LUCAS VINNICIUS DE OLIVEIRA GOMES

Códigos duais de códigos de avaliação

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2023

LUCAS VINNICIUS DE OLIVEIRA GOMES

Códigos duais de códigos de avaliação

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
2023

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

G633 Gomes, Lucas Vinnicius de Oliveira, 1999-
2023 Códigos duais de códigos de avaliação [recurso eletrônico] / Lucas Vinnicius de Oliveira Gomes. - 2023.

Orientador: Cícero Fernandes de Carvalho.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2023.24
Inclui bibliografia.

1. Matemática. I. Carvalho, Cícero Fernandes de,1960-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 160 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4209/4154 - www.posgrad.famat.ufu.br - pgmat@famat.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 105, PPGMAT				
Data:	16 de fevereiro de 2023	Hora de início:	14:30	Hora de encerramento:	16:30
Matrícula do Discente:	12112MAT008				
Nome do Discente:	Lucas Vinnicius de Oliveira Gomes				
Título do Trabalho:	Códigos duais de códigos de avaliação				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Sobre pesos de Hamming de ordem superior em códigos projetivos de Reed-Muller				

Reuniu-se em webconferência pela plataforma Mconf-RNP, em conformidade com a PORTARIA Nº 36, DE 19 DE MARÇO DE 2020 da COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR - CAPES, pela Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Pietro Speziali - IMECC/UNICAMP; Victor Gonzalo Lopez Neumann - FAMAT/UFU e Cícero Fernandes de Carvalho - FAMAT/UFU, orientador do candidato.

Iniciando os trabalhos o presidente da mesa, Dr. Cícero Fernandes de Carvalho, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao Discente a palavra para a exposição do seu trabalho. A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

A seguir o senhor(a) presidente concedeu a palavra, pela ordem sucessivamente, aos(às) examinadores(as), que passaram a arguir o(a) candidato(a). Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o(a) candidato(a):

Aprovado.

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Pietro Speziali**, **Usuário Externo**, em 16/02/2023, às 15:44, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Cícero Fernandes de Carvalho**, **Professor(a) do Magistério Superior**, em 16/02/2023, às 15:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 16/02/2023, às 17:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4241107** e o código CRC **148D4A83**.

Dedicatória

Dedico este trabalho à minha mãe Maria Aparecida de Oliveira.

Agradecimentos

Agradeço primeiramente à Deus por estar sempre ao meu lado.

Agradeço ao meu orientador Cícero Fernandes de Carvalho pela oportunidade de realizar este trabalho, por todos os ensinamentos, conselhos e por nossa amizade.

Agradeço aos meus pais Alessandro Isaias Marcelino Gomes e Maria Aparecida de Oliveira por todo o apoio e carinho que me ofereceram durante esses anos.

Agradeço aos vários amigos que fiz durante esses dois anos de mestrado. Em especial, aos meus amigos Fellipe Diniz, Thiago Henrique e Tiago Aprigio.

Agradeço à minha querida avó Dinorá de Oliveira, que faleceu neste último ano e se tornou um dos maiores incentivos para a realização deste trabalho.

Agradeço à CAPES pelo auxílio financeiro durante todo o mestrado.

GOMES, L. V. O. *Códigos duais de códigos de avaliação.* 2023. (27 pág) p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho apresentamos inicialmente a teoria das bases de Gröbner com ênfase no conceito de pegada de um ideal. Em seguida, introduzimos os conceitos de código de avaliação afim e o de dual algébrico. Após apresentar o conceito de funções indicadoras e o de códigos monomialmente equivalentes, iniciamos o estudo de códigos monomiais e seus duais. O principal resultado prova que o dual de um código monomial é monomialmente equivalente a um código monomial. Ao fim deste trabalho estudamos um exemplo específico de códigos sobre o toro degenerado.

Palavras-chave: (Bases de Gröbner, Códigos de avaliação, Dual algébrico, Funções indicadoras, Códigos monomiais).

GOMES, L. V. O. *Dual codes of evaluation codes* 2023. (27 pages) p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

We start this work by presenting the theory of Gröbner bases with emphasis on the concept of the footprint of an ideal. Then we introduce the concepts of affine evaluation code and the algebraic dual. After presenting the concepts of indicator functions and of mononomially equivalent codes, we start the study of monomial codes and their duals. The main result proves that the dual of a monomial code is monomially equivalent to a monomial code. At the end of this work we study an specific example of codes on the degenerate torus.

Keywords: (Gröbner bases, Evaluation codes, Algebraic dual, Indicator functions, Monomial Codes).

Sumário

Resumo viii

Abstract ix

Introdução 1

1 Conceitos Básicos 2
1.1 Bases de Gröbner 2
1.2 Códigos lineares 7

2 O dual algébrico 8

3 Funções indicadoras 10

4 Códigos monomialmente equivalentes 13

5 Um exemplo específico: Códigos sobre o toro degenerado 15

Introdução

Este trabalho está divido em cinco partes. Na primeira parte introduzimos o conceito de ordem monomial e o processo de divisão polinomial em várias variáveis, que são essenciais para a definição e cálculo das bases de Gröbner. Veremos o conceito de pegada de um ideal I e como está relacionada com a base de Gröbner, além de sua importância para o algoritmo de Buchberger que determina uma base de Gröbner para o ideal I a partir de um conjunto finito de geradores.

Na segunda parte apresentamos a função avaliação ev e definimos código de avaliação afim sobre um k-subespaço vetorial de $k[\boldsymbol{X}]/I$. Em seguida definimos o dual algébrico desse k-subespaço vetorial e mostramos que o dual de um código de avaliação é o código de avaliação do dual algébrico. Apresentamos também algumas propriedades sobre o dual algébrico.

Na terceira parte introduzimos o conceito de funções indicadoras e suas propriedades. Definimos funções indicadoras padrão e mostramos que o conjunto formado pelas funções indicadoras padrão formam uma k-base para $k\Delta(I)$, o k-espaço vetorial gerado pelos monômios da pegada do ideal I.

Na quarta parte definimos código monomial e o conceito de códigos monomialmente equivalentes. Apresentamos a definição de um monômio ser essencial e dados dois códigos monomiais C_1 e C_2 mostramos uma condição para C_1 ser monomialmente equivalente ao dual de C_2.

Na quinta parte apresentamos um exemplo específico de códigos sobre o toro degenerado e um resultado que determina uma base de monômios para o dual algébrico.

Este trabalho é baseado no artigo [2].

Lucas Vinnicius de Oliveira Gomes.
Uberlândia-MG, 16 de Fevereiro de 2023.

Capítulo 1

Conceitos Básicos

1.1 Bases de Gröbner

Seja k um corpo e denote por $k[\mathbf{X}]$ o anel de polinômios $k[X_1, \ldots, X_n]$. Um produto da forma $aX_1^{\alpha_1}.\cdots.X_n^{\alpha_n}$, onde $a \in k^*$ e $\alpha_1, \ldots, \alpha_n$ são inteiros não negativos é chamado de *termo* e $X_1^{\alpha_1}.\cdots.X_n^{\alpha_n}$ é chamado de *monômio*. Um monômio $X_1^{\alpha_1}.\cdots.X_n^{\alpha_n}$ é denotado por $\mathbf{X}^{\boldsymbol{\alpha}}$ onde $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ e $\mathbb{N}_0$ é o conjunto dos inteiros não negativos. Denotaremos o conjunto dos monômios de $k[\mathbf{X}]$ por $\mathcal{M}$. Dado um polinômio $f \in k[\mathbf{X}]$, dizemos que um monômio M *aparece* em f se o coeficiente de M em f é não nulo.

Definição 1.1. Uma *ordem monomial* $\preceq$ em $\mathcal{M}$ é uma ordem total sobre monômios que possui as seguintes propriedades:

i) se $\mathbf{X}^{\boldsymbol{\alpha}} \preceq \mathbf{X}^{\boldsymbol{\beta}}$ então $\mathbf{X}^{\boldsymbol{\alpha}+\boldsymbol{\gamma}} \preceq \mathbf{X}^{\boldsymbol{\beta}+\boldsymbol{\gamma}}$, para todos $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma} \in \mathbb{N}_0^n$;

ii) qualquer subconjunto não vazio $\mathcal{A} \subset \mathcal{M}$ tem um menor elemento.

Exemplo 1.2. i) A *ordem lexicográfica* (com $X_n \preceq \cdots \preceq X_1$) é definida para $\mathbf{X}^{\boldsymbol{\alpha}} \preceq \mathbf{X}^{\boldsymbol{\beta}}$ se $\boldsymbol{\alpha} = \boldsymbol{\beta}$ ou a primeira entrada não nula de $\boldsymbol{\beta} - \boldsymbol{\alpha}$ é positiva. Por exemplo, temos $X_2^3 \preceq X_1$ e $X_1^2 X_3^{2022} \preceq X_1^2 X_2$.

ii) A *ordem lexicográfica graduada* (com $X_n \preceq \cdots \preceq X_1$) é definida para $\mathbf{X}^{\boldsymbol{\alpha}} \preceq \mathbf{X}^{\boldsymbol{\beta}}$ se $\boldsymbol{\alpha} = \boldsymbol{\beta}$ ou $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$ ou se $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$, então $X_\alpha \preceq_{\text{lex}} X^\beta$, onde $\preceq_{\text{lex}}$ é a ordem definida em i).

iii) A *ordem lexicográfica graduada inversa* é definida para $\mathbf{X}^{\boldsymbol{\alpha}} \preceq \mathbf{X}^{\boldsymbol{\beta}}$ se $\boldsymbol{\alpha} = \boldsymbol{\beta}$ ou $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$ ou se $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$, então a primeira entrada não nula de $\boldsymbol{\beta} - \boldsymbol{\alpha}$ é negativa.

Definição 1.3. Seja $f = \sum_{i=1}^m a_i M_i \in k[\mathbf{X}]$ um polinômio não nulo, onde $a_i \in k^*$ e $M_i \in \mathcal{M}$ para todo $i = 1, \ldots, m$, e seja $\preceq$ uma ordem monomial definida sobre $\mathcal{M}$. O *monômio líder* de f é $M_l := \text{máx}\{M_i \mid i = 1, \ldots, m\}$, o *coeficiente líder* de f é a_l e o *termo líder* de f é $a_l M_l$. Denotamos esses elementos por $M_l = \text{lm}(f)$, $a_l = \text{lc}(f)$ e $a_l M_l = \text{lt}(f)$ respectivamente.

Exemplo 1.4. Seja $f(X_1, X_2, X_3) = 3X_1^2 X_2^3 + X_1 X_3^5 + 1 \in \mathbb{R}[X_1, X_2, X_3]$. Usando a ordem lexicográfica temos $\text{lm}(f) = X_1^2 X_2^3$, $\text{lc}(f) = 3$ e $\text{lt}(f) = 3X_1^2 X_2^3$. Agora, usando a ordem lexicográfica graduada temos $\text{lm}(f) = X_1 X_3^5$, $\text{lc}(f) = 1$ e $\text{lt}(f) = X_1 X_3^5$.

Um importante procedimento na teoria das bases de Gröbner é a divisão de um polinômio por uma lista de polinômios não nulos.

Definição 1.5. Para dividir $f \in k[\mathbf{X}]$ por $\{g_1, \ldots, g_t\} \subset k[\mathbf{X}] \setminus \{0\}$ com respeito a uma ordem monomial fixada, devemos encontrar quocientes $q_1, \ldots, q_t$ e um resto r em $k[\mathbf{X}]$ tal que $f = q_1 g_1 + \cdots + q_t g_t + r$, onde $r = 0$ ou nenhum monômio de r é múltiplo de $\mathrm{lm}(g_i)$ para todo $i \in \{1, \ldots, t\}$.

Na literatura sobre bases de Gröbner citada na introdução, temos uma descrição do algoritmo usual usado para determinar os quocientes e o resto e também a prova de que o algoritmo de fato termina após um número finito de passos. Aqui apenas descrevemos o algoritmo e mostramos como ele funciona em um exemplo. A ideia básica é a mesma que conhecemos ao dividir dois polinômios de uma variável: usaremos os termos líderes de $g_1, \ldots, g_t$ para "eliminar" o termo principal de f e dos polinômios subsequentes que aparecem nas etapas intermediárias da divisão. A novidade aqui é que às vezes o termo principal de um polinômio intermediário não é um múltiplo de nenhum $\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t)$, então devemos movê-lo para o resto e continuar com a divisão.

Exemplo 1.6. Vamos dividir $f = X^2Y + XY^2 + Y^2$ por $g_1 = XY - 1$ e $g_2 = Y^2 - 1$. Usaremos a ordem lexicográfica com $Y \preceq X$. Como $\mathrm{lm}(f) = X^2Y$ é múltiplo de $\mathrm{lm}(g_1) = XY$ começamos a divisão escrevendo $f = X \cdot g_1 + X + XY^2 + Y^2$. Agora $\mathrm{lm}(X + XY^2 + Y^2) = XY^2$ é novamente múltiplo de $\mathrm{lm}(g_1) = XY$, então escrevemos $f = X \cdot g_1 + Y \cdot g_1 + X + Y + Y^2$. Observe que $\mathrm{lm}(X + Y + Y^2) = X$ não é múltiplo de $\mathrm{lm}(g_1)$ ou $\mathrm{lm}(g_2) = Y^2$, então devemos considerar X como uma parte do resto. Logo $f = (X + Y) \cdot g_1 + Y + Y^2 + r_1$, onde $r_1 = X$ e continuamos com o processo da divisão. Como $\mathrm{lm}(Y + Y^2) = Y^2$ não é múltiplo de $\mathrm{lm}(g_1)$ mas é múltiplo de $\mathrm{lm}(g_2)$ escrevemos $f = (X + Y) \cdot g_1 + 1 \cdot g_2 + Y + 1 + r_1$. Agora, os termos de $Y + 1$ não são múltiplos de $\mathrm{lm}(g_1)$ e $\mathrm{lm}(g_2)$ então consideramos esses termos como uma parte do resto. Isso termina a divisão e temos $f = q_1 g_1 + q_2 g_2 + r$ com $q_1 = X + Y$, $q_2 = 1$ e $r = X + Y + 1$.

A figura abaixo mostra o cálculo feito acima.

$$
\begin{array}{l|l|l}
X^2Y + XY^2 + Y^2 & XY - 1, \quad Y^2 - 1 & \text{Resto} \\
\cline{2-2}
-X^2Y + X & X + Y, \quad 1 & X + Y + 1 \\
\cline{1-1}
XY^2 + X + Y^2 & & \\
-XY^2 + X & & \\
\cline{1-1}
X + Y + Y^2 & & \\
-X & & \\
\cline{1-1}
Y + Y^2 & & \\
-Y^2 + 1 & & \\
\cline{1-1}
Y + 1 & & \\
-Y - 1 & & \\
\cline{1-1}
0 & &
\end{array}
$$

É importante observar no algoritmo da divisão que se o resto r não for zero, o monômio líder de r é menor ou igual ao monômio líder de f. Além disso, olhando atentamente para o algoritmo, observamos que estamos levando em consideração a ordem em que os divisores $g_1, \ldots, g_t$ são escritos (em outras palavras, estamos na verdade dividindo f por uma sequência $(g_1, \ldots, g_t)$) e podemos perguntar se alterando essa ordem os quocientes e os restos se alteram. A resposta a esta pergunta é sim, e podemos verificar com o exemplo a seguir.

Exemplo 1.7. Vamos dividir $f = X^2Y + XY^2 + Y^2$ por $g_1 = Y^2 - 1$ e $g_2 = XY - 1$. Como $\mathrm{lm}(f) = X^2Y$ não é múltiplo de $\mathrm{lm}(g_1) = Y^2$ mas é múltiplo de $\mathrm{lm}(g_2) = XY$ começamos a divisão escrevendo $f = X \cdot g_2 + X + XY^2 + Y^2$. Agora $\mathrm{lm}(X + XY^2 + Y^2) = XY^2$ é múltiplo de

$\mathrm{lm}(g_1) = Y^2$ então escrevemos $f = X \cdot g_2 + X \cdot g_1 + 2X + Y^2$. Observe que $\mathrm{lm}(2X + Y^2) = 2X$ não é múltiplo de $\mathrm{lm}(g_1)$ e $\mathrm{lm}(g_2)$, então devemos considerar $2X$ como uma parte do resto. Logo $f = X \cdot g_2 + X \cdot g_1 + Y^2 + r_1$, onde $r_1 = 2X$ e continuamos com o processo da divisão. Como $\mathrm{lm}(Y^2) = Y^2$ é múltiplo de $\mathrm{lm}(g_1) = Y^2$ escrevemos $f = X \cdot g_2 + X \cdot g_1 + 1 \cdot g_1 + 1 + r_1$. O termo 1 não é múltiplo de $\mathrm{lm}(g_1)$ e $\mathrm{lm}(g_2)$, então consideramos esse termo como uma parte do resto. Isso termina a divisão e temos $f = q_1 g_1 + q_2 g_2 + r$ com $q_1 = X + 1$, $q_2 = X$ e $r = 2X + 1$.

A figura abaixo mostra o cálculo feito acima.

$X^2Y + XY^2 + Y^2$	$Y^2 - 1, \quad XY - 1$	Resto
$-X^2Y + X$	$X + 1, \quad X$	$2X + 1$
$XY^2 + X + Y^2$		
$-XY^2 + X$		
$2X + Y^2$		
$-2X$		
Y^2		
$-Y^2 + 1$		
1		
-1		
0		

O conceito de base de Gröbner apareceu pela primeira vez na tese do matemático austríaco Bruno Buchberger, publicada em 1965 (ver [5]). Seu orientador, Wolfgang Gröbner, havia proposto o seguinte problema de tese: dado um ideal $I \subset k[\mathbf{X}]$, encontre uma base para $k[\mathbf{X}]/I$ como um k-espaço vetorial. Se $k[\mathbf{X}]$ é um anel de apenas uma variável então a resposta é bem conhecida: I é gerado por um polinômio de certo grau d (no caso onde $I \neq 0$) e $\{1 + I, X + I, \ldots, X^{d-1} + I\}$ é uma base para $k[\mathbf{X}]/I$. No caso em que $k[\mathbf{X}]$ é um anel de mais de uma variável, a situação muda drasticamente. A partir do teorema da base de Hilbert, sabemos que I é gerado por um número finito de polinômios, mas I não é necessariamente um ideal principal. Além disso, o anel quociente $k[\mathbf{X}]/I$ pode ser um k-espaço vetorial de dimensão infinita (por exemplo, tome $I = (X) \subset k[\mathbf{X}, \mathbf{Y}]$). A solução de Buchberger para este problema foi, tendo fixado uma ordem monomial em $\mathcal{M}$, determinar um conjunto gerador especial para I cuja propriedade principal é que as classes dos monômios que não são múltiplos de nenhum dos monômios líderes dos polinômios nesta base especial formam uma base para $k[\mathbf{X}]/I$ como um k-espaço vetorial. Em 1976 (ver [6]) Buchberger decidiu chamar essa base especial para I de *base de Gröbner* como sinal de reconhecimento da influência das ideias de seu orientador em seu trabalho de tese.

Definição 1.8. Seja $I \subset k[\mathbf{X}]$ um ideal não nulo e fixe uma ordem monomial $\preceq$ sobre $\mathcal{M}$. Um conjunto $\{g_1, \ldots, g_s\} \subset I$ é uma *base de Gröbner* para I se para todo $f \in I$, $f \neq 0$, temos que $\mathrm{lm}(f)$ é um múltiplo de $\mathrm{lm}(g_i)$, para algum $i \in \{1, \ldots, s\}$.

Exemplo 1.9. Seja $I = (XY - 1, Y^2 - 1) \subset \mathbb{R}[X, Y]$ e considere a ordem lexicográfica com $Y \preceq X$ definida sobre $\mathcal{M} \subset \mathbb{R}[X, Y]$. Então $Y(XY - 1) - X(Y^2 - 1) = -Y + X \in I$ e $\mathrm{lm}(X - Y) = X$ não é um múltiplo de $\mathrm{lm}(XY - 1) = XY$ ou $\mathrm{lm}(Y^2 - 1) = Y^2$, então $\{XY - 1, Y^2 - 1\}$ não é uma base de Gröbner para I.

Assumimos a partir de agora que $\mathcal{M}$ possui uma ordem monomial fixada e que $I \neq (0)$. O resultado a seguir mostra que uma base de Gröbner para I é de fato uma base para I, e que podemos usá-la para decidir se um polinômio dado está em I.

Lema 1.10. *Seja $\{g_1, \ldots, g_s\} \subset I$ uma base de Gröbner para I, então $f \in I$ se, e somente se, o resto da divisão de f por $\{g_1, \ldots, g_s\}$ é zero. Consequentemente $I = (g_1, \ldots, g_s)$.*

Demonstração. A recíproca é trivial. Por outro lado, para $f \in I$, seja $f = \sum_{i=1}^{s} q_i g_i + r$ a divisão de f por $\{g_1, \ldots, g_s\}$. Então $r = f - \sum_{i=1}^{s} q_i g_i \in I$. Devemos ter $r = 0$, caso contrário r seria um polinômio não nulo em I cujo monômio líder não é um múltiplo de $\mathrm{lm}(g_i)$, para todo $i \in 1, \ldots, s$, contradizendo o fato de $\{g_1, \ldots, g_s\}$ ser uma base de Gröbner para I. Logo $I \subset (g_1, \ldots, g_s)$ e portanto $I = (g_1, \ldots, g_s)$. □

Uma propriedade importante de uma base de Gröbner é a seguinte.

Proposição 1.11. *Seja $\{g_1, \ldots, g_s\} \subset I$ uma base de Gröbner para I. Na divisão de $f \in k[\mathbf{X}]$ por $\{g_1, \ldots, g_s\}$ o resto é sempre o mesmo, independente da ordem que escolhemos para $g_1, \ldots, g_s$ no algoritmo da divisão.*

Demonstração. Suponha que $f = q_1 g_1 + \cdots + q_s g_s + r = \tilde{q}_1 g_1 + \cdots + \tilde{q}_s g_s + \tilde{r}$, onde $q_i, \tilde{q}_i \in k[\mathbf{X}]$ e nenhum monômio de r ou $\tilde{r}$ é um múltiplo de $\mathrm{lm}(g_i)$ para todo $i = 1, \ldots, s$. Como $r - \tilde{r} = \sum_{i=1}^{s} (\tilde{q}_i - q_i) g_i \in I$, devemos ter $r - \tilde{r} = 0$, caso contrário $r - \tilde{r}$ seria um polinômio não nulo em I cujo monômio líder não é múltiplo de $\mathrm{lm}(g_i)$ para todo $i = 1, \ldots, s$, contradizendo o fato de $\{g_1, \ldots, g_s\}$ ser uma base de Gröbner para I. □

Os resultados acima listam algumas propriedades interessantes das bases de Gröbner, mas até agora não está claro se todo ideal $I \subset k[\mathbf{X}]$ admite tal base. Esta é a principal parte da contribuição de Buchberger em seu trabalho de tese. Ele apresenta um algoritmo, o qual parte de uma base finita dada para I e acrescenta novos elementos, se necessário, em uma sequência de passos até que em algum ponto a base aumentada seja uma base de Gröbner.

A seguir, temos um conceito importante no algoritmo de Buchberger.

Definição 1.12. Sejam $f, g \in k[\mathbf{X}] \setminus \{0\}$, com $\mathrm{lt}(f) = a\mathbf{X}^{\boldsymbol{\alpha}}$ e $\mathrm{lt}(g) = b\mathbf{X}^{\boldsymbol{\beta}}$, para $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n), \boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbb{N}_0^n$. Seja $\gamma_i = \max\{\alpha_i, \beta_i\}$, para todo $i = 1, \ldots, n$ e $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_n) \in \mathbb{N}_o^n$. O S-*polinômio* de f e g é definido como

$$S(f, g) = (1/a)\mathbf{X}^{\boldsymbol{\gamma}-\boldsymbol{\alpha}} f - (1/b)\mathbf{X}^{\boldsymbol{\gamma}-\boldsymbol{\beta}} g.$$

Observe que $\mathrm{lt}((1/a)\mathbf{X}^{\boldsymbol{\gamma}-\boldsymbol{\alpha}} f) = \mathbf{X}^{\gamma} = \mathrm{lt}((1/b)\mathbf{X}^{\boldsymbol{\gamma}-\boldsymbol{\beta}} g)$. Buchberger provou que $\{g_1, \ldots, g_s\} \subset I$ é uma base de Gröbner para I se, e somente se, o resto da divisão de $S(g_i, g_j)$ por $\{g_1, \ldots, g_s\}$ é zero para todos os pares de inteiros distintos $i, j \in \{1, \ldots, s\}$. Ele também provou que o seguinte procedimento pode ser usado em um algoritmo que produz uma base de Gröbner $\{g_1, \ldots, g_s, g_{s+1}\}$ para $I = (g_1, \ldots, g_s)$ em um número finito de passos: suponha que para algum par de inteiros distintos $i, j \in \{1, \ldots, s\}$ o resto $R_{i,j}$ na divisão de $S(g_i, g_j)$ por $\{g_1, \ldots, g_s\}$ não é zero. Defina $g_{s+1} = R_{i,j}$ e considere o conjunto $\{g_1, \ldots, g_s, g_{s+1}\}$. É claro que $I = (g_1, \ldots, g_s, g_{s+1})$ pois $g_{s+1} \in I$. Se o resto da divisão de $S(g_i, g_j)$ por $\{g_1, \ldots, g_s, g_{s+1}\}$ é zero para todos os pares de inteiros distintos $i, j \in \{1, \ldots, s+1\}$, então $\{g_1, \ldots, g_s, g_{s+1}\}$ é uma base de Gröbner para I. Se para algum par de inteiros distintos $i, j \in \{1, \ldots, s+1\}$ o resto $R_{i,j}$ na divisão de $S(g_i, g_j)$ por $\{g_1, \ldots, g_{s+1}\}$ não é zero, então defina $g_{s+2} = R_{i,j}$ e considere o conjunto $\{g_1, \ldots, g_{s+2}\}$. Buchberger provou que após um número finito de passos este processo produzirá um conjunto $\{g_1, \ldots, g_t\}$ que é uma base de Gröbner para I.

Exemplo 1.13. Vimos no Exemplo 1.9 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 a ordem lexicográfica com $Y \preceq X$. Vamos aplicar o algoritmo de Buchberger para encontrar uma base de Gröbner para I. Seja $g_1 = XY - 1$ e $g_2 = Y^2 - 1$ então $S(g_1, g_2) = Y g_1 - X g_2 = X - Y$ e o resto da divisão de $S(g_1, g_2)$ por $\{g_1, g_2\}$ é $X - Y$. Seja $g_3 = X - Y$ e considere o conjunto $\{XY - 1, Y^2 - 1, X - Y\}$. Agora o resto da divisão de $S(g_1, g_2)$ e $S(g_2, g_3)$ por $\{XY - 1, Y^2 - 1, X - Y\}$ é zero. Logo $\{XY - 1, Y^2 - 1, X - Y\}$ é uma base de Gröbner para I.

Apresentamos agora o conceito que resolveu o problema da tese de Buchberger.

Definição 1.14. Seja $I \subset k[\mathbf{X}]$ um ideal. A *pegada* de I é o conjunto

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

A pegada de um ideal I está relacionada com a base de Gröbner para I (ambos sendo definidos em relação a mesma ordem monomial fixada em $\mathcal{M}$).

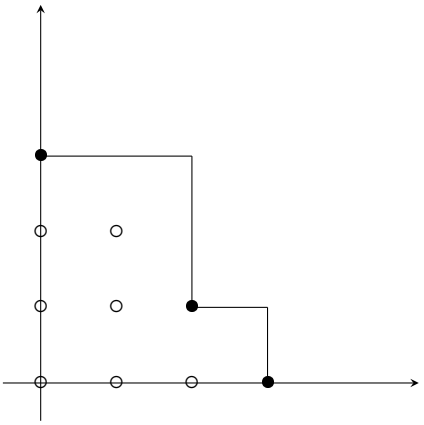
Proposição 1.15. *Seja $I \subset k[\mathbf{X}]$ um ideal e seja $\{g_1, \ldots, g_s\}$ uma base de Gröbner para I. Então, um monômio M está em $\Delta(I)$ se, e somente se, M não é múltiplo de $\mathrm{lm}(g_i)$, para todo $i = 1, \ldots s$.*

Demonstração. A recíproca segue da definição de $\Delta(I)$. Por outro lado, da definição de base de Gröbner sabemos que se M não é um múltiplo de $lm(g_i)$, para todo $i = 1, \ldots s$, então M não é monômio líder de nenhum polinômio em I. □

Observação 1.16. *Definido o que é uma base de Gröbner para um ideal I, podemos definir a pegada de I usando a afirmação da proposição acima. Por outro lado, podemos começar com a Definição* 1.14 *e então definir uma base de Gröbner para I como sendo um conjunto $\{g_1, \ldots, g_s\} \subset I$ tal que o conjunto de monômios que são múltiplos de $\mathrm{lm}(g_i)$, para algum $i \in \{1, \ldots, s\}$, é exatamente $\mathcal{M} \setminus \Delta(I)$. Então pode-se provar que tal conjunto $\{g_1, \ldots, g_s\}$ de fato existe e satisfaz a condição na Definição* 1.8. (ver [1, p. 13])

No exemplo a seguir, mostramos como obter uma representação gráfica da pegada.

Exemplo 1.17. Seja $I = (X^3 - X, Y^3 - Y, X^2Y - Y) \subset \mathbb{R}[X, Y]$. Considere a ordem lexicográfica sobre $\mathcal{M}$ com $Y \preceq X$. É possível verificar que $\{X^3 - X, Y^3 - Y, X^2Y - Y\}$ é uma base de Gröbner para I. Temos $\mathrm{lm}(X^3 - X) = X^3$, $\mathrm{lm}(Y^3 - Y) = Y^3$, $\mathrm{lm}(X^2Y - Y) = X^2Y$ e aplicando a Proposição 1.15 podemos determinar $\Delta(I)$. Um monômio $X^\alpha X^\beta$ será representado pelo par ordenado (α, β) na figura abaixo.



Os pontos $(3, 0)$, $(0, 3)$ e $(2, 1)$ correspondem aos monômios líderes da base de Gröbner. A partir deles é fácil determinar os monômios que não são múltiplos desses monômios líderes. Assim, pela Proposição 1.15, segue que $\Delta(I) = \{1, X, X^2, Y, XY, Y^2, XY^2\}$.

Apresentamos agora a solução para o problema da tese de Buchberger, que será muito útil na próxima seção.

Teorema 1.18. *Seja $I \subset k[\mathbf{X}]$ um ideal. Então*

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

é uma base para $k[\mathbf{X}]/I$ como um k-espaço vetorial.

Demonstração. Seja $\mathcal{G}$ uma base de Gröbner para I com respeito a mesma ordem monomial usada para determinar $\Delta(I)$, e seja $f \in k[\mathbf{X}]$. Dividindo f por $\mathcal{G}$ temos que o resto é da forma $r = \sum_{i=1}^{t} a_i M_i$, onde $a_i \in k[\mathbf{X}]$ e $M_i \in \Delta(I)$, para todo $i = 1, \ldots, t$. Como $f + I = r + I$ temos que $\mathcal{B}$ gera $k[\mathbf{X}]/I$ como um k-espaço vetorial. Agora, 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 $i = 1, \ldots, l$. Então $\sum_{i=1}^{l} b_i M_i \in I$ implica $b_i = 0$, para todo $i = 1, \ldots, l$, caso contrário $\sum_{i=1}^{l} b_i M_i \in I$ seria um elemento não nulo de I cujo monômio líder não é um monômio líder de um polinômio em I. Isso mostra que $\mathcal{B}$ é um conjunto linearmente independente sobre k. □

Exemplo 1.19. Usando o resultado acima no Exemplo 1.17 temos que $\mathbb{R}[X, Y]/I$ é um $\mathbb{R}$-espaço vetorial de dimensão 7 e $\{1 + I, X + I, X^2 + I, Y + I, XY + I, Y^2 + I, XY^2 + I\}$ é uma base para esse espaço vetorial.

Observação 1.20. *Seja $I \subset k[\boldsymbol{X}]$ um ideal e seja $\{f_1, \ldots, f_t\}$ uma base para I. Definimos*

$$\Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t)) := \{M \in \mathcal{M} \mid M \text{ não é múltiplo de } f_i, \text{ para todo } i = 1, \ldots, t\}.$$

Observe que $\Delta(I) \subset \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$. Consequentemente, pela Proposição 1.15, temos $\Delta(I) = \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$ se, e somente se, $\{f_1, \ldots, f_t\}$ é uma base de Gröbner para I.

1.2 Códigos lineares

Definição 1.21. Um código linear $\mathcal{C}$ definido sobre o alfabeto $\mathbb{F}_q$ e de comprimento n é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q^n$. Os elementos de $\mathcal{C}$ são chamados de *palavras do código*.

Seja $\boldsymbol{a} = (a_1, \ldots, a_n)$, $\boldsymbol{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, a *distância de Hamming* entre $\boldsymbol{a}$ e $\boldsymbol{b}$ é definida como $\mathrm{d}(\boldsymbol{a}, \boldsymbol{b}) = |\{i \mid a_i \neq b_i, \text{ onde } i \in \{1, \ldots, n\}\}|$. Se $\mathcal{C} \subset \mathbb{F}_q^n$ é um código e $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{C}$ então $\boldsymbol{a} - \boldsymbol{b} \in \mathcal{C}$ e $\mathrm{d}(\boldsymbol{a}, \boldsymbol{b}) = \mathrm{d}(\boldsymbol{a} - \boldsymbol{b}, \boldsymbol{0})$, onde $\boldsymbol{0}$ é o vetor nulo em $\mathbb{F}_q^n$.

Definição 1.22. Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código. A distância miníma de $\mathcal{C}$ é o inteiro positivo definido como $\mathrm{d}_{\min}(\mathcal{C}) = \min\{\mathrm{d}(\boldsymbol{a}, \boldsymbol{b}) \mid \boldsymbol{a}, \boldsymbol{b} \in \mathcal{C}, \boldsymbol{a} \neq \boldsymbol{b}\}$. Logo $\mathrm{d}_{\min}(\mathcal{C}) = \min\{\mathrm{d}(\boldsymbol{a}, \boldsymbol{0}) \mid \boldsymbol{a} \in \mathcal{C}, \boldsymbol{a} \neq \boldsymbol{0}\}$.

A importância da distância mínima está em sua relação com a capacidade de correção de erros do código. Suponha que um remetente transmita uma n-upla $\boldsymbol{a}$ do código $\mathcal{C}$ para um receptor por meio de um canal (por exemplo, como na comunicação entre dois computadores ou um telefone celular e uma antena próxima). Normalmente o canal tem "ruídos", ou seja, altera algumas das entradas na n-upla original. Suponha que o canal muda no máximo t entradas, com $t \leq (\mathrm{d}_{\min}(\mathcal{C}) - 1)/2$. O receptor conhece o código e portanto verá se $\boldsymbol{a}$ foi alterado, e que a palavra recebida $\boldsymbol{a}'$ não é uma palavra do código (e de fato não é porque $0 < \mathrm{d}(\boldsymbol{a}, \boldsymbol{a}') \leq t < \mathrm{d}_{\min}(\mathcal{C})$) e além disso, pode-se mostrar que, entre todas as palavras do código, apenas $\boldsymbol{a}$ satisfaz $\mathrm{d}(\boldsymbol{a}, \boldsymbol{a}') \leq t$, de modo que o receptor pode determinar que a palavra enviada é $\boldsymbol{a}$. A importância da dimensão $k(\mathcal{C})$ de um código é que ela é uma medida de quanta informação o código pode carregar, já que o número de palavras será então q^k. A importância do comprimento n do código é que quanto mais longo for o código, mais energia será gasta para transmitir cada palavra de código. Os parâmetros $k(\mathcal{C})/n$ e $\mathrm{d}_{\min}(\mathcal{C})/n$ são conceitos chave que aparecem na análise do desempenho de um código, e também possuem um papel importante quando se deseja comparar códigos distintos. O código ideal teria uma dimensão grande, uma distância mínima grande e um comprimento curto, mas esses requisitos não podem ser atendidos ao mesmo tempo. De fato, uma relação básica entre esses parâmetros é a chamada desigualdade de Singleton, que afirma que $k(\mathcal{C}) + \mathrm{d}_{\min}(\mathcal{C}) \leq n + 1$ (ver, por exemplo, [7, p. 33]).

Capítulo 2

O dual algébrico

Seja $k = \mathbb{F}_q$ um corpo finito e denote por $k[\boldsymbol{X}]$ o anel de polinômios $k[X_1, \ldots, X_s]$ com respeito a uma ordem monomial fixada. Seja $\mathcal{X} = \{P_1, \ldots, P_m\}$ um conjunto de pontos distintos em k^s, com $|\mathcal{X}| \geq 2$ e seja $I = I(\mathcal{X})$ o ideal dos polinômios de $k[\boldsymbol{X}]$ que se anulam em todos os pontos de $\mathcal{X}$. A partir de agora, considere a função

$$\begin{aligned} \text{ev} : k[\boldsymbol{X}]/I &\longrightarrow k^m \\ f + I &\longmapsto (f(P_1), \ldots, f(P_m)). \end{aligned}$$

Observe que $(X_1^q - X_1, \ldots, X_s^q - X_s) \subset I(\mathcal{X})$, logo de [4, p. 148] temos o seguinte resultado.

Proposição 2.1. *A função* ev *é um isomorfismo de k-espaços vetoriais.*

Definição 2.2. Seja $L \subset k[\boldsymbol{X}]/I$ um k-subespaço vetorial de $k[\boldsymbol{X}]/I$. A imagem $\text{ev}(L) =: C(L)$ é chamada de *código de avaliação afim* associado a L.

Considere a função

$$\begin{aligned} \varphi : k[\boldsymbol{X}] &\longrightarrow k \\ f &\longmapsto f(P_1) + \cdots + f(P_m). \end{aligned}$$

Definição 2.3. Seja $L \subset k[\boldsymbol{X}]/I$ um k-subespaço vetorial de $k[\boldsymbol{X}]/I$. O *dual algébrico de L* é

$$L^\perp := \{g + I \mid gh \in \ker \varphi, \text{ para todo } h + I \in L\}.$$

Observação 2.4. *O critério para que $g+I$ seja elemento de $L^\perp$ não depende do representante de $h+I \in L$. De fato, vamos mostrar que se $gh \in \ker \varphi$ para todo $h+I \in L$ e $h+I = h'+I$, então $gh' \in \ker \varphi$. Seja $h' = h + f$, onde $f \in I$. Logo $\varphi(gh') = \varphi(gh + gf) = \sum_{i=1}^m (gh + gf)(P_i) = \sum_{i=1}^m gh(P_i) + \sum_{i=1}^m gf(P_i) = \varphi(gh) + \sum_{i=1}^m g(P_i)f(P_i) = \varphi(gh)$, pois $f(P_i) = 0$, para todo $i = 1, \ldots, m$.*

Lema 2.5. *$L^\perp$ é um k-subespaço vetorial de $k[\boldsymbol{X}]/I$.*

Demonstração. De fato, se $g_1+I, g_2+I \in L^\perp$ então $(g_1+ag_2)+I \in L^\perp$ para todo $a \in k$, já que, dado $h \in k[\boldsymbol{X}]$ tal que $h+I \in L$ temos $\varphi((g_1+ag_2)h) = \varphi(g_1h)+\varphi(ag_2h) = \varphi(g_1h)+a\varphi(g_2h) = 0$, isto é, $g_1 + ag_2 + I \in L^\perp$. □

O próximo resultado mostra que o dual de um código de avaliação é o código de avaliação do dual algébrico.

Teorema 2.6. *Seja $C(L)$ um código de avaliação. Então*

$$C(L^\perp) = C(L)^\perp.$$

Demonstração. Seja $(b_1, \ldots, b_m) \in C(L^\perp)$, então existe $g + I \in L^\perp$ tal que $\mathrm{ev}(g + I) = (b_1, \ldots, b_m)$, isto é, $g(P_i) = b_i$ para todo $i = 1, \ldots, m$. Seja $(a_1, \ldots, a_m) \in C(L)$, então existe $h + I \in L$ tal que $\mathrm{ev}(h + I) = (a_1, \ldots, a_m)$, isto é, $h(P_i) = a_i$, para todo $i = 1, \ldots, m$. Temos que $(a_1, \ldots, a_m).(b_1, \ldots, b_m) = \sum_{i=1}^m a_i b_i = \sum_{i=1}^m h(P_i)g(P_i) = \sum_{i=1}^m (hg)(P_i) = \varphi(hg) = 0$.

Por outro lado, seja $(c_1, \ldots, c_m) \in C(L)^\perp$, então $(c_1, \ldots, c_m).(a_1, \ldots, a_m) = 0$, para todo $(a_1, \ldots, a_m) \in C(L)$, onde $h+I \in L$ tal que $\mathrm{ev}(h+I) = (a_1, \ldots, a_m)$. Como ev é um isomorfismo, existe $g + I \in k[\mathbf{X}]/I$ tal que $\mathrm{ev}(g + I) = (c_1, \ldots, c_m)$. De $(c_1, \ldots, c_m).(a_1, \ldots, a_m) = 0$, temos $\sum_{i=1}^m c_i a_i = 0$, isto é, $0 = \sum_{i=1}^m g(P_i)h(P_i) = \sum_{i=1}^m (gh)(P_i) = \varphi(gh)$, logo $gh \in \ker \varphi$, para todo $h + I \in L$. Assim $g + I \in L^\perp$. □

Apresentamos agora algumas propriedades sobre o dual algébrico de L.

Proposição 2.7. *Sejam $C(L)$ um código de avaliação e $I = I(\mathcal{X})$. Temos que*

(a) $\dim(L) + \dim(L^\perp) = |\mathcal{X}|$.

(b) *As seguintes condições são equivalentes:*

$$\text{(i) } C(L) \cap C(L)^\perp = \{\mathbf{0}\} \subset k^m, \quad \text{(ii) } L \cap L^\perp = \{0 + I\}, \quad \text{(iii) } L \oplus L^\perp = k[\boldsymbol{X}]/I.$$

(c) $C(L) = C(L)^\perp$ *se, e somente se,* $L = L^\perp$.

(d) $(L^\perp)^\perp = L$.

Demonstração. (a) Temos que $\dim(L) = \dim(C(L))$ e $\dim(L^\perp) = \dim(C(L)^\perp)$. Logo, $\dim(L) + \dim(L^\perp) = m = |\mathcal{X}|$.

(b) (i) $\Rightarrow$ (ii) Suponha que $C(L) \cap C(L)^\perp = \{\mathbf{0}\} \subset k^m$. Seja $g + I \in L \cap L^\perp$. Assim, $\mathrm{ev}(g) \in C(L) \cap C(L)^\perp = \{\mathbf{0}\}$. Logo, $g \in I$ e portanto $g + I = 0 + I$.

(ii) $\Rightarrow$ (iii) Temos que $\dim(L) = \dim(C(L))$ e $\dim(L^\perp) = \dim(C(L)^\perp)$, assim $\dim(L) + \dim(L^\perp) = m$. Por outro lado, $\dim(L + L^\perp) = \dim(L) + \dim(L^\perp) - \dim(L \cap L^\perp)$. Como $L \cap L^\perp = \{0 + I\}$, temos $\dim(L + L^\perp) = m = \dim(k[\mathbf{X}]/I)$. Logo $k[\boldsymbol{X}]/I = L \oplus L^\perp$.

(iii) $\Rightarrow$ (i) Da hipótese vem que se $g + I \in L \cap L^\perp$, então $g + I = 0 + I$. Assim $C(L) \cap C(L)^\perp = \{\mathbf{0}\} \subset k^m$.

(c) Vem do fato de ev ser um isomorfismo, e de $C(L) = \mathrm{ev}(L)$ e $C(L)^\perp = \mathrm{ev}(L^\perp)$.

(d) É um fato conhecido da Álgebra Linear em espaços de dimensão finita.

□

Capítulo 3

Funções indicadoras

Seja $k = \mathbb{F}_q$ um corpo finito e denote por $k[\boldsymbol{X}]$ o anel de polinômios $k[X_1, \ldots, X_s]$ com respeito a uma ordem monomial fixada. Seja $\mathcal{X} = \{P_1, \ldots, P_m\}$ um conjunto de pontos distintos em k^s, com $|\mathcal{X}| \geq 2$ e seja $I = I(\mathcal{X})$ o ideal dos polinômios de $k[\boldsymbol{X}]$ que se anulam em todos os pontos de $\mathcal{X}$. Neste capítulo vamos introduzir o conceito de funções indicadoras de $\mathcal{X}$.

Começaremos com a noção de função indicadora de um ponto em $\mathcal{X}$. Como a função $\mathrm{ev} : k[\boldsymbol{X}]/I \longrightarrow k^m$ é um isomorfismo temos que, dado $i \in \{1, \ldots, m\}$ e dado $\lambda \in k^*$ existe $f + I$ tal que $\mathrm{ev}(f + I) = \lambda \boldsymbol{e}_i$, onde $\boldsymbol{e}_i$ é o i-ésimo vetor da base canônica para k^m. Como $\{M + I \mid M \in \Delta(I)\}$ é uma base para $k[\boldsymbol{X}]/I$, existe um único representante f tal que $f \in k\Delta(I)$, onde $k\Delta(I)$ é o k-espaço vetorial gerado pelos monômios de $\Delta(I)$.

Definição 3.1. Sejam $\mathcal{X} = \{P_1, \ldots, P_m\} \subset k^m$, $i \in \{1, \ldots, m\}$ e $\lambda \in k^*$. O único polinômio $f \in \Delta(I)$ tal que $f(P_i) = \lambda$ e $f(P_j) = 0$, para $j \neq i$, é chamado de *função indicadora* de P_i.

O seguinte lema lista as propriedades básicas das funções indicadoras.

Lema 3.2. (a) *Se f, g são funções indicadoras de P_i em $k\Delta(I)$, então $g(P_i)f = f(P_i)g$.*

(b) *Existe uma única função indicadora f de P_i em $k\Delta(I)$ tal que $f(P_i) = 1$.*

Demonstração. (a) O polinômio $h = g(P_i)f - f(P_i)g$ se anula em todos os pontos de $\mathcal{X}$, isto é, $h \in I$. Se $h \neq 0$, então o monômio líder de h está em $\Delta(I)$, absurdo.

(b) É uma consequência do item (a).

□

Definição 3.3. Seja $i \in \{1, \ldots, m\}$, se $f_i \in k\Delta(I)$ é uma função indicadora para P_i e $f_i(P_i) = 1$ então dizemos que f_i é uma *função indicadora padrão* para P_i. O conjunto $F = \{f_1, \ldots, f_m\}$ será chamado *conjunto das funções indicadoras padrão para $\mathcal{X}$*.

Proposição 3.4. *Sejam $\mathcal{X} = \{P_1, \ldots, P_m\} \subset k^s$, $I = I(\mathcal{X})$ e $\preceq$ uma ordem monomial fixada. Temos*

(a) *Para cada $1 \leq i \leq m$, existe uma única $f_i \in k\Delta(I)$ tal que $f_i(P_i) = 1$ e $f_i(P_j) = 0$ se $j \neq i$. O conjunto $F = \{f_1, \ldots, f_m\}$ é uma k-base para $k\Delta(I)$.*

(b) $\ker \varphi = k\{f_i - f_m\}_{i=1}^{m-1} + I$.

Demonstração. (a) A existência e unicidade de f_i segue do Lema 3.2. Para mostrar que o conjunto F é linearmente independente, suponha $\sum_{i=1}^m a_i f_i = 0$ com $a_i \in k$, para todo $i = 1, \ldots, m$. Assim, $0 = \left(\sum_{i=1}^m a_i f_i\right)(P_j) = \sum_{i=1}^m a_i f_i(P_j) = a_j$. Como a dimensão de $k\Delta(I)$ é $m = |\mathcal{X}|$ temos que F é uma k-base para $k\Delta(I)$.

(b) Temos que $\ker\varphi \supset I$. Como $\varphi(f_i - f_m) = f_i(P_i) - f_m(P_m) = 0$, segue que $f_i - f_m \in \ker\varphi$, para todo $i = 1, \ldots, m$. Logo $\ker\varphi \supset k\{f_i - f_m\}_{i=1}^{m-1} + I$. Por outro lado, seja $f \in \ker\varphi$. Pelo algoritmo da divisão, podemos escrever $f = h + r_f$ para algum $h \in I$ e $r_f \in k\Delta(I)$. Como $F = \{f_1, \ldots, f_m\}$ é uma k-base para $k\Delta(I)$, podemos escrever $r_f = \sum_{i=1}^{m} a_i f_i$, com $a_i \in k$ para todo $i = 1, \ldots, m$. Além disso, como $h \in I \subset \ker\varphi$, temos $r_f \in \ker\varphi$. Logo

$$\varphi(r_f) = \varphi\left(\sum_{i=1}^{m} a_i f_i\right) = \sum_{i=1}^{m} a_i \varphi(f_i) = \sum_{i=1}^{m} a_i \left(\sum_{j=1}^{m} f_i(P_j)\right) = \sum_{i=1}^{m} a_i = 0,$$

então $\sum_{i=1}^{m} a_i = 0$ implica $a_m = -\sum_{i=1}^{m-1} a_i$ e

$$r_f = \left(\sum_{i=1}^{m-1} a_i f_i\right) + a_m f_m = \left(\sum_{i=1}^{m-1} a_i f_i\right) - \left(\sum_{i=1}^{m-1} a_i\right) f_m = \sum_{i=1}^{m-1} a_i (f_i - f_m).$$

Logo, $f = h + r_f \in I + k\{f_i - f_m\}_{i=1}^{m-1}$. Portanto, $\ker\varphi = k\{f_i - f_m\}_{i=1}^{m-1} + I$.

□

Observação 3.5. É conveniente utilizar uma interpretação matricial das funções indicadoras padrão para $\mathcal{X}$. Usando que $\mathrm{ev} : k[\boldsymbol{X}]/I \longrightarrow k^m$ é um isomorfismo é fácil ver que

$$\begin{aligned} \widetilde{\mathrm{ev}} : k\Delta(I) &\longrightarrow k^m \\ M &\longmapsto (M(P_1), \ldots, M(P_m)), \end{aligned}$$

onde M é um monômio em $\Delta(I)$, também é um isomorfismo de k-espaços vetoriais. Seja $B := \{M_1, \ldots, M_m\}$ a base para $k\Delta(I)$ formada pelos monômios de $\Delta(I)$ ordenados segundo $\preceq$, e seja $B' := \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m\}$ a base canônica para k^m. A matriz $M_{\widetilde{\mathrm{ev}}}$ de $\widetilde{\mathrm{ev}}$ com relação às bases B e B' tem na j-ésima coluna o vetor (coluna) $(M_j(P_1), \ldots, M_j(P_m))$, para todo $j = 1, \ldots, m$. Como $\widetilde{\mathrm{ev}}$ é isomorfismo a matriz $M_{\widetilde{\mathrm{ev}}}$ é invertível, e temos, de $M_{\widetilde{\mathrm{ev}}} M_{\widetilde{\mathrm{ev}}}^{-1} = Id$, que se $(a_{1j}, \ldots, a_{mj})$ são os elementos da j-ésima coluna de $M_{\widetilde{\mathrm{ev}}}^{-1}$, então

$$f_j = \sum_{i=1}^{m} a_{ij} M_i$$

é a função indicadora padrão para P_j, para todo $j = 1, \ldots, m$. De fato, a matriz $M_{\widetilde{\mathrm{ev}}}$ de $\widetilde{\mathrm{ev}}$ com relação às bases B e B' é dada por

$$M_{\widetilde{\mathrm{ev}}} = \begin{pmatrix} M_1(P_1) & \ldots & M_m(P_1) \\ \vdots & & \vdots \\ M_1(P_m) & \ldots & M_m(P_m) \end{pmatrix}.$$

Também escrevemos

$$M_{\widetilde{\mathrm{ev}}}^{-1} = \begin{pmatrix} a_{11} & \ldots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mm} \end{pmatrix}.$$

De $M_{\widetilde{\mathrm{ev}}} \cdot M_{\widetilde{\mathrm{ev}}}^{-1} = Id$, isto é

$$\begin{pmatrix} M_1(P_1) & \ldots & M_m(P_1) \\ \vdots & & \vdots \\ M_1(P_m) & \ldots & M_m(P_m) \end{pmatrix} \cdot \begin{pmatrix} a_{11} & \ldots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mm} \end{pmatrix} = \begin{pmatrix} 1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 1 \end{pmatrix}_{m \times m}.$$

Temos, multiplicando as linhas de $M_{\widetilde{\text{ev}}}$ pela primeira coluna de $M_{\widetilde{\text{ev}}}^{-1}$, que

$$\sum_{i=1}^{m} M_i(P_1)a_{i1} = 1 \quad \text{e} \quad \sum_{i=1}^{m} M_i(P_j)a_{i1} = 0$$

para todo $j = 2, 3, \ldots, m$. Logo $f_1 = \sum_{i=1}^{m} a_{i1}M_i$ é a função indicadora padrão para P_1.

Analogamente, concluímos que

$$f_j = \sum_{i=1}^{m} a_{ij}M_i$$

é a função indicadora padrão para P_j, para todo $j = 1, \ldots, m$.

Capítulo 4

Códigos monomialmente equivalentes

Seja $k = \mathbb{F}_q$ um corpo finito, $\mathcal{X}$ um subconjunto de k^s com pelo menos dois elementos, e $I = I(\mathcal{X})$ o ideal dos polinômios de $k[\boldsymbol{X}]$ que se anulam em todos os pontos de $\mathcal{X}$. Fixemos uma ordem monomial $\preceq$ e seja $\Delta(I)$ a pegada do ideal I.

Definição 4.1. Seja $\Lambda \subset \mathbb{N}^s$ o conjunto de vetores formados pelos expoentes de monômios de $\Delta(I)$. Dado um subconjunto $\Gamma \subset \Lambda$, seja $L(\Gamma)$ o k-subespaço de $k[\mathbf{X}]/I$ gerado pelo conjunto $\{\mathbf{X}^{\boldsymbol{\alpha}} + I \mid \boldsymbol{\alpha} \in \Gamma\}$. Então $C(L(\Gamma))$ é chamado *código monomial* correspondente a Γ.

Definição 4.2. Dizemos que dois códigos lineares $C_1, C_2 \in k^m$ são *monomialmente equivalentes* se existe $\beta = (\beta_1, \ldots, \beta_m) \in k^m$ tal que $\beta_i \neq 0$ para todo i e $C_2 = \beta \cdot C_1 = \{\beta \cdot c \mid c \in C_1\}$, onde $\beta \cdot c$ é o vetor dado por $(\beta_1 c_1, \ldots, \beta_m c_m)$, para $c = (c_1, \ldots, c_m) \in C_1$.

Considere dois códigos monomiais $C(L(\Gamma_1))$ e $C(L(\Gamma_2))$ para quaisquer $\Gamma_1, \Gamma_2 \subset \Lambda$. O objetivo principal deste capítulo é apresentar uma condição para $C(L(\Gamma_1))$ ser monomialmente equivalente ao dual $C(L(\Gamma_2)^\perp)$. Definimos

$$\Gamma_1 + \Gamma_2 = \{a_1 + a_2 \in \mathbb{N}^s \mid a_1 \in \Gamma_1, a_2 \in \Gamma_2\}.$$

Definição 4.3. Dizemos que um monômio $\mathbf{X}^{\boldsymbol{e}} \in \Delta(I)$ é *essencial* se ele aparece em cada função indicadora padrão de $\mathcal{X}$, isto é, se o coeficiente de $\mathbf{X}^{\boldsymbol{e}}$ é não nulo em cada função indicadora padrão de $\mathcal{X}$.

O principal resultado desse trabalho é o seguinte.

Teorema 4.4. *Seja $\mathcal{X} \subset k^s$ tal que $m = |\mathcal{X}| \geq 2$, e $I = I(\mathcal{X})$. Fixemos uma ordem monomial $\preceq$ e seja $\mathbf{X}^{\boldsymbol{e}} \in \Delta(I)$ o maior monômio com respeito a ordem monomial fixada. Suponha que $\mathbf{X}^{\boldsymbol{e}}$ é essencial. Então, para quaisquer $\Gamma_1, \Gamma_2 \subset \Lambda$ satisfazendo*

(1) $|\Gamma_1| + |\Gamma_2| = |\mathcal{X}|$;

(2) $\boldsymbol{e} \notin \Gamma_1 + \Gamma_2$,

temos $\beta \cdot C(L(\Gamma_1)) = C(L(\Gamma_2))^\perp$, para algum $\beta = (\beta_1, \ldots, \beta_m) \in (k^*)^m$. Além disso, β_j é o coeficiente de $\mathbf{X}^{\boldsymbol{e}}$ na j-ésima função indicadora padrão f_j, para $j = 1, \ldots, m$.

Demonstração. Para cada $j = 1, \ldots, m$, seja β_j o coeficiente de $\mathbf{X}^{\boldsymbol{e}}$ na j-ésima função indicadora padrão f_j. Então, pela Observação 3.5, como $\mathbf{X}^{\boldsymbol{e}} \in \Delta(I)$ é o maior monômio com respeito a ordem monomial fixada, β é a última linha da matriz $M_{\widetilde{\text{ev}}}^{-1}$, isto é, $\beta = (a_{m1}, \ldots, a_{mm})$. De $M_{\widetilde{\text{ev}}}^{-1} \cdot M_{\widetilde{\text{ev}}} = Id$ temos que a última linha da matriz $M_{\widetilde{\text{ev}}}^{-1}$ é ortogonal a todas as colunas de $M_{\widetilde{\text{ev}}}$, exceto a última. De fato,

$$\begin{pmatrix} a_{11} & \ldots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mm} \end{pmatrix} \cdot \begin{pmatrix} M_1(P_1) & \ldots & M_m(P_1) \\ \vdots & & \vdots \\ M_1(P_m) & \ldots & M_m(P_m) \end{pmatrix} = \begin{pmatrix} 1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 1 \end{pmatrix}_{m \times m}$$

implica

$$\sum_{j=1}^{m} a_{mj} M_i(P_j) = \sum_{j=1}^{m} \beta_j M_i(P_j) = 0$$

para todo $i = 1, \ldots, m-1$ e

$$\sum_{j=1}^{m} a_{mj} M_m(P_j) = \sum_{j=1}^{m} \beta_j M_m(P_j) = 1.$$

Logo β é ortogonal a todas as colunas de $M_{\widetilde{\mathrm{ev}}}$, exceto a última. Como $\widetilde{\mathrm{ev}}$ é um isomorfismo, existe um único polinômio $g \in k\Delta(I)$ tal que $\widetilde{\mathrm{ev}}(g) = \beta$, ou seja $g(P_j) = \beta_j = a_{mj}$, com $P_j \in \mathcal{X}$, para todo $j = 1, \ldots, m$. Provemos que a ortogonalidade de β implica $\varphi(gf) = 0$ para todo $f \in k(\Delta(I) \setminus \{\mathbf{X}^{\boldsymbol{e}}\})$. Para todo monômio $\mathbf{X}^{\boldsymbol{\alpha}} \in \Delta(I), \mathbf{X}^{\boldsymbol{\alpha}} \neq \mathbf{X}^{\boldsymbol{e}}$, temos

$$\varphi(g\mathbf{X}^{\boldsymbol{\alpha}}) = g(P_1)\mathbf{X}^{\boldsymbol{\alpha}}(P_1) + \cdots + g(P_m)\mathbf{X}^{\boldsymbol{\alpha}}(P_m) = a_{m1}\mathbf{X}^{\boldsymbol{\alpha}}(P_1) + \cdots + a_{mm}\mathbf{X}^{\boldsymbol{\alpha}}(P_m) = 0.$$

Seja $f \in k(\Delta(I) \setminus \{\mathbf{X}^{\boldsymbol{e}}\})$, temos $f = a_1 X^{\alpha_1} + \cdots + a_l X^{\alpha_l}$ com $X^{\alpha_i} \neq \mathbf{X}^{\boldsymbol{e}}$, para todo $i = 1, \ldots, l$. Assim,

$$\begin{aligned}
\varphi(gf) &= gf(P_1) + \cdots + gf(P_m) \\
&= (g(a_1 X^{\alpha_1} + \cdots + a_l X^{\alpha_l}))(P_1) + \cdots + (g(a_1 X^{\alpha_1} + \cdots + a_l X^{\alpha_l}))(P_m) \\
&= a_1(gX^{\alpha_1})(P_1) + \cdots + a_l(gX^{\alpha_l})(P_1) + \cdots + a_1(gX^{\alpha_1})(P_m) + \cdots + a_l(gX^{\alpha_l})(P_m) \\
&= a_1[(gX^{\alpha_1})(P_1) + \cdots + (gX^{\alpha_1})(P_m)] + \cdots + a_l[(gX^{\alpha_l})(P_1) + \cdots + (gX^{\alpha_l})(P_m)] \\
&= a_1\varphi(gX^{\alpha_1}) + \cdots + a_l\varphi(gX^{\alpha_l}) \\
&= 0. \qquad (4.1)
\end{aligned}$$

Para $i = 1, 2$ seja $h_i + I \in L(\Gamma_i)$, com $h_i \in k\Delta(I)$, e considere $f = h_1 h_2$. O monômio $\mathbf{X}^{\boldsymbol{e}}$ não aparece em f pela condição (2). Seja $\{g_1, \ldots, g_s\}$ uma base de Grobner para I, isto é, para todo $f \in I$, $f \neq 0$, temos $\mathrm{lm}(f)$ é múltiplo de $\mathrm{lm}(g_i)$, para algum $i \in \{1, \ldots, s\}$. Pelo algoritmo da divisão, existem $q_1, \ldots, q_s, f_2 \in k[\boldsymbol{X}]$ tais que

$$f = q_1 g_1 + \cdots + q_s g_s + f_2,$$

onde $f_2 = 0$ ou nenhum monômio em f_2 é múltiplo de $\mathrm{lm}(g_i)$, para todo $i \in \{1, \ldots, s\}$, isto é, todos os monômios de f_2 estão em $\Delta(I)$ e $\mathrm{lm}(f_2) \preceq \mathrm{lm}(f)$. Então, podemos escrever $f = f_1 + f_2$, com $f_1 \in I$ e $f_2 \in k\Delta(I)$. Temos que $\mathbf{X}^{\boldsymbol{e}}$ não aparece em f_2, pois $\mathrm{lm}(f_2) \preceq \mathrm{lm}(f) \prec \mathrm{lm}(\mathbf{X}^{\boldsymbol{e}})$ (pela condição (2)). Seja $(g+I)L(\Gamma_1) := \{(g+I)(f+I) \mid f + I \in L(\Gamma_1)\}$. Queremos mostrar

$$(g+I)L(\Gamma_1) \subset \{g' + I \mid g'h \in \ker\varphi \text{ para todo } h + I \in L(\Gamma_2)\} = L(\Gamma_2)^{\perp}.$$

Sejam $(g+I)(h_1+I) \in (g+I)L(\Gamma_1)$ e $(h_2+I) \in L(\Gamma_2)$. Temos $(g+I)(h_1+I) = gh_1 + I$, $(gh_1+I)(h_2+I) = gh_1h_2 + I$ e $\varphi(gh_1h_2) = \varphi(g(f_1+f_2)) = \varphi(gf_1 + gf_2) = \varphi(gf_2) \overset{(4.1)}{=} 0$. Logo

$$(g+I)L(\Gamma_1) \subset L(\Gamma_2)^{\perp}.$$

Aplicando ev em ambos os lados temos $\mathrm{ev}(g+I) = (g(P_1), \ldots, g(P_m)) = \beta$ concluímos

$$\beta \cdot C(L(\Gamma_1)) \subset C(L(\Gamma_2)^{\perp}).$$

Como $\mathbf{X}^{\boldsymbol{e}}$ é essencial temos $\beta_j \neq 0$, para todo $j = 1, \ldots, m$. Logo, pela condição (1)

$$\dim(\beta \cdot C(L(\Gamma_1))) = \dim(C(L(\Gamma_1))) = |\Gamma_1| = |\mathcal{X}| - |\Gamma_2| = \dim(C(L(\Gamma_2)^{\perp})).$$

Portanto $\beta \cdot C(L(\Gamma_1)) = C(L(\Gamma_2)^{\perp})$. Pelo Teorema 2.6 temos que $C(L(\Gamma_1))$ e $C(L(\Gamma_2))^{\perp}$ são monomialmente equivalentes. □

Capítulo 5

Um exemplo específico: Códigos sobre o toro degenerado

Seja $K = \mathbb{F}_q$ um corpo finito e sejam $A_1, \ldots, A_s$ subgrupos do grupo multiplicativo $(K^*, \cdot)$. O produto cartesiano

$$T := A_1 \times \cdots \times A_s = \{P_1, \ldots, P_m\}$$

é chamado *toro degenerado*. Denotemos por d_i a ordem de cada grupo cíclico A_i para todo $i = 1, \ldots, s$. Seja $\tilde{f}_i = X_i^{d_i} - 1$, com $i = 1, \ldots, s$, temos que $\{\tilde{f}_1, \ldots, \tilde{f}_n\}$ é uma base de Grobner para I pois os monômios líderes dos geradores são coprimos dois a dois (veja [3, §9, Cap. 2]) e logo

$$\Delta(I) = \{\mathbf{X}^{\mathbf{c}} = X_1^{c_1}.\cdots.X_m^{c_m} \mid 0 \leq c_i \leq d_i - 1 \text{ para todo } i = 1, \ldots, m\}.$$

Sejam $\{\mathbf{X}^{\boldsymbol{\alpha}_1}, \ldots, \mathbf{X}^{\boldsymbol{\alpha}_k}\} \subset \Delta(I)$ e $A = \{\mathbf{X}^{\boldsymbol{\alpha}_i} + I\}$ uma base de L tal que cada monômio $\mathbf{X}^{\boldsymbol{\alpha}_i} = X_1^{a_{i,1}}.\cdots.X_s^{a_{i,s}}$ para todo $i = 1, \ldots, k$ e definimos $\mathbf{X}^{\boldsymbol{\beta}_i} = X_1^{b_{i,1}}.\cdots.X_s^{b_{i,s}}$ onde $b_{i,j} = d_j - a_{i,j}$ se $a_{i,j} \neq 0$ e $b_{i,j} = 0$ se $a_{i,j} = 0$, para todo $j = 1, \ldots, s$. Seja $B := \{\mathbf{X}^{\boldsymbol{\beta}_1}, \ldots, \mathbf{X}^{\boldsymbol{\beta}_k}\}$ e observe que $B \subset \Delta(I)$.

Lema 5.1. *Seja $\mathbf{X}^{\boldsymbol{\gamma}}$ um monômio de $\Delta(I)$ onde $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_s)$. Se $\boldsymbol{\gamma} = \mathbf{0}$, então $\mathbf{X}^{\boldsymbol{\gamma}} \notin \ker \varphi$ e se $\gamma_i \neq \mathbf{0}$ para algum $i \in \{1 \ldots, s\}$, então $\mathbf{X}^{\boldsymbol{\gamma}} \in \ker \varphi$.*

Demonstração. Sejam $T = \{P_1, \ldots, P_m\}$ e t_i um gerador do grupo multiplicativo cíclico A_i, para todo $i = 1, \ldots, s$. Lembrando que $q = p^v$, p primo e $v \in \mathbb{N}_+$. Como $d_i = |A_i|$ divide $q - 1 = |k^*| = |\mathbb{F}_q^*|$ temos que $\text{mdc}(d_i, p) = 1$, para todo $i = 1, \ldots, s$. Logo $\text{mdc}(m, p) = 1$, pois $m = |T| = d_1 \cdots d_s$. Suponha $\boldsymbol{\gamma} = \mathbf{0}$. Então, $\varphi(\mathbf{X}^{\boldsymbol{\gamma}}) = \sum_{i=1}^{m} \mathbf{X}^{\boldsymbol{\gamma}}(P_i) = m \cdot 1$ e $m \cdot 1 \neq 0$ pois $\text{mdc}(m, p) = 1$. Portanto, $\mathbf{X}^{\boldsymbol{\gamma}} \notin \ker \varphi$. Suponha agora que $\gamma_i \neq \mathbf{0}$ para algum $i \in \{1 \ldots, s\}$. Então $\gamma_i \geq 1$. Suponha $i = 1$ por simplicidade de notação. Seja $T_1 := A_2 \times \cdots \times A_s$. O produto cartesiano T pode ser particionado como

$$T = \{P_1, \ldots, P_m\} = \bigcup_{i=1}^{d_1} \{(t_1^i, Q) \mid Q \in T_1\} = \{(1, Q), (t_1, Q), (t_1^2, Q), \ldots, (t_1^{d_1 - 1}, Q) \mid Q \in T_1\}.$$

Suponha $T_1 = \{Q_1, \ldots, Q_p\}$. Então

$$\begin{aligned}
\varphi(\mathbf{X}^{\boldsymbol{\gamma}}) &= \mathbf{X}^{\boldsymbol{\gamma}}(1, Q_1) + \cdots + \mathbf{X}^{\boldsymbol{\gamma}}(1, Q_p) + \cdots + \mathbf{X}^{\boldsymbol{\gamma}}(t_1^{d_1 - 1}, Q_1) + \cdots + \mathbf{X}^{\boldsymbol{\gamma}}(t_1^{d_1 - 1}, Q_p) \\
&= 1 \cdot X_2^{\gamma_2} \cdots X_s^{\gamma_s}(Q_1) + \cdots + 1 \cdot X_2^{\gamma_2} \cdots X_s^{\gamma_s}(Q_p) + \cdots + (t_1^{d_1 - 1})^{\gamma_1} \cdot X_2^{\gamma_2} \cdots X_s^{\gamma_s}(Q_1) \\
&\quad + \cdots + (t_1^{d_1 - 1})^{\gamma_1} \cdot X_2^{\gamma_2} \cdots X_s^{\gamma_s}(Q_p) \\
&= \left(1 + \cdots + (t_1^{d_1 - 1})^{\gamma_1}\right) (X_2^{\gamma_2} \cdots X_s^{\gamma_s}(Q_1)) + \cdots + \left(1 + \cdots + (t_1^{d_1 - 1})^{\gamma_1}\right) (X_2^{\gamma_2} \cdots X_s^{\gamma_s}(Q_p)) \\
&= \left(1 + \cdots + (t_1^{d_1 - 1})^{\gamma_1}\right) (X_2^{\gamma_2} \cdots X_s^{\gamma_s}(Q_1) + \cdots + X_2^{\gamma_2} \cdots X_s^{\gamma_s}(Q_p)) \\
&= \left(1 + \cdots + (t_1^{d_1 - 1})^{\gamma_1}\right) \left(\sum_{Q \in T_1} X_2^{\gamma_2} \cdots X_s^{\gamma_s}(Q) \right).
\end{aligned}$$

Como $|A_1| = d_1$ então $(t_1^{\gamma_1})^{d_1} - 1 = 0$. Como $(t_1^{\gamma_1})^{d_1} - 1 = (t_1^{\gamma_1} - 1)((t_1^{\gamma_1})^{d_1-1} + \ldots + 1)$ e $t_1^{\gamma_1} - 1 \neq 0$ (pois $\gamma_1 \neq 0$) segue que $(t_1^{\gamma_1})^{d_1-1} + \ldots + 1 = 0$. Logo $\varphi(\mathbf{X}^{\boldsymbol{\gamma}}) = 0$ e $\mathbf{X}^{\boldsymbol{\gamma}} \in \ker\varphi$.

□

O principal resultado em relação aos códigos de avaliação sobre T é o seguinte.

Proposição 5.2. *Seja $L \subset k[\boldsymbol{X}]/I$ um subespaço vetorial de $k[\boldsymbol{X}]/I$ com uma base do tipo $A = \{\mathbf{X}^{\boldsymbol{\alpha}_1} + I, \ldots, \mathbf{X}^{\boldsymbol{\alpha}_k} + I\}$, com $\mathbf{X}^{\boldsymbol{\alpha}_i} \in \Delta(I), i = 1, \ldots, k$, e seja $B := \{\mathbf{X}^{\boldsymbol{\beta}_1}, \ldots, \mathbf{X}^{\boldsymbol{\beta}_k}\}$ como definido acima. Então o conjunto $\{\mathbf{X}^{\mathbf{c}} + I \mid \mathbf{X}^{\mathbf{c}} \in (\Delta(I) \setminus B)\}$ é uma base para $L^{\perp}$.*

Demonstração. Como $|\Delta(I)| = |T|$, pela Proposição 2.7 temos

$$\dim(L^{\perp}) = |T| - \dim(L) = |T| - k = |\Delta(I) \setminus B|.$$

Seja $\mathbf{X}^{\mathbf{c}} \in (\Delta(I) \setminus B)$. Como $A = \{\mathbf{X}^{\boldsymbol{\alpha}_i} + I, i = 1, \ldots, k\}$ é uma base para L é suficiente mostrar que $\mathbf{X}^{\mathbf{c}} \cdot \mathbf{X}^{\boldsymbol{\alpha}_i} \in \ker\varphi$, para todo $i = 1, \ldots, k$. Se $\mathbf{X}^{\boldsymbol{\alpha}_i} = 1$, então $\mathbf{X}^{\boldsymbol{\beta}_i} = 1$ para todo $i = 1, \ldots, k$ e $\mathbf{X}^{\mathbf{c}} \neq 1$. Assim $\mathbf{X}^{\mathbf{c}} \cdot \mathbf{X}^{\boldsymbol{\alpha}_i} = \mathbf{X}^{\mathbf{c}} \cdot 1 \in \ker\varphi$, para todo $i = 1, \ldots, k$ pelo lema anterior. Se $\mathbf{X}^{\boldsymbol{\alpha}_i} \neq 1$, então

$$\mathbf{X}^{\boldsymbol{\alpha}_i} \cdot \mathbf{X}^{\mathbf{c}} = X_1^{a_{i,1}+c_1} \cdot \cdots \cdot X_s^{a_{i,s}+c_s} = X_1^{d_1-b_{i,1}+c_1} \cdot \cdots \cdot X_s^{d_s-b_{i,s}+c_s}.$$

Se $d_j - b_{i,j} + c_j \not\equiv 0 \pmod{d_j}$ então $\mathbf{X}^{\boldsymbol{\alpha}_i} \cdot \mathbf{X}^{\mathbf{c}} \equiv \mathbf{X}^{\boldsymbol{\delta}} \pmod{I}$ onde, no monômio $\mathbf{X}^{\boldsymbol{\delta}}$, a potência de X_j é um inteiro positivo menor do que d_j. Fazendo isso para cada índice j tal que $d_j - b_{i,j} + c_j \not\equiv 0 \pmod{d_j}$, podemos concluir que $\mathbf{X}^{\boldsymbol{\alpha}_i} \cdot \mathbf{X}^{\mathbf{c}} \in \ker\varphi$ pelo lema anterior. Se $d_j - b_{i,j} + c_j \equiv 0 \pmod{d_j}$ para todo $j = 1, \ldots, s$ então pela definição de $\boldsymbol{\beta}_i$, e do fato de que $0 \leq b_{i,j} \leq d_j - 1$, $j = 1, \ldots, s$, bem como $0 \leq c_j \leq d_j - 1$ temos que ter $d_j - b_{i,j} + c_j = d_j$ para $j = 1, \ldots, s$, isto é, $\mathbf{X}^{\boldsymbol{\beta}_i} = \mathbf{X}^{\mathbf{c}}$, contradição pois $\mathbf{X}^{\mathbf{c}} \notin B$. Logo $\{\mathbf{X}^{\mathbf{c}} + I \mid \mathbf{X}^{\mathbf{c}} \in (\Delta(I) \setminus B)\} \subset L^{\perp}$ e como os elementos desse conjunto são linearmente independentes, segue que é base para $L^{\perp}$. □

Corolário 5.3. *Seja $C(L)$ um código monomial sobre T e seja $L^{\perp}$ o dual algébrico. Então $C(L)^{\perp} = C(L^{\perp})$ e $C(L)^{\perp}$ é um código monomial sobre T.*

Demonstração. O código linear $C(L)^{\perp}$ é o código de avaliação $C(L^{\perp})$ sobre T (segue do Teorema 2.6) e $L^{\perp}$ é gerado pelo conjunto de monômios em $(\Delta(I) \setminus B)$ (Proposição 5.2), logo $C(L)^{\perp}$ é um código monomial . □

Corolário 5.4. *Seja $C(L)$ um código tórico generalizado em $T = (K^*)^S$, $K = \mathbb{F}_q$, e seja $L^{\perp}$ o dual algébrico. Então, $C(L)^{\perp} = C(L^{\perp})$ e $C(L)^{\perp}$ é um código tórico generalizado.*

Demonstração. Segue do Corolário anterior para $A_i = K^*$ para todo $i = 1, \ldots, s$. □

Referências Bibliográficas

[1] CARVALHO, C. **Gröbner bases methods in coding theory**. Contemp. Math. vol. 642, pp. 73-86, 2015. https://doi.org/10.1090/conm/642/12881

[2] LÓPEZ, H. H.; SOPRUNOV, I.; VILLAREAL, R. H. **The dual of an evaluation code**. Des. Codes and Cryptogr., vol. 71, pp. 5-19, 2021.

[3] COX, D. A.; LITTLE, J.; O'SHEA, D. **Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra**. 4rd ed., Springer Science & Business Media, 2015. https://doi.org/10.1007/978-3-319-16721-3

[4] FITZGERALD, J.; LAX, R.F. **Decoding affine variety codes using Gröbner bases**. Des. Codes and Cryptogr., vol. 13, pp. 147-158, 1998. https://doi.org/10.1023/A:1008274212057

[5] BUCHBERGER, B. **Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal**. Mathematical Institute, University of Innsbruck, Austria. PhD Thesis. 1965. An English translation appeared in J. Symbolic Comput. 41 pp. 475-511, 2006. https://doi.org/10.1016/j.jsc.2005.09.007

[6] BUCHBERGER, B. **A theoretical basis for the reduction of polynomials to canonical forms**. SIGSAM Bull. (ACM Special Interest Group on Symbolic and Algebraic Manipulation) 10 (3), pp. 19-29, 1976. https://doi.org/10.1145/1088216.1088219

[7] MACWILLIAMS, F.J; SLOANE, N.J.A. **The Theory of Error-Correcting Codes**. Amsterdam, Netherlands: North-Holland, 1977.