que é um absurdo, visto que $G_1(X, Y)$ é irredutível.

□

3.4 Estudo da Hierarquia de Pesos de Certos Códigos

A seguir vamos encontrar ou estimar a hierarquia de peso para alguns códigos. Para isso, lembremos que pelo Teorema 3.1.2, o problema de estimar o peso generalizado de Hamming é traduzido para o problema de estimar o número de soluções comuns para um certo conjunto de equações polinomiais.

A Códigos de Klein Melhorados

Seja V o conjunto dos 22 pontos sobre a curva de Klein $X^3Y + Y^3 + X = 0$ sobre $\mathbb{F}_8$. Considere o código sobre $\mathbb{F}_8$ com a matriz checagem de paridade

$$H := [\varphi(1), \varphi(X), \varphi(Y), \varphi(X^2), \varphi(XY), \varphi(X^3), \varphi(Y^2)]^T$$

onde φ é definida como na Seção 3.2.

Encontraremos D_1, D_2 e estimaremos D_3.

Primeiro determinaremos D_1.

- $D_{\{[1]\}} = 0$ é óbvio.
- $D_{\{[X]\}} \leq 3$
  Queremos estimar o número máximo de soluções para o conjunto de equações

$$\begin{cases} X + a & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a \in \mathbb{F}_8$. Fazendo $X = -a$ em $X^3Y + Y^3 + X$, temos $Y^3 - a^3 Y - a$, um polinômio não-nulo em Y de grau 3. Assim existem no máximo 3 soluções. Logo, $D_{\{[X]\}} \leq 3$.
- $D_{\{[Y]\}} \leq 4$
  Queremos estimar o número máximo de soluções para o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

onde $a, b \in \mathbb{F}_8$.

Se $a = 0$, temos $Y = -b$ e substituindo em $X^3Y + Y^3 + X$, obtemos um polinômio não-nulo em X de grau no máximo 3. Assim existem no máximo 3 soluções.

Se $a \neq 0$, pela Proposição 3.3.6 (onde a, b, i e j, da proposição são, respectivamente, 1, 1, 3, 1, $F' = \frac{b}{a}$ e $G' = Y^3 + X$), temos no máximo $bi + aj = 4$ soluções. Logo, $D_{\{[Y]\}} \leq 4$.

- $D_{\{[X^2]\}} \leq 6$

  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c \in \mathbb{F}_8$.

  Escolhendo $\omega(X) = 1$ e $\omega(Y) = 1.6$ e tomando

$$I = \langle X^2 + aY + bX + c, X^3Y + Y^3 + X \rangle$$

  temos

$$I_{lead} = \langle X^2, Y^3 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, Y, Y^2, XY, XY^2\}$$

  Assim, o número máximo de soluções é 6. Logo, $D_{\{[X^2]\}} \leq 6$.

- $D_{\{[XY]\}} \leq 7$

  Considere o conjunto de equações

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d \in \mathbb{F}_8$.

  Se $a \neq 0$, temos pelo Corolário 3.3.7 (onde i, j, a, b e c do corolário são, respectivamente, 1, 1, 2, 2, 3, $F' = bY + cX + d$ e $G' = X$), existem no máximo $(a+b)j + ci = 7$ soluções.

  Se $a = 0$, temos:

$$\begin{cases} XY + bY + cX + d & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  e então a resultante com respeito a X é:

$$\begin{vmatrix} c+Y & bY+d & 0 & 0 \\ 0 & c+Y & bY+d & 0 \\ 0 & 0 & c+Y & bY+d \\ Y & 0 & 1 & Y^3 \end{vmatrix} =$$

$$Y^6 + 3cY^5 + (3c^2 - b)Y^4 + (c^3 - 3bc - d)Y^3 + (-3bc^2 - 3dc)Y^2 + (-bc^3 - dc)Y - dc^3$$

  que é um polinômio em Y de grau 6. Esse polinômio tem seis soluções em $\overline{\mathbb{F}_8}$, logo tem no máximo seis soluções em $\mathbb{F}_8$. Assim, pela Proposição 1.9.4 (ii) temos que

para cada solução α desse polinômio diferente de $-c$ ou 0 temos uma única solução do sistema, pois $(\alpha + c)X + b\alpha + d$ tem grau 1 em X; pelo mesmo motivo, temos no máximo uma solução da forma $(\beta, 0)$ ou $(\beta, -c)$. Portanto, o nosso sistema tem no máximo 6 soluções.

Logo, $D_{\{[XY]\}} \leq 7$.

- $D_{\{[X^3]\}} \leq 9$

  Considere o conjunto de equações

$$\begin{cases} X^3 + aXY + bX^2 + cY + dX + e &= 0 \\ X^3Y + Y^3 + X &= 0 \end{cases}$$

  onde $a, b, c, d, e \in \mathbb{F}_8$.

  Escolhendo $\omega(X) = 1$ e $\omega(Y) = 1.6$, temos:

$$I_{lead} = \langle X^3, Y^3 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, X^2, Y, Y^2, XY, XY^2, X^2Y, X^2Y^2\}$$

  Assim, o número máximo de soluções é 9. Logo, $D_{\{[X^3]\}} \leq 9$.

- $D_{\{[Y^2]\}} \leq 9$

  Considere o conjunto de equações

$$\begin{cases} Y^2 + aX^3 + bXY + cX^2 + dY + eX + f &= 0 \\ X^3Y + Y^3 + X &= 0 \end{cases}$$

  onde $a, b, c, d, e, f \in \mathbb{F}_8$.

  Se $a = 0$ mas $c \neq 0$ temos:

$$\begin{cases} Y^2 + bXY + cX^2 + dY + eX + f &= 0 \\ X^3Y + Y^3 + X &= 0 \end{cases}$$

  o que é equivalente a:

$$\begin{cases} X^2 + \frac{1}{c}Y^2 + \frac{b}{c}XY + \frac{d}{c}Y + \frac{e}{c}X + \frac{f}{c} &= 0 \\ X^3Y + Y^3 + X &= 0 \end{cases}$$

  Pelo Corolário 3.3.8 (onde os elementos a, b, i e j do corolário são, respectivamente, 2, 2, 3, 1, $F' = \frac{b}{c}XY + \frac{d}{c}Y + \frac{e}{c}X + \frac{f}{c}$ e $G' = Y^3 + X$), temos no máximo $bi + aj = 8$ soluções.

  Se $a = 0$ e $c = 0$ temos:

$$\begin{cases} Y^2 + bXY + dY + eX + f &= 0 \\ X^3Y + Y^3 + X &= 0 \end{cases}$$

  a resultante com respeito a X é:

$$\begin{vmatrix} bY + e & Y^2 + dY + f & 0 & 0 \\ 0 & bY + e & Y^2 + dY + f & 0 \\ 0 & 0 & bY + e & Y^2 + dY + f \\ Y & 0 & 1 & Y^3 \end{vmatrix} =$$

$$\begin{aligned} &- Y^7 + (b^3 - 3d)Y^6 + (3b^2e - 3d^2 - 2f)Y^5 + (3be^2 - b^2 - 6df - d^3)Y^4 + \\ &+ (-b^2d - 2be + e^3 - 3f^2 - 3d^2f)Y^3 + (-2bde - b^2f - e^2 + 3df^2)Y^2 \\ &+ (-de^2 - bef + f^3)Y - bef - e^2f \end{aligned}$$

que é um polinômio em Y de grau 7. Esse polinômio tem sete soluções em $\overline{\mathbb{F}_8}$, logo tem no máximo sete soluções em $\mathbb{F}_8$. Assim, pela Proposição 1.9.4 (ii) temos que para cada solução α desse polinômio diferente de $-e/b$, se $b \neq 0$ (respectivamente, $-e$, se $b = 0$), ou 0 temos uma única solução do sistema, pois $(\alpha)^2 + bX(\alpha) + d(\alpha) + eX + f$ tem grau 1 em X; pelo mesmo motivo, temos no máximo uma solução da forma $(\beta, 0)$ ou $(\beta, -c)$ (respectivamente, $(\beta, 0)$ ou $(\beta, -e)$, se $b = 0$). Logo, existem no máximo 7 soluções.

Agora, se $a \neq 0$, substituindo $Y^2 = -aX^3 - bXY - cX^2 - dY - eX - f$ na segunda equação, temos:

$$\begin{aligned} X^3Y + Y^3 + X = 0 \therefore & X^3Y + YY^2 + X = 0 \\ \therefore & X^3Y + Y(-aX^3 - bXY - cX^2 - dY - eX - f) + X = 0 \\ \therefore & (1-a)X^3Y - bXY^2 - cX^2Y - dY^2 - eXY - fY + X = 0 \end{aligned}$$

Como as mudanças feitas não alteram as soluções do sistema original, vamos então resolver o seguinte sistema:

$$\begin{cases} Y^2 + aX^3 + bXY + cX^2 + dY + eX + f & = 0 \\ (1-a)X^3Y - bXY^2 - cX^2Y - dY^2 - eXY - fY + X & = 0 \end{cases}$$

Agora:

- Se $a \neq 0$ e $a \neq 1$
  Podemos transformar o sistema para:

  $$\begin{cases} X^3 + \frac{1}{a}Y^2 + \frac{b}{a}XY + \frac{c}{a}X^2 + \frac{d}{a}Y + \frac{e}{a}X + \frac{f}{a} & = 0 \\ (1-a)X^3Y - bXY^2 - cX^2Y - dY^2 - eXY - fY + X & = 0 \end{cases}$$

  Assim, pela Proposição 3.3.6 (onde os elementos a, b, i e j, da proposição são, respectivamente, 3, 2, 3, 1, $F' = \frac{b}{a}XY + \frac{c}{a}X^2 + \frac{d}{a}Y + \frac{e}{a}X + \frac{f}{a}$ e $G' = -bXY^2 - cX^2Y - dY^2 - eXY - fY + X$), temos no máximo $bi + aj = 9$ soluções.
- Se $a \neq 0$, $a = 1$ e $b \neq 0$
  O sistema torna-se

  $$\begin{cases} X^3 + Y^2 + bXY + cX^2 + dY + eX + f & = 0 \\ XY^2 + \frac{c}{b}X^2Y + \frac{d}{b}Y^2 + \frac{e}{b}XY + \frac{f}{b}Y + \frac{1}{b}X & = 0 \end{cases}$$

  Assim, pela Proposição 3.3.6 (onde os elementos a, b, i e j da proposição são, respectivamente, 3, 2, 1, 2, $F' = bXY + cX^2 + dY + eX + f$ e $G' = \frac{c}{b}X^2Y + \frac{d}{b}Y^2 + \frac{e}{b}XY + \frac{f}{b}Y + \frac{1}{b}X$), temos no máximo $bi + aj = 8$ soluções.
- Se $a \neq 0$, $a = 1$, $b = 0$ e $c \neq 0$
  O sistema torna-se

  $$\begin{cases} X^3 + Y^2 + cX^2 + dY + eX + f & = 0 \\ X^2Y + \frac{d}{c}Y^2 + \frac{e}{c}XY + \frac{f}{c}Y + \frac{1}{c}X & = 0 \end{cases}$$

  Assim, pela Proposição 3.3.6 (onde os elementos a, b, i e j da proposição são, respectivamente, 3, 2, 2, 1, $F' = cX^2 + dY + eX + f$ e $G' = \frac{d}{c}Y^2 + \frac{e}{c}XY + \frac{f}{c}Y + \frac{1}{c}X$), temos no máximo $bi + aj = 7$ soluções.

– Se $a \neq 0$, $a = 1$, $b = 0$ e $c = 0$
O sistema torna-se

$$\begin{cases} X^3 + Y^2 + dY + eX + f &= 0 \\ -dY^2 - eXY - fY + X &= 0 \end{cases}.$$

Fazendo a resultante em relação a X temos:

$$\begin{vmatrix} 1 - eY & -dY^2 - fY & 0 & 0 \\ 0 & 1 - eY & -dY^2 - fY & 0 \\ 0 & 0 & 1 - eY & -dY^2 - fY \\ 1 & 0 & e & Y^2 + dY + f \end{vmatrix}$$

$$= d^3Y^6 + (3d^2f - e^3)Y^5 + (3df^2 + 3e^2)Y^4 + (de^2 + f^3 - 3e)Y^3 + \\ +(1 + fe^2 - 2de)Y^2 + (d - 2fe)Y + f$$

que é um polinômio em Y de grau no máximo 6. Como antes, concluímos, usando a Proposição 1.9.4 que existem no máximo 6 soluções em $\mathbb{F}_8^2$, já que o segundo polinômio tem grau igual a 1 em X.

Logo, $D_{\{[Y^2]\}} \leq 9$.

Assim, $D_1 \leq 9$.

Pela inspeção do conjunto de equações

$$\begin{cases} X^3 + XY + X^2 + Y + X + 1 &= 0 \\ X^3Y + Y^3 + X = 0 \end{cases}$$

temos nove soluções: $(1, \alpha)$, $(1, \alpha^2)$, $(1, \alpha^4)$, (α, α^6), (α^2, α^5), (α^3, α^2), (α^4, α^3), (α^5, α) e (α^6, α^4), onde α é uma raiz em $T^3 + T + 1$.

De fato,

Podemos representar $\mathbb{F}_8$ como

$$\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1) = \{\overline{0}, \overline{1}, \overline{X}, \overline{1 + X}, \overline{X^2}, \overline{1 + X^2}, \overline{X + X^2}, \overline{1 + X + X^2}\}.$$

Tomando $\alpha = \overline{X}$, temos que:

- $\alpha^3 = 1 + \alpha$, já que, $0 = \alpha^3 + \alpha + 1$ implica $\alpha^3 = -(1 + \alpha)$ mas, como em $\mathbb{F}_2$ temos $1 = -1$, então $\alpha^3 = 1 + \alpha$;
- $\alpha^4 = \alpha(\alpha^3) = \alpha(1 + \alpha) = \alpha + \alpha^2$.
- $\alpha^5 = (\alpha^3)(\alpha^2) = (1 + \alpha)(\alpha^2) = \alpha^2 + \alpha^3 = 1 + \alpha + \alpha^2$.
- $\alpha^6 = (\alpha^3)(\alpha^3) = (1 + \alpha)(1 + \alpha) = 1 + 2\alpha + \alpha^2$ mas, como em $\mathbb{F}_2$ temos $2 = 0$, então $\alpha^6 = 1 + \alpha^2$.

  e assim, sucessivamente.

Utilizando esses fatos, temos que:

- $(1, \alpha)$ é solução do sistema acima.
  $\begin{cases} 1^3 + 1 \cdot \alpha + 1^2 + \alpha + 1 + 1 = 4 + 2 \cdot \alpha = 0 \text{ pois, } 4 = 2 = 0 \\ 1^3 \cdot \alpha + \alpha^3 + 1 = 0 \text{ pois, } \alpha \text{ é raiz de } X^3 + X + 1 \end{cases}$

- $(1, \alpha^2)$ é solução do sistema acima.
  $\begin{cases} 1^3 + 1 \cdot \alpha^2 + 1^2 + \alpha^2 + 1 + 1 = 2 \cdot \alpha^2 + 4 \\ 1^3 \cdot \alpha^2 + (\alpha^2)^3 + 1 = \alpha^2 + \alpha^6 + 1 = \alpha^2 + 1 + \alpha^2 + 1 = 2 \cdot \alpha^2 + 2 \cdot \alpha + 2 \cdot 1 = 0 \end{cases}$.
  Os outros casos são semelhantes.

Então, temos $D_1 \geq 9$ e concluímos $D_1 = 9$.

Agora, vamos determinar D_2.

- $D_{\{[1],*\}} = 0$ é óbvio.
- $D_{\{[X],*\}} \leq 3$
  Queremos estimar o número máximo de soluções para o conjunto de equações

$$\begin{cases} * & = 0 \\ X + a & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $*$ representa um polinômio do tipo $bY^2 + cX^3 + dXY + eX^2 + fY + gX + h$ com $a, b, c, d, e, f, g, h \in \mathbb{F}_8$ e nem todos b, c, d, e, f nulos.
  Como vimos,

$$\begin{cases} X + a & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  possui no máximo 3 soluções. Logo,

$$\begin{cases} * & = 0 \\ X + a & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  possui no máximo 3 soluções e $D_{\{[X],*\}} \leq 3$.
- $D_{\{[Y],*\}} \leq 4$
  Queremos estimar o número máximo de soluções para o conjunto de equações

$$\begin{cases} * & = 0 \\ Y + aX + b & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $*$ representa um polinômio do tipo $cY^2 + dX^3 + eXY + fX^2 + gY + hX + i$ com $a, b, c, d, e, f, g, h, i \in \mathbb{F}_8$ e nem todos c, d, e, f nulos.
  Como vimos,

$$\begin{cases} Y + aX + b & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  possui no máximo 4 soluções. Logo,

$$\begin{cases} * & = 0 \\ Y + aX + b & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  possui no máximo 4 soluções e $D_{\{[Y]\}} \leq 4$.

- $D_{\{[X^2],*\}} \leq 6$
  Considere o conjunto de equações

$$\begin{cases} * & = 0 \\ X^2 + aY + bX + c & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $*$ representa um polinômio do tipo $dY^2 + eX^3 + fXY + gX^2 + hY + iX + j$ com $a, b, c, d, e, f, g, h, i, j \in \mathbb{F}_8$ e nem todos d, e, f nulos.
  Como vimos,

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  possui no máximo 6 soluções, logo

$$\begin{cases} * & = 0 \\ X^2 + aY + bX + c & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  possui no máximo 6 soluções e $D_{\{[X^2]\}} \leq 6$.

- $D_{\{[XY],[X^3]\}} \leq 5$
  Considere o conjunto de equações

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ X^3 + eX^2 + fY + gX + h & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h \in \mathbb{F}_8$.
  Se $f \neq 0$, aplicando a Proposição 3.3.6 nas duas primeiras equações (onde os elementos a, b, i e j da proposição são, respectivamente, 3, 1, 1, 1, $F' = eX^2+gX+h$ e $G' = aX^2 + bY + cX + d$) temos no máximo $bi + aj = 4$ soluções.
  Se $f = 0$, temos que resolver o sistema:

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ X^3 + eX^2 + gX + h & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}.$$

  Assim, resolvendo a segunda equação, temos no máximo 3 soluções para X. Se nenhuma solução é igual a $-b$ então para cada uma que substituímos na primeira equação temos apenas um valor para Y, e então temos 3 soluções para o nosso sistema. Se $-b$ é uma das soluções da segunda equação, observe que a primeira equação não possui mais a variável Y e, na terceira equação, encontramos no máximo mais 3 valores para Y. Assim, temos no máximo 5 soluções para o sistema. Logo, $D_{\{[XY],[X^3]\}} \leq 5$.

- $D_{\{[XY],[Y^2]\}} \leq 5$
  Considere o conjunto de equações

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ Y^2 + eX^3 + fX^2 + gY + hX + i & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h \in \mathbb{F}_8$.

Se $e \neq 0$, aplicando a Proposição 3.3.6 nas duas primeiras equações (onde os elementos a, b, i e j da proposição são, respectivamente, 3, 2, 1, 1, $F' = \frac{f}{e}X^2 + \frac{g}{e}Y + \frac{h}{e}X + \frac{i}{e}$ e $G' = aX^2 + bY + cX + d$) temos no máximo $bi + aj = 5$ soluções.
Se $e = 0$ mas $a \neq 0$, fazendo, $\omega(X) = 1$ e $\omega(Y) = 1.1$ podemos considerar o S-polinômio:

$$\begin{aligned} S(F_1, F_3) =& \frac{X^3Y}{XY}(XY + aX^2 + bY + cX + d) - \frac{X^3Y}{X^3Y}(X^3Y + Y^3 + X) \\ =& X^2(XY + aX^2 + bY + cX + d) - (X^3Y + Y^3 + X) \\ =& aX^4 + bX^2Y + cX^3 + dX^2 - Y^3 - X \end{aligned}$$

e assim, temos

$$I_* := \langle XY, Y^2, X^3Y, X^4 \rangle \text{ e logo } \Delta(I_*) = \{1, X, X^2, X^3, Y\},$$

ou seja, temos no máximo 5 soluções, pois $\Delta(I) \subseteq \Delta(I_*)$.
Se $e = a = h = 0$ e $f \neq 0$ temos:

$$\begin{cases} XY + bY + cX + d &= 0 \\ X^2 + \frac{1}{f}Y^2 + \frac{g}{f}Y + \frac{i}{f} &= 0 \\ X^3Y + Y^3 + X &= 0 \end{cases}$$

e utilizando a Proposição 3.3.6 nas duas primeiras equações (onde os elementos a, b, i e j da proposição são, respectivamente, 2, 2, 1, 1, $F' = \frac{g}{f}Y + \frac{i}{f}$ e $G' = bY + cX + d$) temos no máximo $bi + aj = 4$ soluções.
Se $e = a = f = 0$ e $h \neq 0$ temos:

$$\begin{cases} XY + bY + cX + d &= 0 \\ X + \frac{1}{h}Y^2 + \frac{g}{h}Y + \frac{i}{h} &= 0 \\ X^3Y + Y^3 + X &= 0 \end{cases}$$

e utilizando a Proposição 3.3.6 nas duas primeiras equações (onde os elementos a, b, i e j da proposição são, respectivamente, 1, 2, 1, 1, $F' = \frac{g}{h}Y + \frac{i}{h}$ e $G' = bY + cX + d$) temos no máximo $bi + aj = 3$ soluções.
Se $e = a = 0$, $f \neq 0$ e $h \neq 0$ temos:

$$\begin{cases} XY + bY + cX + d &= 0 \\ X^2 + \frac{1}{f}Y^2 + \frac{g}{f}Y + \frac{h}{f}X + \frac{i}{f} &= 0 \\ X^3Y + Y^3 + X &= 0 \end{cases}$$

e utilizando a Proposição 3.3.6 nas duas primeiras equações (onde os elementos a, b, i e j da proposição são, respectivamente, 2, 2, 1, 1, $F' = \frac{g}{h}Y + \frac{h}{f} + \frac{i}{f}$ e $bY + cX + d$) temos no máximo $bi + aj = 4$ soluções.
Finalmente, se $e = a = f = h = 0$ temos:

$$\begin{cases} XY + bY + cX + d &= 0 \\ Y^2 + gY + i &= 0 \\ X^3Y + Y^3 + X &= 0 \end{cases}.$$

Assim, resolvendo a segunda equação, temos no máximo 2 soluções para Y. Se nenhuma raiz é igual a $-c$ então substituindo na primeira equação, temos apenas

um valor para X e então temos 2 soluções para o nosso sistema. Se $-c$ é uma das soluções da segunda equação, observe que a primeira equação não possui mais a variável X e, na terceira equação, encontramos no máximo mais 3 valores para X. Assim, temos no máximo 4 soluções para o sistema. Logo, $D_{\{[XY],[Y^2]\}} \leq 5$.

- $D_{\{[X^3],[Y^2]\}} \leq 6$
  Queremos resolver o conjunto de equações

$$\begin{cases} X^3 + aXY + bX^2 + cY + dX + e & = 0 \\ Y^2 + fX^3 + gXY + hX^2 + iY + jX + k & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k \in \mathbb{F}_8$.
  Fazendo, $\omega(X) = 1$ e $\omega(Y) = 1.6$, temos

$$I_{lead} = \langle X^3, Y^2, Y^3 \rangle = \langle X^3, Y^2 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, X^2, Y, XY, X^2Y\},$$

  ou seja, o sistema possui no máximo 6 soluções.
  Logo, $D_{\{[X^3],[Y^2]\}} \leq 6$.

Portanto, $D_2 \leq 6$.

Pela inspeção do conjunto de equações

$$\begin{cases} X^2 + Y + 1 & = 0 \\ X^3 + XY + X^2 + Y + X + 1 & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

têm as soluções (α, α^6), (α^2, α^5), (α^3, α^2), (α^4, α^3), (α^5, α) e (α^6, α^4). Então $D_{\{[X^2],[X^3]\}} \geq 6$ e concluímos que $D_2 = 6$.

Observação 3.4.1 *Para provar que o sistema acima tem estas soluções dadas acima, o procedimento é análogo ao caso de* D_1.

Agora estimaremos D_3.

- $D_{\{[1],*,*\}} = 0$, $D_{\{[X],*,*\}} \leq 3$ e $D_{\{[Y],*,*\}} \leq 4$ como acima.
- $D_{\{[X^2],[XY],[Y^2]\}} \leq 3$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ XY + dX^2 + eY + fX + g & = 0 \\ Y^2 + hX^3 + iXY + jX^2 + kY + lX + m & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m \in \mathbb{F}_8$.
  Fazendo, $\omega(X) = 1$ e $\omega(Y) = 1.6$, temos

$$I_{lead} = \langle X^2, XY, Y^2, Y^3 \rangle = \langle XY, X^2, Y^2 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, Y\},$$

  ou seja, o sistema possui no máximo 3 soluções.
  Portanto, $D_{\{[X^2],[XY],[Y^2]\}} \leq 3$.

- $D_{\{[X^2],[X^3],[Y^2]\}} \leq 4$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ X^3 + dXY + eX^2 + fY + gX + h & = 0 \\ Y^2 + iX^3 + jXY + kX^2 + lY + mX + n & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n \in \mathbb{F}_8$.
  Fazendo, $\omega(X) = 1$ e $\omega(Y) = 1.6$, temos

$$I_{lead} = \langle X^2, X^3, Y^2, Y^3 \rangle = \langle X^2, Y^2 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, Y, XY\},$$

  ou seja, o sistema possui no máximo 4 soluções.
  Portanto, $D_{\{[X^2],[X^3],[Y^2]\}} \leq 4$.

- $D_{\{[XY],[X^3],[Y^2]\}} \leq 4$.
  Considere o conjunto de equações

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ X^3 + eXY + fX^2 + gY + hX + i & = 0 \\ Y^2 + jX^3 + kXY + lX^2 + mY + nX + o & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, o \in \mathbb{F}_8$.
  Fazendo, $\omega(X) = 1$ e $\omega(Y) = 1.6$, temos

$$I_{lead} = \langle XY, X^3, Y^2, Y^3 \rangle = \langle Y^2, XY, X^3 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, X^2, Y\},$$

  ou seja, o sistema possui no máximo 4 soluções.
  Portanto, $D_{\{[XY],[X^3],[Y^2]\}} \leq 4$.

- $D_{\{[X^2],[XY],[X^3]\}} \leq 4$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ XY + dX^2 + eY + fX + g & = 0 \\ X^3 + hXY + iX^2 + jY + kX + l & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l \in \mathbb{F}_8$.
  Fazendo, $\omega(X) = 1$ e $\omega(Y) = 1.6$, temos

$$I_{lead} = \langle X^2, XY, X^3, Y^3 \rangle = \langle X^2, XY, Y^3 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, Y, Y^2\},$$

  ou seja, o sistema possui no máximo 4 soluções.
  Portanto, $D_{\{[X^2],[XY],[X^3]\}} \leq 4$.

Assim, $D_3 \leq 4$.

Agora, tratemos das distâncias generalizadas do código. É óbvio que $n = 22$. A seguir determinaremos a hierarquia de pesos.

Temos que $d_1 = 6$, já que pelo Teorema 3.1.2, de $D_{7-6+1+1} = D_3 \leq 4$ temos $d_1 \geq 6$ e de $D_{7-6+1} = D_2 \geq 6$ vem que $d_1 \leq 6$.

Temos que $d_2 = 8$, já que pelo Teorema 3.1.2, de $D_{7-8+2+1} = D_2 \leq 6$ temos $d_2 \geq 8$ e de $D_{7-8+2} = D_1 \geq 8$ vem que $d_2 \leq 8$.

Analogamente, temos que $d_3 = 9$, já que pelo Teorema 3.1.2, de $D_{7-9+3+1} = D_2 \leq 7$ temos $d_3 \geq 9$ e de $D_{7-9+3} = D_1 \geq 9$ vem que $d_1 \leq 9$.

Agora, por um lado, $d_i \geq i + 7$ para $i = 4, \ldots, k$, já que $D_{7-(i+7)+i+1} = D_1 \leq 9$. Por outro lado, a Cota de Singleton Generalizada implica que $d_i \leq i + (n-k)$ para $i \leq k$, e de $i+7 \leq d_i \leq i+(n-k)$ temos $n-k \geq 7$. Como $n-k$ não pode exceder o número de linhas de H, pois $dim C^{\perp} = n-k$ e H é a matriz geradora de $C^{\perp}$, temos que $n-k \leq 7$. Assim, $n-k = 7$ o que implica $22-k = 7$, ou seja, $k = 15$. Logo, concluímos que $d_i = i+7$ para $i = 4, \ldots, k$.

Vamos agora considerar outro código sobre $\mathbb{F}_8$, que é o código com matriz checagem de paridade

$$H := [\varphi(1), \varphi(X), \varphi(Y), \varphi(X^2), \varphi(XY), \varphi(X^3 + Y^2)]^T;$$

onde φ é dada como na Seção 3.2. Como acima V é o conjunto de pontos da quártica de Klein sobre $\mathbb{F}_8$.

Vamos estimar os valores de D_1, D_2 e D_3.

Primeiro estimaremos D_1.

- $D_{\{[1]\}} = 0$, $D_{\{[X]\}} \leq 3$, $D_{\{[Y]\}} \leq 4$, $D_{\{[X^2]\}} \leq 6$ e $D_{\{[XY]\}} \leq 7$ são encontrados como anteriormente.
- $D_{\{[X^3+Y^2]\}} \leq 8$
  Considere o conjunto de equações

$$\begin{cases} X^3 + Y^2 + aXY + bX^2 + cY + dX + e &= 0 \\ X^3Y + Y^3 + X &= 0 \end{cases}$$

  onde $a, b, c, d, e \in \mathbb{F}_8$.
  Multiplicando a primeira equação por Y e subtraindo a segunda equação desta, obtemos $aXY^2 + bX^2Y + cY^2 + dXY + eY - X = 0$ e o nosso sistema fica equivalente ao sistema:

$$\begin{cases} X^3 + Y^2 + aXY + bX^2 + cY + dX + e &= 0 \\ aXY^2 + bX^2Y + cY^2 + dXY + eY - X &= 0 \end{cases}.$$

  Se $a \neq 0$, pela Proposição 3.3.6 (onde os elementos a, b, i e j da proposição são, respectivamente, 3, 2, 1, 2, $F' = aXY + bX^2 + cY + dX + e$ e $G' = \frac{b}{a}X^2Y + \frac{c}{a}Y^2 + \frac{d}{a}XY + \frac{e}{a}Y - \frac{1}{a}X$), temos no máximo $bi + aj = 8$ soluções.
  Se $a = 0$ e $b \neq 0$, pela Proposição 3.3.6 (onde os elementos a, b, i e j da proposição são, respectivamente, 3, 2, 2, 1, $F' = aXY + bX^2 + cY + dX + e$ e $G' = \frac{c}{b}Y^2 + \frac{d}{b}XY + \frac{e}{b}Y - \frac{1}{b}X$), temos no máximo $bi + aj = 7$ soluções.
  Se $a = b = 0$ e $c \neq 0$, fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos:

$$I_{lead} = \langle X^3, Y^2 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, X^2, Y, XY, X^2Y\}$$

  e assim, temos que o sistema possui no máximo 6 soluções.

Se $a = b = c = 0$ e $d \neq 0$, pela Proposição 3.3.6 (onde os elementos a, b, i e j da proposição são, respectivamente, 3, 2, 1, 1, $F' = dX + e$ e $G' = \frac{e}{d}Y - \frac{1}{d}X$), temos no máximo $bi + aj = 5$ soluções.

Se $a = b = c = d = 0$ temos o seguinte sistema:

$$\begin{cases} X^3 + Y^2 + e & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}.$$

Observe que de $X^3 + Y^2 + e = 0$ temos $X^3 + Y^2 = -e$, logo $X^3Y + Y^3 = -eY$ e assim, nosso sistema fica equivalente ao sistema:

$$\begin{cases} X^3 + Y^2 + e & = 0 \\ -eY + X & = 0 \end{cases}.$$

Substituindo $X = eY$ na primeira equação temos no máximo 3 soluções.

Logo, $D_{\{[X^3+Y^2]\}} \leq 8$.

E, assim, $D_1 \leq 8$.

Agora, vamos determinar D_2.

- $D_{\{[1],*\}} = 0$, $D_{\{[X],*\}} \leq 3$, $D_{\{[Y],*\}} \leq 4$ são encontrados como anteriormente.
- $D_{\{[X^2],[XY]\}} \leq 4$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ XY + dX^2 + eY + fX + g & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g \in \mathbb{F}_8$.
  Considerando $\omega(X) = 1$ e $\omega(Y) = 1.6$, temos:

$$I_{lead} = \langle X^2, XY, Y^3 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, Y, Y^2\}$$

  e assim, temos que o sistema possui no máximo 4 soluções.
  Logo, $D_{\{[X^2],[XY]\}} \leq 4$.
- $D_{\{[X^2],[X^3+Y^2]\}} \leq 4$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ X^3 + Y^2 + dXY + eX^2 + fY + gX + h & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h \in \mathbb{F}_8$.
  Considerando $\omega(X) = 1$ e $\omega(Y) = 1.6$, temos:

$$I_{lead} = \langle X^2, Y^2, Y^3 \rangle = \langle X^2, Y^2 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, Y, XY\}$$

  e assim, temos que o sistema possui no máximo 4 soluções.
  Logo, $D_{\{[X^2],[X^3+Y^2]\}} \leq 4$.

- $D_{\{[XY],[X^3+Y^2]\}} \leq 5$.
  Considere o conjunto de equações

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ X^3 + Y^2 + eXY + fX^2 + gY + hX + i & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i \in \mathbb{F}_8$.

  Pela Proposição 3.3.6 (onde os elementos a, b, i e j da proposição são, respectivamente, 3, 2, 1, 1, $F' = eXY + fX^2 + gY + hX + i$ e $aX^2 + bY + cX + d$), temos no máximo $bi + aj = 5$ soluções.

  Logo, $D_{\{[XY],[X^3+Y^2]\}} \leq 5$.

Assim, $D_2 \leq 5$.

Vamos determinar D_3.

- $D_{\{[1],*,*\}} = 0$, $D_{\{[X],*,*\}} \leq 3$ são encontrados como anteriormente.
- $D_{\{[Y],[X^2],[XY]\}} \leq 2$.
  Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ X^2 + cY + dX + e & = 0 \\ XY + fX^2 + gY + hX + i & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i \in \mathbb{F}_8$.

  Considerando $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos:

$$I_{lead} = \langle Y, X^2, XY, X^3Y \rangle = \langle Y, X^2 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X\}$$

  e assim, temos que o sistema possui no máximo 2 soluções.

  Logo, $D_{\{[Y],[X^2],[XY]\}} \leq 2$.

- $D_{\{[Y],[X^2],[X^3+Y^2]\}} \leq 2$.
  Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ X^2 + cY + dX + e & = 0 \\ X^3 + Y^2 + fXY + gX^2 + hY + iX + j & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j \in \mathbb{F}_8$.

  Considerando $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos:

$$I_{lead} = \langle Y, X^2, X^3, X^3Y \rangle = \langle Y, X^2 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X\}$$

  e assim, temos que o sistema possui no máximo 2 soluções.

  Logo, $D_{\{[Y],[X^2],[X^3+Y^2]\}} \leq 2$.

- $D_{\{[Y],[XY],[X^3+Y^2]\}} \leq 3$.
  Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ XY + cX^2 + dY + eX + f & = 0 \\ X^3 + Y^2 + gXY + hX^2 + iY + jX + k & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k \in \mathbb{F}_8$.
  Considerando $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos:

$$I_{lead} = \langle Y, XY, X^3, X^3Y \rangle = \langle Y, X^3 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, X^2\}$$

  e assim, temos que o sistema possui no máximo 3 soluções.
  Logo, $D_{\{[Y],[XY],[X^3+Y^2]\}} \leq 3$.

- $D_{\{[X^2],[XY],[X^3+Y^2]\}} \leq 3$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ XY + dX^2 + eY + fX + g & = 0 \\ X^3 + Y^2 + hXY + iX^2 + jY + kX + l & = 0 \\ X^3Y + Y^3 + X & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l \in \mathbb{F}_8$.
  Considerando $\omega(X) = 1$ e $\omega(Y) = 1.6$, temos:

$$I_{lead} = \langle X^2, XY, Y^2, Y^3 \rangle = \langle X^2, XY, Y^2 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, Y\}$$

  e assim, temos que o sistema possui no máximo 3 soluções.
  Logo, $D_{\{[X^2],[XY],[X^3+Y^2]\}} \leq 3$.

Assim, $D_3 \leq 3$.

Agora tratemos as distâncias generalizadas do código. Novamente, $n = 22$. Da Teorema 3.1.1 temos $d_1 \geq 5$, $d_2 \geq 7$, $d_1 \geq 8$ e $d_i \geq i + 6$ para $i = 4, \ldots, k$, já que $D_3 \leq 3$, $D_2 \leq 5$ e $D_1 \leq 8$. A Cota de Singleton Generalizada implica que $d_i \leq i + (n - k)$ para qualquer $i \leq k$. Usando o fato que $n - k$ não pode exceder o número de linhas de H temos $k = 16$ e $d_i = i + 6$ para $i = 4, \ldots, k$.

B Código Hermitiano Melhorado

Seja V os 64 pontos sobre a curva Hermitiana $X^5 + Y^4 + Y = 0$ sobre $\mathbb{F}_{16}$. Considere o código sobre $\mathbb{F}_{16}$ com matriz checagem de paridade

$$H := [\varphi(1), \varphi(X), \varphi(Y), \varphi(X^2), \varphi(XY), \varphi(Y^2), \varphi(X^3), \varphi(Y^3 + X^4)]^T$$

onde φ é definida como na Seção 3.2.

Vamos estimar D_1, D_2 D_3 e D_4 e, a seguir vamos estimar a hierarquia de pesos da curva Hermitiana.

Primeiro considere D_1.

- $D_{\{[1]\}} = 0$ é óbvio.

- $D_{\{[X]\}} \leq 4$
  Queremos estimar o número máximo de soluções para o conjunto de equações

$$\begin{cases} X + a & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a \in \mathbb{F}_{16}$.
  Fazendo $X = -a$ em $X^5 + Y^4 + Y$, temos $Y^4 - a^5 + Y$, que se torna um polinômio não-nulo em Y de grau 4. Assim existem no máximo 4 soluções. Logo, $D_{\{[X]\}} \leq 4$.
- $D_{\{[Y]\}} \leq 5$
  Queremos estimar o número máximo de soluções para o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b \in \mathbb{F}_{16}$.
  Fazendo $Y = -aX - b$ e substituindo em $X^5 + Y^4 + Y$, obtemos um polinômio não-nulo em X de grau no máximo 5. Assim existem no máximo 5 soluções.
  Logo, $D_{\{[Y]\}} \leq 5$.
- $D_{\{[X^2]\}} \leq 8$
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c \in \mathbb{F}_{16}$.
  Escolhendo $\omega(X) = 1$ e $\omega(Y) = 1.3$, temos

$$I_{lead} = \langle X^2, Y^4 \rangle \text{ e logo } \Delta(I_{lead}) = \{1, X, Y, Y^2, Y^3, XY, XY^2, XY^3\}$$

  Assim, o número máximo de soluções é 8, e temos $D_{\{[X^2]\}} \leq 8$.
- $D_{\{[XY]\}} \leq 9$.
  Considere o conjunto de equações

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d \in \mathbb{F}_{16}$.
  Pela Proposição 3.3.6 (onde os elementos a, b, i e j da proposição são, respectivamente, 5, 4, 1, 1, $F' = Y$ e $G' = aX^2 + bY + cX + d$) temos no máximo $bi + aj = 9$ soluções, logo $D_{\{[XY]\}} \leq 9$.
- $D_{\{[Y^2]\}} \leq 10$
  Considere o conjunto de equações

$$\begin{cases} Y^2 + aXY + bX^2 + cY + dX + e & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e \in \mathbb{F}_{16}$.
  Considerando $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y^2, X^5 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2, X^3, X^4, Y, XY, , X^2Y, X^3Y, X^4Y\}$$

  e assim o sistema possui no máximo 10 soluções, logo $D_{\{[Y^2]\}} \leq 10$.

- $D_{\{[X^3]\}} \leq 12$
  Considere o conjunto de equações

$$\begin{cases} X^3 + aY^2 + bXY + cX^2 + dY + eX + f & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.3$, temos

$$I_{lead} = \langle X^3, Y^4 \rangle$$

  logo,

$$\Delta(I_{lead}) = \{1, X, X^2, Y, Y^2, Y^3, XY, XY^2, XY^3, X^2Y, X^2Y^2, X^2Y^3\}.$$

  Assim, o número máximo de soluções é 12, e $D_{\{[X^3]\}} \leq 12$.

- $D_{\{[Y^3+X^4]\}} \leq 16$
  Considere o conjunto de equações

$$\begin{cases} Y^3 + X^4 + aX^3 + bY^2 + cXY + dX^2 + eY + fX + g & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.3$, temos

$$I_{lead} = \langle X^4, Y^4 \rangle$$

  logo,

$$\begin{aligned} \Delta(I_{lead}) = \{&1, X, X^2, X^3, Y, Y^2, Y^3, XY, XY^2, XY^3, X^2Y, X^2Y^2, X^2Y^3, \\ &X^3Y, X^3Y^2, X^3Y^3\}. \end{aligned}$$

  Assim, o número máximo de soluções é 16 e $D_{\{[X^3]\}} \leq 16$, logo $D_{\{[Y^3+X^4]\}} \leq 16$.

Portanto, $D_1 \leq 16$.

Tratemos agora da estimativa de D_2.

- $D_{\{[1],*\}} = 0$, $D_{\{[X],*\}} \leq 4$, $D_{\{[Y],*\}} \leq 5$, $D_{\{[X^2,*]\}} \leq 8$, segue do fato de $D_{\{[1]\}} = 0$, $D_{\{[X]\}} \leq 4$, $D_{\{[Y]\}} \leq 5$, $D_{\{[X^2]\}} \leq 8$.
- $D_{\{[XY],[Y^2]\}} \leq 6$.
  Considere o conjunto de equações

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ Y^2 + eXY + fX^2 + gY + hX + i & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle XY, Y^2, X^5 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2, X^3, X^4, Y\}.$$

  Assim, o número máximo de soluções é 6, e $D_{\{[XY],[Y^2]\}} \leq 6$.

- $D_{\{[XY],[X^3]\}} \leq 6$.
  Considere o conjunto de equações

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ X^3 + eY^2 + fXY + gX^2 + hY + iX + j & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.3$, temos

$$I_{lead} = \langle XY, X^3, Y^4 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2, Y, Y^3, Y^3\}.$$

  Assim, o número máximo de soluções é 6, e $D_{\{[XY],[X^3]\}} \leq 6$.

- $D_{\{[XY],[Y^3+X^4]\}} \leq 7$.
  Considere o conjunto de equações

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ Y^3 + X^4 + eX^3 + fY^2 + gXY + hX^2 + iY + jX + k & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k \in \mathbb{F}_{16}$.
  Considerando apenas as duas primeiras equações e aplicando a Proposição 3.3.6 (onde os elementos a, b, i e j da proposição são, respectivamente, 4, 3, 1, 1, $F' = eX^3 + fY^2 + gXY + hX^2 + iY + jX + k$ e $G' = aX^2 + bY + cX + d$) temos no máximo $bi + aj = 7$ soluções, logo, $D_{\{[XY],[Y^3+X^4]\}} \leq 7$.

- $D_{\{[Y^2],[X^3]\}} \leq 6$.
  Considere o conjunto de equações

$$\begin{cases} Y^2 + aXY + bX^2 + cY + dX + e & = 0 \\ X^3 + fY^2 + gXY + hX^2 + iY + jX + k & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y^2, X^3, X^5 \rangle = \langle Y^2, X^3 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2, Y, XY, X^2Y\}.$$

  Assim, o número máximo de soluções é 6, e $D_{\{[Y^2],[X^3]\}} \leq 6$.

- $D_{\{[Y^2],[Y^3+X^4]\}} \leq 8$.
  Considere o conjunto de equações

$$\begin{cases} Y^2 + aXY + bX^2 + cY + dX + e & = 0 \\ Y^3 + X^4 + fX^3 + gY^2 + hXY + iX^2 + jY + kX + l & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y^2, X^4, X^5 \rangle = \langle Y^2, X^4 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2, X^3, Y, XY, X^2Y, X^3Y\}.$$

  Assim, o número máximo de soluções é 8, e $D_{\{[Y^2],[Y^3+X^4]\}} \leq 8$.

- $D_{\{[X^3],[Y^3+X^4]\}} \leq 9$.
  Considere o conjunto de equações

$$\begin{cases} X^3 + aY^2 + bXY + cX^2 + dY + eX + f & = 0 \\ Y^3 + X^4 + gX^3 + hY^2 + iXY + jX^2 + kY + lX + m & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.4$, temos

$$I_{lead} = \langle X^3, Y^3, Y^4 \rangle = \langle X^3, Y^3 \rangle$$

  logo,

$$\Delta(I_{lead}) = \{1, X, X^2, Y, Y^2, XY, XY^2, X^2Y, X^2Y^2\}.$$

  Assim, o número máximo de soluções é 9, e $D_{\{[X^3],[Y^3+X^4]\}} \leq 9$; portanto, $D_2 \leq 9$.

Considere D_3.

- $D_{\{[1],*,*\}} = 0$, $D_{\{[X],*,*\}} \leq 4$, $D_{\{[Y],*,*\}} \leq 5$ segue do fato de $D_{\{[1]\}} = 0$, $D_{\{[X]\}} \leq 4$, $D_{\{[Y]\}} \leq 5$.
- $D_{\{[X^2],[XY],[Y^2]\}} \leq 3$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ XY + dX^2 + eY + fX + g & = 0 \\ Y^2 + hXY + iX^2 + jY + kX + l & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.3$, temos

$$I_{lead} = \langle X^2, XY, Y^2, Y^4 \rangle = \langle X^2, XY, Y^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, Y\}.$$

  Assim, o número máximo de soluções é 3, e $D_{\{[X^2],[XY],[Y^2]\}} \leq 3$.
- $D_{\{[X^2],[XY],[X^3]\}} \leq 5$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ XY + dX^2 + eY + fX + g & = 0 \\ X^3 + hY^2 + iXY + jX^2 + kY + lX + m & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.3$, temos

$$I_{lead} = \langle X^2, XY, X^3, Y^4 \rangle = \langle X^2, XY, Y^4 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, Y, Y^2, Y^3\}.$$

  Assim, o número máximo de soluções é 5, e $D_{\{[X^2],[XY],[X^3]\}} \leq 5$.

- $D_{\{[X^2],[XY],[Y^3+X^4]\}} \leq 5$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ XY + dX^2 + eY + fX + g & = 0 \\ Y^3 + X^4 + hX^3 + iY^2 + jXY + kX^2 + lY + mX + n & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.3$, temos

$$I_{lead} = \langle X^2, XY, X^4, Y^4 \rangle = \langle X^2, XY, Y^4 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, Y, Y^2, Y^3\}.$$

  Assim, o número máximo de soluções é 5, e $D_{\{[X^2],[XY],[Y^3+X^4]\}} \leq 5$.

- $D_{\{[X^2],[Y^2],[X^3]\}} \leq 4$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ Y^2 + dXY + eX^2 + fY + gX + h & = 0 \\ X^3 + iY^2 + jXY + kX^2 + lY + mX + n & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle X^2, Y^2, X^3, X^5 \rangle = \langle X^2, Y^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, Y, XY\}.$$

  Assim, o número máximo de soluções é 4, e $D_{\{[X^2],[Y^2],[X^3]\}} \leq 4$.

- $D_{\{[X^2],[Y^2],[Y^3+X^4]\}} \leq 4$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ Y^2 + dXY + eX^2 + fY + gX + h & = 0 \\ Y^3 + X^4 + iX^3 + jY^2 + kXY + lX^2 + mY + nX + o & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle X^2, Y^2, X^4, X^5 \rangle = \langle X^2, Y^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, Y, XY\}.$$

  Assim, o número máximo de soluções é 4, e $D_{\{[X^2],[Y^2],[Y^3+X^4]\}} \leq 4$.

- $D_{\{[X^2],[X^3],[Y^3+X^4]\}} \leq 6$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ X^3 + dY^2 + eXY + fX^2 + gY + hX + i & = 0 \\ Y^3 + X^4 + jX^3 + kY^2 + lXY + mX^2 + nY + oX + p & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.4$, temos

$$I_{lead} = \langle X^2, X^3, Y^3, Y^4 \rangle = \langle X^2, Y^3 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, Y, Y^2, XY, XY^2\}.$$

Assim, o número máximo de soluções é 6, e $D_{\{[X^2],[X^3],[Y^3+X^4]\}} \leq 6$.

- $D_{\{[XY],[Y^2],[X^3]\}} \leq 4$.
  Considere o conjunto de equações

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ Y^2 + eXY + fX^2 + gY + hX + i & = 0 \\ X^3 + jY^2 + kXY + lX^2 + mY + nX + o & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle XY, Y^2, X^3, X^5 \rangle = \langle XY, Y^2, X^3 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2, Y\}.$$

  Assim, o número máximo de soluções é 4, e $D_{\{[XY],[Y^2],[X^3]\}} \leq 4$.

- $D_{\{[XY],[Y^2],[Y^3+X^4]\}} \leq 5$.
  Considere o conjunto de equações

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ Y^2 + eXY + fX^2 + gY + hX + i & = 0 \\ Y^3 + X^4 + jX^3 + kY^2 + lXY + mX^2 + nY + oX + p & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle XY, Y^2, X^4, X^5 \rangle = \langle XY, Y^2, X^4 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2, X^3, Y\}.$$

  Assim, o número máximo de soluções é 5, e $D_{\{[XY],[Y^2],[Y^3+X^4]\}} \leq 5$.

- $D_{\{[Y^2],[X^3],[Y^3+X^4]\}} \leq 6$.
  Considere o conjunto de equações

$$\begin{cases} Y^2 + aXY + bX^2 + cY + dX + e & = 0 \\ X^3 + fY^2 + gXY + hX^2 + iY + jX + k & = 0 \\ Y^3 + X^4 + lX^3 + mY^2 + nXY + oX^2 + pY + qX + r & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y^2, X^3, X^4, X^5 \rangle = \langle Y^2, X^3 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2, Y, XY, X^2Y\}.$$

  Assim, o número máximo de soluções é 6, e $D_{\{[Y^2],[X^3],[Y^3+X^4]\}} \leq 6$, portanto, $D_3 \leq 6$.

Considere D_4.

- $D_{\{[1],*,*,*\}} = 0$, $D_{\{[X],*,*,*\}} \leq 4$ segue como anteriormente.
- $D_{\{[Y],[X^2],[XY],[Y^2]\}} \leq 2$.
  Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ X^2 + cY + dX + e & = 0 \\ XY + fX^2 + gY + hX + i & = 0 \\ Y^2 + jXY + kX^2 + lY + mX + n & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y, X^2, XY, Y^2, X^5 \rangle = \langle Y, X^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X\}.$$

  Assim, o número máximo de soluções é 2, e $D_{\{[Y],[X^2],[XY],[Y^2]\}} \leq 2$.
- $D_{\{[Y],[X^2],[XY],[X^3]\}} \leq 2$.
  Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ X^2 + cY + dX + e & = 0 \\ XY + fX^2 + gY + hX + i & = 0 \\ X^3 + jY^2 + kXY + lX^2 + mY + nX + o & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y, X^2, XY, X^3, X^5 \rangle = \langle Y, X^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X\}.$$

  Assim, o número máximo de soluções é 2, e $D_{\{[Y],[X^2],[XY],[X^3]\}} \leq 2$.
- $D_{\{[Y],[X^2],[XY],[Y^3+X^4]\}} \leq 2$.
  Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ X^2 + cY + dX + e & = 0 \\ XY + fX^2 + gY + hX + i & = 0 \\ Y^3 + X^4 + jX^3 + kY^2 + lXY + mX^2 + nY + oX + p & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y, X^2, XY, X^4, X^5 \rangle = \langle Y, X^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X\}.$$

  Assim, o número máximo de soluções é 2, e $D_{\{[Y],[X^2],[XY],[X^3]\}} \leq 2$.
- $D_{\{[Y],[XY],[Y^2],[X^3]\}} \leq 3$.
  Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ XY + cX^2 + dY + eX + f & = 0 \\ Y^2 + gXY + hX^2 + iY + jX + k & = 0 \\ X^3 + lY^2 + mXY + nX^2 + oY + pX + q & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q \in \mathbb{F}_{16}$.
Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y, XY, Y^2, X^3, X^5 \rangle = \langle Y, X^3 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2\}.$$

Assim, o número máximo de soluções é 3, e $D_{\{[Y],[XY],[Y^2],[X^3]\}} \leq 3$.

- $D_{\{[Y],[XY],[Y^2],[Y^3+X^4]\}} \leq 4$.
Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ XY + cX^2 + dY + eX + f & = 0 \\ Y^2 + gXY + hX^2 + iY + jX + k & = 0 \\ Y^3 + X^4 + lX^3 + mY^2 + nXY + oX^2 + pY + qX + r & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r \in \mathbb{F}_{16}$.
Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y, XY, Y^2, X^4, X^5 \rangle = \langle Y, X^4 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2, X^3\}.$$

Assim, o número máximo de soluções é 4, e $D_{\{[Y],[XY],[Y^2],[Y^3+X^4]\}} \leq 4$.

- $D_{\{[Y],[Y^2],[X^3],[Y^3+X^4]\}} \leq 3$.
Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ Y^2 + cXY + dX^2 + eY + fX + g & = 0 \\ X^3 + hY^2 + iXY + jX^2 + kY + lX + m & = 0 \\ Y^3 + X^4 + nX^3 + oY^2 + pXY + qX^2 + rY + sX + t & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, t \in \mathbb{F}_{16}$.
Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y, Y^2, X^3, X^4, X^5 \rangle = \langle Y, X^3 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2\}.$$

Assim, o número máximo de soluções é 3, e $D_{\{[Y],[Y^2],[X^3],[Y^3+X^4]\}} \leq 3$.

- $D_{\{[Y],[X^2],[Y^2],[X^3]\}} \leq 2$.
Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ X^2 + cY + dX + e & = 0 \\ Y^2 + fXY + gX^2 + hY + iX + j & = 0 \\ X^3 + kY^2 + lXY + mX^2 + nY + oX + p & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p \in \mathbb{F}_{16}$.
Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y, X^2, Y^2, X^3, X^5 \rangle = \langle Y, X^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X\}.$$

Assim, o número máximo de soluções é 2, e $D_{\{[Y],[X^2],[Y^2],[X^3]\}} \leq 2$.

- $D_{\{[Y],[X^2],[X^3],[Y^3+X^4]\}} \leq 2$.
Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ X^2 + cY + dX + e & = 0 \\ X^3 + fY^2 + gXY + hX^2 + iY + jX + k & = 0 \\ Y^3 + X^4 + lX^3 + mY^2 + nXY + oX^2 + pY + qX + r & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r \in \mathbb{F}_{16}$.
Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y, X^2, X^3, X^4, X^5 \rangle = \langle Y, X^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X\}.$$

Assim, o número máximo de soluções é 2, e $D_{\{[Y],[X^2],[X^3],[Y^3+X^4]\}} \leq 2$.

- $D_{\{[Y],[X^2],[Y^2],[Y^3+X^4]\}} \leq 2$.
Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ X^2 + cY + dX + e & = 0 \\ Y^2 + fXY + gX^2 + hY + iX + j & = 0 \\ Y^3 + X^4 + kX^3 + lY^2 + mXY + nX^2 + oY + pX + q & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q \in \mathbb{F}_{16}$.
Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y, X^2, Y^2, X^4, X^5 \rangle = \langle Y, X^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X\}.$$

Assim, o número máximo de soluções é 2, e $D_{\{[Y],[X^2],[Y^2],[Y^3+X^4]\}} \leq 2$.

- $D_{\{[Y],[XY],[X^3],[Y^3+X^4]\}} \leq 3$.
Considere o conjunto de equações

$$\begin{cases} Y + aX + b & = 0 \\ XY + cX^2 + dY + eX + f & = 0 \\ X^3 + gY^2 + hXY + iX^2 + jY + kX + l & = 0 \\ Y^3 + X^4 + mX^3 + nY^2 + oXY + pX^2 + qY + rX + s & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s \in \mathbb{F}_{16}$.
Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle Y, XY, X^3, X^4, X^5 \rangle = \langle Y, X^3 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2\}.$$

Assim, o número máximo de soluções é 3, e $D_{\{[Y],[XY],[X^3],[Y^3+X^4]\}} \leq 3$.

- $D_{\{[X^2],[XY],[Y^2],[X^3]\}} \leq 3$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ XY + dX^2 + eY + fX + g & = 0 \\ Y^2 + hXY + iX^2 + jY + kX + l & = 0 \\ X^3 + mY^2 + nXY + oX^2 + pY + qX + r & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle X^2, XY, Y^2, X^3, X^5 \rangle = \langle X^2, XY, Y^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, Y\}.$$

  Assim, o número máximo de soluções é 3, e $D_{\{[X^2],[XY],[Y^2],[X^3]\}} \leq 3$.

- $D_{\{[X^2],[XY],[Y^2],[Y^3+X^4]\}} \leq 3$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ XY + dX^2 + eY + fX + g & = 0 \\ Y^2 + hXY + iX^2 + jY + kX + l & = 0 \\ Y^3 + X^4 + mX^3 + nY^2 + oXY + pX^2 + qY + rX + s & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle X^2, XY, Y^2, X^4, X^5 \rangle = \langle X^2, XY, Y^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, Y\}.$$

  Assim, o número máximo de soluções é 3, e $D_{\{[X^2],[XY],[Y^2],[Y^3+X^4]\}} \leq 3$.

- $D_{\{[X^2],[XY],[X^3],[Y^3+X^4]\}} \leq 4$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ XY + dX^2 + eY + fX + g & = 0 \\ X^3 + hY^2 + iXY + jX^2 + kY + lX + m & = 0 \\ Y^3 + X^4 + nX^3 + oY^2 + pXY + qX^2 + rY + sX + t & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.4$, temos

$$I_{lead} = \langle X^2, XY, X^3, Y^3, Y^4 \rangle = \langle X^2, XY, Y^3 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, Y, Y^2\}.$$

  Assim, o número máximo de soluções é 4, e $D_{\{[X^2],[XY],[X^3],[Y^3+X^4]\}} \leq 4$.

- $D_{\{[X^2],[Y^2],[X^3],[Y^3+X^4]\}} \leq 4$.
  Considere o conjunto de equações

$$\begin{cases} X^2 + aY + bX + c & = 0 \\ Y^2 + dXY + eX^2 + fY + gX + h & = 0 \\ X^3 + iY^2 + jXY + kX^2 + lY + mX + n & = 0 \\ Y^3 + X^4 + oX^3 + pY^2 + qXY + rX^2 + sY + tX + u & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u \in \mathbb{F}_{16}$.
Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle X^2, Y^2, X^3, X^4, X^5 \rangle = \langle X^2, Y^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, Y, XY\}.$$

Assim, o número máximo de soluções é 4, e $D_{\{[X^2],[Y^2],[X^3],[Y^3+X^4]\}} \leq 4$.

- $D_{\{[XY],[Y^2],[X^3],[Y^3+X^4]\}} \leq 4$.
  Considere o conjunto de equações

$$\begin{cases} XY + aX^2 + bY + cX + d & = 0 \\ Y^2 + eXY + fX^2 + gY + hX + i & = 0 \\ X^3 + jY^2 + kXY + lX^2 + mY + nX + o & = 0 \\ Y^3 + X^4 + pX^3 + qY^2 + rXY + sX^2 + tY + uX + v & = 0 \\ X^5 + Y^4 + Y & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v \in \mathbb{F}_{16}$.
  Fazendo $\omega(X) = 1$ e $\omega(Y) = 1.1$, temos

$$I_{lead} = \langle XY, Y^2, X^3, X^4, X^5 \rangle = \langle XY, Y^2, X^3 \rangle \text{ logo } \Delta(I_{lead}) = \{1, X, X^2, Y\}.$$

  Assim, o número máximo de soluções é 4, e $D_{\{[XY],[Y^2],[X^3],[Y^3+X^4]\}} \leq 4$, portanto, $D_4 \leq 4$.

Agora, tratemos as distâncias generalizadas do código.

- Como $D_{8-6+1+1} = D_4 \leq 4$ segue pelo Teorema 3.1.2 que $d_1 \geq 6$.
- Como $D_{8-8+2+1} = D_3 \leq 6$ segue pelo Teorema 3.1.2 que $d_2 \geq 8$.
- Como $D_{8-9+3+1} = D_3 \leq 7$ segue pelo Teorema 3.1.2 que $d_3 \geq 9$.
- Como $D_{8-(i+7)+i+1} = D_2 \leq k + 7$ segue pelo Teorema 3.1.2 que $d_i \geq i + 7$.
  Similarmente ao que foi feito anteriormente, pela Cota de Singleton Generalizada e pelo número de linhas de H, concluímos que $n - k = 8$, ou seja, $64 - k = 8$, logo $k = 56$.
  Assim, como $D_{8-(i+7)+i+1} = D_2 \leq 63$ segue pela Proposição 3.1.2, que $d_i \geq i + 7$.

C Códigos Sobre uma Curva no Espaço

Seja

$$V := V_{\mathbb{F}_4}(\langle X^3 + Y^2 + Y, Y^3 + Z^2 + Z \rangle).$$

Do estudo de curvas hermitianas vem que V tem 16 pontos da forma $(\alpha, \beta, \gamma) \in \mathbb{F}_4^3$, onde $\alpha \in \mathbb{F}_4$, $\beta \in \mathbb{F}_4$ e é tal que $\alpha^3 + \beta^2 + \beta = 0$ (existem dois β's para cada α dado) e $\gamma \in \mathbb{F}_4$ é tal que $\beta^3 + \gamma^2 + \gamma = 0$ (existem dois γ's para cada β dado).

Considere o código cuja matriz checagem de paridade é dada por

$$H := [\varphi(1), \varphi(X), \varphi(Y), \varphi(X^2), \varphi(Z), \varphi(XY), \varphi(XZ + YZ)]^T.$$

onde φ é definida como na Seção 3.2.

Afirmamos que a distância mínima desse código é 4.

Para ver isto, tomamos $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1) = \{\overline{0}, \overline{1}, \overline{X}, \overline{1 + X}\}$. Temos:

- $\overline{X^2} = \overline{1+X}$, já que, $\overline{0} = \overline{X^2+X+1} = \overline{X^2} + \overline{1+X}$, ou seja, $\overline{X^2} = -(\overline{1+X})$ mas, como em $\mathbb{F}_2$ temos $\overline{1} = \overline{-1}$, então $\overline{X^2} = \overline{1+X}$;
- $\overline{X^3} = \overline{X(X^2)} = \overline{X(1+X)} = \overline{X+X^2} = \overline{X+(1+X)} = \overline{2X+1}$ mas, como em $\mathbb{F}_2$ temos $\overline{2} = \overline{0}$, então $\overline{X^3} = 1$.

  e assim, sucessivamente.

Seja $\alpha = \overline{X}$. Então o conjunto de equações

$$\begin{cases} Y+X+1 & = 0 \\ X^2+X+1 & = 0 \\ XY+1 & = 0 \\ XZ+YZ+Z & = 0 \\ X^3+Y^2+Y & = 0 \\ Y^3+Z^2+Z & = 0 \end{cases}$$

têm as soluções $(\alpha, \alpha^2, \alpha)$, $(\alpha, \alpha^2, \alpha^2)$, $(\alpha^2, \alpha, \alpha)$ e $(\alpha^2, \alpha, \alpha^2)$. Logo, $D_4 = D_{7-4+1} \geq 4$ e, pelo Teorema 3.1.2, temos que $d_1 \leq 4$.

Por outro lado, temos que $D_5 \leq 2$, pois:

- $D_{\{[1],*,*,*,*\}} = 0$ é óbvio.
- $D_{\{[X],[Y],[X^2],[Z],[XY]\}} \leq 1$.
  Considere o conjunto de equações

$$\begin{cases} X+a & = 0 \\ Y+bX+c & = 0 \\ X^2+dY+eX+f & = 0 \\ Z+gX^2+hY+iX+j & = 0 \\ XY+kZ+lX^2+mY+nX+o & = 0 \\ X^3+Y^2+Y & = 0 \\ Y^3+Z^2+Z & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o \in \mathbb{F}_4$.
  Fazendo $\omega(X) = 1$, $\omega(Y) = 1.2$ e $\omega(Z) = 2.1$, temos

$$I_{lead} = \langle X, Y, X^2, Z, XY, X^3, Z^2 \rangle = \langle X, Y, Z \rangle \text{ logo } \Delta(I_{lead}) = \{1\}.$$

  Assim, o número máximo de soluções é 1, e $D_{\{[X],[Y],[X^2],[Z],[XY]\}} \leq 1$.
- $D_{\{[X],[Y],[X^2],[Z],[XZ+YZ]\}} \leq 1$.
  Considere o conjunto de equações

$$\begin{cases} X+a & = 0 \\ Y+bX+c & = 0 \\ X^2+dY+eX+f & = 0 \\ Z+gX^2+hY+iX+j & = 0 \\ XZ+YZ+kXY+lZ+mX^2+nY+oX+p & = 0 \\ X^3+Y^2+Y & = 0 \\ Y^3+Z^2+Z & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p \in \mathbb{F}_4$.

Fazendo $\omega(X) = 1$, $\omega(Y) = 1.1$ e $\omega(Z) = 2.2$, temos

$$I_{lead} = \langle X, Y, X^2, Z, YZ, X^3, Z^2 \rangle = \langle X, Y, Z \rangle \text{ logo } \Delta(I_{lead}) = \{1\}.$$

Assim, o número máximo de soluções é 1, e $D_{\{[X],[Y],[X^2],[Z],[XZ+YZ]\}} \leq 1$.

- $D_{\{[X],[Y],[X^2],[XY],[XZ+YZ]\}} \leq 2$.
  Considere o conjunto de equações

$$\begin{cases} X + a & = 0 \\ Y + bX + c & = 0 \\ X^2 + dY + eX + f & = 0 \\ XY + gZ + hX^2 + iY + jX + k & = 0 \\ XZ + YZ + lXY + mZ + nX^2 + oY + pX + q & = 0 \\ X^3 + Y^2 + Y & = 0 \\ Y^3 + Z^2 + Z & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q \in \mathbb{F}_4$.
  Fazendo $\omega(X) = 1$, $\omega(Y) = 1.1$ e $\omega(Z) = 2$, temos

$$I_{lead} = \langle X, Y, X^2, XY, YZ, X^3, Z^2 \rangle = \langle X, Y, Z^2 \rangle \text{ logo } \Delta(I_{lead}) = \{1, Z\}.$$

  Assim, o número máximo de soluções é 2, e $D_{\{[X],[Y],[X^2],[XY],[XZ+YZ]\}} \leq 2$.

- $D_{\{[X],[Y],[Z],[XY],[XZ+YZ]\}} \leq 1$.
  Considere o conjunto de equações

$$\begin{cases} X + a & = 0 \\ Y + bX + c & = 0 \\ Z + dX^2 + eY + fX + g & = 0 \\ XY + hZ + iX^2 + jY + kX + l & = 0 \\ XZ + YZ + mXY + nZ + oX^2 + pY + qX + r & = 0 \\ X^3 + Y^2 + Y & = 0 \\ Y^3 + Z^2 + Z & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r \in \mathbb{F}_4$.
  Fazendo $\omega(X) = 1$, $\omega(Y) = 1.1$ e $\omega(Z) = 2.2$, temos

$$I_{lead} = \langle X, Y, Z, YZ, X^3, Z^2 \rangle = \langle X, Y, Z \rangle \text{ logo } \Delta(I_{lead}) = \{1\}.$$

  Assim, o número máximo de soluções é 1, e $D_{\{[X],[Y],[Z],[XY],[XZ+YZ]\}} \leq 1$.

- $D_{\{[X],[X^2],[Z],[XY],[XZ+YZ]\}} \leq 2$.
  Considere o conjunto de equações

$$\begin{cases} X + a & = 0 \\ X^2 + bY + cX + d & = 0 \\ Z + eX^2 + fY + gX + h & = 0 \\ XY + iZ + jX^2 + kY + lX + m & = 0 \\ XZ + YZ + nXY + oZ + pX^2 + qY + rX + s & = 0 \\ X^3 + Y^2 + Y & = 0 \\ Y^3 + Z^2 + Z & = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s \in \mathbb{F}_4$.

Fazendo $\omega(X) = 1$, $\omega(Y) = 1.6$ e $\omega(Z) = 2.2$, temos

$$I_{lead} = \langle X, X^2, Z, XY, YZ, Y^2, Y^3 \rangle = \langle X, Y^2, Z \rangle \text{ logo } \Delta(I_{lead}) = \{1, Y\}.$$

Assim, o número máximo de soluções é 2, e $D_{\{[X],[X^2],[Z],[XY],[XZ+YZ]\}} \leq 2$.

- $D_{\{[Y],[X^2],[Z],[XY],[XZ+YZ]\}} \leq 2$.
  Considere o conjunto de equações

$$\begin{cases} Y + aX + b = 0 \\ X^2 + cY + dX + e = 0 \\ Z + fX^2 + gY + hX + i = 0 \\ XY + jZ + kX^2 + lY + mX + n = 0 \\ XZ + YZ + oXY + pZ + qX^2 + rY + sX + t = 0 \\ X^3 + Y^2 + Y = 0 \\ Y^3 + Z^2 + Z = 0 \end{cases}$$

  onde $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t \in \mathbb{F}_4$.
  Fazendo $\omega(X) = 1$, $\omega(Y) = 1.2$ e $\omega(Z) = 2.1$, temos

$$I_{lead} = \langle Y, X^2, Z, XY, YZ, X^3, Z^2 \rangle = \langle X^2, Y, Z \rangle \text{ logo } \Delta(I_{lead}) = \{1, X\}.$$

  Assim, o número máximo de soluções é 2, e $D_{\{[Y],[X^2],[Z],[XY],[XZ+YZ]\}} \leq 2$.

Do que tratamos acima vem que $D_5 = D_{7-4+1+1} \leq 2$. E, novamente, pelo Teorema 3.1.2, temos $d_1 \geq 4$, concluindo assim que $d_1 = 4$.

D Códigos construídos a partir de Pegadas

Considere uma variedade $V = \{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q^m$. Seja $\{G_1, \ldots, G_s\} \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ uma base de Groebner para $J := I(V)$ com respeito a alguma ordem de monômios $>$ no conjunto de monômios de $\mathbb{F}_q[X_1, \ldots, X_m]$. Suponha que $\sharp(\Delta(J)) = n$ e seja $\Delta(J) = \{F_1, \ldots, F_n\}$, onde $F_{i+1} > F_i$, $i = 1, \ldots, n-1$, a pegada de $J := I(V)$.

Dado $r \in \{1, \ldots, n\}$ considere o código $\mathbb{F}_q$-linear $C_r^\perp$ (respectivamente, C_r) com matriz checagem de paridade (respectivamente, matriz geradora)

$$H := [\mathbf{h}_1, \ldots, \mathbf{h}_r]^T \tag{3.2}$$

onde $\mathbf{h}_i = (F_i(P_1), \ldots, F_i(P_n))$ para todo $i = 1, \ldots, r$.

Sabemos pela Proposição 1.8.4 que quando $J \subseteq K[X]$ é um ideal e $\Delta(J)$ é a pegada, então $\{M + J | M \in \Delta(J)\}$ constitui uma base para $K[X]/J$ como um espaço vetorial sobre K. No presente caso, então, $\{\mathbf{h}_1, \ldots, \mathbf{h}_n\}$ constitui uma base para $\mathbb{F}_q^n$.

Assim, em particular, $\mathbf{h}_1, \ldots, \mathbf{h}_r$ são linearmente independentes, o que leva a dimensão de $C_r^\perp$ igual a $k := n - r$ e a dimensão de C_r igual a r.

A seguir, vamos determinar as cotas inferiores para os pesos generalizados de Hamming de $C_r^\perp$.

Primeiramente, vamos investigar D_1.

Para um F_i fixo o número de soluções P para

$$F_i(P) + \sum_{j=1}^{i-1} a_j F_j(P) = G_1(P) = \ldots = G_s(P) = 0$$

é limitado pelo tamanho de $\Delta(I)$, onde $I := \left\langle F_i + \sum_{j=1}^{i-1} a_j F_j, G_1, \ldots, G_s \right\rangle$.
Entretanto,

$$\Delta(I) \subseteq \Delta(I_{lead})$$

onde

$$I_{lead} := \left\langle ML\left(F_i + \sum_{j=1}^{i-1} a_j F_j\right), ML(G_1), \ldots, ML(G_s) \right\rangle = \langle F_i, ML(G_1), \ldots, ML(G_s) \rangle$$

pois, $F_{i+1} > F_i$, $i = 1, \ldots, n-1$. E assim, temos $\Delta(I_{lead}) \subset \Delta(J)$, mais ainda,

$$\Delta(I_{lead}) = \{X^\alpha \in \Delta(J) |\ F_i \text{ não divide } X^\alpha\}.$$

Agora, defina:

$$\Lambda_{\{i\}} := \Delta(J) \backslash \Delta(I_{lead}) = \{X^\alpha \in \Delta(J) |\ F_i \text{ divide } X^\alpha\}$$

e

$$S_1 := min\{\sharp(\Lambda_{\{i\}}) |\ i = 1, \ldots, r\}.$$

Afirmamos que D_1 é limitado por $D_1 \leq n - S_1$.
De fato, lembrando que $\sharp(\Delta(J)) = n$, temos que $S_1 = min\{\sharp(\Lambda_{\{i\}}) |\ i = 1, \ldots, r\}$ e logo

$$n - S_1 = max\{\sharp(\Delta(I_{lead})) |\ i = 1, \ldots, r\}.$$

E utilizando o fato que

$$\begin{aligned} D_1 \leq & max\left\{\sharp\left(\left\{P | F_i(P) + \sum_{j=1}^{i-1} a_j F_j(P) = G_1(P) = \ldots = G_s(P) = 0, i = 1 \ldots, n\right\}\right)\right\} \\ \leq & max\left\{\sharp\left(\Delta(I_{lead})\right) \mid i = 1, \ldots, r\right\} \end{aligned}$$

temos, $D_1 \leq n - S_1$.
Agora, vamos estimar D_j para j arbitrário, $1 \leq j \leq r$. Temos que:

$$I_{lead} = \langle F_{i_1}, F_{i_2}, \ldots, F_{i_j}, ML(G_1), \ldots, ML(G_s) \rangle$$

e

$$\Delta(I_{lead}) = \{X^\alpha \in \Delta(I) |\ F_{i_t} \text{ não divide } X^\alpha,\ \forall t = 1, \ldots, j\}.$$

E generalizando a terminologia definida acima, temos:

$$\begin{aligned}\Lambda_{\{i_1,i_2,\ldots,i_j\}} :=& \{X^\alpha \in \Delta(I)|\ F_{i_t} \text{ divide } X^\alpha \text{ para algum } t \in \{1,\ldots,j\}\} \\ =& \bigcup_{l=1}^{j} \Lambda_{\{i_l\}}\end{aligned}$$

$$S_j := min\left\{\sharp(\Lambda_{\{i_1,i_2,\ldots,i_j\}})|\ 1 \leq i_1 < i_2 < \ldots < i_j \leq r\right\}.$$

Logo, D_j é limitado por $D_j \leq n - S_j$.

Teorema 3.4.2 *Considere o código $C_r^\perp$ sobre $\mathbb{F}_q$ com matriz checagem de paridade dada por (3.2). Seja h, i inteiros com $1 \leq h \leq n-r$, $1 \leq i \leq r$. Se $r+h-1-i \geq n-S_i$, então $d_h \geq n - S_i + 2$.*

Demonstração: Dados h, i inteiros com $1 \leq h \leq n-r$, $1 \leq i \leq r$, defina $d^* := r+h+1-i$. Assuma $r+h-1-i \geq n-S_i$, isto é, assuma $d^* \geq n - S_i + 2$. Temos:

$$D_{r-d^*+h+1} = D_i \leq n - S_i \leq d^* - 2$$

que pelo Teorema 3.1.2 implica $d_h \geq d^*$. Mas $d^* \geq n - S_i + 2$ e o teorema segue.

□

Referências Bibliográficas

[1] COX, D.; LITTLE, J.; O'SHEA, D. *Ideals, varieties, and algorithms*. Springer, segunda edição, 1996.

[2] GEIL, O. *Footprints or generalized Bezout's theorem*, IEEE Transactions on information theory, vol.46, nº2, pp. 635-641, 2000.

[3] LEMES, L. C. *Códigos de Goppa e distâncias generalizadas de Hamming*, Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG, 2009.

[4] STICHTENOTH, H. *Algebraic function fields and Codes*. Springer-Verlag, 1993.

[5] TANG, L. *Consecutive Weierstrass gaps and weight hierarchy of geometric Goppa codes*, Algebra Colloq., vol.3, nº1, pp. 1-10, 1996.

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