

AUGUSTO DUARTE PENA

Pesos de Hamming generalizados e códigos parametrizados



UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2018

AUGUSTO DUARTE PENA

Pesos de Hamming generalizados e códigos parametrizados

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.

Orientador: Prof. Dr. Cícero Fernandes de Carvalho.

UBERLÂNDIA - MG
2018

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

P397p Pena, Augusto Duarte, 1992-
2018 Pesos de Hamming generalizados e códigos parametrizados /
Augusto Duarte Pena. - 2018.
51 f. : il.

Orientador: Cícero Fernandes de Carvalho.
Dissertação (mestrado) - Universidade Federal de Uberlândia,
Programa de Pós-Graduação em Matemática.
Disponível em: <http://dx.doi.org/10.14393/ufu.di.2018.242>
Inclui bibliografia.

1. Matemática - Teses. 2. Bases de Gröbner - Teses. 3. Geometria
algébrica - Teses. 4. Códigos de controle de erros (Teoria da informação)
- Teses. I. Carvalho, Cícero Fernandes de. II. Universidade Federal de
Uberlândia. Programa de Pós-Graduação em Matemática. III. Título.

CDU: 51

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

ALUNO: Augusto Duarte Pena.

NÚMERO DE MATRÍCULA: 116MAT12002.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Pesos de Hamming generalizados e códigos parametrizados.

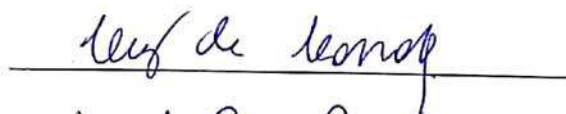
ORIENTADOR: Prof. Dr. Cícero Fernandes de Carvalho.

Esta dissertação foi APROVADA em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 20 de Fevereiro de 2018, às 15h10min, pela seguinte Banca Examinadora:

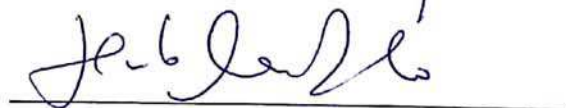
NOME

ASSINATURA

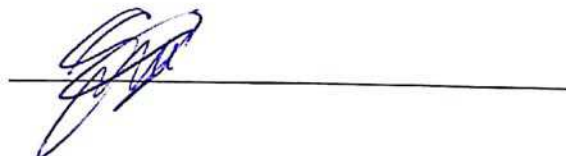
Prof. Dr. Cícero Fernandes de Carvalho
UFU - Universidade Federal de Uberlândia



Prof. Dr. Herivelto Martins Borges Filho
USP - Universidade de São Paulo



Prof. Dr. Guilherme Chaud Tizziotti
UFU - Universidade Federal de Uberlândia



Uberlândia-MG, 20 de Fevereiro de 2018.

Dedicatória

Dedico este trabalho à minha mãe.

Agradecimentos

Agradeço primeiramente aos meus pais Anilza e Maurício pelo dom da vida.

Agradeço ao meu orientador Cícero Fernandes de Carvalho por todo o apoio dado e por ter sido muito mais que apenas um orientador durante estes dois anos e também durante meus tempos de graduação. Sou grato por todos os ensinamentos e lições que pude aprender com ele.

Agradeço à minha família por todo o apoio, paciência e carinho comigo.

Agradeço aos vários amigos que fiz em todos esses anos de UFU. Em especial, agradeço aos meus amigos Alexandre, Paulo Victor e Ueslei. Agradeço também aos amigos da minha turma: Aluizio, Zé Henrique, Júlian, Javier e Milton Gabriel, que tornaram as aulas mais divertidas e os estudos mais proveitosos.

Agradeço aos excelentes professores que tive na UFU que certamente contribuíram para a minha formação. Em especial agradeço aos professores Geraldo Botelho, Victor Gonzalo, Mário Henrique, Alonso Sepúlveda, Guilherme Tizziotti, Márcio Dantas e Daniel Cariello.

Agradeço à FAPEMIG pelo auxílio financeiro durante todo o mestrado.

PENA, A. D. *Pesos de Hamming generalizados e códigos parametrizados*. 2018. (51 pág) p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Este trabalho tem como objetivo estudar os pesos de Hamming generalizados de códigos parametrizados por conjuntos tóricos. Mostramos que em alguns casos particulares encontramos cotas mais refinadas para os pesos generalizados. Definimos o que são conjuntos mergulhados e apresentamos a relação de seus pesos generalizados com os conjuntos nos quais estão mergulhados. Utilizamos aqui ferramentas da Teoria de Códigos, Bases de Gröbner e Geometria Algébrica. O trabalho dá uma breve introdução dos conceitos apresentados e utiliza os resultados dos capítulos iniciais para fundamentar os resultados do último capítulo.

Palavras-chave: Códigos parametrizados, Pesos de Hamming generalizados, Conjuntos mergulhados.

PENA, A. D. *Generalized Hamming weights and parameterized codes* 2018. (51 pages) p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

This goal of this work is to study the generalized Hamming weights of parameterized codes associated to toric sets. We show that in some particular cases we find sharper bounds for the generalized weights. We define embedded sets and present their relation to the sets they are embedded to. The tools here used come from coding theory, Gröbner basis and algebraic geometry. This work gives a brief introduction to the presented concepts and uses the results from the initial chapters to reach its goal.

Keywords: Parameterized codes, Generalized Hamming Weights, Embedded sets.

Sumário

Resumo	vii
Abstract	viii
Introdução	1
1 Introdução	2
1.1 Códigos e a Métrica de Hamming	2
1.2 Códigos Lineares	4
1.3 Cotas superiores	6
1.4 Pesos de Hamming generalizados e códigos MDS	6
2 Preliminares	9
2.1 Polinômios e Bases de Gröbner	9
2.2 Variedades afins e a pegada de um ideal	13
2.3 Geometria Projetiva	14
2.3.1 Espaço Projetivo	14
2.3.2 Variedades Projetivas	16
2.4 Grafos	22
3 Códigos produto	24
3.1 O produto tensorial	24
3.2 O produto direto e a imersão de Segre	26
4 Códigos parametrizados	31
4.1 Cotas para códigos parametrizados	33
4.1.1 O grafo bipartido completo $\mathcal{K}_{m,n}$	35
4.2 Uma cota geral	38
4.3 Conjuntos mergulhados	40

Introdução

Este é um trabalho sobre teoria de códigos, e em especial, sobre a teoria de códigos corretores de erros. Durante a transmissão de informações, o canal utilizado pode apresentar ruídos e comprometer a transmissão, gerando erros nas informações que desejamos enviar. De modo a sanar este problema agregamos, de maneira adequada, uma redundância à informação original de modo que, após a transmissão o receptor seja capaz de detectar se houveram erros, e em caso afirmativo, corrigi-los com o auxílio da redundância adicionada.

O poder de correção de um código corretor de erros está diretamente ligado à sua distância mínima. Um código tem três parâmetros fundamentais: comprimento, dimensão e distância mínima. O conceito de distância mínima pode ser generalizado, obtendo-se então o que chamamos de pesos de Hamming generalizados. Neste trabalho estudamos estes pesos para códigos que são parametrizados por conjuntos tóricos. Veremos que tal estudo é bem interessante, e em alguns casos específicos, conseguimos determinar cotas que melhor estimam os pesos de Hamming generalizados do que resultados clássicos na literatura.

Este trabalho está dividido em quatro partes. Na primeira parte introduzimos as definições e conceitos iniciais e damos uma motivação sobre a importância de códigos com distâncias mínimas altas em relação ao seu comprimento. Veremos que os parâmetros de um código devem satisfazer algumas relações, definimos o conceito de código MDS e em seguida exibimos cotas correspondentes aos pesos de Hamming generalizados.

Na segunda parte fazemos um tratado de polinômios em várias variáveis e introduzimos conceitos tais como Bases de Gröbner e o Algoritmo de Buchberger. Vemos também a definição de variedades afins e pegada de um ideal. Depois apresentamos o conceito de espaço projetivo e trabalhamos com polinômios neste espaço, em especial, lidando com polinômios homogêneos e por fim, fazemos uma breve introdução de grafos.

Na terceira parte apresentamos o produto tensorial entre espaços vetoriais, sua construção e motivamos a construção do código produto. Vemos algumas propriedades e parâmetros do código produto e através da imersão de Segre podemos estabelecer uma conexão entre o código produto e o produto tensorial de espaços vetoriais.

Na quarta parte introduzimos os conceitos de códigos parametrizados por conjuntos tóricos e seus parâmetros. Veremos alguns códigos parametrizados específicos e cotas para seus pesos de Hamming generalizados e também algumas cotas para códigos parametrizados por monômios de mesmo grau. Por fim definiremos o que são conjuntos tóricos mergulhados, afim de estudarmos como cotas para os pesos de Hamming generalizados de conjuntos tóricos se relacionam com as cotas de conjuntos tóricos mergulhados.

Augusto Duarte Pena
Uberlândia-MG, 20 de Fevereiro de 2018.

Capítulo 1

Introdução

Inicialmente usaremos este capítulo para introduzirmos os objetos centrais deste trabalho. Veremos o que são códigos, a métrica de Hamming e uma interpretação geométrica do que significa corrigir um erro em um código. Além disso veremos um tipo especial de código, chamado código linear e algumas de suas propriedades.

1.1 Códigos e a Métrica de Hamming

Começaremos tomando um conjunto finito A , cujo número de elementos é denotado por $|A|$ e simbolizado por q . Um **código corretor de erros** é um subconjunto próprio (isto é, não é vazio e estritamente diferente) qualquer de A^n , para algum número natural n .

Observação 1.1.1. Quando não houver ambiguidade escreveremos os elementos (a_1, \dots, a_n) de A^n como $a_1 \dots a_n$.

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

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

Vemos que da maneira como foi definida, a distância de Hamming mede o número de coordenadas que os elementos u e v diferem.

Exemplo 1.1.2. Tomando $A = \{0, 1\}$ e $n = 3$, temos

$$d(001, 111) = 2, \quad d(000, 111) = 3.$$

O próximo resultado mostra que a distância de Hamming satisfaz as condições necessárias para ser chamada de métrica, sendo assim é usual chamá-la de **métrica de Hamming**.

Proposição 1.1.3. [8, Proposição 1.2.1] Dados $u, v, w \in A^n$, as seguintes propriedades se verificam:

1. $d(u, v) \geq 0$ e vale a igualdade se, e somente se $u = v$;
2. $d(u, v) = d(v, u)$;
3. $d(u, v) \leq d(u, w) + d(w, v)$.

Dado um elemento $a \in A^n$ e um número real $r \geq 0$, definimos o **disco** e a **esfera** de centro em a e raio r como sendo, respectivamente, os conjuntos

$$D(a, r) = \{u \in A^n : d(u, a) \leq r\}, \quad S(a, r) = \{u \in A^n : d(u, a) = r\}.$$

Os conjuntos acima definidos são finitos e nos ajudarão a dar uma interpretação geométrica da situação.

Lema 1.1.4. [8, Lema 1.2.1] Para todo $a \in A^n$ e todos os números naturais $r, i > 0$, temos que

$$|D(a, r)| = \sum_{i=0}^r \binom{n}{i} (q-1)^i \text{ e } |S(a, i)| = \binom{n}{i} (q-1)^i.$$

Observemos que a cardinalidade de $D(a, r)$ depende de n, q e r . Dado um código C , definiremos a **distância mínima** de C como o número

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

Como códigos são conjuntos finitos, em teoria podemos facilmente calcular a distância mínima de qualquer código. Caso não haja nenhum método desenvolvido, este cálculo se mostra trabalhoso pois é necessário calcular $\binom{M}{2}$ distâncias, onde M aqui representa o número de elementos do código, e isto tem um custo computacional elevado.

Dado um código C com distância mínima d , definimos

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

onde $[t]$ representa a parte inteira do número real t . O próximo resultado nos mostra a importância da variável κ :

Lema 1.1.5. [8, Lema 1.2.2] Seja C um código com distância mínima d . Se c e c' são elementos distintos de C , então

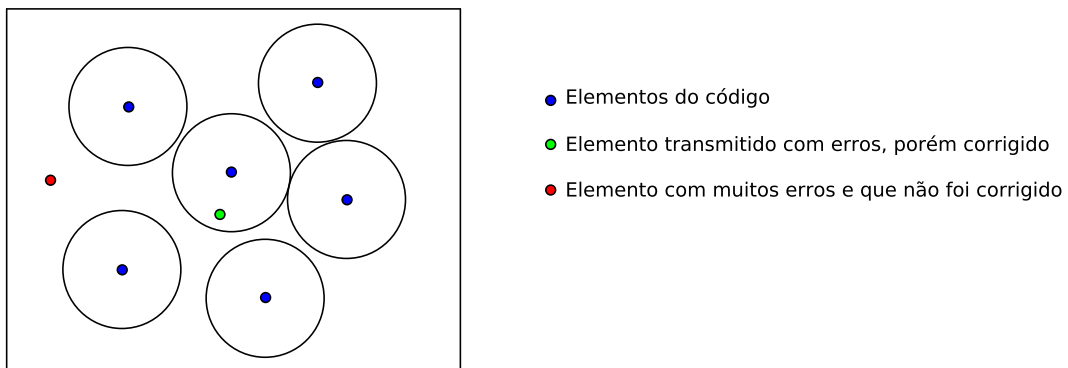
$$D(c, \kappa) \cap D(c', \kappa) = \emptyset.$$

O próximo resultado nos mostra a importância da distância mínima do código.

Teorema 1.1.6. [8, Teorema 1.2.1] Seja C um código com distância mínima d . Então C pode corrigir até κ erros e detectar até $d-1$ erros.

Em virtude deste teorema, quanto maior for sua distância mínima, maior será sua capacidade de correção e detecção de erros. Sendo assim, é importante podermos calcular d ou ao menos determinar cotas inferiores ou superiores para ele.

Com os resultados acima podemos dar a seguinte interpretação geométrica de códigos corretores de erros:



Um código C sobre um conjunto finito A possui três parâmetros fundamentais n, M e d que são, respectivamente, seu comprimento, seu número de elementos e sua distância mínima. São interessantes códigos cujo número de elementos e distância mínima são grandes relativamente ao comprimento. Na próxima seção veremos que com uma estrutura algébrica adicional, conseguiremos alguns resultados relacionados aos parâmetros de um código.

1.2 Códigos Lineares

Ao definirmos um código, bastava que o conjunto C fosse um subconjunto próprio de A^n . Agora, tomaremos A como um corpo finito de q elementos, a fim de acrescentar ao código uma estrutura de espaço vetorial, o que nos permitirá trabalhar com combinações lineares de elementos do código.

Seja \mathbb{F}_q um corpo finito com q elementos, temos que para cada número natural n , o conjunto \mathbb{F}_q^n é um \mathbb{F}_q -espaço vetorial de dimensão n . Um código $C \subset \mathbb{F}_q^n$ será chamado de **código linear** se for um subespaço vetorial de \mathbb{F}_q^n .

Todo código linear é por definição um espaço vetorial de dimensão finita. Seja k a dimensão do código C e seja v_1, \dots, v_k uma de suas bases. Todo elemento de C é unicamente escrito na forma $\lambda_1 v_1 + \dots + \lambda_k v_k$, onde $\lambda_i, i = 1, \dots, k$ são elementos de \mathbb{F}_q e assim segue que $M = |C| = q^k$. Chamaremos de **parâmetros do código linear** C a terna de inteiros (n, k, d) , onde n é o comprimento de C , k é a dimensão de C como espaço vetorial e d é a distância mínima de C .

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

$$\omega(x) = |\{i \in \{1, \dots, n\} : x_i \neq 0\}| = d(x, 0),$$

onde d é a métrica de Hamming. Definimos também o **peso de um código linear** C como sendo o número inteiro

$$\omega(C) = \min\{\omega(x) : x \in C - \{0\}\}.$$

Da estrutura de espaço vetorial do código, temos a seguinte proposição:

Proposição 1.2.1. [8, Proposição 5.1.1] *Seja $C \subset \mathbb{F}_q^n$ um código linear com distância mínima d . Então vale que:*

1. Para todos $x, y \in \mathbb{F}_q^n$, $d(x, y) = \omega(x - y)$;
2. $d = \omega(C)$.

Aqui é possível ver uma vantagem da estrutura de espaço vetorial: a distância mínima é exatamente o peso do código, que é obtido através do cálculo de $q^k - 1$ distâncias.

Como códigos lineares são espaços vetoriais, podemos pensar em duas maneiras elementares de se gerar espaços vetoriais: considerando o núcleo ou imagem de transformações lineares. Durante todo o nosso trabalho, lidaremos apenas com códigos vistos como imagem de transformações lineares. Para isto, seja C um código linear e escolha v_1, \dots, v_k como uma base de C e considere a aplicação linear

$$\begin{aligned} T : \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ x = (x_1, \dots, x_k) &\longmapsto x_1 v_1 + \dots + x_k v_k \end{aligned} \tag{1.1}$$

Segue que T é uma transformação linear injetora tal que sua imagem é C , isto é, $T(\mathbb{F}_q^k) = C$. Seja $\mathcal{B} = \{v_1, \dots, v_k\}$ uma base ordenada de C e considere a matriz G , cujas linhas são os vetores $v_i = (v_{i1}, \dots, v_{in}), i = 1, \dots, k$, isto é

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}.$$

A matriz G é chamada de **matriz geradora** de C associada à base \mathcal{B} . Notemos que a matriz G não é unicamente determinada por C , pois depende da escolha da base ordenada.

Observamos que de (1.1), o código linear C pode ser escrito como combinação linear (com coeficientes em \mathbb{F}_q) de todas as linhas da matriz geradora. Diremos que uma matriz geradora G de um código C está na **forma padrão** se tivermos $G = (\text{Id}_k | A)$, onde Id_k é a matriz identidade de ordem k e A , uma matriz $k \times (n - k)$.

Dados $u = (u_1, \dots, u_n)$ e $v = (v_1, \dots, v_n)$ elementos de \mathbb{F}_q^n , definimos o **produto interno** de u e v por

$$\langle u, v \rangle = u_1 v_1 + \dots + u_n v_n.$$

Esta operação satisfaz as propriedades usuais de produto interno, isto é,

$$\langle u, v \rangle = \langle v, u \rangle \text{ e } \langle u + \lambda w, v \rangle = \langle u, v \rangle + \lambda \langle w, v \rangle, \text{ para todo } \lambda \in \mathbb{F}_q.$$

Seja $C \subset \mathbb{F}_q^n$ um código linear. Definiremos o **código dual** de C como o conjunto

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

Proposição 1.2.2. [8, Lema 5.3.1] Se $C \subset \mathbb{F}_q^n$ é um código linear com matriz geradora G , então:

1. C^\perp é um subespaço vetorial de \mathbb{F}_q^n ;
2. $x \in C^\perp \iff Gx^t = 0$.

Seja $C \subset \mathbb{F}_q^n$ um código de dimensão k com matriz geradora $G = (\text{Id}_k | A)$. Definimos a **matriz de teste de paridade** de C como sendo $H = (-A^t | \text{Id}_k)$.

Proposição 1.2.3. [8, Proposição 5.3.2] Usando a notação acima, temos que:

1. $\dim C^\perp = n - k$;
2. H é uma matriz geradora de C^\perp .

Decidir se um elemento pertence ou não a um código, em geral, consiste em resolver um sistema linear. A matriz teste de paridade nos permite solucionar este problema de forma mais fácil.

Proposição 1.2.4. [8, Proposição 5.3.4] Seja C um código linear e suponhamos que H seja uma matriz geradora de C^\perp . Então

$$v \in C \iff Hv^t = 0.$$

Exemplo 1.2.5. Tomando $\mathbb{F}_q = \mathbb{F}_2$, o comprimento $n = 7$ e a dimensão $k = 4$, temos

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

e o código gerado por G é $C = \{0000000, 0001111, 0110011, 1010101, 1111111, 0111100, 1011010, 1110000, 1100110, 1001100, 0101010, 1101001, 1000011, 0100101, 0011001, 0010110\}$ e uma breve verificação mostra que a distância mínima é $d_C = 3$.

Agora, mantendo o mesmo corpo e o comprimento e tomando a dimensão $k = 3$, temos

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

e o código gerado por H é $C^\perp = \{0000000, 0001111, 0110011, 1010101, 0111100, 1011010, 1100110, 1101001\}$, e uma breve verificação mostra que a distância mínima é $d_{C^\perp} = 4$.

1.3 Cotas superiores

Como mencionamos anteriormente é importante que a dimensão e distância mínima de um código sejam grandes em relação ao comprimento. Veremos agora algumas relações que os parâmetros de um código devem satisfazer. Durante este trabalho estaremos interessados em três cotas: a de Singleton, a de Plotkin e a de Griesmer.

Teorema 1.3.1. *Seja C um código com comprimento n , com M elementos e distância mínima d , definido sobre um corpo finito com q elementos. Temos que*

$$M \leq q^{n-d+1}.$$

Demonstração. Seja $C \subset \mathbb{F}_q^n$ o código com os parâmetros dados e considere a projeção

$$\begin{aligned} \text{Pr} : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^{n-d+1} \\ (x_1, \dots, x_n) &\longmapsto (x_d, x_{d+1}, \dots, x_n) \end{aligned}$$

A restrição de Pr a C é injetora, pois se $\text{Pr}(x) = \text{Pr}(y)$ para $x, y \in C$, então $d(x, y) \leq d - 1$, e pela definição de distância isto pode acontecer apenas se $d(x, y) = 0$, e assim temos que $x = y$. Portanto, temos que $\text{Pr}(C)$ é um subconjunto de \mathbb{F}_q^{n-d+1} com M elementos, daí segue que $M \leq q^{n-d+1}$. □

Corolário 1.3.2 (Cota de Singleton). *Os parâmetros (n, k, d) de um código linear satisfazem à desigualdade*

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

Demonstração. Basta observar que em um código linear, $M = q^k$, assim

$$q^k \leq q^{n-d+1} \Rightarrow d \leq n - k + 1.$$
□

Teorema 1.3.3. [11, Cota de Plotkin] *Os parâmetros (n, k, d) de um código linear com $n < 2d$ satisfazem às desigualdades*

1. $q^k \leq 2qn$, se $d = (1 - \frac{1}{q})n$;
2. $q^k \leq \frac{qd}{qd - (q - 1)n}$, se $d > (1 - \frac{1}{q})n$.

Teorema 1.3.4. [11, Cota de Griesmer] *Os parâmetros (n, k, d) de um código linear satisfazem à desigualdade*

$$\sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \leq n.$$

1.4 Pesos de Hamming generalizados e códigos MDS

Definiremos agora um dos conceitos centrais deste trabalho. Relembramos que em um código linear, o peso do código coincide com a distância mínima. O peso é definido como a menor das distâncias com zero dentre todos os elementos não nulos do código.

Seja \mathcal{B} um subconjunto de \mathbb{F}_q^n , definiremos o **suporte** deste conjunto como

$$\text{supp}(\mathcal{B}) = \{i : \text{existe } (w_1, \dots, w_n) \in \mathcal{B} \text{ tal que } w_i \neq 0\}.$$

O r -ésimo peso de Hamming generalizado de um código C é dado por

$$d_r(C) = \min\{|\text{supp}(\mathcal{D})| : \mathcal{D} \text{ é um subcódigo de } C \text{ e } \dim_{\mathbb{F}_q} \mathcal{D} = r\},$$

para $1 \leq r \leq k$, onde k é a dimensão do código C . A hierarquia de pesos do código C é o conjunto de inteiros $\{d_r(C) : 1 \leq r \leq k\}$. É fácil ver que tomando $r = 1$, o primeiro peso de Hamming generalizado é precisamente a distância mínima do código.

Teorema 1.4.1. *Seja C um código linear de comprimento n e dimensão k . Valem as desigualdades*

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

Demonstração. Seja $r \in \{2, \dots, k\}$, temos

$$\min\{|\text{supp}(\mathcal{D})| : \mathcal{D} \subseteq C \text{ e } \dim_{\mathbb{F}_q} \mathcal{D} = r - 1\} \leq \min\{|\text{supp}(\mathcal{D})| : \mathcal{D} \subseteq C \text{ e } \dim_{\mathbb{F}_q} \mathcal{D} = r\},$$

e logo $d_{r-1}(C) \leq d_r(C)$. Queremos mostrar que a desigualdade é estrita. Seja D um subcódigo de C tal que $|\text{supp}(D)| = d_r(C)$ e $\dim_{\mathbb{F}_q}(D) = r$. Seja $i \in \text{supp}(D)$ e $D_i := \{\mathbf{x} \in D : \mathbf{x}_i = 0\}$ e considere a aplicação

$$\begin{aligned} P : D &\longrightarrow \mathbb{F}_q \\ \mathbf{x} &\longmapsto \mathbf{x}_i. \end{aligned}$$

De $i \in \text{supp}(D)$ segue que a aplicação P é sobrejetora e seu núcleo é exatamente o conjunto D_i . Assim $\dim_{\mathbb{F}_q}(D_i) = r - 1$ e $d_{r-1}(C) \leq |\text{supp}(D_i)| \leq |\text{supp}(D)| - 1 = d_r(C) - 1$. □

Exemplo 1.4.2. *Seja $C = \langle 11000, 00110, 00011 \rangle$ (ou, equivalentemente, o código que tem estes vetores como linhas em sua matriz geradora). Então $d_1(C) = 2$, por exemplo usando $D_1 = \langle 11000 \rangle$, $d_2(C) = 3$, por exemplo usando $D_2 = \langle 00110, 00011 \rangle$ e $d_3(C) = 5$, por exemplo usando $D_3 = C$.*

Um código será chamado de **código MDS** (maximum distance separable) se atinge a igualdade na cota de Singleton, isto é,

$$d = n - k + 1.$$

Para $r = 1, \dots, k$, um código será chamado de r -**MDS** se vale

$$d_r(C) = n - k + r.$$

Exemplo 1.4.3 (Códigos de Reed-Solomon). *Seja K um corpo finito e considere o K -espaço vetorial $K[X]_{k-1}$ dos polinômios em $K[X]$ de grau menor ou igual a $k - 1$, incluindo o polinômio nulo, isto é,*

$$K[X]_{k-1} = \{P \in K[X] : \text{grau}(P) \leq k - 1\} \cup \{0\}.$$

Claramente $K[X]_{k-1}$ é um espaço vetorial de dimensão k e uma base é dada por $\{1, X, X^2, \dots, X^{k-1}\}$. Seja n um inteiro, tal que $n \geq k$, e $\alpha_1, \dots, \alpha_n$ elementos distintos de K . Considere a função definida por

$$\begin{aligned} T : K[X]_{k-1} &\longrightarrow K^n \\ P &\longmapsto (P(\alpha_1), \dots, P(\alpha_n)). \end{aligned}$$

T é claramente uma transformação linear injetora. De fato,

$$\ker(T) = \{P \in K[X]_{k-1} : P(\alpha_1) = 0 = \dots = P(\alpha_n) = 0\} = \{0\},$$

pois um polinômio não nulo P de grau menor que k não pode ter n raízes distintas.

A imagem C de T será chamada de **Código de Reed-Solomon** de comprimento n e dimensão k definido por $\alpha_1, \dots, \alpha_n$ e uma matriz geradora de C é dada por

$$G = \begin{pmatrix} T(1) \\ T(X) \\ T(X^2) \\ \vdots \\ T(X^{k-1}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}$$

Determinemos agora a distância mínima de C : dado um elemento não nulo c de C , existe $P \in K[X]_{k-1}$ tal que $c = (P(\alpha_1), \dots, P(\alpha_n))$. Assim,

$$\begin{aligned} w(c) &= |\{i \in \{1, \dots, n\} : P(\alpha_i) \neq 0\}| \\ &= n - |\{i \in \{1, \dots, n\} : P(\alpha_i) = 0\}| \\ &\geq n - \text{grau}(P) \\ &\geq n - (k-1) = n - k + 1, \end{aligned}$$

ou seja, $d \geq n - k + 1$. Da cota de Singleton, temos a desigualdade contrária. Portanto, $d = n - k + 1$ e C é um código MDS.

Por fim, daremos agora a generalização das três cotas apresentadas anteriormente.

Teorema 1.4.4. [14, Cota de Singleton] Os parâmetros (n, k, d) de um código linear, onde $d_i(C)$ é o i -ésimo peso de Hamming generalizado, satisfazem à desigualdade

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

Teorema 1.4.5. [14, Cota de Plotkin] Os parâmetros (n, k, d) de um código linear, onde $d_i(C)$ é o i -ésimo peso de Hamming generalizado, satisfazem à desigualdade

$$d_r(C) \leq \left\lfloor \frac{n(q^r - 1)q^{k-r}}{q^k - 1} \right\rfloor.$$

Teorema 1.4.6. [14, Cota de Griesmer] Os parâmetros (n, k, d) de um código linear, onde $d_i(C)$ é o i -ésimo peso de Hamming generalizado, satisfazem à desigualdade

$$\sum_{i=0}^{r-1} \left\lceil \frac{d_1(C)}{q^i} \right\rceil \leq d_r(C).$$

Capítulo 2

Preliminares

2.1 Polinômios e Bases de Gröbner

Um **monômio** nas variáveis x_1, \dots, x_n é um produto da forma $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, onde as entradas da n -upla $\alpha = (\alpha_1, \dots, \alpha_n)$ são inteiros não negativos. O **grau total** deste monômio é dado pela soma $\alpha_1 + \cdots + \alpha_n = |\alpha|$.

Um **polinômio** f nas variáveis x_1, \dots, x_n com coeficientes em um corpo K é uma combinação linear finita (com coeficientes em K) de monômios. Para simplificar a notação para polinômios escrevemos $x_1^{\alpha_1} \cdots x_n^{\alpha_n} = x^\alpha$, e assim um polinômio f se escreve como

$$f = \sum_{\alpha} a_{\alpha} x^{\alpha}, \quad a_{\alpha} \in K,$$

onde a soma se dá sobre um número finito de n -uplas $\alpha = (\alpha_1, \dots, \alpha_n)$. O conjunto de todos os polinômios nas variáveis x_1, \dots, x_n com coeficientes em K é denotado por $K[x_1, \dots, x_n]$.

Seja $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ um polinômio em $K[x_1, \dots, x_n]$, cada a_{α} é chamado de **coeficiente** do monômio x^{α} . Se $a_{\alpha} \neq 0$, chamaremos $a_{\alpha} x^{\alpha}$ de **termo** de f . O **grau total** de f é o maior $|\alpha|$ tal que o coeficiente a_{α} é não nulo. Denotaremos o conjunto de todos os monômios de $K[x_1, \dots, x_n]$ por \mathcal{M} . Uma **ordem monomial** em \mathcal{M} é uma ordem total $<$ definida em \mathcal{M} satisfazendo:

1. Se $x^{\alpha} < x^{\beta}$ então $x^{\alpha+\gamma} < x^{\beta+\gamma}$, para todos $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}^n$;
2. Todo subconjunto $\mathcal{A} \subset \mathcal{M}$ possui um menor elemento.

Seja $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ um polinômio não nulo em $K[x_1, \dots, x_n]$ e seja $<$ uma ordem monomial. O **multigrau** de f é $\text{multigrau}(f) = \beta$ onde $x^{\beta} = \max(x^{\alpha} : a_{\alpha} \neq 0)$. O **coeficiente líder** de f é $\text{CL}(f) = a_{\text{multigrau}(f)} \in K$. O **monômio líder** de f é $\text{ML}(f) = x^{\text{multigrau}(f)}$ (com coeficiente 1). O **termo líder** de f é $\text{TL}(f) = \text{CL}(f) \cdot \text{ML}(f)$. Daremos agora exemplos de três ordens monomiais bem conhecidas.

1. **Ordem lexicográfica** - Sejam $\alpha = (\alpha_1, \dots, \alpha_n)$ e $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. Dizemos que $x^{\alpha} >_{\text{lex}} x^{\beta}$ se na diferença de vetores $\alpha - \beta \in \mathbb{Z}^n$, a coordenada não nula mais a esquerda é positiva.
2. **Ordem lexicográfica graduada** - Sejam $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. Dizemos que $x^{\alpha} >_{\text{grlex}} x^{\beta}$ se

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i, \quad \text{ou} \quad |\alpha| = |\beta| \text{ e } x^{\alpha} >_{\text{lex}} x^{\beta}.$$

3. Ordem lexicográfica graduada reversa - Sejam $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. Dizemos que $x^\alpha >_{\text{grevlex}} x^\beta$ se

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i, \quad \text{ou} \quad |\alpha| = |\beta|,$$

e a coordenada não nula mais a direita de $\alpha - \beta \in \mathbb{Z}_{\geq 0}^n$ é negativa.

Exemplo 2.1.1. Considere o polinômio $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in K[x, y, z]$. Reordenando os termos de maneira decrescente de acordo com cada ordem, temos:

- Com respeito a ordem lexicográfica: $f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$.
- Com respeito a ordem lexicográfica graduada: $f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$.
- Com respeito a ordem lexicográfica graduada reversa: $f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$.

Definiremos agora o que significa dividir polinômios em várias variáveis e listaremos alguns resultados relacionados. Dividir um polinômio $f \in K[x_1, \dots, x_n]$ por uma lista de polinômios $\{g_1, \dots, g_t\} \subset K[x_1, \dots, x_n] \setminus \{0\}$, com respeito a uma ordem monomial significa encontrar quocientes q_1, \dots, q_t e um resto r em $K[x_1, \dots, x_n]$ de forma que $f = q_1g_1 + \dots + q_tg_t + r$, com $r = 0$ ou nenhum monômio que aparece em r é um múltiplo de $\text{ML}(g_i)$, para todo $i \in \{1, \dots, t\}$. É importante observar que ao dividirmos um polinômio por uma lista de polinômios, os quocientes e restos variam de acordo com a ordem que tomamos a lista de polinômios. Não entraremos em detalhes sobre o algoritmo da divisão, mas com um exemplo podemos ver que

$$\begin{aligned} x^2y + xy^2 + y^2 &= (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1 \\ &= x \cdot (xy - 1) + (x + 1) \cdot (y^2 - 1) + 2x + 1. \end{aligned}$$

Seja $I \subset K[x_1, \dots, x_n]$ um ideal não nulo de $K[x_1, \dots, x_n]$ e fixemos uma ordem monomial em \mathcal{M} , dizemos que um conjunto $\{g_1, \dots, g_s\} \subset I$ é uma **base de Gröbner** para I (com respeito à ordem monomial fixada) se para todo polinômio $f \in I, f \neq 0$, temos que $\text{ML}(f)$ é um múltiplo de $\text{ML}(g_i)$ para algum $i \in \{1, \dots, s\}$.

Exemplo 2.1.2. Daremos agora um exemplo de um conjunto que **não** é uma base de Gröbner. Considere $I = (xy - 1, y^2 - 1) \subset \mathbb{R}[x, y]$ e fixe a ordem lexicográfica no conjunto de monômios de $\mathbb{R}[x, y]$. Observemos que $y \cdot (xy - 1) - x \cdot (y^2 - 1) = -y + x \in I$ e $\text{ML}(x - y) = x$, que não é um múltiplo de $\text{ML}(xy - 1)$ ou $\text{ML}(y^2 - 1)$, e portanto $\{xy - 1, y^2 - 1\}$ não é uma base de Gröbner para I .

A partir de agora assumiremos que todo ideal I é não nulo e que \mathcal{M} possui uma ordem monomial fixada. O próximo resultado nos mostra que uma base de Gröbner é uma base para o ideal I no sentido usual, e isto nos permite facilmente determinar se um dado polinômio pertence ou não ao ideal.

Lema 2.1.3. Seja $\{g_1, \dots, g_s\} \subset I$ uma base de Gröbner para I . Então $f \in I$ se, e somente se, o resto da divisão de f por $\{g_1, \dots, g_s\}$ é zero. Consequentemente, $I = (g_1, \dots, g_s)$.

Demonstração. Suponha que $f \in I$ e seja $f = \sum_{i=1}^s q_i g_i + r$ a divisão de f por $\{g_1, \dots, g_s\}$. Segue então que $r = f - \sum_{i=1}^s q_i g_i \in I$ e devemos ter $r = 0$ pois caso contrário r seria um polinômio não nulo em I cujo monômio líder não é múltiplo de nenhum $\text{ML}(g_i)$, para todo $i \in \{1, \dots, s\}$, o que contradiz o fato de $\{g_1, \dots, g_s\}$ ser uma base de Gröbner.

Reciprocamente, se o resto da divisão de f por $\{g_1, \dots, g_s\}$ é zero, segue que f é uma combinação de polinômios em I e portanto pertence à I . \square

Apresentamos agora um importante resultado da teoria de bases de Gröbner.

Proposição 2.1.4. *Seja $\{g_1, \dots, g_s\} \subset I$ uma base de Gröbner para I . Na divisão de $f \in K[x_1, \dots, x_n]$ por $\{g_1, \dots, g_s\}$ o resto da divisão é sempre o mesmo, independente da ordem que escolhemos para g_1, \dots, g_s no algoritmo da divisão.*

Demonstração. Suponha que $f = q_1 g_1 + \dots + q_s g_s + r = \bar{q}_1 g_1 + \dots + \bar{q}_s g_s + \bar{r}$, onde $q_i, \bar{q}_i \in K[x_1, \dots, x_n]$ para todo $i \in \{1, \dots, s\}$ e $r, \bar{r} \in K[x_1, \dots, x_n]$ e nenhum monômio que aparece em r ou \bar{r} é um múltiplo de $\text{ML}(g_i)$ para todo $i \in \{1, \dots, s\}$. Segue que $r - \bar{r} = \sum_{i=1}^s (\bar{q}_i - q_i) g_i \in I$ e assim devemos ter $r - \bar{r} = 0$ pois caso contrário $r - \bar{r}$ seria um polinômio não nulo em I cujo monômio líder não é um múltiplo de $\text{ML}(g_i)$ para todo $i \in \{1, \dots, s\}$, contradizendo o fato de $\{g_1, \dots, g_s\}$ ser uma base de Gröbner para I . \square

Ainda não é claro se todo ideal admite uma base de Gröbner. Existe um algoritmo que gera uma base de Gröbner a partir de uma base do ideal I , mas não entraremos em detalhes sobre esse algoritmo neste trabalho, aqui apenas descreveremos como ele funciona e daremos um exemplo.

Sejam $f, g \in K[x_1, \dots, x_n] \setminus \{0\}$, com $\text{TL}(f) = ax^\alpha$ e $\text{TL}(g) = bx^\beta$ com $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. Seja $\gamma_i = \max(\alpha_i, \beta_i)$ para todo $i \in \{1, \dots, s\}$ e seja $\gamma = (\gamma_1, \dots, \gamma_n) \in \mathbb{Z}_{\geq 0}^n$. O **S-polinômio** de f e g é definido como

$$S(f, g) = \frac{1}{a} x^{\gamma-\alpha} f - \frac{1}{b} x^{\gamma-\beta} g.$$

O teorema a seguir, juntamente com o pseudocódigo do algoritmo, garante que todo ideal possui uma base de Gröbner.

Teorema 2.1.5. [4, Algoritmo de Buchberger] *Seja $I = (f_1, \dots, f_s)$ um ideal de polinômios não nulo. Então uma base de Gröbner para I pode ser construída em um número finito de etapas através do seguinte algoritmo:*

Algoritmo de Buchberger

Input. $F = (f_1, \dots, f_s)$

Output. uma base de Gröbner $G = (g_1, \dots, g_t)$ para I com $F \subseteq G$

1. $G := F$
2. Repetir
3. $G' := G$
4. Para cada par $\{p, q\}$ com $p \neq q$ em G' , faça
5. $S :=$ resto da divisão de $S(p, q)$ por G
6. Se $S \neq 0$, então $G := G \cup S$
7. Até $G = G'$
8. Retorne G

Exemplo 2.1.6. *Vimos no exemplo anterior que $\{xy - 1, y^2 - 1\}$ não é uma base de Gröbner para $I = (xy - 1, y^2 - 1) \subset \mathbb{R}[x, y]$ com respeito à ordem lexicográfica (escolhendo $y < x$). Aplicando*

o algoritmo de Buchberger, escolha $f_1 = xy - 1$ e $f_2 = y^2 - 1$, então $S(f_1, f_2) = y \cdot f_1 - x \cdot f_2 = x - y$ e o resto da divisão de $S(f_1, f_2)$ por $\{f_1, f_2\}$ é $x - y$. Seja $f_3 = x - y$ e considere o conjunto $\{xy - 1, y^2 - 1, x - y\}$. Temos agora que o resto da divisão de $S(f_1, f_2)$ por $\{xy - 1, y^2 - 1, x - y\}$ é zero. Calculando $S(f_1, f_3) = y^2 - 1$ e $S(f_2, f_3)$, podemos ver que o resto da divisão destes polinômios por $\{xy - 1, y^2 - 1, x - y\}$ é zero, então $\{xy - 1, y^2 - 1, x - y\}$ é uma base de Gröbner para I (com respeito à ordem lexicográfica).

Introduziremos agora um conceito que será essencial para dar prosseguimento à teoria. Seja $I \subset K[x_1, \dots, x_n]$ um ideal. A **pegada** de I (com respeito à uma ordem monomial fixada em \mathcal{M}) é o conjunto

$$\Delta(I) = \{M \in \mathcal{M} : M \text{ não é o monômio líder de nenhum polinômio em } I\}.$$

O resultado seguinte mostra que a pegada de um ideal está relacionada com uma base de Gröbner para I .

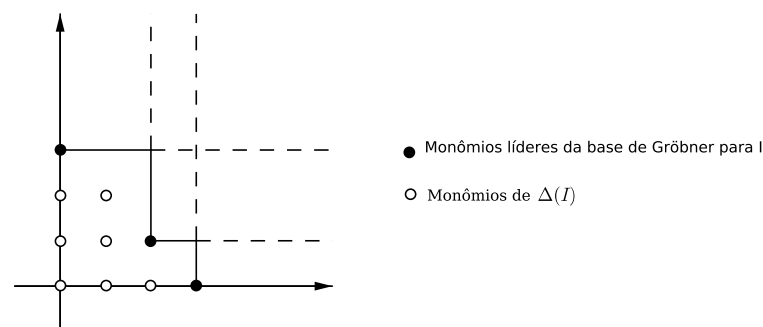
Proposição 2.1.7. *Seja $I \subset K[x_1, \dots, x_n]$ um ideal e seja $\{g_1, \dots, g_s\}$ uma base de Gröbner para I . Então um monômio M pertence a $\Delta(I)$ se, e somente se, M não é um múltiplo de $\text{ML}(g_i)$ para todo $i \in \{1, \dots, s\}$.*

Demonstração. Se M é um monômio em $\Delta(I)$, pela definição de pegada segue que M não é o monômio líder de nenhum polinômio em I , em particular, M não é múltiplo de $\text{ML}(g_i)$ para todo $i \in \{1, \dots, s\}$.

Reciprocamente, da definição de base de Gröbner sabemos que se M não é um múltiplo de $\text{ML}(g_i)$ para todo $i \in \{1, \dots, s\}$, então M não é o monômio líder de nenhum polinômio em I . \square

Façamos agora um exemplo que utiliza o resultado acima para obter uma representação gráfica de uma pegada. Nesse exemplo associamos a um par ordenado (a, b) , com entradas não negativas e inteiras, o monômio $x^a y^b$.

Exemplo 2.1.8. *Seja $I = (x^3 - x, y^3 - y, x^2 y - y) \subset \mathbb{R}[x, y]$ e tomemos \mathcal{M} com a ordem lexicográfica (escolhendo $y < x$). Uma verificação mostra $\{x^3 - x, y^3 - y, x^2 y - y\}$ é uma base de Gröbner para I . Temos $\text{ML}(x^3 - x) = x^3$, $\text{ML}(y^3 - y) = y^3$, $\text{ML}(x^2 y - y) = x^2 y$ e aplicando a proposição acima, a seguinte representação nos mostra a pegada.*



Os pontos $(3, 0)$, $(0, 3)$ e $(2, 1)$ correspondem aos monômios líderes da base de Gröbner e a partir destes é possível determinar quais monômios são múltiplos de pelo menos um deles. Segue que $\Delta(I) = \{1, x, x^2, y, xy, y^2, xy^2\}$.

O teorema a seguir é o principal resultado da tese de doutorado de Bruno Buchberger [3], e foi o que motivou a introdução por ele do conceito de bases de Gröbner.

Teorema 2.1.9. *Seja $I \subset K[x_1, \dots, x_n]$ um ideal. Então*

$$\mathcal{B} = \{M + I : M \in \Delta(I)\}$$

é uma base para $K[x_1, \dots, x_n]/I$ como um K -espaço vetorial.

Demonstração. Seja \mathcal{G} uma base de Gröbner para I com respeito à mesma ordem monomial usada para determinar $\Delta(I)$, e seja $f \in K[x_1, \dots, x_n]$. Dividindo f por \mathcal{G} obtemos um resto na forma $r = \sum_{i=1}^t a_i M_i$ onde $a_i \in K[x_1, \dots, x_n]$ e $M_i \in \Delta(I)$ para todo $i = 1, \dots, t$.

Como $f + I = r + I$ segue que \mathcal{B} gera $K[x_1, \dots, x_n]/I$ como um K -espaço vetorial. Vejamos agora que os vetores em \mathcal{B} são linearmente independentes.

Suponha que $\sum_{i=1}^l b_i (M_i + I) = 0 + I$, onde $b_i \in K$ e $M_i \in \Delta(I)$ para todo $i = 1, \dots, l$. Então $\sum_{i=1}^l b_i M_i \in I$ e assim devemos ter que cada $b_i = 0$ para todo $i = 1, \dots, l$, pois caso contrário $\sum_{i=1}^l b_i M_i$ seria um elemento não nulo de I cujo monômio líder não é o monômio líder de um polinômio em I . □

Exemplo 2.1.10. *Tomando o exemplo (2.1.8), temos que o conjunto $\{1 + I, x + I, x^2 + I, y + I, xy + I, y^2 + I, xy^2 + I\}$ é uma base para $\mathbb{R}[x, y]/I$ como um \mathbb{R} -espaço vetorial.*

2.2 Variedades afins e a pegada de um ideal

Apresentaremos nessa seção uma relação entre a variedade afim associada a um ideal I e a sua pegada quando $\Delta(I)$ é um conjunto finito.

Seja $I \subset K[x_1, \dots, x_n]$ um ideal. A **variedade afim** associada a I é o conjunto

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

É fácil ver que se $I = (g_1, \dots, g_t)$, então $(a_1, \dots, a_n) \in V(I)$ se, e somente se, $g_i(a_1, \dots, a_n) = 0$, para todo $i = 1, \dots, t$.

Dado V uma variedade afim, o **ideal da variedade** V é o conjunto de todos os polinômios que se anulam em V , ou seja,

$$I(V) = \{f \in K[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0, \text{ para todo } (a_1, \dots, a_n) \in V\}.$$

Pode-se mostrar que este conjunto é de fato um ideal de $K[x_1, \dots, x_n]$.

Proposição 2.2.1. *Se W é uma variedade afim, então $V(I(W)) = W$.*

Demonstração. Das definições de ideal de uma variedade e variedade afim temos $W \subseteq V(I(W))$. Por outro lado, sabemos que $W = V(J)$ para algum ideal $J \in K[x_1, \dots, x_n]$ e claramente $J \subseteq I(W)$, logo $V(I(W)) \subseteq V(J)$, isto é, $V(I(W)) \subseteq W$. □

Lema 2.2.2. *Sejam p_1, \dots, p_r pontos distintos de K^n . Então existem polinômios f_1, \dots, f_r em $K[x_1, \dots, x_n]$ tais que $f_i(p_j) = \delta_{ij}$, para todos $i, j \in \{1, \dots, r\}$, onde δ_{ij} é o delta de Kronecker.*

Demonstração. Sejam $p_i = (a_{i1}, \dots, a_{in}) \in K^n$, com $i = 1, \dots, r$. Vejamos como obter f_1 . Como todos os pontos são distintos, para $i = 2, \dots, r$ existe $j_i \in \{1, \dots, n\}$ tal que $a_{1j_i} \neq a_{ij_i}$. Seja

$$h_i = \frac{x_{j_i} - a_{ij_i}}{a_{1j_i} - a_{ij_i}},$$

então $h_i(p_1) = 1$ e $h_i(p_i) = 0$ para todo $i = 2, \dots, r$.

Tome

$$f_1 := \prod_{i=2}^r h_i,$$

assim nós temos $f_1(p_1) = 1$ e $f_1(p_i) = 0$, para todo $i = 2, \dots, r$. Procedendo de forma análoga construímos f_2, \dots, f_r . □

Teorema 2.2.3. *Seja $I \subset K[x_1, \dots, x_n]$ um ideal tal que $\Delta(I)$ é um conjunto finito. Então $V(I)$ é também um conjunto finito e $|V(I)| \leq |\Delta(I)|$.*

Demonstração. Sejam p_1, \dots, p_r pontos distintos de $V(I)$. Do lema anterior sabemos que existem $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ tais que $f_i(p_j) = \delta_{ij}$, para todo $i, j = 1, \dots, r$.

Vejamos que $\{f_1 + I, \dots, f_r + I\}$ é um conjunto linearmente independente em $K[x_1, \dots, x_n]/I$. De fato, suponha que

$$\sum_{i=1}^r a_i(f_i + I) = 0 + I, \text{ onde } a_1, \dots, a_r \in K,$$

então $\sum_{i=1}^r a_i f_i \in I$. Logo, $\sum_{i=1}^r a_i f_i(p_j) = 0$, isto é, $a_j = 0$ para todo $j = 1, \dots, r$. Assim, $\{f_1 + I, \dots, f_r + I\}$ é linearmente independente em $K[x_1, \dots, x_n]/I$.

Portanto,

$$|V(I)| = r \leq \dim(K[x_1, \dots, x_n]/I) = |\Delta(I)|,$$

onde na última igualdade usamos o Teorema 2.1.9. □

Teorema 2.2.4. *[1, Teorema 8.2] Seja $I \subset K[x_1, \dots, x_n]$ um ideal tal que $\Delta(I)$ é um conjunto finito e seja L uma extensão algebricamente fechada de K . Então $V_L(I) := \{(a_1, \dots, a_n) \in L^n : f(a_1, \dots, a_n) = 0 \text{ para todo } f \in I\}$ é um conjunto finito e $|V_L(I)| \leq |\Delta(I)|$. Além disso, se K é um corpo perfeito e I é um ideal radical então $|V_L(I)| = |\Delta(I)|$.*

2.3 Geometria Projetiva

2.3.1 Espaço Projetivo

Nesta seção descreveremos o espaço projetivo. Denotaremos o espaço afim K^n por $\mathbb{A}^n(K)$. Definiremos uma relação de equivalência em $\mathbb{A}^{n+1}(K) - \{0\}$ da seguinte maneira:

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \iff (x_0, \dots, x_n) = \lambda(y_0, \dots, y_n), \text{ para algum } \lambda \in K^*.$$

Definimos assim o **espaço projetivo** n -dimensional sobre K como sendo o conjunto

$$\mathbb{P}^n(K) = (\mathbb{A}^{n+1}(K) - \{0\}) / \sim,$$

e denotamos um ponto de $\mathbb{P}^n(K)$ por

$$p = [x_0 : \dots : x_n] = \{(y_0, \dots, y_n) : (x_0, \dots, x_n) \sim (y_0, \dots, y_n)\},$$

e dizemos que (x_0, \dots, x_n) são as **coordenadas homogêneas** de p . Podemos pensar em $\mathbb{P}^n(K)$ como sendo o conjunto de retas que passam pela origem em $\mathbb{A}^{n+1}(K)$.

Vejamos agora alguns resultados que nos permitem entender melhor o espaço projetivo.

Proposição 2.3.1. *Seja $U_0 = \{[x_0 : \cdots : x_n] \in \mathbb{P}^n(K) : x_0 \neq 0\}$. Então a aplicação*

$$\begin{aligned} \phi : \mathbb{A}^n(K) &\longrightarrow \mathbb{P}^n(K) \\ (a_1, \dots, a_n) &\longmapsto [1 : a_1 : \cdots : a_n] \end{aligned}$$

é injetora e $\text{Img}(\phi) = U_0$.

Demonstração. Como $\phi(\mathbb{A}^n(K)) \subseteq U_0$, consideraremos $\phi : \mathbb{A}^n(K) \longrightarrow U_0$ e mostraremos que ϕ é uma bijeção.

Defina $\psi : U_0 \longrightarrow \mathbb{A}^n(K)$ por $[a_0 : \cdots : a_n] \longmapsto \left(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}\right)$. Vejamos que ψ está bem definida:

Sejam $[a_0 : \cdots : a_n] = [b_0 : \cdots : b_n]$ em U_0 , então para algum $\lambda \in K^*$ vale $(b_0, \dots, b_n) = \lambda(a_0, \dots, a_n)$. Assim $b_i = \lambda a_i$ para $i = 0, \dots, n$. Logo,

$$\psi([b_0 : \cdots : b_n]) = \left(\frac{b_1}{b_0}, \dots, \frac{b_n}{b_0}\right) = \left(\frac{\lambda a_1}{\lambda a_0}, \dots, \frac{\lambda a_n}{\lambda a_0}\right) = \left(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}\right) = \psi([a_0 : \cdots : a_n]).$$

Vejamos agora que $\psi \circ \phi = \text{Id}_{\mathbb{A}^n(K)}$ e $\phi \circ \psi = \text{Id}_{U_0}$:

$$\begin{aligned} \psi \circ \phi(a_1, \dots, a_n) &= \psi([1 : a_1 : \cdots : a_n]) = \left(\frac{a_1}{1}, \dots, \frac{a_n}{1}\right) = (a_1, \dots, a_n) \\ \phi \circ \psi([a_0 : \cdots : a_n]) &= \phi\left(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}\right) = \left[1 : \frac{a_1}{a_0} : \cdots : \frac{a_n}{a_0}\right] = [a_0 : \cdots : a_n]. \end{aligned}$$

□

Podemos então identificar $\mathbb{P}^n(K) = U_0 \cup H$, onde

$$H = \{p \in \mathbb{P}^n(K) : p = [0 : x_1 : \cdots : x_n]\}.$$

Como ϕ é bijetora sobre sua imagem, identificaremos U_0 com $\mathbb{A}^n(K)$. Como $\mathbb{P}^{n-1}(K) \longrightarrow H$ dada por $[x_1 : \cdots : x_n] \longmapsto [0 : x_1 : \cdots : x_n]$ é uma bijeção (esta demonstração é análoga a demonstração do teorema), identificaremos H com $\mathbb{P}^{n-1}(K)$. Assim escrevemos

$$\mathbb{P}^n(K) = \mathbb{A}^n(K) \cup \mathbb{P}^{n-1}(K).$$

Tomando como exemplo o caso em que $n = 1$, temos que $\mathbb{P}^1(K) = \mathbb{A}^1(K) \cup \mathbb{P}^0(K)$, onde indentificamos $\mathbb{P}^0(K)$ como o conjunto $\{[0 : y] : y \in K\} = \{[0 : 1]\}$. Logo, $\mathbb{P}^0(K)$ tem um único ponto, que é usualmente denotado por ∞ . Sendo assim a reta projetiva pode ser escrita como

$$\mathbb{P}^1(K) = \mathbb{A}^1(K) \cup \{\infty\}.$$

No teorema acima escolhemos tomar $x_0 \neq 0$ na construção do conjunto U_0 . O corolário a seguir, cuja demonstração é análoga à do teorema acima, mostra que além de U_0 temos outras cópias de $\mathbb{A}^n(K)$ dentro de $\mathbb{P}^n(K)$ e que podemos fazer a mesma construção tomando uma coordenada qualquer não nula.

Corolário 2.3.2. *Para cada $i = 0, \dots, n$ seja $U_i = \{[x_0 : \cdots : x_n] \in \mathbb{P}^n(K) : x_i \neq 0\}$.*

1. *Existe uma bijeção entre U_i e $\mathbb{A}^n(K)$ para todo $i = 0, \dots, n$.*

2. *$\mathbb{P}^n(K) - U_i$ pode ser identificado por $\mathbb{P}^{n-1}(K)$.*

3. $\mathbb{P}^n(K) = \bigcup_{i=0}^n U_i.$

2.3.2 Variedades Projetivas

Buscaremos agora trazer o conceito de variedades para o espaço projetivo. Se tomamos, por exemplo, $f = 4x_1 - x_2^2 \in \mathbb{R}[x_0, x_1, x_2]$ podemos pensar em $V(f) \subset \mathbb{P}^2(\mathbb{R})$ como sendo o conjunto de pontos $[a : b : c]$ em $\mathbb{P}^2(\mathbb{R})$ tais que $f(a, b, c) = 0$. Neste caso, como $f(5, 1, 2) = 0$ teríamos que $p = [5 : 1 : 2] \in V(f)$. Entretanto, observemos que $[5 : 1 : 2] = [10 : 2 : 4]$ e $f(10, 2, 4) = -8 \neq 0$, assim $q = [10 : 2 : 4] \notin V(f)$. De modo a remediar esta situação, vamos definir variedades projetivas através de polinômios homogêneos.

Um polinômio f é **homogêneo de grau d** se todo termo de f tem grau total igual a d .

Exemplo 2.3.3. Em $\mathbb{R}[x, y, z]$ o polinômio $f = xy^2 + y$ não é homogêneo, enquanto que o polinômio $g = x^2z + xyz + z^3$ é homogêneo de grau 3.

Proposição 2.3.4. Seja $f \in K[x_0, \dots, x_n]$ um polinômio homogêneo de grau d . Se $f(a_0, \dots, a_n) = 0$, então $f(b_0, \dots, b_n) = 0$ sempre que $[b_0 : \dots : b_n] = [a_0 : \dots : a_n]$. Em particular,

$$V(f) = \{[a_0 : \dots : a_n] \in \mathbb{P}^n(K) : f(a_0, \dots, a_n) = 0\}$$

está bem definido como um subconjunto de $\mathbb{P}^n(K)$.

Demonstração. Seja (b_0, \dots, b_n) tal que $[b_0 : \dots : b_n] = [a_0 : \dots : a_n]$, então existe $\lambda \in K^*$ tal que $(b_0, \dots, b_n) = \lambda(a_0, \dots, a_n)$. Do fato que f é um polinômio homogêneo de grau d , temos

$$f(b_0, \dots, b_n) = f(\lambda a_0, \dots, \lambda a_n) = \lambda^d f(a_0, \dots, a_n) = 0.$$

□

Sejam $f_1, \dots, f_s \in K[x_0, \dots, x_n]$ polinômios homogêneos. O conjunto

$$V(f_1, \dots, f_s) = \{[a_0 : \dots : a_n] \in \mathbb{P}^n(K) : f_i(a_0, \dots, a_n) = 0, i = 1, \dots, s\}$$

é chamado de **variedade projetiva** definida por f_1, \dots, f_s .

O resultado a seguir relaciona variedades afins e variedades projetivas.

Proposição 2.3.5. Seja $V = V(f_1, \dots, f_s)$ uma variedade projetiva em $\mathbb{P}^n(K)$. Então $W = V \cap U_0$ pode ser identificado como a variedade afim $V(g_1, \dots, g_s) \subset \mathbb{A}^n(K)$, onde $g_i(y_1, \dots, y_n) = f_i(1, y_1, \dots, y_n)$, para todo $i = 1, \dots, s$.

Demonstração. Já sabemos que $\psi : U_0 \rightarrow \mathbb{A}^n(K), [a_0 : \dots : a_n] \mapsto \left(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}\right)$ é uma bijeção. Queremos mostrar que $\psi(W) = V(g_1, \dots, g_s)$.

$$\psi(W) \subseteq V(g_1, \dots, g_s):$$

Seja $\left(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}\right) = \psi([a_0 : \dots : a_n])$, onde $[a_0 : \dots : a_n] \in W = V \cap U_0$, logo $[a_0 : \dots : a_n] \in U_0$ e portanto $a_0 \neq 0$. Como $[a_0 : \dots : a_n] = [1 : \frac{a_1}{a_0} : \dots : \frac{a_n}{a_0}] \in V$, temos $f_i(1, \frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}) = 0$, para todo $i = 1, \dots, s$. Logo, $g_i(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}) = 0$, para todo $i = 1, \dots, s$. Portanto, $(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}) \in V(g_1, \dots, g_s)$.

$$V(g_1, \dots, g_s) \subseteq \psi(W):$$

Seja $(a_1, \dots, a_n) \in V(g_1, \dots, g_s)$. Claramente $[1 : a_1 : \dots : a_n] \in U_0$ e $f_i(1, a_1, \dots, a_n) = g_i(a_1, \dots, a_n) = 0$, para todo $i = 1, \dots, s$. Logo $[1 : a_1 : \dots : a_n] \in V \cap U_0 = W$, ou seja, $\psi^{-1}((a_1, \dots, a_n)) \in W$ e logo $(a_1, \dots, a_n) \in \psi(W)$.

□

Exemplo 2.3.6. Considere a variedade projetiva $V = V(x_0^3 + x_1x_2^2, x_0 + x_1 + x_2) \subseteq \mathbb{P}^3(\mathbb{R})$. Tomando $W = V \cap U_0$ temos

$$W = V(1 + x_1x_2^2, 1 + x_1 + x_2) \subseteq \mathbb{A}^3(\mathbb{R}).$$

Note que podemos escolher intersectar V com U_1 , e nesse caso fazemos $x_1 = 1$ na definição de V .

Dado $f \in K[x_1, \dots, x_n]$ com $\text{grau}(f) = d$, podemos escrever f de maneira única como

$$f = \sum_{i=0}^d f_i,$$

onde $\text{grau}(f_i) = i$ ou $f_i = 0$, para todo $i = 0, \dots, d$. Dizemos que os polinômios f_0, \dots, f_d são os **componentes homogêneos** de f .

Vejamos agora que dado uma variedade afim em U_i , podemos escrevê-la como $V \cap U_i$ para alguma variedade projetiva V .

Exemplo 2.3.7. Considere a variedade afim $W = V(x_2 - x_1^3 + x_1^2)$ em $U_0 = \mathbb{A}^2(\mathbb{R})$. Como $f = x_2 - x_1^3 + x_1^2$ não é um polinômio homogêneo, vamos acrescentar a variável x_0 de modo a tornar f homogêneo. Como f tem grau total igual a 3, modificaremos f de modo que todo termo tenha grau total igual a 3. Assim, obtemos

$$f^h = x_2x_0^2 - x_1^3 + x_1^2x_0.$$

Logo, $W = U_0 \cap V(f^h)$. Note que podemos recuperar f do polinômio f^h tomando $x_0 = 1$.

Proposição 2.3.8. Seja $g(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ um polinômio de grau total d .

1. Seja $g = \sum_{i=0}^d g_i$ a expansão de g como uma soma de componentes homogêneas, onde g_i tem grau total i . Então

$$g^h(x_0, \dots, x_n) = \sum_{i=0}^d g_i(x_1, \dots, x_n)x_0^{d-i}$$

é um polinômio homogêneo de grau total d em $K[x_0, \dots, x_n]$. (Chamaremos g^h a homogeneização de g com respeito a x_0).

2. A homogeneização de g com respeito a x_0 pode ser calculada através da fórmula

$$g^h = x_0^d g\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right).$$

3. Desomogeneizando g^h com respeito a x_0 obtemos o polinômio g , ou seja,

$$g^h(1, x_1, \dots, x_n) = g(x_1, \dots, x_n).$$

4. Seja $F(x_0, \dots, x_n)$ um polinômio homogêneo e seja x_0^e a maior potência de x_0 que divide F . Se $f = F(1, x_1, \dots, x_n)$ é uma desomogeneização de F , então $F = x_0^e f^h$.

Demonstração.

1. Como g_i tem grau total i segue que $g_i x_0^{d-i}$ tem grau total $i + d - i = d$. Assim,

$$g^h = g_0(x_1, \dots, x_n)x_0^d + g_1(x_1, \dots, x_n)x_0^{d-1} + \dots + g_d(x_1, \dots, x_n)x_0^{d-d}$$

é um polinômio homogêneo de grau total d em $K[x_1, \dots, x_n]$.

2. Observe que

$$\begin{aligned}
 x_0^d g\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) &= x_0^d \sum_{i=0}^d g_i\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \\
 &= x_0^d \left(g_0\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) + g_1\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) + \dots + g_d\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \right) \\
 &= x_0^d \left(g_0(x_1, \dots, x_n) + \frac{1}{x_0} g_1(x_1, \dots, x_n) + \dots + \frac{1}{x_0^d} g_d(x_1, \dots, x_n) \right) \\
 &= x_0^d g_0(x_1, \dots, x_n) + x_0^{d-1} g_1(x_1, \dots, x_n) + \dots + x_0^{d-d} g_d(x_1, \dots, x_n) \\
 &= g^h.
 \end{aligned}$$

3. Como $g^h(x_0, \dots, x_n) = \sum_{i=0}^d g_i(x_1, \dots, x_n) x_0^{d-i}$, temos

$$g^h(1, x_1, \dots, x_n) = \sum_{i=0}^d g_i(x_1, \dots, x_n) 1^{d-i} = g(x_1, \dots, x_n).$$

4. Seja $d = \text{grau}(F)$. Digamos que $F = a_1 x_0^{p_1} x^{\alpha_1} + \dots + a_t x_0^{p_t} x^{\alpha_t}$, onde $a_i \in K$ e x^{α_i} é um monômio em $K[x_1, \dots, x_n]$.

Como F é homogêneo de grau d , temos que $p_i + |\alpha_i| = d$, para todo $i = 1, \dots, t$. Como $f = F(1, x_1, \dots, x_n)$ temos

$$f = a_1 x^{\alpha_1} + \dots + a_t x^{\alpha_t}.$$

Observe que $\text{grau}(f) = d - e$, pois x_0^e é a maior potência de x_0 que divide F . Digamos agora que

$$f^h = a_1 x_0^{q_1} x^{\alpha_1} + \dots + a_t x_0^{q_t} x^{\alpha_t}.$$

Logo $q_i + |\alpha_i| = d - e$, para todo $i = 1, \dots, t$. Assim, $q_i + e = d - |\alpha_i| = p_i$, para todo $i = 1, \dots, t$.

Portanto,

$$\begin{aligned}
 x_0^e f^h &= a_1 x_0^{q_1+e} x^{\alpha_1} + \dots + a_t x_0^{q_t+e} x^{\alpha_t} \\
 &= a_1 x_0^{p_1} x^{\alpha_1} + \dots + a_t x_0^{p_t} x^{\alpha_t} \\
 &= F.
 \end{aligned}$$

□

Observemos que pelo corolário (2.3.2) o processo de homogeneização e desomogeneização de um polinômio pode ser feito de forma análoga tomando qualquer outra variável.

Exemplo 2.3.9. Seja $g = y - x^3 + x \in K[x, y]$ e considere a variedade afim $V(g) \subseteq U_2 = \mathbb{A}^2(K)$. Temos que $g^h = yz^2 - x^3 + xz^2$. Logo $V(g)$ pode ser identificada como $V \cap U_2$ em $\mathbb{P}^2(K)$ onde $V = V(g^h)$.

Seja I um ideal em $K[x_0, \dots, x_n]$. Dizemos que I é um **ideal homogêneo** se para cada $f \in I$, as componentes homogêneas f_i de f também pertencem a I .

Exemplo 2.3.10. Seja $I = (y - x^2) \subseteq K[x, y]$. As componentes homogêneas de $f = y - x^2$ são $f_1 = y$ e $f_2 = -x^2$. Note que tanto f_1 quanto f_2 não pertencem a I pois não são múltiplos de $y - x^2$. Portanto, I não é um ideal homogêneo.

Proposição 2.3.11. *Sejam $f, f_1, \dots, f_s \in K[x_1, \dots, x_n]$ polinômios homogêneos. Dividindo f por f_1, \dots, f_s (com respeito a qualquer ordem monomial) escrevemos*

$$f = a_1 f_1 + \dots + a_s f_s + r,$$

onde $a_1, \dots, a_s, r \in K[x_1, \dots, x_n]$ e nenhum termo de r é divisível por nenhum dos termos líderes dos f_i 's. Então a_1, \dots, a_s, r também são polinômios homogêneos. Mais precisamente, $\text{grau}(r) = \text{gt}(f)$ e $\text{grau}(a_i) = \text{grau}(f) - \text{grau}(f_i)$, para $i = 1, \dots, s$.

Demonstração. Sejam $d = \text{grau}(f)$ e $d_i = \text{grau}(f_i)$, para $i = 1, \dots, s$. Dividindo f por f_1, \dots, f_s , olhamos para $\text{TL}(f)$ e digamos que seja divisível por $\text{TL}(f_j)$, assim a_j recebe um termo p de grau $d - d_j$ para que haja o cancelamento. Assim, temos que $f' = f - p f_j$ é o novo polinômio a ser dividido por f_1, \dots, f_s . Agora, observe que $p f_j$ é homogêneo de grau d . Logo f' é homogêneo de grau d . Caso haja necessidade de retirar o $\text{TL}(f')$ e adicioná-lo ao resto, temos que r já começa como um polinômio homogêneo de grau d .

Prosseguindo, vamos dividir f' por f_1, \dots, f_s . Digamos que $\text{TL}(f')$ seja divisível por $\text{TL}(f_i)$, assim a_i recebe um termo q de grau $d - d_i$ para que ocorra o cancelamento. Assim, temos que $f'' = f' - q f_i$ é o novo polinômio a ser dividido por f_1, \dots, f_s . Observe que $q f_i$ é homogêneo de grau d , logo f'' é homogêneo de grau d . Caso haja necessidade de retirar o $\text{TL}(f'')$ e adicioná-lo ao resto, temos que r continua sendo um polinômio de grau d . Observe também que se $i = j$, temos que $a_j = p + q$ continua sendo um polinômio homogêneo de grau $d - d_j$. Prosseguindo com o algoritmo da divisão, terminaremos com cada a_j homogêneo de grau $d - d_j$ e o resto homogêneo de grau d . □

Proposição 2.3.12. *Se $f, g \in K[x_1, \dots, x_n]$ são polinômios homogêneos, então o S -polinômio $S(f, g)$ é homogêneo.*

Demonstração. Seja $x^\gamma = \text{mmc}(\text{ML}(f), \text{ML}(g))$ e digamos que $\text{grau}(x^\gamma) = d$. Temos

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

Sejam $d_1 = \text{grau}(f)$ e $d_2 = \text{grau}(g)$. Assim, $\text{grau}\left(\frac{x^\gamma}{\text{TL}(f)}\right) = d - d_1$ e $\text{grau}\left(\frac{x^\gamma}{\text{TL}(g)}\right) = d - d_2$.

Como f é homogêneo cada termo de f tem grau d_1 , logo cada termo de $\frac{x^\gamma}{\text{TL}(f)} f$ tem grau

$(d - d_1) + d_1 = d$. Portanto, $\frac{x^\gamma}{\text{TL}(f)} f$ é um polinômio homogêneo de grau d .

Como g é homogêneo cada termo de g tem grau d_2 , logo cada termo de $\frac{x^\gamma}{\text{TL}(g)} g$ tem grau

$(d - d_2) + d_2 = d$. Portanto, $\frac{x^\gamma}{\text{TL}(g)} g$ é um polinômio homogêneo de grau d .

Logo, $S(f, g)$ é um polinômio homogêneo de grau d . □

Teorema 2.3.13. *Seja I um ideal em $K[x_0, \dots, x_n]$. As seguintes afirmações são equivalentes:*

1. I é um ideal homogêneo;
2. $I = (f_1, \dots, f_s)$, onde f_1, \dots, f_s são polinômios homogêneos;
3. Uma base de Gröbner para I (com respeito a qualquer ordem monomial) é formada por polinômios homogêneos.

Demonstração.

(1) \Rightarrow (2):

Suponha que I é um ideal homogêneo. Pelo Teorema da Base de Hilbert, temos $I = (F_1, \dots, F_t)$, para alguns $F_1, \dots, F_t \in K[x_0, \dots, x_n]$. Escreva cada F_j como soma de suas componentes homogêneas

$$F_j = \sum_i F_{ji}.$$

Como I é homogêneo, temos que todos os F_{ji} pertencem a I . Seja I' o ideal gerado pelos polinômios homogêneos F_{ji} . Assim, cada $F_j = \sum_i F_{ji}$ pertencem a I' . Logo $I \subseteq I'$. Como $F_{ji} \in I$ para todos i, j , temos $I' \subseteq I$. Portanto, $I = I'$.

(2) \Rightarrow (1):

Se $f = \sum_i p_i$ e $g = \sum_i q_i$ são as expansões de dois polinômios como a soma de suas componentes homogêneas, então as componentes homogêneas h_k do produto $h = fg$ são dadas por

$$h_k = \sum_{i+j=k} p_i q_j,$$

pois

$$fg = \sum_{i+j=0} p_i q_j + \sum_{i+j=1} p_i q_j + \dots$$

é a expansão de fg como soma de componentes homogêneas. Por hipótese, $I = (f_1, \dots, f_s)$ onde f_1, \dots, f_s são polinômios homogêneos. Seja $f \in I$, então $f = a_1 f_1 + \dots + a_s f_s$, para alguns $a_1, \dots, a_s \in K[x_0, \dots, x_n]$. Escrevendo a_1 como soma de suas componentes homogêneas temos

$$a_1 = \sum_i a_{1i}.$$

Como f_1 é homogêneo, digamos de grau d , temos $f_1 = f_d$ é a expansão de f_1 como soma de suas componentes homogêneas. Logo, a expansão de $a_1 f_1$ como soma de suas componentes homogêneas é

$$a_1 f_1 = \sum_{i+d=0} a_{1i} f_d + \sum_{i+d=1} a_{1i} f_d + \dots$$

Como $f_d = f_1 \in I$ temos que cada componente homogênea de $a_1 f_1$ pertence a I . Este processo pode ser feito para cada $a_i f_i$. Logo, cada componente homogênea de $a_i f_i$ pertence a I . Assim, cada componente homogênea de f pertence a I . Portanto, I é um ideal homogêneo.

(2) \Rightarrow (3):

Por hipótese, $I = (f_1, \dots, f_s)$, onde f_1, \dots, f_s são polinômios homogêneos. Pela proposição (2.3.12) os S -polinômios $S(f_i, g_i)$ são homogêneos. Utilizando o Algoritmo de Buchberger obtemos uma base de Gröbner $G = \{f_1, \dots, f_s, f_{s+1}, \dots, f_m\}$ para I , onde f_{s+1}, \dots, f_m são obtidos como restos nas divisões dos S -polinômios por uma lista de f_i s e logo f_{s+1}, \dots, f_m são polinômios homogêneos pela proposição (2.3.11). Assim, temos uma base de Gröbner G para I formada por polinômios homogêneos.

(3) \Rightarrow (2):

É imediato.

□

Seja I um ideal homogêneo em $K[x_0, \dots, x_n]$. Vejamos que

$$V(I) = \{p \in \mathbb{P}^n(K) : f(p) = 0, \text{ para todo } f \in I\},$$

está bem definido como conjunto. Seja $[a_0 : \dots : a_n] = [b_0 : \dots : b_n] \in \mathbb{P}^n(K)$ e suponha que $f(a_0, \dots, a_n) = 0$, para todo $f \in I$. Queremos mostrar que $f(b_0, \dots, b_n) = 0$, para todo $f \in I$. Seja $f \in I$. Como $[a_0 : \dots : a_n] = [b_0 : \dots : b_n]$, existe $\lambda \in K^*$ tal que $(b_0, \dots, b_n) = \lambda(a_0, \dots, a_n)$. Como I é um ideal homogêneo, existem polinômios homogêneos $f_1, \dots, f_s \in K[x_0, \dots, x_n]$ tais que $I = (f_1, \dots, f_s)$ e $\text{grau}(f_i) = d_i$. Como $f \in I$, temos

$$f = g_1 f_1 + \dots + g_s f_s,$$

para alguns $g_1, \dots, g_s \in K[x_0, \dots, x_n]$. Temos $f_i(a_0, \dots, a_n) = 0$, para todo $i = 1, \dots, s$, logo

$$\begin{aligned} f(b_0, \dots, b_n) &= \sum_{i=1}^s g_i(b_0, \dots, b_n) f_i(b_0, \dots, b_n) = \sum_{i=1}^s g_i(\lambda a_0, \dots, \lambda a_n) f_i(\lambda a_0, \dots, \lambda a_n) \\ &= \sum_{i=1}^s g_i(\lambda a_0, \dots, \lambda a_n) \lambda^{d_i} f_i(a_0, \dots, a_n) = 0 \end{aligned}$$

Proposição 2.3.14. *Seja I um ideal homogêneo em $K[x_0, \dots, x_n]$ e suponha que $I = (f_1, \dots, f_s)$, onde f_1, \dots, f_s são polinômios homogêneos. Então*

$$V(I) = V(f_1, \dots, f_s).$$

Demonstração. Seja $p \in V(I)$. Como $f_1, \dots, f_s \in I$, temos $f_i(p) = 0$, para todo $i = 1, \dots, s$. Logo $p \in V(f_1, \dots, f_s)$.

Agora seja $q \in V(f_1, \dots, f_s)$. Dado $f \in I$, temos que

$$f = g_1 f_1 + \dots + g_s f_s,$$

para alguns $g_1, \dots, g_s \in K[x_0, \dots, x_n]$. Assim temos

$$f(q) = g_1(q) f_1(q) + \dots + g_s(q) f_s(q) = 0.$$

Portanto, $q \in V(I)$.

□

Proposição 2.3.15. *Seja $V \subseteq \mathbb{P}^n(K)$ uma variedade projetiva e seja*

$$I(V) = \{f \in K[x_0, \dots, x_n] : f(a_0, \dots, a_n) = 0, \text{ para todo } [a_0 : \dots : a_n] \in V\}.$$

Se K é infinito, então $I(V)$ é um ideal homogêneo em $K[x_0, \dots, x_n]$.

Demonstração. O fato de $I(V)$ ser um ideal se dá pelo fato de ser fechado para a soma e fechado para produtos com elementos de $K[x_0, \dots, x_n]$.

Seja $f \in I(V)$, digamos que $\text{grau}(f) = d$ e seja $a = [a_0 : \dots : a_n] \in V$. Escreva

$$f = \sum_{i=0}^d f_i,$$

onde f_0, \dots, f_d são as componentes homogêneas de f . Queremos mostrar que $f_i \in I(V)$, para todo $i = 0, \dots, d$.

Como $f \in I(V)$ e $[a_0 : \dots : a_n] \in V$ temos $f(\lambda a_0, \dots, \lambda a_n) = 0$, para todo $\lambda \in K^*$.
Observe que

$$f(\lambda a_0, \dots, \lambda a_n) = \sum_{i=0}^d f_i(\lambda a_0, \dots, \lambda a_n) = \sum_{i=0}^d \lambda^i f_i(a_0, \dots, a_n),$$

logo $\sum_{i=0}^d \lambda^i f_i(a_0, \dots, a_n) = 0$, para todo $\lambda \in K^*$.

Defina

$$p(x) = \sum_{i=0}^d x^i f_i(a_0, \dots, a_n) \in K[x].$$

Como $p(\lambda) = 0$, para todo $\lambda \in K^*$ e K^* é infinito, temos que $p = 0$, ou seja, todos os coeficientes de p são iguais a zero, isto é, $f_i(a_0, \dots, a_n) = 0$, para todo $i = 0, \dots, d$.

Como f_i é homogêneo temos que f_i se anula em todas as coordenadas homogêneas de a . Portanto, para cada $i = 0, \dots, d$ temos $f_i(a) = 0$, para todo $a \in V$, ou seja $f_i \in I(V)$. Isto prova que $I(V)$ é um ideal homogêneo. □

Proposição 2.3.16. *Seja $W \subseteq \mathbb{P}^n(K)$ uma variedade projetiva e suponha que $I(W)$ é um ideal homogêneo. Então $V(I(W)) = W$.*

Demonstração.

$$W \subseteq V(I(W)):$$

Dado $p \in W$ temos $f(p) = 0$ para todo $f \in I(W)$, logo $p \in V(I(W))$. Portanto, $W \subseteq V(I(W))$.

$$V(I(W)) \subseteq W:$$

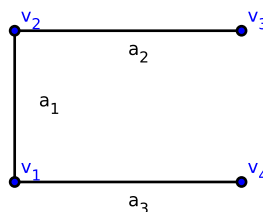
Como W é uma variedade projetiva, temos $W = V(f_1, \dots, f_s)$ para alguns polinômios homogêneos f_1, \dots, f_s . Seja $J = (f_1, \dots, f_s)$, temos $W = V(J)$. Assim, $I(W) = I(V(J))$. É claro que $J \subseteq I(V(J)) = I(W)$ e logo $V(I(W)) \subseteq V(J)$, ou seja, $V(I(W)) \subseteq W$. □

2.4 Grafos

Estudaremos agora o conceito de grafos, que serão usados na última parte deste trabalho.

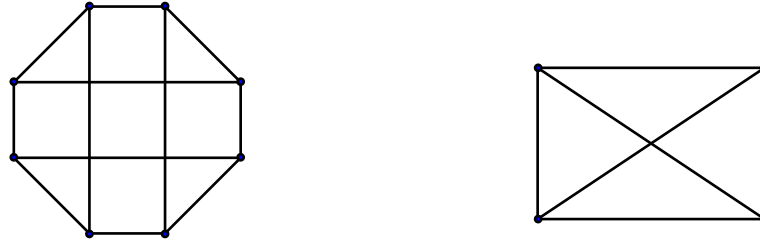
Um **grafo** G é uma estrutura formada por um par (V_G, A_G) , onde V_G é um conjunto finito não vazio e A_G é uma família de pares não ordenados de elementos de V_G , não necessariamente distintos. Os elementos de V_G são chamados **vértices** do grafo e os elementos de A_G são chamados **arestas**.

Exemplo 2.4.1. O grafo a seguir possui vértices $\{v_1, v_2, v_3, v_4\}$ e arestas $\{a_1, a_2, a_3\}$.



Um grafo G é dito **bipartido** se existe uma partição de V_G em dois conjuntos não vazios e disjuntos X e Y tais que toda aresta de G possui um vértice em X e outro em Y . Os conjuntos X e Y são chamados de conjunto partição. Se G contém todas as linhas ligando X a Y , dizemos que G é um grafo **completo**.

Exemplo 2.4.2. Os grafos a seguir são um grafo bipartido e um grafo completo, ambos sem os rótulos de vértices e arestas.



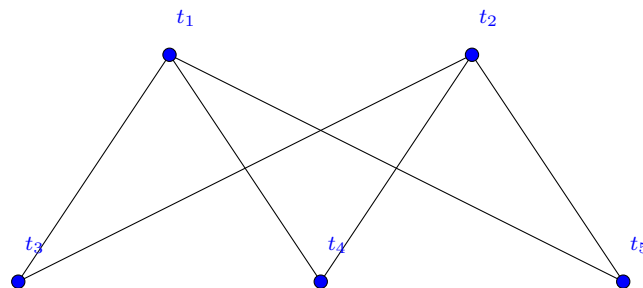
Dado um grafo G com vértices $V_G = \{v_1, \dots, v_m\}$ e arestas $A_G = \{a_1, \dots, a_n\}$, definimos a matriz $M = (m_{ij})$, chamada de **matriz de incidência** de G , por

$$m_{ij} = \begin{cases} 1, & \text{se o vértice } v_i \text{ é uma das pontas da aresta } a_j, \\ 0, & \text{caso contrário,} \end{cases}$$

para todo $i = 1, \dots, m$ e todo $j = 1, \dots, n$.

Denotaremos grafos que são bipartidos e completos por $\mathcal{K}_{m,n}$.

Exemplo 2.4.3. Considere o grafo bipartido completo $G = \mathcal{K}_{2,3}$ com vértices $V_G = \{t_1, t_2, t_3, t_4, t_5\}$.



Sua matriz de incidência é dada por

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Capítulo 3

Códigos produto

3.1 O produto tensorial

Sejam V e W espaços vetoriais sobre um corpo K . Desejamos definir um novo tipo de operação entre elementos de V e W . O resultado de tal produto deve estar em um espaço vetorial e, de forma geral, desejamos ter a distributividade usual neste produto. Em outras palavras, se denotamos $v \otimes w$ o produto dos elementos $v \in V$ e $w \in W$, então devemos ter as seguintes relações:

1. Se $v_1, v_2 \in V$ e $w \in W$, então

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w;$$

2. Se $w_1, w_2 \in W$ e $v \in V$, então

$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2;$$

3. Se $c \in K$, então

$$(cv) \otimes w = c(v \otimes w) = v \otimes cw.$$

Construiremos tal produto e provaremos algumas de suas propriedades.

Sejam U, V e W espaços vetoriais sobre K . Relembramos que uma aplicação bilinear

$$g : V \times W \longrightarrow U$$

é uma aplicação que para cada par de elementos (v, w) com $v \in V$ e $w \in W$ associa um elemento $g(v, w) \in U$, satisfazendo a seguinte propriedade: para cada $v \in V$, a aplicação $w \mapsto g(v, w)$ de W em U é linear, e para cada $w \in W$, a aplicação $v \mapsto g(v, w)$ de V em U é linear.

Teorema 3.1.1. *Sejam V, W espaços vetoriais de dimensão finita sobre um corpo K . Existe um espaço vetorial de dimensão finita T sobre K , e uma aplicação bilinear*

$$\begin{aligned} V \times W &\longrightarrow T \\ (v, w) &\longmapsto v \otimes w, \end{aligned}$$

satisfazendo as seguintes propriedades:

1. Se U é um espaço vetorial sobre K , e $g : V \times W \longrightarrow U$ é uma aplicação bilinear, então existe uma única aplicação linear

$$g_* : T \longrightarrow U$$

tal que para todos os pares (v, w) com $v \in V$ e $w \in W$ temos

$$g(v, w) = g_*(v \otimes w).$$

2. Se $\{v_1, \dots, v_n\}$ e $\{w_1, \dots, w_m\}$ são bases de V e W , respectivamente, então os elementos

$$v_i \otimes w_j \quad (i = 1, \dots, n \text{ e } j = 1, \dots, m)$$

formam uma base de T .

Demonstração. Sejam $\{v_1, \dots, v_n\}$ e $\{w_1, \dots, w_m\}$ bases de V e W , respectivamente. Para cada par (i, j) com $1 \leq i \leq n$ e $1 \leq j \leq m$ sejam t_{ij} símbolos. Vamos considerar T como o espaço vetorial sobre K consistindo de todas as combinações lineares formais destes elementos t_{ij} com coeficientes em K , de modo que estes elementos formam uma base de T sobre K . Assim os elementos de T consistem de combinações lineares

$$\sum_{i=1}^n \sum_{j=1}^m c_{ij} t_{ij}, \quad \text{com } c_{ij} \in K.$$

Se $v = x_1 v_1 + \dots + x_n v_n$ e $w = y_1 w_1 + \dots + y_m w_m$, com $x_i, y_i \in K$, então definimos $v \otimes w$ como o elemento

$$v \otimes w = \sum_{i=1}^n \sum_{j=1}^m x_i y_j t_{ij}$$

de T . Em particular, $v_i \otimes w_j = t_{ij}$. Vamos agora provar que o nosso produto $v \otimes w$ tem as propriedades requeridas no teorema. Vamos provar (2) inicialmente.

2. Sejam $\{v'_1, \dots, v'_n\}$ e $\{w'_1, \dots, w'_m\}$ bases de V e W , respectivamente. Devemos provar que os elementos $v'_i \otimes w'_j$ formam uma base de T . Quaisquer elementos $v \in V$ e $w \in W$ podem ser expressos como combinações lineares

$$v = x'_1 v'_1 + \dots + x'_n v'_n \text{ e } w = y'_1 w'_1 + \dots + y'_m w'_m,$$

com $x'_i, y'_i \in K$. Então

$$v \otimes w = \sum_{i=1}^n \sum_{j=1}^m x'_i y'_j (v'_i \otimes w'_j).$$

Dessa forma os elementos $v'_i \otimes w'_j$ geram T sobre K , e existem mn destes elementos. Se eles fossem linearmente dependentes, a dimensão de T seria estritamente menor que mn , contradizendo o fato dos elementos t_{ij} formarem uma base de T .

1. Provaremos que a aplicação $(v, w) \longmapsto v \otimes w$ é bilinear. Seja

$$v' = x'_1 v_1 + \dots + x'_n v_n$$

e sejam v, w expressos como combinações lineares das bases de elementos acima. Então

$$v + v' = (x_1 + x'_1)v_1 + \dots + (x_n + x'_n)v_n.$$

Por definição,

$$\begin{aligned}
 (v + v') \otimes w &= \sum_{i=1}^n \sum_{j=1}^m (x_i + x'_i) y_j t_{ij} \\
 &= \sum_{i=1}^n \sum_{j=1}^m (x_i y_j + x'_i y_j) t_{ij} \\
 &= \sum_{i=1}^n \sum_{j=1}^m (x_i y_j t_{ij} + x'_i y_j t_{ij}) \\
 &= \sum_{i=1}^n \sum_{j=1}^m x_i y_j t_{ij} + \sum_{i=1}^n \sum_{j=1}^m x'_i y_j t_{ij} \\
 &= v \otimes w + v' \otimes w.
 \end{aligned}$$

De maneira análoga mostra-se também que $v \otimes (w + w') = v \otimes w + v \otimes w'$.

Se $c \in K$, então

$$\begin{aligned}
 (cv) \otimes w &= \sum_{i=1}^n \sum_{j=1}^m (cx_i) y_j t_{ij} \\
 &= \sum_{i=1}^n \sum_{j=1}^m cx_i y_j t_{ij} \\
 &= c \sum_{i=1}^n \sum_{j=1}^m x_i y_j t_{ij} \\
 &= c(v \otimes w).
 \end{aligned}$$

Isto prova que o produto \otimes é bilinear.

Seja $g : V \times W \rightarrow U$ uma aplicação bilinear. Vimos em (2) que o conjunto $\{t_{ij} : 1 \leq i \leq n, 1 \leq j \leq m\}$ é uma base para T , logo existe uma única aplicação linear $g_* : T \rightarrow U$ tal que $g_*(t_{ij}) = g(v_i, w_j)$. Então para todo v, w expressos como acima através de combinações lineares das bases dadas,

$$\begin{aligned}
 g(v, w) &= g\left(\sum_{i=1}^n x_i v_i, \sum_{j=1}^m y_j w_j\right) \\
 &= \sum_{i=1}^n \sum_{j=1}^m x_i y_j g(v_i, w_j) \\
 &= g_*(v \otimes w).
 \end{aligned}$$

Assim a aplicação g_* em questão existe e é unicamente determinada.

Isto conclui a demonstração do teorema.

□

O espaço T no teorema anterior é chamado de **produto tensorial** de V e W e é denotado por $V \otimes W$. Da construção no teorema segue que sua dimensão é dada por

$$\dim(V \otimes W) = \dim V \cdot \dim W. \quad (3.1)$$

3.2 O produto direto e a imersão de Segre

Dados $A \subseteq \mathbb{F}_q^{n_1}$ e $B \subseteq \mathbb{F}_q^{n_2}$ códigos lineares com comprimento e dimensões iguais a n_1, n_2 e k_1, k_2 , respectivamente, segue do que foi feito acima que o código produto $A \otimes B$ possui

comprimento igual a $n_1 n_2$ e que a dimensão deste código é igual a $k_1 k_2$.

Sejam $C_1 \subset \mathbb{F}_q^{s_1}$ e $C_2 \subset \mathbb{F}_q^{s_2}$ dois códigos lineares e seja $M_{s_1 \times s_2}$ o espaço vetorial sobre \mathbb{F}_q de todas as matrizes de tamanho $s_1 \times s_2$ com entradas em \mathbb{F}_q . O **produto direto** (também chamado de produto de Kronecker) de C_1 e C_2 , denotado por $C_1 \underline{\otimes} C_2$, é definido como o código linear que consiste de todas as $s_1 \times s_2$ matrizes cujas linhas pertencem a C_2 e colunas pertencem a C_1 .

Veremos que o código produto possui parâmetros similares aos do produto tensorial e com a imersão de Segre, mostraremos que existe uma relação entre ambos.

Teorema 3.2.1. [10, Teorema 2.5.2] *Sejam $C_1 \subset K^{s_1}$ e $C_2 \subset K^{s_2}$ códigos lineares de comprimento s_1, s_2 e dimensão k_1, k_2 , respectivamente. Então $C_1 \underline{\otimes} C_2$ tem comprimento $s_1 s_2$ e dimensão $k_1 k_2$.*

Lema 3.2.2. [16, Lema 1] *Sejam D, D' subcódigos de A e E, E' subcódigos de B . Então*

1. $\text{supp}(D \underline{\otimes} E) = \text{supp}(D) \times \text{supp}(E)$;
2. $\text{supp}(D \underline{\otimes} E) \cap \text{supp}(D' \underline{\otimes} E') = [\text{supp}(D) \cap \text{supp}(D')] \times [\text{supp}(E) \cap \text{supp}(E')]$;
3. $\text{supp}(D \underline{\otimes} E) \cup \text{supp}(D' \underline{\otimes} E') = \text{supp}(D) \times [\text{supp}(E) \cup \text{supp}(E')]$.

Baseado no lema acima e em algumas propriedades básicas dos pesos de Hamming generalizados, temos o seguinte resultado:

Teorema 3.2.3. [16, Teorema 3] *Sejam A e B dois códigos lineares. Então*

1. $d_r(A \underline{\otimes} B) \leq \min\{d_{r_1}(A)d_{r_2}(B) : r_1 r_2 = r\}$;
2. $d_r(A \underline{\otimes} B) \leq \min\{d_{r_1}(A)d_{r_2}(B) - (r_1 r_2 - r) : r_1 r_2 \geq r\}$;
3. $d_1(A \underline{\otimes} B) = d_1(A)d_1(B)$;
4. $d_2(A \underline{\otimes} B) = \min\{d_1(A)d_2(B), d_2(A)d_1(B)\}$.

Dados $\mathbb{X}_1 \subset \mathbb{P}^{n-1}$ e $\mathbb{X}_2 \subset \mathbb{P}^{m-1}$, denotamos por $I(\mathbb{X}_1)$ e $I(\mathbb{X}_2)$ os **ideais anuladores** de \mathbb{X}_1 e \mathbb{X}_2 , ou seja, os ideais gerados pelos polinômios homogêneos de $K[x_1, \dots, x_n]$ e $K[x_1, \dots, x_m]$ que se anulam em todos os pontos de \mathbb{X}_1 e \mathbb{X}_2 , respectivamente.

A **imersão de Segre** é dada por

$$\begin{aligned} \psi : \mathbb{P}^{n-1} \times \mathbb{P}^{m-1} &\longrightarrow \mathbb{P}^{nm-1} \\ ([\alpha_1 : \dots : \alpha_n], [\beta_1 : \dots : \beta_m]) &\longmapsto [\alpha_1 \beta_1 : \alpha_1 \beta_2 : \dots : \alpha_1 \beta_m : \dots : \alpha_n \beta_1 : \alpha_n \beta_2 : \dots : \alpha_n \beta_m]. \end{aligned}$$

A aplicação ψ está bem definida e é injetora [7, pag. 13]. A imagem de $\mathbb{X}_1 \times \mathbb{X}_2$ pela aplicação ψ , denotada por \mathbb{X} é chamada de **produto de Segre** de \mathbb{X}_1 e \mathbb{X}_2 .

Definiremos agora o produto direto de códigos e veremos que através da imersão de Segre, podemos relacionar o produto direto com o produto tensorial.

Existe um isomorfismo natural $\text{vec} : M_{s_1 \times s_2}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^{s_1 s_2}$ de espaços vetoriais sobre \mathbb{F}_q dado por

$$\text{vec}(A) = (F_1, \dots, F_{s_1}),$$

onde F_1, \dots, F_{s_1} são as linhas de A . Considere a aplicação bilinear ψ_0 dada por

$$\begin{aligned} \psi_0 : \mathbb{F}_q^{s_1} \times \mathbb{F}_q^{s_2} &\longrightarrow M_{s_1 \times s_2}(\mathbb{F}_q) \\ ((a_1, \dots, a_{s_1}), (b_1, \dots, b_{s_2})) &\longmapsto \begin{bmatrix} a_1 b_1 & a_1 b_2 & \cdots & a_1 b_{s_2} \\ a_2 b_1 & a_2 b_2 & \cdots & a_2 b_{s_2} \\ \vdots & \vdots & & \vdots \\ a_{s_1} b_1 & a_{s_1} b_2 & \cdots & a_{s_1} b_{s_2} \end{bmatrix} \end{aligned}$$

A imersão de Segre, como definida anteriormente, é dada por

$$\psi([a], [b]) = [(\text{vec} \circ \psi_0)(a, b)],$$

onde $a = (a_1, \dots, a_{s_1})$ e $b = (b_1, \dots, b_{s_2})$. O próximo lema faz a conexão entre o produto direto e o produto tensorial.

Lema 3.2.4. *Existe um isomorfismo $T : C_1 \otimes C_2 \longrightarrow C_1 \underline{\otimes} C_2$ de espaços vetoriais sobre \mathbb{F}_q tal que*

$$T(a \otimes b) = \psi_0(a, b),$$

para $a \in C_1$ e $b \in C_2$.

Demonstração. Escreveremos $k_1 = \dim_K(C_1)$ e $k_2 = \dim_K(C_2)$. Restringindo ψ_0 ao produto $C_1 \times C_2$ e usando a propriedade universal do produto tensorial [5, pag. 573], temos que a aplicação bilinear ψ_0 induz uma aplicação linear

$$\begin{aligned} T : C_1 \otimes C_2 &\longrightarrow C_1 \underline{\otimes} C_2, \\ a \otimes b &\longmapsto \psi_0(a, b) \end{aligned}$$

para $a \in C_1$ e $b \in C_2$. Pela discussão inicial e pelo Teorema 3.2.1 sabemos que $C_1 \otimes C_2$ e $C_1 \underline{\otimes} C_2$ têm dimensão $k_1 k_2$. Dessa forma, provar que T é um isomorfismo consiste em provar que T é uma aplicação injetora.

Fixemos bases $\{\alpha_1, \dots, \alpha_{k_1}\}$ e $\{\beta_1, \dots, \beta_{k_2}\}$ de C_1 e C_2 , respectivamente. Tome um elemento γ no núcleo de T . Podemos escrever

$$\gamma = \sum \lambda_{i,j} \alpha_i \otimes \beta_j$$

com $\lambda_{i,j}$ em K , para todos i, j . Então

$$\begin{aligned} T(\gamma) &= \lambda_{1,1} T(\alpha_1 \otimes \beta_1) + \cdots + \lambda_{1,k_2} T(\alpha_1 \otimes \beta_{k_2}) + \\ &\quad \lambda_{2,1} T(\alpha_2 \otimes \beta_1) + \cdots + \lambda_{2,k_2} T(\alpha_2 \otimes \beta_{k_2}) + \\ &\quad \vdots \\ &\quad \lambda_{k_1,1} T(\alpha_{k_1} \otimes \beta_1) + \cdots + \lambda_{k_1,k_2} T(\alpha_{k_1} \otimes \beta_{k_2}). \end{aligned}$$

Escrevendo $\alpha_i = (\alpha_{i,1}, \dots, \alpha_{i,s_1})$, $\beta_j = (\beta_{j,1}, \dots, \beta_{j,s_2})$, para $i = 1, \dots, k_1$ e $j = 1, \dots, k_2$, obtemos

$$T(\gamma) = \begin{bmatrix} (\lambda_{1,1} \alpha_{1,1} \beta_1 + \cdots + \lambda_{1,k_2} \alpha_{1,1} \beta_{k_2}) + \cdots + (\lambda_{k_1,1} \alpha_{k_1,1} \beta_1 + \cdots + \lambda_{k_1,k_2} \alpha_{k_1,1} \beta_{k_2}) \\ (\lambda_{1,1} \alpha_{1,2} \beta_1 + \cdots + \lambda_{1,k_2} \alpha_{1,2} \beta_{k_2}) + \cdots + (\lambda_{k_1,1} \alpha_{k_1,2} \beta_1 + \cdots + \lambda_{k_1,k_2} \alpha_{k_1,2} \beta_{k_2}) \\ \vdots \\ (\lambda_{1,1} \alpha_{1,s_1} \beta_1 + \cdots + \lambda_{1,k_2} \alpha_{1,s_1} \beta_{k_2}) + \cdots + (\lambda_{k_1,1} \alpha_{k_1,s_1} \beta_1 + \cdots + \lambda_{k_1,k_2} \alpha_{k_1,s_1} \beta_{k_2}) \end{bmatrix}$$

Como $T(\gamma) = 0$, colocando os β_i 's em evidência, podemos escrever com a notação mencionada acima

$$\lambda_{1,j}\alpha_1^\top\beta_1 + \cdots + \lambda_{k_1,j}\alpha_{k_1}^\top\beta_{k_2} = 0, \text{ para } j = 1, \dots, k_2$$

e do fato de que os β_i são linearmente independentes, podemos escrever

$$\begin{aligned} \lambda_{1,1}\alpha_1^\top + \cdots + \lambda_{k_1,1}\alpha_{k_1}^\top &= 0 \\ \lambda_{1,2}\alpha_1^\top + \cdots + \lambda_{k_1,2}\alpha_{k_1}^\top &= 0 \\ &\vdots \\ \lambda_{1,k_2}\alpha_1^\top + \cdots + \lambda_{k_1,k_2}\alpha_{k_1}^\top &= 0. \end{aligned}$$

Agora, do fato de que os α_i são linearmente independentes segue que $\lambda_{i,j} = 0$ para todo i, j e assim $\gamma = 0$.

Portanto, $\ker(T) = \{0\}$ e temos que a aplicação T é um isomorfismo. \square

O teorema a seguir será utilizado na próxima seção com grafos bipartidos completos.

Teorema 3.2.5. *Seja K um corpo. Se $\mathbb{X}_1, \mathbb{X}_2$ são subconjuntos dos espaços projetivos $\mathbb{P}^{n-1}, \mathbb{P}^{m-1}$, respectivamente, e \mathbb{X} é o produto de Segre de \mathbb{X}_1 e \mathbb{X}_2 , então*

$$(K[x_1, \dots, x_n]/I(\mathbb{X}_1))_d \otimes (K[x_1, \dots, x_m]/I(\mathbb{X}_2))_d \simeq (K[\mathbf{x}]/I(\mathbb{X}))_d,$$

como espaços vetoriais sobre K para $d \geq 0$ e $K[\mathbf{x}] = K[x_{1,1}, \dots, x_{n,m}]$.

Demonstração. Seja σ o epimorfismo de K -álgebras

$$\begin{aligned} \sigma : K[\mathbf{t}] &\longrightarrow K[\{x_i y_j : i = 1, \dots, a_1, j = 1, \dots, a_2\}] \\ t_{ij} &\longmapsto x_i y_j. \end{aligned}$$

Para cada monômio $x^b y^c$ com $\deg(x^b) = \deg(y^c) = d$ existe um único monômio $t^a \in K[\mathbf{t}]_d$ tal que $t^a = t_{i_1, j_1} \cdots t_{i_d, j_d}$ com $1 \leq i_1 \leq \cdots \leq i_d$ e $1 \leq j_1 \leq \cdots \leq j_d$ e $\sigma(t^a) = x^b y^c$.

Observe que se $\sigma(t^\alpha) = x^b y^c$ para algum outro monômio $t^\alpha \in K[\mathbf{t}]_d$, então $t^a - t^\alpha \in I(\mathbb{X})$. Isto será usado pra garantir que a aplicação (3.2) é sobrejetora.

Definindo $\psi_0(x^b, y^c) = t^a$, obtemos uma aplicação bilinear sobre K

$$\psi_0 : K[\mathbf{x}]_d \times K[\mathbf{y}]_d \longrightarrow K[\mathbf{t}]_d$$

induzida por $\psi_0(x^b, y^c) = t^a$. Observe que

$$\psi_0\left(\sum \lambda_k x^{b_k}, \sum \mu_l y^{c_l}\right) = \sum \lambda_k \mu_l \psi_0(x^{b_k}, y^{c_l}),$$

onde os λ_k 's e μ_l 's pertencem a K . Para mostrar que ψ_0 induz uma aplicação bilinear sobre K

$$\begin{aligned} \psi : (K[\mathbf{x}]_d/I(\mathbb{X}_1)_d \times (K[\mathbf{y}]_d/I(\mathbb{X}_2)_d) &\longrightarrow K[\mathbf{t}]_d/I(\mathbb{X})_d \\ (\overline{x^b}, \overline{y^c}) &\longmapsto \overline{\psi_0(x^b, y^c)}, \end{aligned} \quad (3.2)$$

que é sobrejetora, basta mostrar que para todo $f \in K[\mathbf{x}]_d$ que se anula em \mathbb{X}_1 e todo $g \in K[\mathbf{y}]_d$ que se anula em \mathbb{X}_2 temos que $\psi_0(f, g)$ se anula em todos os pontos de \mathbb{X} .

Suponha que $f = \lambda_1 x^{b_1} + \cdots + \lambda_m x^{b_m}$ é um polinômio em $K[\mathbf{x}]_d$ que se anula em \mathbb{X}_1 e que $g = \mu_1 y^{c_1} + \cdots + \mu_r y^{c_r}$ é um polinômio em $K[\mathbf{y}]_d$ com λ_k, μ_l em K para todo k, l . Para cada monômio $x^{b_k} y^{c_l}$ existe um monômio $t^{a_{kl}} \in K[\mathbf{t}]$ tal que $\sigma(t^{a_{kl}}) = x^{b_k} y^{c_l}$. Então

$$\begin{aligned} \psi_0(f, g) &= \sum \lambda_k \mu_l \psi_0(x^{b_k}, y^{c_l}) = \sum \lambda_k \mu_l t^{a_{kl}} \\ \psi_0(f, g)(x_i y_j) &= (\lambda_1 x^{b_1} + \cdots + \lambda_m x^{b_m})(\mu_1 y^{c_1} + \cdots + \mu_r y^{c_r}), \end{aligned}$$

onde usamos $(x_i y_j)$ para representar $(x_1 y_1, x_1 y_2, \dots, x_1 y_{a_2}, \dots, x_{a_1} y_1, x_{a_1} y_2, \dots, x_{a_1} y_{a_2})$. Agora se $[\alpha_1 : \dots : \alpha_{a_1}] \in \mathbb{X}_1$ e $[\beta_1 : \dots : \beta_{a_2}] \in \mathbb{X}_2$, tomando $x_i = \alpha_i$ e $y_j = \beta_j$ para todo i, j na última igualdade, obtemos $\psi_0(f, g)(\alpha_i \beta_j) = 0$. Portanto, pela propriedade universal do produto tensorial, existe uma aplicação sobrejetora $\bar{\psi}$ que faz o seguinte diagrama comutar

$$\begin{array}{ccc} (K[\mathbf{x}]_d/I(\mathbb{X}_1)_d) \times (K[\mathbf{y}]_d/I(\mathbb{X}_2)_d) & \xrightarrow{\phi} & (K[\mathbf{x}]_d/I(\mathbb{X}_1)_d) \otimes (K[\mathbf{y}]_d/I(\mathbb{X}_2)_d) \\ \downarrow \varphi & & \nwarrow \bar{\varphi} \\ K[\mathbf{t}]_d/I(\mathbb{X})_d & & \end{array}$$

onde ϕ é a aplicação canônica, dada por $\phi(\bar{f}, \bar{g}) = \bar{f} \otimes \bar{g}$ e $\psi = \bar{\psi}\phi$.

Para cada monômio $t^\alpha \in K[\mathbf{t}]_d$ sejam $x^b \in K[\mathbf{x}]_d$ e $y^c \in K[\mathbf{y}]_d$ monômios tais que $\sigma(t^\alpha) = x^b y^c$. Definimos $\sigma_1(t^\alpha) = x^b$ e $\sigma_2(t^\alpha) = y^c$. Assim temos uma aplicação linear sobre K sobrejetora

$$\sigma_0^* : K[\mathbf{t}]_d \longrightarrow K[\mathbf{x}]_d/I(\mathbb{X}_1)_d \otimes K[\mathbf{y}]_d/I(\mathbb{X}_2)_d$$

dada por $\sigma_0^* : (\sum \lambda_\alpha t^\alpha) \mapsto \sum \lambda_\alpha \overline{\sigma_1(t^\alpha)} \otimes \overline{\sigma_2(t^\alpha)}$, onde os λ_α 's estão em K . Observe que o K -espaço vetorial do lado direito é gerado por todos os $\overline{x^b} \otimes \overline{y^c}$ tais que $x^b \in K[\mathbf{x}]_d$ e $y^c \in K[\mathbf{y}]_d$. Tome $f \in I(\mathbb{X})_d$, então $\sigma(f)(\alpha_i \beta_j) = 0$ para todo $\alpha = [\alpha_1 : \dots : \alpha_{a_1}] \in \mathbb{X}_1$ e todo $\beta = [\beta_1 : \dots : \beta_{a_2}] \in \mathbb{X}_2$. Podemos escrever $\sigma(f) = \sum_{l=1}^k f_l g_l$ com $f_l \in K[\mathbf{x}]_d$ e $g_l \in K[\mathbf{y}]_d$ para $l = 1, \dots, k$ e $\sigma_0^*(f) = \sum_{l=1}^k \overline{f_l} \otimes \overline{g_l}$.

Mostraremos agora, por indução em k , que $\sigma_0^*(f) = 0$, isto é, $f \in \ker(\sigma_0^*)$. Se $k = 1$, podemos assumir que $f_1 \notin I(\mathbb{X}_1)$ pois caso contrário $\overline{f_1} = \bar{0}$. Escolha $\alpha \in \mathbb{X}_1$ tal que $f_1(\alpha) \neq 0$. Então, se $f_1(\alpha)g_1(\beta) = 0$ para todo $\beta \in \mathbb{X}_2$, temos que $g_1 \in I(\mathbb{X}_2)$ e $\overline{g_1} = \bar{0}$. Suponhamos agora que $k > 1$ e $\overline{f_k} \neq 0$. Escolha $\alpha \in \mathbb{X}_1$ tal que $f_k(\alpha) \neq 0$. Pela hipótese o polinômio

$$f_1(\alpha)g_1 + \dots + f_k(\alpha)g_k$$

está em $K[\mathbf{y}]_d$ e se anula em todos os pontos de \mathbb{X}_2 . Assim

$$\overline{g_k} = - \left(\frac{f_1(\alpha)}{f_k(\alpha)} \right) \overline{g_1} - \dots - \left(\frac{f_{k-1}(\alpha)}{f_k(\alpha)} \right) \overline{g_{k-1}}.$$

Portanto, definindo $h_l = f_l - (f_l(\alpha)/f_k(\alpha))f_k$ para $l = 1, \dots, k-1$, obtemos

$$\sigma_0^*(f) = \sum_{l=1}^k \overline{f_l} \otimes \overline{g_l} = \sum_{l=1}^{k-1} \overline{h_l} \otimes \overline{g_l}$$

e $\sum_{l=1}^{k-1} h_l(\gamma)g_l(\beta) = 0$ para todo $\gamma \in \mathbb{X}_1$ e $\beta \in \mathbb{X}_2$. Assim, por indução, $\sigma_0^*(f) = 0$. Dessa forma $I(\mathbb{X})_d \subset \ker(\sigma_0^*)$. Portanto σ_0^* induz uma sobrejeção linear sobre K

$$\sigma_0^* : K[\mathbf{t}]_d/I(\mathbb{X})_d \longrightarrow (K[\mathbf{x}]_d/I(\mathbb{X}_1)_d) \otimes (K[\mathbf{y}]_d/I(\mathbb{X}_2)_d).$$

Concluimos então que as aplicações lineares $\bar{\psi}$ e σ^* são bijeções. □

Capítulo 4

Códigos parametrizados

Seja $L = \mathbb{F}_q[Z_1, \dots, Z_n] = \bigoplus_{d \geq 0} L_d$ o anel polinomial com n variáveis. Considere o seguinte conjunto de m monômios

$$\mathbf{Z}^{a_1}, \dots, \mathbf{Z}^{a_m}, \quad (4.1)$$

onde cada $\mathbf{Z}^{a_i} = Z_1^{a_{i1}} \dots Z_n^{a_{in}}$ e a_{ij} é um inteiro não negativo para todo $i = 1, \dots, m$, $j = 1, \dots, n$.

Um **conjunto tórico** parametrizado pelos monômios dados em (4.1) é o seguinte subconjunto do espaço projetivo \mathbb{P}^{m-1}

$$X = \{[\mathbf{t}^{a_1} : \dots : \mathbf{t}^{a_m}] \in \mathbb{P}^{m-1} : t_i \in \mathbb{F}_q^*, \quad (4.2)$$

onde $\mathbf{t}^{a_i} = t_1^{a_{i1}} \dots t_n^{a_{in}}$, para todo $i = 1, \dots, m$, e $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$.

Além disso, consideremos $S = \mathbb{F}_q[X_1, \dots, X_m] = \bigoplus_{d \geq 0} S_d$ como outro anel de polinômios, graduado usualmente. Seja $X = \{P_1, \dots, P_{|X|}\}$ o conjunto tórico dado em (4.2) e consideremos a aplicação de avaliação

$$\begin{aligned} av_d : S_d &\rightarrow \mathbb{F}_q^{|X|} \\ f &\mapsto av_d(f) := \left(\frac{f(P_1)}{X_1^d(P_1)}, \dots, \frac{f(P_{|X|})}{X_1^d(P_{|X|})} \right). \end{aligned}$$

Estaremos interessados na imagem desta aplicação, que é uma aplicação linear entre os \mathbb{F}_q -espaços vetoriais S_d e $\mathbb{F}_q^{|X|}$

Proposição 4.0.1. *A aplicação avaliação, como definida acima, é uma aplicação linear.*

Demonstração. Claramente S_d e $\mathbb{F}_q^{|X|}$ são \mathbb{F}_q -espaços vetoriais. Sejam $f, g \in S_d$ e $\lambda \in \mathbb{F}_q$. Segue que

$$\begin{aligned} av_d(f + \lambda g) &= \left(\frac{f + \lambda g(P_1)}{X_1^d(P_1)}, \dots, \frac{f + \lambda g(P_{|X|})}{X_1^d(P_{|X|})} \right) \\ &= \left(\frac{f(P_1)}{X_1^d(P_1)}, \dots, \frac{fg(P_{|X|})}{X_1^d(P_{|X|})} \right) + \left(\frac{\lambda g(P_1)}{X_1^d(P_1)}, \dots, \frac{\lambda g(P_{|X|})}{X_1^d(P_{|X|})} \right) \\ &= \left(\frac{f(P_1)}{X_1^d(P_1)}, \dots, \frac{fg(P_{|X|})}{X_1^d(P_{|X|})} \right) + \lambda \left(\frac{g(P_1)}{X_1^d(P_1)}, \dots, \frac{g(P_{|X|})}{X_1^d(P_{|X|})} \right) \\ &= av_d(f) + \lambda av_d(g). \end{aligned}$$

□

O **código parametrizado de ordem** d associado ao conjunto tórico X , ou o código de ordem d parametrizado pelos monômios (4.1), é a imagem da aplicação avaliação av_d e é denotado por $C_X(d)$. Portanto

$$C_X(d) = \left\{ \left(\frac{f(P_1)}{X_1^d(P_1)}, \dots, \frac{f(P_{|X|})}{X_1^d(P_{|X|})} \right) : f \in S_d \right\}. \quad (4.3)$$

Estudaremos agora o caso em que o conjunto parametrizado é um toro no espaço projetivo.

Um **toro projetivo** em \mathbb{P}^{n-1} é um conjunto tórico parametrizado pelos monômios Z_1, \dots, Z_n , isto é,

$$\mathbb{T}_{n-1} = \{[t_1 : \dots : t_n] \in \mathbb{P}^{n-1} : t_i \in \mathbb{F}_q^* \text{ para todo } i\}, \quad (4.4)$$

e o código parametrizado de ordem d associado a este toro projetivo é o subespaço de $\mathbb{F}_q^{|\mathbb{T}_{n-1}|}$ dado por

$$C_{\mathbb{T}_{n-1}}(d) = \left\{ \left(\frac{g(R_1)}{Z_1^d(R_1)}, \dots, \frac{g(R_{|\mathbb{T}_{n-1}|})}{Z_1^d(R_{|\mathbb{T}_{n-1}|})} \right) : g \in L_d \right\}, \quad (4.5)$$

onde $\mathbb{T}_{n-1} = \{R_1, \dots, R_{|\mathbb{T}_{n-1}|}\}$ e $|\mathbb{T}_{n-1}| = (q-1)^{n-1}$.

Exemplo 4.0.2. Veremos neste exemplo em que o caso $q = 2$ é trivial.

Suponha que $q = 2$ e seja d qualquer. Segue então que $\mathbb{F}_q = \mathbb{F}_2$ logo $\mathbb{F}_2^* = \{1\}$, assim $X = \{[1 : \dots : 1]\} = \mathbb{T}_{n-1}$ e portanto $|X| = |\mathbb{T}_{n-1}| = 1$. Agora, escolhendo os polinômios homogêneos $f_1 = X_1^d$ e $f_2 = X_1^d + X_2^d$, temos que a imagem através da aplicação de avaliação será sobrejetora, logo $C_X(d) = \mathbb{F}_2^n$. Assim, a distância mínima do código $C_X(d)$ é 1.

Se $d = 0$ temos que S_d é o conjunto de polinômios constantes que assumem valores em \mathbb{F}_q . Desta forma $C_X(d) = \{(\beta, \dots, \beta) : \beta \in \mathbb{F}_q\}$, $H_X(d) = 1$ e a distância mínima de $C_X(d)$ é $|X|$.

Relembramos que $I(X)$ é o ideal anulador de X gerado pelos polinômios homogêneos de S que se anulam em todos os pontos de X . O conjunto S_d é um K -espaço vetorial de dimensão $\binom{d+s-1}{s-1}$. Definimos

$$I(X)_d := I(X) \cap S_d,$$

como o conjunto de polinômios homogêneos em $I(X)$ de grau total d , junto do polinômio zero. Note que $I(X)_d$ é um subespaço vetorial de S_d . O núcleo da aplicação avaliação é exatamente $I(X)_d$, logo existe um isomorfismo de K -espaços vetoriais $S_d/I(X)_d \simeq C_X(d)$.

A **função de Hilbert** do anel quociente $S/I(X)$, denotada por $H_X(d)$, é definida como

$$H_X(d) := \dim_K(S_d/I(X)_d).$$

De acordo com um resultado clássico sobre polinômios de Hilbert [2, Teorema 4.1.3], existe um único polinômio

$$h_X(t) = c_k t^k + (\text{termos de grau inferior})$$

de grau $k \geq 0$, com coeficientes racionais, tal que $h_X(d) = H_X(d)$ para d suficientemente grande. O inteiro $k+1$ é a **dimensão de Krull** de $S/I(X)$, k é a dimensão de X , e $h_X(t)$ é o **polinômio de Hilbert** de $S/I(X)$. O inteiro positivo $c_k(k!)$ é o grau de $S/I(X)$. O **índice de regularidade** de $S/I(X)$, denotado por $\text{reg}(S/I(X))$ é o menor inteiro $r \geq 0$ tal que $h_X(d) = H_X(d)$ para $d \geq r$.

A seguinte proposição sumariza as relações entre os códigos projetivos definidos acima e a teoria de funções de Hilbert.

Proposição 4.0.3. [13, Proposição 2.7] As seguintes afirmações são verdadeiras:

1. $H_X(d) = \dim_K C_X(d)$ para $d \geq 0$;
2. $d_X(d) = 1$ para $d \geq \text{reg}(S/I(X))$;
3. $C_X(d) \neq (0)$ para $d \geq 0$.

Trabalharemos então assumindo que $q > 2$ e $d \geq 1$.

4.1 Cotas para códigos parametrizados

Seja \mathbb{F}_q um corpo finito com q elementos. Nesta seção usaremos o comportamento do código $C_{\mathbb{T}_1}(d)$ para encontrar a hierarquia de pesos do código parametrizado pelas arestas do ciclo C_4 , e uma cota superior para os pesos de Hamming generalizados do código associado com o grafo bipartido completo $\mathcal{K}_{2,n}$.

Exemplo 4.1.1. Vamos calcular explicitamente o código $C_{\mathbb{T}_1}(2)$ e seus parâmetros.

Suponha que $q = 3$, logo $\mathbb{T}_1 = \{[1 : 1], [1 : 2]\}$ e $C_{\mathbb{T}_1}(2)$ é um subespaço de \mathbb{F}_3^2 .

Temos $L_2 = \{x^2, y^2, 2x^2, 2y^2, x^2 + y^2, x^2 + 2y^2, 2x^2 + y^2, 2x^2 + 2y^2, x^2 + xy, y^2 + xy, 2x^2 + xy, 2y^2 + xy, x^2 + y^2 + xy, x^2 + 2y^2 + xy, 2x^2 + y^2 + xy, 2x^2 + 2y^2 + xy, x^2 + 2xy, y^2 + 2xy, 2x^2 + 2xy, 2y^2 + 2xy, x^2 + y^2 + 2xy, x^2 + 2y^2 + 2xy, 2x^2 + y^2 + 2xy, 2x^2 + 2y^2 + 2xy, xy, 2xy\}$.

Avaliando os pontos de \mathbb{T}_1 nos polinômios acima obtemos

$$C_{\mathbb{T}_1}(2) = \{00, 10, 01, 11, 12, 21, 20, 02, 22\}.$$

Segue que os seu comprimento é 9, sua dimensão é 2 (pois $\{10, 01\}$ geram o código), sua distância mínima é 1 e seu segundo peso de Hamming generalizado é 2.

Em geral, para $q = 3$ e d qualquer, o índice de regularidade é $q - 2$, a dimensão é $H_{\mathbb{T}_1} = 2$ para todo $d \geq 1$. Então $C_{\mathbb{T}_1}(d) = \mathbb{F}_3^2$, $d_1(C_{\mathbb{T}_1}(d)) = 1$, e $d_2(C_{\mathbb{T}_1}(d)) = 2$.

Motivados pelo exemplo acima, apenas nesta seção suporemos que $q > 3$. O resultado a seguir nos garante que $C_{\mathbb{T}_1}(d)$ é um código MDS e nos dá uma fórmula para a sua distância mínima.

Proposição 4.1.2. [12, Proposição 3.6] Se X é um toro projetivo em \mathbb{P}^1 , então $C_X(d)$ é um código MDS e sua distância mínima é dada por

$$\delta_d = \begin{cases} q - 1 - d & \text{se } 1 \leq d \leq q - 3 \\ 1 & \text{se } d > q - 2, \end{cases}$$

Se X é um toro projetivo em \mathbb{P}^2 , então a distância mínima de $C_X(d)$ é dada por

$$\delta_d = \begin{cases} (q - 1)^2 - d(q - 1) & \text{se } 1 \leq d \leq q - 2 \\ 2q - d - 3 & \text{se } q - 1 \leq d \leq 2q - 5 \\ 1 & \text{se } d > 2q - 4. \end{cases}$$

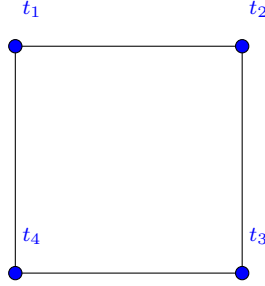
Em [6] temos um resultado que diz que código $C_{\mathbb{T}_1}(d)$ é um código r -MDS e vale

$$d_r(C_{\mathbb{T}_1}(d)) = \begin{cases} q + r - d - 2 & \text{se } 1 \leq d \leq q - 3 \\ r & \text{se } d > q - 3, \end{cases} \quad (4.6)$$

para todo $r = 1, \dots, d + 1$. Isto juntamente com o fato de que o comprimento do código $C_{\mathbb{T}_1}(d)$ é $|\mathbb{T}_1| = q - 1$, sua dimensão é $H_{\mathbb{T}_1}(d) = d + 1$ para todo $1 \leq d \leq q - 3$ e $H_{\mathbb{T}_1}(d) = q - 1$

para todo $d \geq q - 2$.

Considere agora o ciclo C_4 dado pela figura a seguir:



O conjunto tórico parametrizado pelas arestas do ciclo C_4 é dado por

$$X = \{[t_1 t_2 : t_2 t_3 : t_3 t_4 : t_4 t_1] \in \mathbb{P}^3 : t_i \in \mathbb{F}_q^*\}.$$

O código $C_X(d)$ tem comprimento $|X| = (q-1)^2$, dimensão $H_X(d) = (d+1)^2$ se $1 \leq d \leq q-2$ e índice de regularidade dado por $q-2$. Observe que C_4 é o grafo bipartido completo $\mathcal{K}_{2,2}$, e o código parametrizado pelas arestas deste grafo é $C_{T_1}(d) \otimes C_{T_1}(d)$, onde \otimes é o produto tensorial de espaços lineares. Como vimos antes, $C_{T_1}(d)$ é um código *MDS* e podemos assim computar os pesos de Hamming generalizados de $C_X(d)$.

Temos

$$d_r(C_X(d)) = \begin{cases} \min\{(q-1-d)(q-d+s+a-2) + r - s - a\} & \text{se } 1 \leq d \leq q-3 \\ r & \text{se } d > q-3, \end{cases}$$

onde s, a são inteiros que satisfazem $r = sa + t$, $1 \leq a \leq m$, $m = \max\{b \in \mathbb{Z} : b^2 \leq r\}$, $0 \leq s \leq d+1$, e $0 < t \leq a$. Em particular, se considerarmos a distância mínima do código $C_X(d)$ obtemos

$$d_1(C_X(d)) = \begin{cases} (q-1-d)^2 & \text{se } 1 \leq d \leq q-3 \\ 1 & \text{se } d > q-3, \end{cases}$$

e o segundo peso de Hamming generalizado é dado por

$$d_2(C_X(d)) = \begin{cases} (q-1-d)(q-d) & \text{se } 1 \leq d \leq q-3 \\ 2 & \text{se } d > q-3. \end{cases}$$

Inclusive se tomarmos o grafo bipartido completo $\mathcal{K}_{2,n}$ com $n \geq 3$, obtemos uma cota superior explícita para o r -ésimo peso de Hamming generalizado do código parametrizado por suas arestas.

Lema 4.1.3. [12, Proposição 3.5] Se $X = \{[x_1 : \dots : x_s] \in \mathbb{P}^{s-1} : x_i \in \mathbb{F}_q^* \text{ para todo } i\}$ é um toro projetivo em \mathbb{P}^{s-1} e $d \geq 1$, então a distância mínima de $C_X(d)$ é dada por

$$\delta_d = \begin{cases} (q-1)^{s-(k+2)}(q-1-l) & \text{se } d \leq (q-2)(s-1) - 1, \\ 1 & \text{se } d \geq (q-2)(s-1), \end{cases}$$

onde k e l são os únicos inteiros tais que $k \geq 0$, $1 \leq l \leq q-2$ e $d = k(q-2) + l$.

Proposição 4.1.4. *Seja X o conjunto tórico associado as arestas do grafo bipartido completo $\mathcal{K}_{2,n}$, com $n \geq 3$. O r -ésimo peso de Hamming generalizado do código $C_X(d)$ parametrizado por suas arestas, $1 \leq r \leq H_X(d)$ é limitado por*

$$d_r(C_X(d)) \leq \begin{cases} (q-1)^{n-2}(q-1-d)(q+r-d-2) & \text{se } 1 \leq d \leq q-3 \\ r(q-1)^{n-(k+2)}(q-1-l) & \text{se } q-3 < d < (q-2)(n-1), \end{cases}$$

e $d_r(C_X(d)) = r$ para $d \geq (q-2)(n-1)$, onde k e l são os inteiros únicos tais que $k \geq 0, 1 \leq l \leq q-2$ e $d = k(q-2) + l$. Se $r = 1$ a igualdade é verificada.

Demonstração. Como o índice de regularidade associado ao grafo $\mathcal{K}_{2,n}$ é $(q-2)(n-1)$, se $d \geq (q-2)(n-1)$ então $C_X(d) = \mathbb{F}_q^{|X|}$ e neste caso, $d_r(C_X(d)) = r$. Além disso sabemos que se $C_X(d)$ é o produto tensorial $C_{\mathbb{T}_1} \otimes C_{\mathbb{T}_{n-1}}(d)$. Assim,

$$d_r(C_X(d)) \leq d_r(C_{\mathbb{T}_1}(d)) \cdot d_1(C_{\mathbb{T}_{n-1}}(d)). \quad (4.7)$$

Se $1 \leq d \leq q-3$ então pela equação (4.6) temos

$$d_r(C_{\mathbb{T}_1}(d)) = q + r - d - 2. \quad (4.8)$$

Ainda $d = 0 \cdot (q-2) + l$ e assim $k = 0, l = d$ na fórmula para a distância mínima do toro projetivo. Logo

$$d_1(C_{\mathbb{T}_{n-1}}(d)) = (q-1)^{n-2}(q-1-d). \quad (4.9)$$

Das equações (4.7) e (4.9) concluímos que

$$d_r(C_X(d)) \leq (q-1)^{n-2}(q-1-d)(q+r-d-2).$$

O caso $q-3 < d < (q-2)(n-1)$ é similar. Se $r = 1$ então $d_1(C_X(d)) = d_1(C_{\mathbb{T}_1}(d)) \cdot d_1(C_{\mathbb{T}_{n-1}}(d))$, e o resultado segue. \square

4.1.1 O grafo bipartido completo $\mathcal{K}_{m,n}$

A seguir apresentaremos um exemplo de um grafo bipartido completo. Listaremos alguns resultados importantes quando X é um conjunto tórico, afim de calcular os parâmetros do código associado a este grafo.

Seja $\mathcal{K}_{m,n}$ um grafo bipartido completo. A matriz de incidência associada a $\mathcal{K}_{m,n}$ é a matriz $B = (b_{ij})$, de ordem $(m+n) \cdot (mn)$ com $b_{ij} = 1$ se o vértice v_i e a aresta a_j são incidentes e $b_{ij} = 0$ caso contrário. Em geral, a variedade tórica X associada à matriz de incidência do grafo bipartido completo $\mathcal{K}_{m,n}$ é dada por

$$X = \{[t_1 t_{m+1} : \cdots : t_1 t_{m+n} : \cdots : t_m t_{m+1} : \cdots : t_m t_{m+n}] : t_i \in \mathbb{F}_q^* \text{ para todo } i = 1, \dots, m+n\}.$$

Escolhendo a primeira coordenada, podemos reescrever X como

$$X = \{[1 : \alpha_1 : \cdots : \alpha_{n-1} : \beta_1 : \alpha_1 \beta_1 : \cdots : \alpha_{n-1} \beta_1 : \cdots : \beta_{m-1} : \alpha_1 \beta_{m-1} : \cdots : \alpha_{n-1} \beta_{m-1}]\}.$$

Sejam

$$X_1 = \{[1 : \alpha_1 : \cdots : \alpha_{n-1}] : \alpha_1, \dots, \alpha_{n-1} \in \mathbb{F}_q^*\} \text{ e } X_2 = \{[1 : \beta_1 : \cdots : \beta_{m-1}] : \beta_1, \dots, \beta_{m-1} \in \mathbb{F}_q^*\}.$$

É claro que $|X_1| = (q-1)^{n-1}$ e $|X_2| = (q-1)^{m-1}$.

Lema 4.1.5. Com a notação utilizada acima, o comprimento do código de avaliação associado à matriz de incidência do grafo bipartido completo $\mathcal{K}_{m,n}$ é dado por

$$s = (q - 1)^{m+n-2}.$$

Demonstração. Considere ψ a seguinte aplicação

$$\begin{aligned} \psi : \mathbb{P}^{n-1} \times \mathbb{P}^{m-1} &\rightarrow \mathbb{P}^{nm-1} \\ (x, y) &\mapsto [1 : \alpha_1 : \cdots : \alpha_{n-1} : \cdots : \beta_{m-1} : \alpha_1\beta_{m-1} : \cdots : \alpha_{n-1}\beta_{m-1}], \end{aligned}$$

com $x = [1 : \alpha_1 : \cdots : \alpha_{n-1}]$ e $y = [1 : \beta_1 : \cdots : \beta_{m-1}]$, restrita ao conjunto $X_1 \times X_2 \subseteq \mathbb{P}^{n-1} \times \mathbb{P}^{m-1}$. Segue que a imagem desta aplicação é o conjunto X . Além disso, como esta aplicação é sobrejetora, concluímos que

$$s = |X| = |X_1| \cdot |X_2| = (q - 1)^{m-1}(q - 1)^{n-1} = (q - 1)^{m+n-2}.$$

□

Lema 4.1.6. A dimensão do código de avaliação de ordem d associada a matriz de incidência do grafo bipartido completo $\mathcal{K}_{m,n}$ é dada por

$$\dim_{\mathbb{F}_q} C_X(d) = H_{X_1}(d) \cdot H_{X_2}(d).$$

Demonstração. Seja

$$\begin{aligned} \theta_1 : \mathbb{F}_q[X_0, \dots, X_{n-1}]_d &\rightarrow \mathbb{F}_q^{s_1} \\ g &\mapsto (g(Q_1), \dots, g(Q_{s_1})), \end{aligned}$$

onde $s_1 = (q - 1)^{n-1}$ e $X_1 = \{Q_1, \dots, Q_{s_1}\}$. Então $C_{X_1}(d)$ é a imagem desta aplicação e

$$\mathbb{F}_q[X_0, \dots, X_{n-1}]_d / I_{X_1}(d) \simeq C_{X_1}(d).$$

De forma análoga, definimos

$$\begin{aligned} \theta_2 : \mathbb{F}_q[Y_0, \dots, Y_{m-1}]_d &\rightarrow \mathbb{F}_q^{s_2} \\ h &\mapsto (h(R_1), \dots, h(R_{s_2})), \end{aligned}$$

onde $s_2 = (q - 1)^{m-1}$ e $X_2 = \{R_1, \dots, R_{s_2}\}$. Então $C_{X_2}(d)$ é a imagem desta aplicação e

$$\mathbb{F}_q[Y_0, \dots, Y_{m-1}]_d / I_{X_2}(d) \simeq C_{X_2}(d).$$

Agora, pelo Teorema 3.2.5 vale o seguinte isomorfismo

$$\mathbb{F}_q[X_0, \dots, X_{n-1}]_d / I_{X_1}(d) \otimes \mathbb{F}_q[Y_0, \dots, Y_{m-1}]_d / I_{X_2}(d) \simeq \mathbb{F}_q[Z_{00}, \dots, Z_{(m-1)(n-1)}] / I_X(d),$$

o que completa a demonstração. □

Lema 4.1.7. A distância mínima do código de avaliação de ordem d associado a matriz de incidência do grafo bipartido completo $\mathcal{K}_{m,n}$, $\delta_X(d)$, é dada por

$$\delta_X(d) = \delta_{X_1}(d) \cdot \delta_{X_2}(d).$$

Demonstração. Seja $f \in \mathbb{F}_q[Z_{00}, \dots, Z_{(n-1)(m-1)}]_d$ e $X = \{P_{11}, \dots, P_{s_1 s_2}\}$ onde $s_1 = (q-1)^{n-1}$ e $s_2 = (q-1)^{m-1}$. Seja $\Gamma = (f(P_{11}), \dots, f(P_{s_1 s_2})) \in C_X(d) - \{0\}$. Sabemos que se ψ é a aplicação de Segre restrita a $X_1 \times X_2$ então, para todo i, j , podemos encontrar $Q_i \in X_1$ e $R_j \in X_2$ de modo que $\psi(Q_i, R_j) = P_{ij}$. Assim

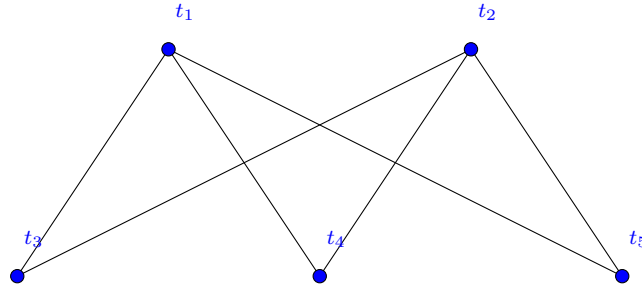
$$\Gamma = (f(X_0 Y_0, \dots, X_{n-1} Y_{m-1})(Q_1, R_1), f(X_0 Y_0, \dots, X_{n-1} Y_{m-1})(Q_{s_1} R_{s_2})).$$

Se tomarmos o polinômio $f(X_0 Y_0, \dots, X_{n-1} Y_{m-1})$, para cada $Q_i \in X_1$ (e respectivamente, $R_j \in X_2$), f_{Q_i} (e respectivamente, f_{R_j}) remete ao último polinômio avaliado em Q_i (e respectivamente, R_j) e então $f_{Q_i} \in \mathbb{F}_q[Y_0, \dots, Y_{m-1}]_d$ (e respectivamente, $f_{R_j} \in \mathbb{F}_q[X_0, \dots, X_{n-1}]_d$). Seja $\Gamma_i = (f_{Q_i}(R_1), \dots, f_{Q_i}(R_{s_2})) \in C_{X_2}(d)$ para todo $i = 1, \dots, s_1$ e seja $s_3 = |\{i : \Gamma_i \neq 0\}|$. Como o peso de Hamming de $\Gamma_i(w(\Gamma_i))$ é tal que $w(\Gamma_i) \geq \delta_{X_2}(d)$ para todo i com $\Gamma_i \neq 0$, concluímos que $w(\Gamma) \geq s_3 \delta_{X_2}(d)$.

Por outro lado, seja $\Lambda_j = (f_{R_j}(Q_1), \dots, f_{R_j}(Q_{s_1})) \in C_{X_1}(d)$ para todo $j = 1, \dots, s_2$. Se j é tal que $\Lambda_j \neq 0$, então $s_3 < \delta_{X_1}(d)$ implica que $w(\Lambda_j) \leq s_3 < \delta_{X_1}(d)$. Portanto, $w(\Gamma) \geq \delta_{X_1}(d) \cdot \delta_{X_2}(d)$.

A outra desigualdade segue pois podemos encontrar uma palavra no código $C_X(d)$ com peso de Hamming igual a $\delta_{X_1}(d) \cdot \delta_{X_2}(d)$. \square

Exemplo 4.1.8. Seja \mathbb{F}_q um corpo finito com $q = 5$ elementos e considere o grafo bipartido completo $\mathcal{K}_{2,3}$.



O conjunto tórico associado as arestas deste grafo é dado por

$$X = \{[t_1 t_3 : t_1 t_4 : t_1 t_5 : t_2 t_3 : t_2 t_4 : t_2 t_5] \in \mathbb{P}^5 : t_i \in \mathbb{F}_5^*\}.$$

Relembramos que sua matriz de incidência é dada por

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Temos $|X| = 4^3 = 64$ e se escolhermos $r = 3, d = 2$ como na proposição acima obtemos

$$d_3(C_X(d)) \leq 4 \cdot 2 \cdot 4 = 32.$$

Além disso $H_X(2) = H_{\mathbb{T}_1}(2) \cdot H_{\mathbb{T}_2}(2) = 3 \cdot 6 = 18$, pelo lema acima. Então a cota de Singleton é

$$d_3(C_X(d)) \leq |X| + 3 - H_X(2) = 4^3 + 3 - 18 = 49,$$

enquanto que a cota de Plotkin é dada por

$$d_3(C_X(d)) \leq \left\lfloor \frac{4^3(5^3 - 1)5^{15}}{5^{18} - 1} \right\rfloor = 63.$$

Portanto a cota na proposição anterior, neste caso, é melhor que ambas as cotas conhecidas.

4.2 Uma cota geral

Considere o conjunto de m monômios dados por (4.1), mas nesta seção assumiremos que todos eles têm o mesmo grau α , isto é, $\mathbf{Z}^{a_i} = Z_1^{a_{i1}} \cdots Z_n^{a_{in}}$ e $\sum_{j=1}^n a_{ij} = \alpha$ para todo $i = 1, \dots, m$. Seja X o conjunto tórico (4.2) parametrizado por estes monômios e consideremos a aplicação

$$\begin{aligned} \mu : \mathbb{T}_{n-1} &\rightarrow X \\ [t_1 : \cdots : t_n] &\mapsto [\mathbf{t}^{a_1} : \cdots : \mathbf{t}^{a_m}]. \end{aligned} \quad (4.10)$$

Considerando \mathbb{T}_{n-1} e X como grupos multiplicativos, temos que μ é um epimorfismo de grupos, isto é, μ é uma aplicação sobrejetiva entre grupos. Além disso, vale que

$$|\ker \mu| = \frac{|(q-1)^{n-1}|}{|X|}. \quad (4.11)$$

Definiremos também a seguinte aplicação:

$$\begin{aligned} \tau : S_d &\rightarrow L_{\alpha d} \\ f(X_1, \dots, X_m) &\mapsto f(\mathbf{Z}^{a_1}, \dots, \mathbf{Z}^{a_m}). \end{aligned} \quad (4.12)$$

Observemos que a aplicação τ é uma aplicação linear entre os espaços lineares S_d e $L_{\alpha d}$. Além disso, se $f \in S_d$ e $Q \in \mathbb{T}_{n-1}$, então

$$\tau(f)(Q) = 0 \iff f(\mu(Q)) = 0. \quad (4.13)$$

Seja $X = \{P_1, \dots, P_{|X|}\}$ o conjunto tórico dado em (4.2). De agora em diante usaremos a seguinte notação: se $f \in S_d$ então $\Lambda_f \in C_X(d)$ denota o vetor

$$\Lambda_f := \left(\frac{f(P_1)}{X_1^d(P_1)}, \dots, \frac{f(P_{|X|})}{X_1^d(P_{|X|})} \right). \quad (4.14)$$

Similarmente se $\mathbb{T}_{n-1} = \{R_1, \dots, R_{|\mathbb{T}_{n-1}|}\}$ e $f \in S_d$ então $\Omega_f \in C_{\mathbb{T}_{n-1}}(\alpha d)$ é definido como o vetor

$$\Omega_f := \left(\frac{\tau(f)(R_1)}{Z_1^{\alpha d}(R_1)}, \dots, \frac{\tau(f)(R_{|\mathbb{T}_{n-1}|})}{Z_1^{\alpha d}(R_{|\mathbb{T}_{n-1}|})} \right) \quad (4.15)$$

Lema 4.2.1. *Com a notação introduzida acima, seja $\mathcal{B}_1 = \{\Lambda_{f_1}, \dots, \Lambda_{f_r}\}$ um subconjunto linearmente independente de $C_X(d)$, e $\mathcal{B}_2 = \{\Omega_{f_1}, \dots, \Omega_{f_r}\}$. Então \mathcal{B}_2 é um subconjunto linearmente independente de $C_{\mathbb{T}_{n-1}}(\alpha d)$ e*

$$|\text{supp}(\mathcal{B}_2)| = |\ker \mu| \cdot |\text{supp}(\mathcal{B}_1)|. \quad (4.16)$$

Demonstração. Seja $\mathcal{B}_1 = \{\Lambda_{f_1}, \dots, \Lambda_{f_r}\}$ um subconjunto linearmente independente de $C_X(d)$

e suponha que existem elementos $b_1, \dots, b_r \in \mathbb{F}_q$ tais que $\sum_{i=1}^r b_i \Omega_{f_i} = \mathbf{0}$.

Assim $\sum_{i=1}^r b_i \tau(f_i)(R_j) = 0$ para todo $j = 1, \dots, (q-1)^{n-1}$. Como τ é uma aplicação linear

podemos concluir que $\tau\left(\sum_{i=1}^r b_i f_i\right)(R_j) = 0$ para todo $j = 1, \dots, (q-1)^{n-1}$.

Portanto da igualdade (4.13) temos $\left(\sum_{i=1}^r b_i f_i\right)(\mu(R_j)) = 0$ para todo $j = 1, \dots, (q-1)^{n-1}$.

Então $\left(\sum_{i=1}^r b_i f_i\right)(P_j) = 0$ para todo $j = 1, \dots, |X|$. Assim $\sum_{i=1}^r b_i \Lambda_{f_i} = \mathbf{0}$ e por hipótese temos que \mathcal{B}_1 é um subconjunto linearmente independente, logo $b_i = 0$ para todo $i = 1, \dots, r$. Isso prova que \mathcal{B}_2 é um subconjunto linearmente independente de $C_{\mathbb{T}_{n-1}}(\alpha d)$. Ainda, sem perda de generalidade, podemos tomar $R_i \in \mathbb{T}_{n-1}$, $i = 1, \dots, |X|$ de tal maneira que $\mu(R_i) = P_i$. Se $|\ker \mu| = l$ e $\ker \mu = \{Q_1, \dots, Q_l\}$ então

$$\mathbb{T}_{n-1} = \bigcup_{i=1}^{|X|} R_i \cdot \ker \mu = \{R_i \cdot Q_j : i = 1, \dots, |X|, j = 1, \dots, l\}.$$

Fazendo uso da notação $T_{(i-1) \cdot l + j} = R_i \cdot Q_j$ para $i = 1, \dots, |X|, j = 1, \dots, l$ temos que se $f \in S_d$, então

$$\tau(f)(T_{(i-1) \cdot l + j}) = f(\mu(R_i Q_j)) = f(\mu(R_i)) = f(P_i).$$

Além disso se definimos os conjuntos $E_i := \{(i-1) \cdot l + j : j = 1, \dots, l\}$ para todo $i = 1, \dots, |X|$, então $|E_i| = l$ e esses conjuntos formam uma partição do conjunto $\{1, \dots, |\mathbb{T}_{n-1}|\}$. Assim é possível ver que $\text{supp}(\mathcal{B}_2) = \cup_{i \in \text{supp}(\mathcal{B}_1)} E_i$.

Portanto

$$|\text{supp}(\mathcal{B}_2)| = \sum_{i \in \text{supp}(\mathcal{B}_1)} |E_i| = l \cdot |\text{supp}(\mathcal{B}_1)|.$$

□

Teorema 4.2.2. *Se X é o conjunto tórico associado ao conjunto de monômios de mesmo grau α , então o r -ésimo peso de Hamming generalizado do código parametrizado de ordem d associado ao conjunto X é limitado por*

$$d_r(C_X(d)) \geq \left\lceil \frac{|X| \cdot d_r(C_{\mathbb{T}_{n-1}}(\alpha d))}{(q-1)^{n-1}} \right\rceil \text{ para todo } r = 1, \dots, H_X(d), \quad (4.17)$$

onde $d_r(C_{\mathbb{T}_{n-1}}(\alpha d))$ é o r -ésimo peso de Hamming generalizado do código de ordem αd associado ao toro projetivo \mathbb{T}_{n-1} .

Demonstração. Seja \mathcal{U} o subespaço de $C_X(d)$ com $\dim_{\mathbb{F}_q} \mathcal{U} = r$ e $d_r(C_X(d)) = |\text{supp}(\mathcal{U})|$. Seja $\mathcal{B}_1 = \{\Lambda_{f_1}, \dots, \Lambda_{f_r}\}$ uma base de \mathcal{U} onde cada Λ_{f_i} é dado por (4.14). Como \mathcal{U} tem dimensão r e \mathcal{B}_1 é uma base para \mathcal{U} , segue que $|\text{supp}(\mathcal{U})| = |\text{supp}(\mathcal{B}_1)|$ e assim $d_r(C_X(d)) = |\text{supp}(\mathcal{B}_1)|$. Por outro lado, como no (4.2.1), seja $\mathcal{B}_2 = \{\Omega_{f_1}, \dots, \Omega_{f_r}\}$ onde cada Ω_{f_i} é dado por (4.15), e seja \mathcal{W} o subespaço de $\mathbb{T}_{n-1}(\alpha d)$ gerado por \mathcal{B}_2 . Pelo Lema 4.2.1 concluímos que \mathcal{B}_2 é uma base de \mathcal{W} e

$$|\text{supp}(\mathcal{W})| = |\text{supp}(\mathcal{B}_2)| = |\ker \mu| \cdot |\text{supp}(\mathcal{B}_1)| = |\ker \mu| \cdot d_r(C_X(d)).$$

Pela equação (4.11) sabemos que $|\ker \mu| = \frac{|(q-1)^{n-1}|}{|X|}$, logo

$$|\text{supp}(\mathcal{W})| = \frac{(q-1)^{n-1}}{|X|} \cdot d_r(C_X(d)).$$

Portanto

$$d_r(C_{\mathbb{T}_{n-1}}(\alpha d)) \leq |\text{supp}(\mathcal{W})| = \frac{(q-1)^{n-1}}{|X|} \cdot d_r(C_X(d)) \Rightarrow d_r(C_X(d)) \geq \frac{|X| \cdot d_r(C_{\mathbb{T}_{n-1}}(\alpha d))}{(q-1)^{n-1}}.$$

□

4.3 Conjuntos mergulhados

Seja X o conjunto tórico dado por (4.2) e seja X' um conjunto tórico parametrizado pelos primeiros s monômios em (4.1), onde s é um inteiro positivo estritamente menor que m . Diremos que X' está **mergulhado** em X .

Seja X um conjunto tórico associado ao conjunto de monômios (não necessariamente de mesmo grau) como foram dados em (4.2), e seja X' um conjunto mergulhado em X . Utilizaremos a aplicação projeção π

$$\begin{aligned} \pi : X &\rightarrow X' \\ [\mathbf{t}^{a_1} : \dots : \mathbf{t}^{a_m}] &\mapsto [\mathbf{t}^{a_1} : \dots : \mathbf{t}^{a_s}]. \end{aligned}$$

Considerando X e X' como grupos multiplicativos, temos que π é um epimorfismo de grupos, isto é, π é uma aplicação sobrejetiva entre grupos. Além disso, se $|\ker \pi| = \eta$, então $|X| = \eta|X'|$.

Seja $X = \{P_1, \dots, P_{|X|}\}$ e $X' = \{Q_1, \dots, Q_{|X'|}\}$. Se f é um elemento de $\mathbb{F}_q[X_1, \dots, X_s]_d$ então nós definimos $\Delta_f \in C_{X'}(d)$ como

$$\Delta_f := \left(\frac{f(Q_1)}{X_1^d(Q_1)}, \dots, \frac{f(Q_{|X'|})}{X_1^d(Q_{|X'|})} \right).$$

Continuaremos com a notação de Λ_f como definida em (4.14). Para provarmos o resultado principal, precisamos do seguinte lema:

Lema 4.3.1. [12, Lema 3.1] *Seja $\mathcal{B}_3 = \{\Delta_{f_1}, \dots, \Delta_{f_r}\}$ um subconjunto linearmente independente de $C_{X'}(d)$. Se $\mathcal{B}_1 = \{\Lambda_{f_1}, \dots, \Lambda_{f_r}\}$ então \mathcal{B}_1 é um subconjunto linearmente independente de $C_X(d)$ e*

$$|\text{supp}(\mathcal{B}_1)| = \eta \cdot |\text{supp}(\mathcal{B}_3)|. \quad (4.18)$$

Teorema 4.3.2. *Sejam $X \subseteq \mathbb{P}^{m-1}$ e $X' \subseteq \mathbb{P}^{s-1}$, com $s < m$, dois conjuntos toricos parametrizados por alguns monômios de modo que X' esteja mergulhado em X e $|X| = \eta|X'|$. Então*

$$d_r(C_X(d)) \leq \eta \cdot d_r(C_{X'}(d)) \text{ para todo } r = 1, \dots, H_X(d). \quad (4.19)$$

Demonstração. Seja W_1 o subespaço de $C_{X'}(d)$ com $\dim_{\mathbb{F}_q} W_1 = r$ e tal que $d_r(C_{X'}(d)) = |\text{supp}(W_1)|$.

Seja $\mathcal{B}_3 = \{\Delta_{f_1}, \dots, \Delta_{f_r}\}$ uma base de W_1 , onde $f_i \in \mathbb{F}_q[X_1, \dots, X_s]_d$ para todo $i = 1, \dots, r$. Note que $d_r(C_{X'}(d)) = |\text{supp}(W_1)| = |\text{supp}(\mathcal{B}_3)|$.

Seja W_2 o subespaço de $C_X(d)$ gerado por $\mathcal{B}_1 = \{\Lambda_{f_1}, \dots, \Lambda_{f_r}\}$. Pelo Lema (4.3.1) concluímos que \mathcal{B}_1 é uma base de W_2 e $|\text{supp}(W_2)| = |\text{supp}(\mathcal{B}_1)| = \eta \cdot |\text{supp}(\mathcal{B}_3)| = \eta \cdot d_r(C_{X'}(d))$.

Então

$$d_r(C_X(d)) \leq |\text{supp}(W_2)| = \eta \cdot d_r(C_{X'}(d)).$$

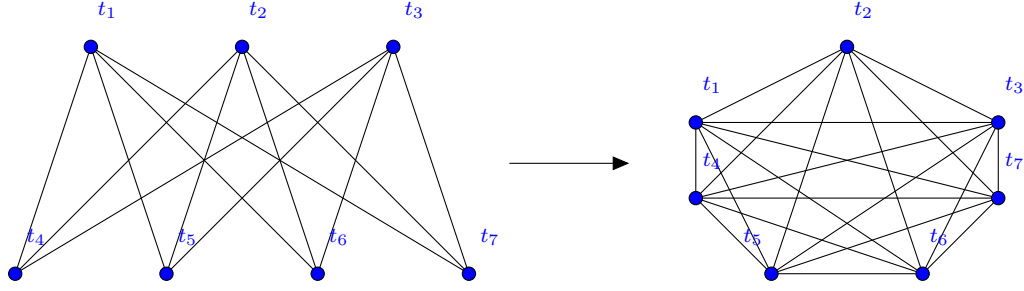
□

Corolário 4.3.3. *Sejam $X \subseteq \mathbb{P}^{m-1}$ e $X' \subseteq \mathbb{P}^{s-1}$, com $s < m$, conjuntos tóricos parametrizados por alguns monômios de mesmo grau α de modo que X' esteja mergulhado em X e $|X| = \eta|X'|$. Então*

$$\left\lceil \frac{|X| \cdot d_r(C_{\mathbb{T}_{n-1}}(\alpha d))}{(q-1)^{n-1}} \right\rceil \leq d_r(C_X(d)) \leq \eta \cdot d_r(C_{X'}(d)), \text{ para todo } r = 1, \dots, H_X(d).$$

Demonstração. A demonstração é consequência imediata dos teoremas acima. Uma das desigualdades é dada pelo teorema 4.2.2 e a outra é dada pelo teorema 4.3.2. □

Exemplo 4.3.4. Seja \mathbb{F}_q um corpo finito com q elementos. Seja $\mathcal{G} = \mathcal{K}_7$ o grafo completo com 7 vértices, e seja X o conjunto tórico parametrizado por suas arestas. Assim $|X| = (q - 1)^6$. Além disso seja \mathcal{G}' o grafo bipartido completo $\mathcal{K}_{3,4}$ e seja X' o conjunto tórico parametrizado por suas arestas. Então $X' = (q - 1)^5$ e X' está mergulhado em X .



Assim $\eta = q - 1$ e, pelo Teorema 4.3.2, $d_2(C_X(d)) \leq (q - 1) \cdot d_2(C_{X'}(d))$, mas devido ao fato de $C_{X'}(d) = C_{\mathbb{T}_2}(d) \otimes C_{\mathbb{T}_3}(d)$, onde \otimes é o produto tensorial de espaços lineares, obtemos

$$d_2(C_{X'}(d)) = \min\{d_1(C_{\mathbb{T}_2}(d)) \cdot d_2(C_{\mathbb{T}_3}(d)), d_2(C_{\mathbb{T}_2}(d)) \cdot d_1(C_{\mathbb{T}_3}(d))\}.$$

Se tomarmos $q = 3$ e $d = 1$ obtemos

$$d_2(C_X(1)) \leq 2 \cdot \min\{d_1(C_{\mathbb{T}_2}(1)) \cdot d_2(C_{\mathbb{T}_3}(1)), d_2(C_{\mathbb{T}_2}(1)) \cdot d_1(C_{\mathbb{T}_3}(1))\}.$$

Utilizando o software Macaulay2 computamos os seguintes valores: $d_1(C_{\mathbb{T}_2}(1)) = 2$, $d_2(C_{\mathbb{T}_3}(1)) = 6$, $d_1(C_{\mathbb{T}_3}(1)) = 4$ e $d_2(C_{\mathbb{T}_1}(1)) = 3$. Portanto $d_2(C_X(1)) \leq 24$. Neste caso, a cota de Singleton é:

$$d_2(C_X(1)) \leq |X| + 2 - H_X(1) = 2^6 + 2 - 21 = 45.$$

Além disso a cota de Plotkin é:

$$d_2(C_X(1)) \leq \left\lfloor \frac{|X| \cdot (q^2 - 1)q^{H_X(1)-2}}{q^{H_X(1)} - 1} \right\rfloor = \left\lfloor \frac{2^6(3^2 - 1)3^{19}}{3^{21} - 1} \right\rfloor = 56.$$

Se tomarmos $q = 5$, $d = 1$ a cota apresentada é $d_2(C_X(1)) \leq 4 \cdot d_2(C_{X'}(1)) = 2880$. A cota de Singleton é $d_2(C_X(1)) = 4^6 + 2 - 21 = 4077$. A cota de Plotkin é $d_2(C_X(1)) \leq \left\lfloor \frac{4^6(5^2-1)5^{19}}{5^{21}-1} \right\rfloor = 3932$. Então, em ambos casos ($q = 3$ e $q = 5$), a cota aqui apresentada refina mais que a cota de Singleton e que a cota de Plotkin.

Referências Bibliográficas

- [1] T. Becker and V. Weispfenning, Gröbner Bases - A computational approach to commutative algebra, Berlin, Germany: Springer Verlag, 1998, 2nd. pr.
- [2] W. Bruns, J. Herzog, Cohen-Macaulay Rings, Revised Edition, Cambridge University Press, 1997.
- [3] B. Buchberger, Ein algorithmus zum affinden der basiselemente des restklassen-rings nach einem nulldimensionalen polynomideal, Tese de Doutorado, Mathematical Institute, University of Innsbruck, 1965.
- [4] D. A. Cox, J. Little, D. O'Shea, Ideals, Varieties and Algorithms, Springer, 2015.
- [5] D. Eisenbud, Commutative Algebra with a view toward Algebraic Geometry, Graduate Texts in Mathematics, 150, Springer-Verlag, 1995.
- [6] M. González-Sarabia, C. R. Márquez, M. A. Hernández de la Torre, Minimum distance and second generalized Hamming weights of two particular linear codes, Congr. Numer. 161 (2003) 105-116.
- [7] R. Hartshorne, Algebraic Geometry, Springer-Verlag, New York, 1977.
- [8] A. Hefez, M. L. T. Villela, Códigos Corretores de Erros, IMPA, 2008.
- [9] S. Lang, Linear Algebra, 2nd edition, Addison-Wesley Publishing Company, 1972.
- [10] J. H. van Lint, Coding Theory, printing, Lecture Notes in Mathematics, Vol. 201, Springer-Verlag, Berlin-New York, 1973.
- [11] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, Amsterdam: North-Holland, 1977.
- [12] E. Sarmiento, M. Vaz Pinto, R.H. Villarreal, The minimum distance of parameterized codes on projective tori, Appl. Algebra Engrg. Comm. Comput. 22 (4) (2011) 249-264. <https://doi.org/10.1007/s00200-011-0148-2>
- [13] A. Tochimani, M. V. Pinto, R. H. Villarreal, Direct Product in Projective Segre Codes, arXiv eprint 1501.01692.
- [14] M. A. Tsfasman, S. G. Vladut, Geometric approach to higher weights, IEEE Trans. Inform. Theory 41 (6) (1995) 1564-1588. <https://doi.org/10.1109/18.476213>
- [15] V.K. Wei, Hamming weights for linear codes, IEEE Trans. Inform. Theory 37 (1991) 1412-1418. <https://doi.org/10.1109/18.133259>
- [16] V.K. Wei, K. Yang, On the generalized Hamming weights of product codes, IEEE Trans. Inform. Theory 39 (5) (1993) 1709-1713. <https://doi.org/10.1109/18.259662>