GUILHERME DOS SANTOS MARTINS DIAS

CÓDIGOS PROJETIVOS PARAMETRIZADOS

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2017

GUILHERME DOS SANTOS MARTINS DIAS

CÓDIGOS PROJETIVOS 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
2017

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

V111c
2017

Dias, Guilherme dos Santos Martins, 1992 -
Códigos projetivos parametrizados / Guiherme dos Santos Martins Dias. - 2017
59 f.: il.

Orientador: Cícero Fernandes de Carvalho
Dissertação (mestrado) - Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática
Inclui bibliografia

1. Matemática - Teses. 2. Códigos de 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: Guilherme dos Santos Martins Dias.

NÚMERO DE MATRÍCULA: 11512MAT005.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Códigos Projetivos Parametrizados.

ORIENTADOR: Prof. Dr. Cícero Fernandes de Carvalho.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala 1F261, Bloco 1F, Campus Santa Mônica, em 23 de Fevereiro de 2017, às 14h, pela seguinte Banca Examinadora:

NOME	ASSINATURA
Prof. Dr. Cicero Fernandes de Carvalho UFU - Universidade Federal de Uberlândia (orientador)	
Prof. Dr. Victor Gonzalo Lopez Neumann UFU - Universidade Federal de Uberlândia	
Prof. Dr. Paulo Roberto Brumatti UNICAMP - Universidade Estadual de Campinas	

Uberlândia-MG, 23 de Fevereiro de 2017.

Dedicatória

Dedico aos meus familiares e amigos.

Agradecimentos

Agradeço primeiramente a Deus por me dar forças para superar cada obstáculo, por me proporcionar inúmeras conquistas e por colocar pessoas boas em meu caminho.

Agradeço também a minha familia, por estar sempre ao meu lado nas dificuldades do dia a dia. Minha mãe Lilian e meu pai Rubens, que sempre abriram mão de muita coisa para me dar amor, carinho e conforto. Este trabalho é o resultado do esforço daqueles que sempre me mostraram o que é certo, honesto e justo. A minha avó Adelina que sempre colocou os meus estudos como meta de vida, me apoiando em cada ocasião. As minhas tias Ângela e Márcia pelos ensinamentos matemáticos fundamentais para que eu seguisse esse caminho. A minha namorada Caroline que sempre me deu muito amor e forças pra não me deixar desanimar nos momentos difíceis. Agradeço também ao meu primo (irmão) Gustavo pelo companheirismo e apoio, aos demais tios e primos que são fonte de amor e carinho.

Aos professores da Universidade Federal de Uberlândia e da Universidade de Coimbra por todos os ensinamentos, conselhos e noites sem dormir que me proporcionaram. São peças fundamentais para a conclusão deste trabalho. Em particular, ao meu orientador Cicero Fernandes de Carvalho.

Aos meus colegas do mestrado José Lucas, Wagner, Suélen, Alexandre e Magna pelos momentos de estudos e também pelos momentos de descontração. A Davidson que sempre esteve disposto a ajudar nos momentos de desespero. Aos colegas de graduação Guilherme Henrique, Paulo Victor e André, que sempre deram apoio e torceram por mim. Agradeço a todos os colegas que tiveram participação nesta caminhada.

Agradeço à Capes pelo auxílio financeiro durante todo o curso de mestrado.

Agradeço também aos professores Victor Gonzalo Lopez Neumann e Paulo Roberto Brumatti por terem aceito o convite para fazerem parte da minha banca.

DIAS, G. S. M. *Códigos Projetivos Parametrizados* 2017. - 58p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Este trabalho tem como objetivo estudar os parâmetros de um código projetivo gerado por um conjunto algébrico tórico X que é parametrizado por uma quantidade finita de monômios em várias variáveis. Também podemos obter conjuntos algébricos tóricos associados a matrizes de incidência de grafos e cluters, e nestes casos obtemos resultados mais precisos, já que os conjuntos algébricos tóricos obtidos são parametrizados por monômios com mesmo grau. Nos capítulos iniciais são apresentados os conceitos básicos que servirão de ferramentas para atingir estes objetivos.

Palavras-chave: Código Projetivo, Parâmetros de um código, conjunto algébrico tórico.

DIAS, G. S. M. *Projecive parameterized linear codes* 2017. - 58p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Abstract

This work aims at studying the parameters of a projective code generated by an algebraic toric set X which is parameterized by a finite number of monomials in several variables. We also can obtain algebraic toric sets associated to graph or clutter incidence matrices and in these cases we obtain more precise results since the algebraic toric sets which are obtained are parameterized by monomials of the same degree. In the first chapters we introduce basic concepts which will serve as tools to reach our aim.

Keywords: Projective codes; Codes parameters; Algebraic toric set.

SUMÁRIO

Resumo vii

Abstract viii

Introdução 1

1 Polinômios 3

2 Espaço Projetivo 7

3 Corpos finitos 16
3.1 A característica de um corpo 16
3.2 Potências da característica 17
3.3 Elementos Primitivos 21

4 Códigos 23
4.1 Códigos Lineares 23
4.2 Código duais 26

5 Grafos 31

6 Parâmetros de um código projetivo Parametrizado 33
6.1 Código projetivo parametrizado por conjunto tórico algébrico 33
6.2 Os Parâmetros de $C_X(d)$ 36
6.2.1 Comprimento 36
6.2.2 Dimensão 39
6.2.3 Distância Mínima 41

7 Aplicação dos resultados apresentados 45
7.1 Códigos projetivos parametrizados pela matriz de incidência de um grafo . 45
7.2 Código projetivo parametrizado pela matriz de incidência de um clutter . . 47

7.3 Código projetivo parametrizado por uma matriz que não representa um clutter 49

Referências Bibliográficas **51**

INTRODUÇÃO

Os códigos corretores de erros estão presentes em nosso cotidiano de inúmeras formas, sempre que fazemos uso de informações digitalizadas como assistir TV, falar ao telefone, ouvir uma música, armazenar dados em um computador. Um código corretor de erros permite recuperar uma informação transmitida, detectando e corrigindo erros que modifiquem essa informação durante a transferência. A Teoria de Códigos Corretores de Erros foi criada pelo matemático *Claude Elwood Shannon*. Em 1948 Shannon publicou o artigo científico intitulado como *"A Mathematical theory of Communication"* e esta publicação deu início à Teoria dos Códigos. A partir da década de 70, com as pesquisas espaciais e a grande popularização dos computadores, essa teoria começou a motivar pesquisas tanto de matemáticos quanto de engenheiros. Hoje em dia os resultados dessas pesquisas são de grande importância para as operações espaciais e comunicações de modo geral.

Este trabalho tem como objetivo estudar alguns tipos de códigos lineares, em particular, os parâmetros principais (a saber, comprimento, dimensão e distância mínima) de um código definido sobre um conjunto tórico, e está dividido em 7 capítulos. No primeiro, veremos alguns conceitos básicos sobre o anel de polinômios de várias variáveis $\mathrm{K}[x_1, \ldots, x_n]$. No segundo capítulo, definiremos o espaço projetivo n-dimensional e apresentaremos algumas propriedades deste espaço. Em seguida definiremos ideais e polinômios homogêneos, variedades projetivas e uma relação entre ideais homogêneos e variedades projetivas. Estes primeiros capítulos são baseados no livro de Cox, D., Little, J., e O'Shea, D., *Ideals, Varieties, e Algorithms* [1].

O terceiro capítulo é voltado ao estudo de corpos finitos. Iniciamos com a definição de característica de um corpo finito e em seguida apresentamos algumas de suas propriedades. Em seguida definimos elementos primitivos e provamos a existência de elementos primitivos em um corpo finito. O quarto capítulo é dedicado ao estudo de códigos lineares, que é ferramenta essencial para o trabalho. Neste capítulo, será definida distância de Hamming e os parâmetros dos códigos lineares e por fim a cota de Singleton, que relaciona estes parâmetros. Estes capítulos são baseados em partes do livro de Hefez, A e Villela, M. L. T., *Códigos Corretores de Erros*, [5].

O quinto capítulo é uma breve introdução à Teoria dos Grafos. Neste capítulo definimos grafo, grafo conexo e a matriz de incidência de um grafo.

No sexto capítulo, definimos o conjunto tórico algébrico X parametrizado por um conjunto finito de monômios em $\mathbb{F}_q[Z_1, \ldots, Z_m]$, onde $\mathbb{F}_q$ é um corpo finito com q elementos. Em seguida, construímos o *código projetivo parametrizado* de ordem d, que é obtido por meio de uma transformação linear e será denotado por $C_X(d)$. Esta transformação avalia polinômios homogêneos de grau d nos pontos de X. Após construirmos este código, estudaremos o comprimento, a distância mínima e a dimensão.

Por fim, daremos alguns exemplos de códigos projetivos parametrizados por certos monômios ou gerados a partir de uma matriz de incidência de um grafo. Apresentaremos algumas tabelas relacionando estes parâmetros nestes casos particulares. Este capítulo é baseado no artigo [4].

CAPÍTULO 1

POLINÔMIOS

Neste capítulo, iremos apresentar uma breve introdução sobre anel de polinômios de várias variáveis, assim como alguns resultados básicos.

Definição 1.1. *Um monômio em $x_1, \ldots, x_n$ é um produto da forma*

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

*onde todos os expoentes $\alpha_1, \cdots, \alpha_n$ são inteiros não negativos. O **grau total** deste monômio é a soma $|\alpha| = \alpha_1 + \cdots + \alpha_n$.*

Podemos simplificar a notação para monômios da seguinte forma: seja $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ uma n-upla de inteiros não negativos. Então definimos

$$\boldsymbol{x^{\alpha}} = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

Definição 1.2. *Um polinômio f nas variáveis $x_1, \ldots, x_n$ com os coeficientes no corpo* K *e uma combinação linear finita de monômios. Onde podemos escrever f na forma:*

$$f = \sum_{\boldsymbol{\alpha}} \boldsymbol{a_{\alpha} x^{\alpha}}, \boldsymbol{a_{\alpha}} \in \mathrm{K}.$$

onde a soma é sobre um número finitos de n-uplas $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_n)$. O conjunto dos polinômios em $x_1, ..., x_n$ com coeficientes em K *é denotado por* $\mathrm{K}[x_1, ..., x_n]$.

Definição 1.3. *Seja $f = \sum_{\boldsymbol{\alpha}} \boldsymbol{a_{\alpha} x^{\alpha}}, \boldsymbol{a_{\alpha}} \in \mathrm{K}$ um polinômio em $\mathrm{K}[x_1, \cdots, x_n]$.*

*(i) Chamamos $a_{\boldsymbol{\alpha}}$ o **coeficiente** do monômio $\boldsymbol{x^{\alpha}}$.*

*(ii) Se $a_{\boldsymbol{\alpha}} \neq 0$, então chamamos $a_{\boldsymbol{\alpha}} \boldsymbol{x^{\alpha}}$ um **termo** de f.*

*(iii) O **grau total** de f, denotado $\deg(f)$, é o máximo $|\boldsymbol{\alpha}|$ tal que os coeficientes $a_{\boldsymbol{\alpha}}$ é diferente de zero.*

Primeiramente, notemos que podemos relacionar o monômio $\boldsymbol{x^{\alpha}} = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ com a n-upla dos expoentes $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. Esta relação estabelece uma correspondência biunívoca entre os monômios em $\mathrm{K}[x_1, \dots, x_n]$ e $\mathbb{Z}_{\geq 0}^n$. Assim, dada uma ordem em $>$ em $\mathbb{Z}_{\geq 0}^n$, dizemos que $\boldsymbol{x^{\alpha}} > \boldsymbol{x^{\beta}}$ se $\boldsymbol{\alpha} > \boldsymbol{\beta}$.

Definição 1.4. *Uma* ***ordem de monômios*** $>$ *em* $\mathrm{K}[x_1, \dots, x_n]$ *é uma relação sobre* $\mathbb{Z}_{\geq 0}^n$*, ou equivalentemente, uma relação sobre o conjunto dos monômios* $\boldsymbol{x^{\alpha}}$*,* $\boldsymbol{\alpha} \in \mathbb{Z}_{\geq 0}^n$*, satisfazendo:*

i) $>$ *é uma relação de ordem total (ou linear) em* $\mathbb{Z}_{\geq 0}^n$*, ou seja, dados* $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$*, apenas uma das condições são verdadeiras:* $\alpha > \beta$*,* $\beta > \alpha$ *ou* $\alpha = \beta$*.*

ii) Dados $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}^n$*, se* $\alpha > \beta$ *e* $\gamma \in \mathbb{Z}_{\geq 0}^n$ *então* $\alpha + \gamma > \beta + \gamma$*.*

iii) $>$ *é bem ordenada sobre* $\mathbb{Z}_{\geq 0}^n$*. Isto significa que toda ordenação de um conjunto não vazio sobre* $\mathbb{Z}_{\geq 0}^n$*, possui o menor elemento.*

Lema 1.5. *Uma relação de ordem* $>$ *em* $\mathbb{Z}_{\geq 0}^n$ *é bem ordenada se, e somente se, toda sequência estritamente decrescente em* $\mathbb{Z}_{\geq 0}^n$*, eventualmente se estabiliza.*

Demonstração. ($\Rightarrow$) Vamos supor que exista uma sequência $(\alpha(1), \alpha(2), \dots \alpha(n), \dots)$ de elementos de $\mathbb{Z}_{\geq 0}^n$, que seja estritamente decrescente e nunca se estabiliza, isto é, $\alpha(1) > \alpha(2) > \alpha(3) > \dots$. Desta forma, o subconjunto não vazio de $\mathbb{Z}_{\geq 0}^n$ dado por $\{\alpha(1), \alpha(2), \dots\}$, não possui um elemento mínimo. Logo $>$ não é bem ordenada sobre $\mathbb{Z}_{\geq 0}^n$.

($\Leftarrow$) Vamos supor agora que $>$ não é bem ordenada sobre $\mathbb{Z}_{\geq 0}^n$. Então, consideremos o subconjunto não vazio como sendo o próprio $\mathbb{Z}_{\geq 0}^n$. Tomemos agora um elemento $\alpha(1)$ neste conjunto. Como supomos que $>$ não é bem ordenada, existe um elemento $\alpha(2) \in \mathbb{Z}_{\geq 0}^n$, tal que $\alpha(1) > \alpha(2)$. Da mesma forma, existe um elemento $\alpha(3) \in \mathbb{Z}_{\geq 0}^n$, tal que $\alpha(2) > \alpha(3)$. Repetindo esse processo infinitamente, o que é possível já que $\mathbb{Z}_{\geq 0}^n$ não possui um elemento mínimo, construímos uma sequência $(\alpha(1), \alpha(2), \dots \alpha(n), \dots)$ de elementos em $\mathbb{Z}_{\geq 0}^n$ que nunca se estabilizará.

□

Definição 1.6. *(**Ordem Lexicográfica**). Seja* $\alpha = (\alpha_1, \dots, \alpha_n)$ *e* $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$*. Diremos que* $\alpha >_{lex} \beta$ *se o vetor diferença* $\alpha - \beta \in \mathbb{Z}_{\geq 0}^n$*, possuir a primeira entrada não nula, da esquerda pra direita, positiva. Vamos escrever* $x^{\alpha} >_{lex} x^{\beta}$ *se* $\alpha >_{lex} \beta$*.*

Por exemplo:

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

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

(iii) As variáveis $x_1, \dots, x_n$ são ordenadas da maneira usual pela ordem lexicográfica:

$$(1, 0, 0, \dots, 0) >_{lex} (0, 1, 0, \dots, 0) >_{lex} \cdots >_{lex} (0, \dots, 0, 1).$$

ou seja, $x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$.

Proposição 1.7. *A ordem lexicográfica em $\mathbb{Z}^n_{\geq 0}$ é uma ordem de monômios.*

Demonstração. Para demonstrar esta proposição, devemos verificar que são satisfeitos os três itens da definição de ordem monomial.

i) Dados dois elementos α e β de $\mathbb{Z}^n_{\geq 0}$. Se a primeira entrada não nula, da direita para a esquerda de $\alpha - \beta$ for positiva, então $\alpha >_{lex} \beta$, se for negativa, $\beta >_{lex} \alpha$. Já se todas as entradas de $\alpha - \beta$ forem nulas, segue que $\alpha = \beta$. Logo, $>_{lex}$ é uma ordem total.

ii) Sejam $\alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$, tais que $\alpha >_{lex} \beta$. Notemos agora que

$$(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$$

tem a primeira entrada nao nula, da direita para a esquerda, positiva. Logo, $\alpha + \gamma >_{lex} \beta + \gamma$.

iii) Suponha que $>_{lex}$ não é bem-ordenado. Então por 1.5, existe uma sequência estritamente decrescente

$$\alpha_1 >_{lex} \alpha_2 >_{lex} \alpha_3 >_{lex} \dots,$$

de elementos de $\mathbb{Z}^n_{\geq 0}$, digamos que $\alpha_j = (\alpha_{j1}, \dots, \alpha_{jn})$, para todo $j \in \mathbb{N}$. Vamos mostrar que isso leva a uma contradição.
Considere as primeiras entradas dos vetores $\alpha_j \in \mathbb{Z}^n_{\geq 0}$. Obtemos assim uma sequência $(\alpha_{11}, \alpha_{21}, \alpha_{31}, \dots)$ de números inteiros não negativos. Pela definição da *ordem lexicográfica*, esta sequência é não crescente, já que $\alpha_j >_{lex} \alpha_{j+1}$. Como $\mathbb{Z}_{\geq 0}$ é bem-ordenado, segue que esta sequência deve "estabilizar", isto é, existe um k tal que $\alpha_{k1} = \alpha_{i1}$, para todo $i \geq k$. Deste modo, as primeiras entradas dos termos da sequência (α_j) serão iguais a partir do termo α_k.

Em seguida, a segunda e subsequentes entradas serão utilizadas para comparar os termos da sequência (a_j), já que as primeiras entradas são iguais. Assim, consideremos a sequência de inteiros não negativos $(\alpha_{k2}, \alpha_{(k+1)2}, \alpha_{(k+2)2}, \dots)$, que também será não crescente pela definição de ordem lexicográfica.

Por um raciocínio análogo ao anterior, existe um termo α_l tal que $\alpha_{j2} = \alpha_{l2}$, para todo $j \geq l$, ou seja, toda as segundas entradas da sequencia (α_j) serão iguais a partir do termo α_l.

Continuando esta ideia, existe um $m \in \mathbb{N}$ tal que todas as entradas de α_m serão iguais às entradas de α_{m+1}. Absurdo, pois $\alpha_m >_{lex} \alpha_{m+1}$.

□

Vejamos agora outros exemplos de ordenação de monômios.

Definição 1.8. *Sejam $\alpha = (\alpha_1, \dots, \alpha_n)$ e $\beta = (\beta_1, \dots, \beta_n)$ em $\mathbb{Z}^n_{\geq 0}$. Considerando $|\alpha| = \sum_{i=1}^{n} \alpha_i$ e $|\beta| = \sum_{i=1}^{n} \beta_i$, definimos as seguintes ordens monomiais:*

- *Ordenação Graduada Lexicográfica: Dizemos* $\alpha >_{grlex} \beta$ *se*

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

- *Ordenação Graduada Lexicográfica Reversa: Dizemos* $\alpha >_{grevlex} \beta$ *se*

$$|\alpha| > |\beta|, \ ou \ |\alpha| = |\beta|$$

e o vetor diferença $\alpha - \beta$ *tem a primeira entrada não nula, da direita para a esquerda, negativa.*

Definição 1.9. *Seja* $f = \sum_{\boldsymbol{\alpha}} a_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$ *um polinômio não nulo em* $\mathrm{K}[x_1, \ldots, x_n]$ *e seja* $>$ *uma ordenação monomial fixada.*

i) O multigrau de f *é*

$$\mathrm{mdeg}(f) = \max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0).$$

ii) O coeficiente líder de f *é*

$$\mathrm{lc}(f) = a_{\mathrm{mdeg}(f)} \in \mathrm{K}.$$

iii) O monômio líder de f *é*

$$\mathrm{lm}(f) = x^{\mathrm{mdeg}(f)}$$

com coeficiente 1*.*

iv) O termo líder de f *é*

$$\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{lm}(f).$$

Para exemplificar, considere o polinômio $f = yz^2 - 9x^3 + xz^2 - 4y \in \mathrm{K}[x, y, z]$ e a ordem lexicográfica. Então $\mathrm{mdeg}(f) = (3, 0, 0)$, $\mathrm{lc}(f) = -9$, $\mathrm{lm}(f) = x^3$ e $\mathrm{lt}(f) = -9x^3$.

CAPÍTULO 2

ESPAÇO PROJETIVO

Seja K um corpo. Definimos uma relação sobre os pontos de $\mathrm{K}^{n+1}\backslash\{0\}$, onde 0 é o vetor nulo do espaço K^{n+1}, da seguinte forma,

$$(x'_0, \ldots, x'_n) \sim (x_0, \ldots, x_n) \Leftrightarrow \text{existe } \lambda \in \mathrm{K}\backslash\{0\}, \text{ tal que } (x'_0, \ldots, x'_n) = \lambda(x_0, \ldots, x_n).$$

É fácil ver que esta é uma relação de equivalência.

Definição 2.1. *O espaço projetivo de dimensão n sobre o corpo* K*, denotado por* $\mathbb{P}^n(\mathrm{K})$*, é o conjunto das classes de equivalência de* $\sim$ *sobre* K^{n+1}*. Isto é*

$$\mathbb{P}^n(\mathrm{K}) = (\mathrm{K}^{n+1}\backslash\{0\})/\sim .$$

Um ponto de $p \in \mathbb{P}^n(\mathrm{K})$, é denotado por $p = (x_0 : \ldots : x_n)$ e dizemos que $(x_0 : \ldots : x_n)$ são as coordenadas homogêneas de p. Observemos que cada ponto no espaço projetivo possui vários conjuntos de coordenadas homogêneas. Por exemplo, em $\mathbb{P}^3(\mathbb{C})$, as coordenadas homogêneas $(0 : \sqrt{2} : 0 : i)$ e $(0 : 2i : 0 : -\sqrt{2})$ descrevem o mesmo ponto, já que $(0, 2i, 0, -\sqrt{2}) = \sqrt{2}i(0, \sqrt{2}, 0, i)$.

Proposição 2.2. *Seja*

$$U_0 = \{(x_0 : \ldots : x_n) \in \mathbb{P}^n(\mathrm{K}) : x_0 \neq 0\} \subset \mathbb{P}^n(\mathrm{K}).$$

A aplicação $\phi : \mathrm{K}^n \longrightarrow \mathbb{P}^n(\mathrm{K})$ *que associa* $(a_1, \ldots, a_n)$ *ao ponto com coordenada homogênea* $(1 : a_1 : \ldots : a_n)$ *é uma bijeção entre* K^n *e* $U_0 \subset \mathbb{P}^n(\mathrm{K})$*.*

Demonstração. Já que a primeira componente de $\phi(a_1, \ldots, a_n) = (1 : a_1 : \ldots : a_n)$ não é nula, temos $\mathrm{Im}(\phi) \subset U_0$. Suponha $\phi(a_1, \ldots, a_n) = \phi(b_1, \ldots, b_n)$, portanto $(1 : a_1 : \ldots : a_n)$ e $(1 : b_1 : \ldots : b_n)$ seriam representantes de um mesmo ponto, portanto $(1 : a_1 : \ldots : a_n) = \lambda(1 : b_1 : \ldots : b_n)$. Da primeira coordenada obtemos que $1 = \lambda 1$, portanto $\lambda = 1$ e $(a_1, \ldots, a_n) = (b_1, \ldots, b_n)$, ou seja, ϕ é injetor.

Seja agora $(x_0 : x_1 : \ldots : x_n) \in U_0$, assim $x_0 \neq 0$. Dessa forma, $(x_0 : x_1 : \ldots : x_n)$ e $\frac{1}{x_0}(x_0 : x_1 : \ldots : x_n)$ representam o mesmo ponto em $\mathbb{P}^n(\mathrm{K})$. Logo

$$(x_0 : x_1 : \ldots : x_n) = \left(1 : \frac{x_1}{x_0} : \ldots : \frac{x_n}{x_0}\right) = \phi\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right), \text{ com } \left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \in \mathrm{K}^n$$

logo ϕ sobrejetor e, portanto, uma bijeção. □

Pela definição de U_0, temos que $\mathbb{P}^n(\mathrm{K}) = U_0 \cup H_0$, onde

$$H_0 = \{p \in \mathbb{P}^n(\mathrm{K}) : p = (0 : x_1 : \ldots : x_n)\}.$$

Se identificarmos U_0 como espaço afim K^n, então podemos pensar em H_0 como sendo o hiperplano do infinito. Como $\mathbb{P}^{n-1}(\mathrm{K}) \to H_0$ dada por $(x_1 : ... : x_n) \mapsto (0 : x_1 : ... : x_n)$ é uma bijeção, podemos identificar H_0 como sendo $\mathbb{P}^{n-1}(\mathrm{K})$.

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

Corolário 2.3. *Para cada $i = 0, ..., n$, seja*

$$U_i = \{(x_0 : ... : x_n) \in \mathbb{P}^n(\mathrm{K}) : x_i \neq 0\}.$$

(*i*) *Cada ponto de U_i tem correspondência injetora com os pontos de* K^n.

(*ii*) *Os complementares de $\mathbb{P}^n(\mathrm{K}) - U_i$ podem ser identificados como $P^{n-1}(\mathrm{K})$.*

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

Demonstração. O ítem (*i*) é análogo a proposição anterior e o item (*ii*) é análogo ao raciocínio usado acima.

Provemos agora a igualdade do item (*iii*). Seja $p \in \mathbb{P}^n(\mathrm{K})$, então $p = (x_0 : \ldots : x_n)$, onde existe $i \in \{0, \ldots, n\}$ tal que $x_i \neq 0$, ou seja, $p \in U_i$ e portanto $p \in \bigcup_{i=0}^{n} U_i$. Reciprocamente, seja agora $p \in \bigcup_{i=0}^{n} U_i$, então existe $i \in \{0, \ldots, n\}$ tal que $p \in U_i$, assim $p = (x_0 : \ldots : x_i : \ldots : x_n)$, onde $x_i \neq 0$, portanto $p \in \mathbb{P}^n(\mathrm{K})$.

□

Dados os polinômios $f_1, \ldots, f_s \in \mathrm{K}[x_1, \ldots, x_n]$, definimos

$$\boldsymbol{V}(f_1, \ldots, f_s) := \{(a_1, \ldots, a_n) \in \mathrm{K}^n : f_i(a_1, \ldots, a_n) = 0, \forall i = 1, \ldots, n\}.$$

Este conjunto é chamado de a *Variedade afim* definida pelos polinômios $f_1, \ldots, f_s$.

Vejamos que para no caso do espaço projetivo este conjunto não está bem definido. Por exemplo, considere $\mathbb{P}^2(\mathbb{R})$, podemos tentar construir $\boldsymbol{V}(x_1 - x_2^2)$. O ponto $p = (x_0 : x_1 : x_2) = (1 : 4 : 2)$ aparece neste conjunto, já que satisfaz $4 - 2^2 = 0$, mas se considerarmos um outro representante de p, sendo ele $(2 : 4 : 8)$, já que $(2, 8, 4) = 2(1, 4, 2)$, temos que essa nova representação para p não pertence à $\boldsymbol{V}(x_1 - x_2^2)$, uma vez que $8 - 4^2 = -8 \neq 0$. Vejamos então como definir $\boldsymbol{V}(f)$.

Definição 2.4. Um polinômio $f \in \mathrm{K}[x_1, \ldots, x_n]$ é dito homogêneo de grau total m se todos os monômios de f têm grau total igual a m.

Proposição 2.5. *Seja $f \in \mathrm{K}[x_0, \ldots, x_n]$ um polinômio homogêneo. Se f anula em um representante de $p \in \mathbb{P}^n(\mathrm{K})$, então f anula para todos representantes de p. Em particular $\boldsymbol{V}(f) = \{p \in \mathbb{P}^n(\mathrm{K}) : f(p) = 0\}$ é um subconjunto bem definido de $\mathbb{P}^n(\mathrm{K})$.*

Demonstração. Sejam $(a_0, \ldots, a_n)$ e $(\lambda a_0, \ldots, \lambda a_n)$ coordenadas homogêneas de $p \in \mathbb{P}^n(\mathrm{K})$ e assumindo que $f(a_0, \ldots, a_n) = 0$. Se f é homogêneo de grau total m, então cada monômio de f é da forma

$$c x_0^{\alpha_0} \cdots x_n^{\alpha_n},$$

onde $\alpha_0 + \cdots + \alpha_n = m$. Se substituirmos $x_i = \lambda a_i$, obtemos $c(\lambda a_0)^{\alpha_0} \ldots (\lambda a_n)^{\alpha_n} = c\lambda^m a_0^{\alpha_0} \ldots a_n^{\alpha_n}$. Ou seja, em todos as parcelas apareceram o termo λ^m quando fizermos a substituição, então podemos colocá-lo em evidência na soma, assim

$$f(\lambda a_0, \ldots, \lambda a_n) = \lambda^m f(a_0, \ldots, a_n) = 0.$$

□

Definição 2.6. Seja K um corpo e sejam $f_1, \ldots, f_s$ polinômios homogêneos em $\mathrm{K}[x_0, \ldots, x_n]$. O conjunto

$$\boldsymbol{V}(f_1, \ldots, f_s) = \{(a_0 : \ldots : a_n) \in \mathbb{P}^n(\mathrm{K}) : f_i(a_0, \ldots, a_n) = 0, \forall 1 \leq i \leq s\}.$$

é chamado variedade projetiva definida por $f_1, \ldots, f_s$.

Proposição 2.7. *Seja $V = \boldsymbol{V}(f_1, \ldots, f_s)$ uma variedade projetiva. Então $W = V \cap U_0$ pode ser identificado como a variedade afim $\boldsymbol{V}(g_1, \ldots, g_s) \subset \mathrm{K}^n$, onde $g_i(x_1, \ldots, x_n) = f_i(1 : x_1 : \cdots : x_n)$ para cada $1 \leq i \leq s$.*

Demonstração. Na proposição 2.2, consideramos a bijeção $\phi : \mathrm{K}^n \longrightarrow U_0$ que leva o ponto $(a_1, \ldots, a_n)$ no ponto $(1 : a_1 : \ldots : a_n)$. Consideremos a restrição de ϕ ao subconjunto $V(g_1, \ldots, g_s)$ de K^n. Vejamos que $\phi(V(g_1, \ldots, g_s)) = W$. De fato, se $(a_1, \ldots, a_n) \in V(g_1, \ldots, g_s)$, ou seja, $g_i(a_1, \ldots, a_n) = 0$, para todo $i = 1, \ldots, s$, então $\phi(a_1, \ldots, a_n) = (1 : a_1 : \ldots : a_n) \in U_0$ e ainda

$$f_i(\phi(a_1, \ldots, a_n)) = f_i(1 : a_1 : \ldots : a_n) = g_i(a_1, \ldots, a_n) = 0 \Longrightarrow \phi(a_1, \ldots, a_n) \in V.$$

Portanto, $\phi(a_1, \ldots, a_n) \in W$. Daí, $\phi(V(g_1, \ldots, g_s)) \subseteq W$.

Por outro lado, seja $(a_0 : a_1 : \ldots : a_n) \in W$. Então $f_i\left(1 : \frac{a_1}{a_0} : \ldots : \frac{a_n}{a_0}\right) = 0$ e $\left(1 : \frac{a_1}{a_0} : \ldots : \frac{a_n}{a_0}\right) = \phi\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right)$. Ainda,

$$g_i\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) = f_i\left(1 : \frac{a_1}{a_0} : \ldots : \frac{a_n}{a_0}\right) = 0, \forall i = 1, \ldots, s.$$

Logo $\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) \in V(g_1, \ldots, g_s)$. Portanto, temos que para cada ponto y de W, existe um ponto x de $V(g_1, \ldots, g_s)$ que $\phi(x) = y$. Concluímos assim que $\phi(V(g_1, \ldots, g_s)) = W$.

□

Proposição 2.8. *Seja $g(x_1, ..., x_n) \in \mathrm{K}[x_1, ..., x_n]$ um polinômio de grau total d.*

(*i*) *Seja $g = \sum_{i=0}^{d} g_i$ uma expansão de g em somas de componentes homogêneas, onde g_i possui grau total i. Então*

$$\begin{aligned} g^h(x_0, ..., x_n) &= \sum_{i=0}^{d} g_i(x_1, ..., x_n) x_0^{d-i} \\ &= g_d(x_1, ..., x_n) + \cdots + g_j(x_1, ..., x_n) x_0^{d-j} + \cdots + g_0(x_1, ..., x_n) x_0^d \end{aligned}$$

é um polinômio homogêneo de grau total d em $\mathrm{K}[x_0, ..., x_n]$. Chamamos g^h a homogeneização de g com respeito a x_0.

(*ii*) *A homogeneização de g com respeito a x_0 pode ser calculada da seguinte forma*

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

(*iii*) *A desomogeneização de g^h é g. Isto é $g^h(1, x_1, ..., x_n) = g(x_1, ..., x_n)$.*

(*iv*) *Seja $F(x_0, ..., x_n)$ um polinômio homogêneo e seja x_0^e a maior potência de x_0 dividindo F. Se $F(1, x_1, ..., x_n) = f$ é a desomogeneização de F, então $F = x_0^e f^h$.*

Demonstração. (*i*) Como o grau de cada componente de $g_i(x_1, \ldots, x_n)$ é i, em $\mathrm{K}[x_1, \ldots, x_n]$, então ao multiplicarmos por x_0^{d-i}, cada componente de $x_0^{d-i} g_i(x_1, \ldots, x_n)$ terá grau total igual a $d - i + i = d$, em $\mathrm{K}[x_0, \ldots, x_n]$, para todo $i = 1, \ldots, d$. Portanto g^h é um polinômio homogêneo de grau total d em $\mathrm{K}[x_0, \ldots, x_n]$.

(*ii*)

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

(*iii*) Como

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

Fazendo $x_0 = 1$, obtemos

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

(iv) Suponha que $F(x_0, ..., x_n)$ seja um polinômio homogêneo de grau total d. Já que x_0^e é a maior potência de x_0 dividindo F, podemos expandir $F(x_0, ..., x_n)$ da seguinte maneira

$$F(x_0, ..., x_n) = \sum_{i=0}^{d-e} x_0^{e+i} h_{d-(e+i)}(x_1, ..., x_n) = x_0^e \sum_{i=0}^{d-e} x_0^i h_{d-(e+i)}(x_1, ..., x_n),$$

onde cada componente $h_{d-(e+i)}(x_1, ..., x_n)$ é homogênea de grau total $d - (e + i)$, para todo $1 \leq i \leq d - e$. Também temos que $F(1, x_1, ..., x_n) = f(x_1, ..., x_n)$, logo

$$f = \sum_{i=0}^{d-e} h_{d-(e+i)}(x_1, ..., x_n),$$

portanto f é um polinômio de grau total $d - e$.

Portanto a homogeneização de f é

$$f^h = \sum_{i=0}^{d-e} h_{d-(e+i)}(x_1, ..., x_n) x_0^i,$$

multiplicando por x^e de ambos os lados, obtemos

$$x^e f^h = x^e \sum_{i=0}^{d-e} h_{d-(e+i)}(x_1, ..., x_n) x_0^i = \sum_{i=0}^{d-e} h_{d-(e+i)}(x_1, ..., x_n) x_0^{i+e} = F(x_0, ..., x_n).$$

□

Para exemplificar, consideremos o polinômio $g = y - x^3 + x \in \mathrm{K}[x, y]$. Temos que $g^h = yz^2 - x^3 + xz^2 \in \mathrm{K}[x, y, z]$ é a homogeneização de g com relação à variável z. Enumeremos as variáveis x, y e z como sendo 0, 1 e 2, respectivamente. Assim, $\boldsymbol{V}(g) \in \mathrm{K}^2 \cong U_2$, pelo corolário (2.3). Ainda, temos que $g(x, y) = g^h(x, y, 1)$. Segue então da proposição (2.7) que a variedade afim $\boldsymbol{V}(g)$ pode ser identificada como $W = V \cap U_2$, onde $V = \boldsymbol{V}(g^h)$.

Definição 2.9. *Um ideal I em $\mathrm{K}[x_0, ..., x_n]$ é dito homogêneo se para cada $f \in I$, as componentes homogêneas f_i de f estão em I.*

Observação: A maioria dos ideais não tem essa propriedade. Seja $I = \langle y - x^2 \rangle$, as componentes homogêneas de $f = y - x^2$ são $f_1 = y$ e $f_2 = -x^2$, estes polinômios não estão em I, portanto I não é um ideal homogêneo.

Proposição 2.10. *Seja $I \subset \mathrm{K}[x_0, ..., x_n]$ um ideal. São equivalentes:*

(i) *I é um ideal homogêneo de $\mathrm{K}[x_0, ..., x_n]$.*

(*ii*) $I = \langle f_1, ..., f_s \rangle$ *onde* $f_1, ..., f_s$ *são polinômios homogêneos.*

Demonstração. $(i) \Longrightarrow (ii)$ Suponha que I é um ideal homogêneo. Pelo teorema da base de Hilbert, I é finitamente gerado, digamos que $I = \langle f_1, ..., f_t \rangle$ para certos $f_1, ..., f_t \in \mathrm{K}[x_0, ..., x_n]$. Escreva cada f_j como soma de suas componentes homogêneas, isto é,

$$f_j = \sum_i f_{ji}, \text{ para cada } j = 1, \ldots, t.$$

Seja I' o ideal gerado pelos polinômios homogêneos f_{ji}. Como $f_j = \sum_i f_{ji} \in I'$, temos que $I \subset I'$.
Agora como I é homogêneo, temos que $f_{ji} \in I$. para todos i, j, segue que, $I' \subset I$. Portanto $I' = I$.

$(ii) \Longrightarrow (i)$ Seja $f \in I = \langle f_1, ..., f_s \rangle$ onde $f_1, ..., f_s$ são polinômios homogêneos, logo $f = a_1 f_1 + \cdots + a_s f_s$ para $a_1, ..., a_s \in \mathrm{K}[x_0, ..., x_n]$. Mostremos que cada componente homogênea de f pertence a I. Para cada $i = 1, \ldots, s$, podemos escrever a_i como somas de suas componentes homogêneas

$$a_i = \sum_j a_{ij}.$$

Suponha que f_i é homogêneo de grau d_i. Assim, temos que

$$a_i f_i = \sum_j a_{ij} f_i,$$

onde cada termo $a_{ij} f_i$ é homogêneo de grau $j + d_i$. Logo, a expressão acima é a expansão de $a_i f_i$ como soma de componentes homogêneas. Claramente, cada componente homogênea de $a_i f_i$ pertence a I, para todo $i = 1, \ldots, s$. Logo, cada componente homogênea de f pertence a I. Portanto I é um ideal homogêneo.

□

Dado um ideal homogêneo $I \subseteq \mathrm{K}[x_0, \ldots, x_n]$, vejamos que

$$\boldsymbol{V}(I) = \{(a_0 : \cdots : a_n) \in \mathbb{P}^n(\mathrm{K}) : f(a_0, \ldots, a_n) = 0, \forall f \in I\}$$

está bem definido como um conjunto, isto é, se $(a_0 : \ldots : a_n) \in \boldsymbol{V}(I)$, então $(\lambda a_0 : \ldots : \lambda a_n) \in \boldsymbol{V}(I)$, para todo $\lambda \in \mathrm{K} - \{0\}$.

Sejam $(a_0 : \ldots : a_n) \in \boldsymbol{V}(I)$, ou seja, $(a_0 : \ldots : a_n) \in \mathbb{P}^n(\mathrm{K})$ e $f(a_0 : \cdots : a_n) = 0$, para todo $f \in I$. Como I é um ideal homogêneo, existem polinômios homogêneos $f_1, \ldots, f_s \in \mathrm{K}[x_0, \ldots, x_n]$, tais que, $I = \langle f_1, \ldots, f_s \rangle$. Digamos $\deg(f_i) = d_i$. Assim, dado $f \in I$, existem $g_1, \ldots, g_s \in \mathrm{K}[x_0, \ldots, x_n]$ tais que

$$f = g_1 f_1 + \cdots + g_s f_s$$

Temos que $f_i(a_0, \ldots, a_n) = 0$, para todo $i \in \{1, \ldots, s\}$, pois cada f_i pertence a I. Logo, para cada $\lambda \in \mathrm{K} - \{0\}$,

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

Portanto $f(\lambda a_0, \ldots, \lambda a_n) = 0$, para todo $f \in I$, e então $(\lambda a_0 : \ldots : \lambda a_n) \in \boldsymbol{V}(I)$, para todo $\lambda \in \mathrm{K} - \{0\}$.

Proposição 2.11. *Seja I um ideal homogêneo em $\mathrm{K}[x_0, \ldots, x_n]$ e suponha que $I = \langle f_1, \ldots, f_s \rangle$ onde $f_1, \ldots, f_s$ são homogêneos. Então*

$$\boldsymbol{V}(I) = \boldsymbol{V}(f_1, \ldots, f_s).$$

Demonstração. ($\subseteq$) Seja $p \in \boldsymbol{V}(I)$ então $f(p) = 0$, para todo $f \in I$ em particular para f_i, onde $i \in \{1, \ldots, s\}$. Assim $p \in \boldsymbol{V}(f_1, \ldots, f_s)$.
($\supseteq$) Agora $p \in \boldsymbol{V}(f_1, \ldots, f_s)$. Dado $f \in I$, temos que

$$f = g_1 f_1 + \cdots + g_s f_s$$

para alguns $g_i \in \mathrm{K}[x_0, \ldots, x_n]$. Assim

$$f(p) = g_1(p) f_1(p) + \cdots + g_s(p) f_s(p) = 0.$$

Portanto $p \in \boldsymbol{V}(I)$. □

Proposição 2.12. *Seja $V \subset \mathbb{P}^n(\mathrm{K})$ uma variedade projetiva e seja*

$$\boldsymbol{I}(V) = \{f \in \mathrm{K}[x_0, \ldots, x_n] : f(a_0, \ldots, a_n) = 0, \forall (a_0 : \ldots : a_n) \in V\}$$

(isto significa que f precisa zerar todas as coordenadas homogêneas de todos os pontos de V.) Se K é infinito, então $\boldsymbol{I}(V)$ é um ideal homogêneo.

Demonstração. Notemos primeiramente que $\boldsymbol{I}(V)$ é um ideal. De fato, sejam $f, g \in \boldsymbol{I}(V)$, então $f(a_0, \ldots, a_n) = g(a_0, \ldots, a_n) = 0$ para todo $(a_0 : \ldots : a_n) \in V$. Como $(f + g)(a_0, \ldots, a_n) = f(a_0, \ldots, a_n) + g(a_0, \ldots, a_n) = 0 + 0 = 0$, segue que $(f + g) \in \boldsymbol{I}(V)$. Agora, sejam $f \in \boldsymbol{I}(V)$ e $h \in \mathrm{K}[x_0, \ldots, x_n]$. Temos que $(fh)(a_0, \ldots, a_n) = f(a_0, \ldots, a_n) h(a_0, \ldots, a_n) = 0$, para todo $(a_0 : \cdots : a_n) \in V$, ou seja, $fh \in \boldsymbol{I}(V)$.

Vejamos agora que $\boldsymbol{I}(V)$ e um ideal homogêneo. Sejam $f \in \boldsymbol{I}(V)$ de grau total d e $a = (a_0 : \cdots : a_n) \in V$. Escreva

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

onde $f_0, \ldots, f_d$ são as componentes homogêneas de f. Vamos mostrar que $f_0, \ldots, f_d \in \boldsymbol{I}(V)$. Como $f \in \boldsymbol{I}(V)$ e $a \in V$, temos que $f(\lambda a_0, \ldots, \lambda a_n) = 0$, para todo $\lambda \in \mathrm{K}^*$.
Observe que

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

Defina $p(x) = \sum_{i=0}^{d} x^i f_i(a_0, \ldots, a_n) \in \mathrm{K}[x]$. Como $p(\lambda) = 0$, para todo $\lambda \in \mathrm{K}^*$ e K^* é infinito, temos que $p(x)$ é o polinômio identicamente nulo, ou seja, todos os coeficientes de p são nulo, isto é, $f_i(a_0, \ldots, a_n) = 0$, para todo $i = 0, \ldots, d$.

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

Proposição 2.13. *Seja* K *um corpo infinito e* $W \in \mathbb{P}^n(\mathrm{K})$ *uma variedade projetiva. Então as aplicações*

$$\textit{variedades projetivas} \xrightarrow{\boldsymbol{I}} \textit{ideais homogêneos}$$

e

$$\textit{ideais homogêneos} \xrightarrow{\boldsymbol{V}} \textit{variedades projetivas}$$

invertem inclusões , ou seja, se $I_1 \subset I_2$*, então* $\boldsymbol{V}(I_1) \supset \boldsymbol{V}(I_2)$ *e similarmente, se* $V_1 \subset V_2$ *variedades, então* $\boldsymbol{I}(V_1) \supset \boldsymbol{I}(V_2)$*. Além do mais, teremos:*

$$\boldsymbol{V}(\boldsymbol{I}(W)) = W.$$

Demonstração. Comecemos por verificar que $\boldsymbol{V}$ e $\boldsymbol{I}$ invertem as inclusões.

Sejam I_1 e I_2 ideais homogêneos em $\mathrm{K}[x_0, \ldots, x_n]$ tais que $I_1 \subset I_2$. Vejamos que $\boldsymbol{V}(I_1) \supset \boldsymbol{V}(I_2)$. De fato, seja $(a_0 : \ldots : a_n) \in \boldsymbol{V}(I_2)$. Assim, $f(a_0, \ldots, a_n) = 0$, para todo $f \in I_2$. Como $I_1 \subset I_2$, se nos restringirmos aos polinômios de I_1, eles continuarão se anulando nestes pontos, isto é, $g(a_0, \ldots, a_n) = 0$, para todo $g \in I_1$. Portanto, $(a_0 : \ldots : a_n) \in \boldsymbol{V}(I_1)$.

Sejam agora V_1 e V_2 variedades projetivas em $\mathbb{P}^n(\mathrm{K})$, tais que $V_1 \subset V_2$. Vejamos que $\boldsymbol{I}(V_1) \supset \boldsymbol{I}(V_2)$. De fato, seja $f \in \boldsymbol{I}(V_2) \subset \mathrm{K}[x_0, \ldots, x_n]$. Assim, $f(a_0, \ldots, a_n) = 0$, para todo $(a_0 : \ldots : a_n) \in V_2$. Em particular, para cada $(b_0 : \ldots b_n) \in V_1$, temos que f se anulará neste ponto, já que $V_1 \subset V_2$. Portanto, $f \in \boldsymbol{I}(V_1)$.

Vamos agora verificar que $\boldsymbol{V}(\boldsymbol{I}(W) = W$.

($\subseteq$) Como W é uma variedade projetiva, temos que $W = \boldsymbol{V}(f_1, \ldots, f_s)$ para alguns polinômios homogêneos $f_1, \ldots, f_s$. Seja $J = \langle f_1, \ldots, f_s \rangle$, temos que $W = \boldsymbol{V}(J)$. Assim, $\boldsymbol{I}(W) = \boldsymbol{I}(\boldsymbol{V}(J))$. Como $J \subseteq \boldsymbol{I}(\boldsymbol{V}(J)) = \boldsymbol{I}(W)$ e como $\boldsymbol{V}$ reverte inclusões, concluímos que $\boldsymbol{V}(J) \supseteq \boldsymbol{V}(\boldsymbol{I}(W))$, ou seja, $\boldsymbol{V}(\boldsymbol{I}(W)) \subseteq W$.

($\supseteq$) Dado $p \in W$, temos que $f(p) = 0$, para todo $f \in \boldsymbol{I}(W)$, logo $p \in \boldsymbol{V}(\boldsymbol{I}(W))$. □

Proposição 2.14. *Seja* $I \subset \mathrm{K}[x_0, \ldots, x_n]$ *um ideal homogêneo. Então* $\sqrt{I} = \{f | f^m \in I,$ *para algum inteiro* $m \geq 1\}$ *também é um ideal homogêneo.*

Demonstração. Se $f \in \sqrt{I}$, então existe um $m \geq 1$ tal que $f^m \in I$. Se $f \neq 0$, decompondo f em suas componentes homogêneas

$$f = \sum_i f_i = f_{max} + \sum_{i<max} f_i$$

onde f_{max} é a componente homogênea não nula de maior grau total de f. Expandindo a potência $f^m = (f_0 + \cdots + f_{max})^m$, vem que $(f^m)_{max} = (f_{max})^m$.
Já que I é um ideal homogêneo, temos que $(f_{max})^m \in I$, como $(f^m)_{max} = (f_{max})^m \in I$, seque que $f_{max} \in \sqrt{I}$. Agora considere o polinômio homogêneo $g = f - f_{max} \in \sqrt{I}$ e repetindo o mesmo argumento, obtemos que $g_{max} \in \sqrt{I}$. Observe que g_{max} também é uma componente homogênea de f. Repetindo esse argumento numa quantidade finita, obteremos que todas as componentes homogêneas de f pertencem a $\sqrt{I}$. Portanto $\sqrt{I}$ é um ideal homogêneo. □

CAPÍTULO 3

CORPOS FINITOS

3.1 A característica de um corpo

Seja K um corpo finito com elemento unidade 1. Considere o conjunto

$$\Lambda_{\mathrm{K}} = \{n \in \mathbb{N} : n1 = \underbrace{1 + ... + 1}_{n-\text{vezes}} = 0\} \subset \mathbb{N}.$$

Pelo fato de K ser finito, existem dois números naturais $n_1 < n_2$, tais que $n_1 1 = n_2 1$. Logo $(n_2 - n_1)1 = 0$, com $n_2 - n_1 > 0$ e, portanto $\Lambda_K \neq \emptyset$. Assim, Λ_K é um conjunto não-vazio de números naturais, então pelo princípio da boa ordem, existe um elemento mínimo. Esta propriedade nos motiva a seguinte definição.

Definição 3.1. *A característica de um corpo finito* K *é o inteiro positivo car*(K)*, definido por*

$$\mathrm{car(K)} = \min \Lambda_{\mathrm{K}} = \min\{n \in \mathbb{N} : n1 = 0\}.$$

Se um corpo F é um subcorpo de um corpo K, então $\mathrm{car(K)} = \mathrm{car}(F)$, pois $\Lambda_{\mathrm{F}} = \Lambda_{\mathrm{K}}$.

Proposição 3.2. *Seja* K *um corpo finito, então* car(K) *é um número primo.*

Demonstração. Seja $m = \mathrm{car(K)}$ e suponhamos que m não seja primo. Logo $m = m_1 m_2$, onde m_1 e m_2 são inteiros maiores que 1 e menores do que m. Assim,

$$0 = m1 = (m_1 m_2)1 = (m_1 1)(m_2 1).$$

Como K é domínio, temos que $m_1 1 = 0$ ou $m_2 1 = 0$, o que contradiz a minimalidade de m. □

Proposição 3.3. *Seja* K *um corpo finito com* $\mathrm{car(K)} = p$*. Se para* $m \in \mathbb{Z}$ *e* $a \in$ K*, tem-se* $ma = 0$*, então* m *é múltiplo de* p *ou* $a = 0$*.*

Demonstração. Suponhamos que $ma = 0$, logo $(m1)a = 0$. E como K é um corpo, temos que $m1 = 0$ ou $a = 0$. Se $m1 = 0$, então m é múltiplo de p, de fato, pelo algoritmo da divisao, temos que $m = pt + r$, onde $0 \leq r < p$. Logo,

$$0 = m1 = (pt + r)1 = (pt)1 + r1 = (p1)t + r1 = r1$$

e como p é o menor inteiro positivo tal que $p1 = 0$, segue que $r = 0$, ou seja, m é múltiplo de p. □

Teorema 3.4. *Seja* K *um corpo finito com* $\text{car}(\text{K}) = p$*, onde* p *é um número primo. Então,* K *contém um subcorpo isomorfo a* $\mathbb{Z}_p$*. Em particular,* K *possui* p^n *elementos para algum número natural* n*.*

Demonstração. Considere a aplicação:

$$\begin{array}{rccc} \psi & : & \mathbb{Z}_p & \to & \text{K} \\ & & \overline{n} & \mapsto & n1 \end{array}$$

Primeiramente, notemos que esta aplicação está bem definida, de fato, considere $\overline{n} = \overline{m}$, então existe um inteiro λ, tal que, $n = \lambda p + m$. Logo,

$$n1 = (\lambda p + m)1 = (\lambda p)1 + m1 = \lambda(p1) + m1 = 0 + m1 = m1.$$

Vamos verificar que está aplicação é um homomorfismo. De fato,

(i) $\psi(\overline{m} + \overline{n}) = \psi(\overline{m + n}) = (m + n)1 = m1 + n1 = \psi(\overline{m}) + \psi(\overline{n})$.

(ii) $\psi(\overline{m} \cdot \overline{n}) = \psi(\overline{mn}) = (mn)1 = (m1)(n1) = \psi(\overline{m})\psi(\overline{n})$.

(iii) $\psi(\overline{1}) = 1$.

Agora como K e $\mathbb{Z}_p$ são corpos e ψ é um homomorfismo, temos que $\psi(\mathbb{Z}_p)$ é um subcorpo de K, isomorfo a $\mathbb{Z}_p$.

Portanto, K é um espaço vetorial sobre $\mathbb{Z}_p$ e como K é finito, segue que, tem dimensão finita sobre $\mathbb{Z}_p$. Seja $a_1, ..., a_n$ uma base de K sobre $\mathbb{Z}_p$, então, todo elemento de K se escreve de modo único na forma

$$\lambda_1 a_1 + \cdots + \lambda_n a_n,$$

onde os $\lambda_i \in \mathbb{Z}_p$, com $1 \leq i \leq n$. Portanto, segue que $\mid \text{K} \mid = p^n$. □

3.2 Potências da característica

Proposição 3.5. *Seja* K *um corpo finito de característica* p *e seja* $q = p^r$*, para algum inteiro positivo* r*. Se* $a, b \in \text{K}$*, então*

$$(a \pm b)^q = a^q \pm b^q.$$

Demonstração. Provemos este resultado por indução sobre r. Pelo binômino de Newton, temos que

$$(a \pm b)^p = a^p \pm \cdots + (\pm 1)^i \begin{pmatrix} p \\ i \end{pmatrix} a^{p-i} b^i + \cdots \pm b^p.$$

Mas como $\begin{pmatrix} p \\ i \end{pmatrix} = \dfrac{p!}{i!(p-i)!}$, temos que $p \mid \begin{pmatrix} p \\ i \end{pmatrix}$, para todo $i = 1, ..., p-1$. Ainda, notemos que $(-b)^p = -b$. De fato, se p é ímpar o resultado é óbvio. Por outro lado, se p é par, então $p = 2$ e $-1 = 1$. Daí segue que

$$(a \pm b)^p = a^p \pm b^p,$$

ou seja, o resultado vale para $r = 1$. Agora, suponha que o resultado seja válido para $r - 1$.

$$(a \pm b)^{p^r} = ((a \pm b)^{p^{r-1}})^p = (a^{p^{r-1}} \pm b^{p^{r-1}})^p = a^{p^r} \pm b^{p^r}$$

Portanto $(a \pm b)^q = a^q \pm b^q$. □

Segue por indução da proposição acima , que, se $a_1, ..., a_n$ são elementos de um corpo finito K, de característica p e se q é uma potência de p, então:

$$(a_1 + \cdots + a_n)^q = a_1^q + \cdots + a_n^q.$$

Temos também que, se $P(x) = a_0 + \cdots + a_{n-1}x^{n-1} + a_n x^n \in \mathrm{K}[x]$, então

$$P(x)^q = a_0^q + \cdots + a_{n-1}^q x^{(n-1)q} + a_n^q x^{nq}.$$

Corolário 3.6. *Seja* K *um corpo finito de característica p. Se $q = p^r$ para algum inteiro positivo r, então a aplicação*

$$\begin{array}{rccc} f_q & : & \mathrm{K} & \to & \mathrm{K}. \\ & & x & \mapsto & x^q \end{array}$$

é um isomorfismo de corpos.

Demonstração. Temos que f_q é um homomorfismo, de fato,

(*i*) $f_q(a+b) = (a+b)^q = a^q + b^q = f_q(a) + f_q(b)$.

(*ii*) $f_q(ab) = (ab)^q = a^q b^q = f_q(a) f_q(b)$.

(*iii*) $f_q(1) = 1^q = 1$.

Como f_q é um homomorfismo entre corpos, segue que f_q é injetora e, como K é finito, segue que f_q é bijetora. Logo é um isomorfismo. □

Corolário 3.7. *Sejam F um corpo de característica $p > 0$ e q uma potência inteira de p. O conjunto* $\mathrm{K} = \{\alpha \in F : \alpha^q - \alpha = 0\}$ *é um subcorpo de F.*

Demonstração. Temos que mostrar que, dados $\alpha, \beta \in \mathrm{K}$, temos $\alpha - \beta$ e $\dfrac{\alpha}{\beta} \in \mathrm{K}$, quando $\beta \neq 0$.

(*i*) $(\alpha-\beta)^q-(\alpha-\beta)=\alpha^q-\beta^q-\alpha+\beta=(\alpha^q-\alpha)-(\beta^q-\beta)=0+0=0$.

(*ii*) Temos que

$$\frac{\alpha}{\beta}^q-\frac{\alpha}{\beta}=\frac{\alpha^q-\alpha\beta^{q-1}}{\beta^q}=\frac{\alpha(\alpha^{q-1}-\beta^{q-1})}{\beta^q}.$$

Se $\alpha=0$, então $\dfrac{\alpha}{\beta}\in \mathrm{K}$. Agora se $\alpha\neq 0$, como $\alpha(\alpha^{q-1}-1)=0$ e K é corpo, então $\alpha^{q-1}=1$, da mesma forma $\beta^{q-1}=1$, portanto $\dfrac{\alpha(1-1)}{\beta^q}=0$, portanto $\dfrac{\alpha}{\beta}\in \mathrm{K}$.

□

Proposição 3.8. *Sejam* K *um corpo finito de característica* p *e* $P(x)\in \mathrm{K}[x]$. *Temos que* $P'(x)=0$ *se, e somente se, existe um polinômio* $Q(x)\in \mathrm{K}[x]$ *tal que* $P(x)=Q(x)^p$.

Demonstração. ($\Longleftarrow$) Seja $Q(x)=a_0+a_1x+\cdots+a_nx^n$, temos que

$$P'(x)=(Q(x)^p)'=p(a_0+a_1x+\cdots+a_nx^n)^{p-1}(a_1+\cdots+na_nx^{n-1}).$$

Como a característica do corpo é p e todos os fatores de $P'(x)$ estão multiplicados por p, segue que $P'(x)=0$.

($\Longrightarrow$) Se $P(x)=a_0+a_1x+\cdots+a_nx^n$, tal que $P'(x)=0$, segue que $ia_i=0$ para todo $i=1,...,n$. Consequentemente, segue que i é um múltiplo de p sempre que $a_i\neq 0$, ou seja, $P(x)=a_0+a_px^p+a_{2p}x^{2p}+\ldots$, escolhendo $b_i\in K$ tal que $b_i^p=a_{ip}$, o que é possível pelo resultado acima, para $p=q$, pondo $Q(x)=b_0+b_1x+b_2x^2+\ldots$ concluímos o resultado. □

Proposição 3.9. *Seja* $F(x)\in \mathrm{K}[x]$ *com um fator múltiplo não constante, de multiplicidade maior do que 1, em* K$[x]$. *Então,* $\mathrm{MDC}(F(x),F'(x))\neq 1$.

Demonstração. Seja $H(x)$ um fator múltiplo não constante de $F(x)\in \mathrm{K}[x]$. Logo, existem um inteiro $r\geq 2$ e um polinômio $G(x)\in \mathrm{K}[x]$ tais que $F(x)=H(x)^rG(x)$. Derivando ambos os lados da igualdade, ficamos com

$$F'(x)=rH(x)^{r-1}G(x)+H(x)^rG'(x).$$

Logo, $H(x)$ divide $F(x)$ e $F'(x)$ e, portanto, $\mathrm{MDC}(F(x),F'(x))\neq 1$. □

Proposição 3.10. *Seja* K *um corpo finito de característica* p *e seja* $q=p^r$, *para algum inteiro positivo* r. *O polinômio* $F(x)=x^q-x$ *não possui fatores irredutíveis múltiplos em* K$[x]$.

Demonstração. Pelo fato de $F'(x)=qx^{q-1}-1=-1$, temos que $F(x)$ e $F'(x)$ são primos entre si. Logo pelo resultado anterior, temos que $F(x)$ não possui fatores irredutíveis múltiplos em K$[x]$. □

Lema 3.11. *Seja* K *um corpo finito com* q *elementos. Para todo* $\alpha\in \mathrm{K}^*$, *onde* $\mathrm{K}^*=\mathrm{K}\backslash\{0\}$, *temos que*

$$\alpha^{q-1}=1.$$

Demonstração. Seja $\alpha \in \mathrm{K}^*$ e considere a aplicação

$$\begin{array}{rccc} \psi_\alpha & : & \mathrm{K}^* & \to & \mathrm{K}^* \\ & & a & \mapsto & \alpha a \end{array}$$

temos que ψ_α é injetora, pois $\psi_\alpha(a) = \psi_\alpha(b)$, assim $\alpha a = \alpha b$, multiplicando ambos os lados pelo inverso de α, ficamos com $a = b$. E como K^* é finito, segue que ψ_α é bijetora. Se $\mathrm{K}^* = \{a_1, ..., a_{q-1}\}$, então

$$\{a_1, ..., a_{q-1}\} = \{\alpha a_1, ..., \alpha a_{q-1}\}.$$

Assim $\alpha a_1 \alpha a_2 \dots \alpha a_{q-1} = a_1 a_2 ... a_{q-1}$, ou seja, $\alpha^{q-1} a_1 ... a_{q-1} = a_1 ... a_{q-1}$, portanto $\alpha^{q-1} = 1$. □

Corolário 3.12. *Seja* K *um corpo finito com q elementos. Para todo $\alpha \in \mathrm{K}$ e para todo $i \in \mathbb{N}$, temos que $\alpha^{q^i} = \alpha$.*

Demonstração. Como $q^i - 1 = (q-1)(1 + q + \cdots + q^{n-1})$, segue que

$$\alpha^{q^i} = \alpha^{(q-1)(1+q+\cdots+q^{n-1})} \cdot \alpha = (\alpha^{q-1})^{(1+q+\cdots+q^{n-1})} \cdot \alpha = 1^{(1+q+\cdots+q^{n-1})} \cdot \alpha = \alpha.$$

□

Corolário 3.13. *Seja* K *um corpo finito de característica p com q elementos. Seja F uma extensão de* K*. Então os elementos de* K *são os elementos de F que são raízes de $x^q - x = 0$, enquanto que os elementos do subcorpo $\mathbb{Z}_p$ de F são as raízes do polinômio $x^p - x = 0$.*

Demonstração. Pelo corolário anterior, temos que os elementos de K são raízes do polinômio $x^q - x$. Mas esse polinômio, tendo grau q, tem no máximo q raízes, logo, as suas raízes são todos os elementos de K. A segunda segue da mesma forma, considerando $\mathbb{Z}_p$ como corpo. □

Definição 3.14. *A ordem de $\alpha \in \mathrm{K}^*$ é o inteiro positivo*

$$\mathrm{ord}\alpha = \min\{n \in \mathbb{N} : \alpha^n = 1\}.$$

Temos que esse conjunto é diferente do vazio, pois $\alpha^{q-1} = 1$, onde K é um corpo finito com q elementos.

Proposição 3.15. *Seja* K *um corpo finito com q elementos e seja $\alpha \in \mathrm{K}^*$. Se para algum inteiro positivo m temos que $\alpha^m = 1$, então* $\mathrm{ord}\alpha \mid m$*. Em particular,* $\mathrm{ord}\alpha \mid (q-1)$*.*

Demonstração. Pelo algoritmo da divisão, $m = (\mathrm{ord}\alpha)s + r$, para alguns inteiros $s \geq 0$ e $0 \leq r < \mathrm{ord}\alpha$. Portanto

$$1 = \alpha^m = (\alpha^{\mathrm{ord}\alpha})^s \alpha^r = 1\alpha^r,$$

o que, pela minimalidade de $\mathrm{ord}\alpha$, implica que $r = 0$, logo, $\mathrm{ord}\alpha \mid m$. Agora, como $\alpha^{q-1} = 1$, pelo que acabamos de demonstrar, temos que $\mathrm{ord}\alpha \mid q - 1$.

□

Proposição 3.16. *Seja* K *um corpo finito. Sejam* $\alpha, \beta \in K$ *tais que* $\text{MDC}(\text{ord}\alpha, \text{ord}\beta) = 1$. *Então* $\text{ord}\alpha\beta = \text{ord}\alpha\ \text{ord}\beta$.

Demonstração. Sejam $m = \text{ord}\alpha$ e $n = \text{ord}\beta$. Temos então que

$$(\alpha\beta)^m n = (\alpha^m)^n(\beta^n)^m = 1.$$

Por outro lado, se $(\alpha\beta)^t = 1$, então

$$1 = ((\alpha\beta)^t)^m = \alpha^{tm}\beta^{tm} = 1\beta^{tm} = \beta^{tm}, \text{e}$$

$$1 = ((\alpha\beta)^t)^n = \alpha^{tn}\beta^{tn} = \alpha^{tn}1 = \alpha^{tn}.$$

Logo, temos que $n \mid tm$ e $m \mid tn$. Como $\text{MDC}(m, n) = 1$, segue que $m \mid t$ e $n \mid t$. Novamente usando o fato de que $\text{MDC}(m, n) = 1$, segue que $mn \mid t$, o que prova que $mn = \min\{t > 0 : (\alpha\beta)^t = 1\}$, concluindo assim que $\text{ord}\alpha\ \text{ord}\beta = mn$. □

Proposição 3.17. *Seja* K *um corpo finito e sejam* $\alpha \in \text{K}^*$ *e* $i \in \mathbb{N}$. *Suponhamos que* $\text{ord}\alpha = m$, *então*

$$\text{ord}\alpha^i = \frac{m}{\text{MDC}(m, i)}.$$

Demonstração. Seja $t = \text{ord}\alpha^i$, logo, t é o menor inteiro positivo tal que

$$\alpha^{it} = (\alpha^i)^t = 1.$$

Ou seja, t é o menor inteiro positivo tal que $m \mid it$, ou, it é o menor múltiplo simultaneamente de m e de i. Logo, $it = \text{MMC}(m, i)$, ou seja,

$$t = \frac{\text{MMC(m, i)}}{i} = \frac{mi}{\text{MDC}(m, i)i} = \frac{m}{\text{MDC(m, i)}}.$$

Já que $\text{MMC}(m, i)\text{MDC}(m, i) = mi$. □

3.3 Elementos Primitivos

Definição 3.18. *Um elemento* α *de um corpo finito* $\mathbb{F}_q$ *é chamado de elemento primitivo se*

$$\mathbb{F}_q^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\},$$

ou seja, se $\text{ord}(\alpha) = q - 1$.

Teorema 3.19. *Todo corpo finito possui elementos primitivos.*

Demonstração. Seja $\mathbb{F}_q$ um corpo com q elementos. Sabemos, pelo lema (3.11), que $x^{q-1} = 1$, para todo $x \in \mathbb{F}_q^*$. Logo, todos os elementos de $\mathbb{F}_q^*$ tem ordem menor ou igual a $q-1$. Queremos provar que existe um elemento em $\mathbb{F}_q^*$ de ordem $q-1$. Seja $a \in \mathbb{F}_q^*$ um elemento de ordem máxima m, vejamos que $m = q-1$. Já temos que $m \leq q-1$.

Vamos inicialmente provar que se $b \in \mathbb{F}_q^*$, então $\text{ord}(b)$ divide $\text{ord}(a) = m$. Escrevamos $\text{ord}(b) = ds$, onde $d = \text{mdc}(\text{ord}(a), \text{ord}(b))$. Segue então que $\text{mdc}(\text{ord}(a), s) = 1$. Queremos provar que $s = 1$. De fato, suponhamos que $s > 1$, pela proposição (3.17), segue que

$$\text{ord}(b^d) = \frac{\text{ord}(b)}{\text{mdc}(\text{ord}(b), d)} = \frac{\text{ord}(b)}{\text{mdc}(\text{ord}(b), \text{mdc}(\text{ord}(a), \text{ord}(b)))} = \frac{\text{ord}(b)}{\text{mdc}(\text{ord}(b), \text{ord}(a))} = s > 1.$$

Agora, pela proposição (3.16), temos que

$$\text{ord}(ab^d) = \text{ord}(a)\text{ord}(b^d) > \text{ord}(a).$$

Ainda, como $ab^d \in \mathbb{F}_q^*$, a desigualdade acima contradiz a maximalidade de $\text{ord}(a)$.

Segue, então, que todo elemento de $\mathbb{F}_q^*$ satisfaz a equação

$$X^m - 1 = 0,$$

em outras palavras, todos os elementos de $\mathbb{F}_q^*$ são raízes do polinômio $p(X) = X^m - 1$. Como o polinômio $p(X)$ tem grau m, segue que ele tem no máximo m raízes. Portanto, o número de elementos de $\mathbb{F}_q^*$ tem que ser menor ou igual a m, ou seja,

$$q - 1 = |\mathbb{F}_q^*| \leq m$$

□

O teorema anterior significa que existe um elemento $\alpha \in \mathbb{F}_q^*$, tal que

$$\mathbb{F}_q^* = \{\alpha^0, \alpha^1, \ldots, \alpha^{q-2}\}$$

É claro que $\alpha^{q-1} = 1$, e portanto, nesta representação, a operação de multiplicação fica extremamente simplificada. Mais precisamente,

$$\alpha^i \cdot \alpha^j = \alpha^{[i+j]},$$

onde $[i+j]$ representa o resto da divisão de $i+j$ por $q-1$.

CAPÍTULO 4

CÓDIGOS

4.1 Códigos Lineares

Seja $\mathbb{F}_q$ um corpo finito com q elementos, que é denominado alfabeto. Temos, portanto, para todo número natural n, um $\mathbb{F}_q$-espaço vetorial de dimensão n, $\mathbb{F}_q^n$.

Definição 4.1. *Um subconjunto $C \subset \mathbb{F}_q^n$ será chamado de código linear se for um subespaço vetorial de $\mathbb{F}_q^n$. Os elementos $(x_1, \ldots, x_n) \in C$ são denominados palavras do código C.*

Todo código linear é, por definição, um espaço vetorial de dimensão finita. Seja k a dimensão do código C e seja $v_1, ..., v_k$ uma de suas bases, portanto, os elementos de C são escritos de modo único na forma $\lambda_1 v_1 + \cdots + \lambda_k v_k$, onde $\lambda_1, \ldots, \lambda_k$, são elementos de $\mathbb{F}_q$. Segue daí que $|C| = q^k$.

Definição 4.2. *Sejam $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_q^n$, a distância de Hamming entre $\boldsymbol{u}$ e $\boldsymbol{v}$ é definida como*

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

em que $\boldsymbol{u} = (u_1, \ldots, u_n)$ e $\boldsymbol{v} = (v_1, \ldots, v_n)$.

Proposição 4.3. *Dados $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \mathbb{F}_q^n$, valem as seguintes propriedades:*

(i) $d(\boldsymbol{u}, \boldsymbol{v}) \geq 0$, *valendo a igualdade se, e somente se,* $\boldsymbol{u} = \boldsymbol{v}$.

(ii) $d(\boldsymbol{u}, \boldsymbol{v}) = d(\boldsymbol{v}, \boldsymbol{u})$.

(iii) $d(\boldsymbol{u}, \boldsymbol{v}) \leq d(\boldsymbol{u}, \boldsymbol{w}) + d(\boldsymbol{w}, \boldsymbol{v})$.

Demonstração. *(i)* Temos que $d(\boldsymbol{u}, \boldsymbol{v}) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}| \geq 0$. Agora

$$d(\boldsymbol{u}, \boldsymbol{v}) = 0 \Leftrightarrow |\{i : u_i \neq v_i, 1 \leq i \leq n\}| = 0 \Leftrightarrow u_i = v_i, \forall i \Leftrightarrow \boldsymbol{u} = \boldsymbol{v}.$$

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

(*iii*) A contribuição das i-ésimas coordenadas de $\boldsymbol{u}$ e $\boldsymbol{v}$ para $d(\boldsymbol{u}, \boldsymbol{v})$ é igual a zero se $u_i = v_i$, e igual a um se $u_i \neq v_i$.

No caso em que a contribuição é zero, certamente a contribuição das i-ésimas coordenadas a $d(\boldsymbol{u}, \boldsymbol{v})$ é menor ou igual a das i-ésimas coordenadas a $d(\boldsymbol{u}, \boldsymbol{w}) + d(\boldsymbol{w}, \boldsymbol{v})$ que é igual a $0, 1$ ou 2.

No outro caso, temos que $u_i \neq v_i$ e ,portanto, não podemos ter $u_i = w_i$ e $w_i = v_i$. Consequentemente, a contribuição das i-ésimas coordenadas a $d(\boldsymbol{u}, \boldsymbol{w}) + d(\boldsymbol{w}, \boldsymbol{v})$ é maior ou igual a 1, que é a contribuição das i-ésimas coordenadas a $d(\boldsymbol{u}, \boldsymbol{v})$.

□

Definição 4.4. *Seja C um código. A distância mínima de C é o número*

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

Definição 4.5. *Dado $\boldsymbol{u} \in \mathbb{F}_q^n$, define-se o peso de $\boldsymbol{u}$ como sendo o número inteiro*

$$\omega(\boldsymbol{u}) := |\{i : u_i \neq 0\}|.$$

Ou seja, $\omega(\boldsymbol{u}) = d(\boldsymbol{u}, \boldsymbol{0})$, em que $\boldsymbol{0}$ é o vetor nulo de $\mathbb{F}_q^n$.

Definição 4.6. *O peso de um código linear C é o inteiro $\omega(C) = \min\{\omega(\boldsymbol{u}) : \boldsymbol{u} \in C - \{\boldsymbol{0}\}\}$.*

Proposição 4.7. *Seja $C \subset \mathbb{F}_q^n$ um código linear com distância mínima d. Temos que:*

(*i*) *Para todos $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_q^n$, temos que $d(\boldsymbol{u}, \boldsymbol{v}) = \omega(\boldsymbol{u} - \boldsymbol{v})$.*

(*ii*) *$d = \omega(C)$.*

Demonstração. (*i*) Temos que $\omega(\boldsymbol{u} - \boldsymbol{v}) = d(\boldsymbol{u} - \boldsymbol{v}, \boldsymbol{0}) = |\{i : u_i - v_i \neq 0, 1 \leq i \leq n\}| = |\{i : u_i \neq v_i, 1 \leq i \leq n\}| = d(\boldsymbol{u}, \boldsymbol{v})$.

(*ii*) Para todo para de elementos $\boldsymbol{u}, \boldsymbol{v}$ em C com $\boldsymbol{u} \neq \boldsymbol{v}$, tem-se que $\boldsymbol{z} = \boldsymbol{u} - \boldsymbol{v} \in C - \{\boldsymbol{0}\}$ e $d(\boldsymbol{u}, \boldsymbol{v}) = \omega(\boldsymbol{z})$.

□

Definição 4.8. *Dois códigos lineares C e C' são linearmente equivalentes se existir uma isometria linear $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ tal que $T(C) = C'$.*

Definição 4.9. *Dado um código linear $C \subset \mathbb{F}_q^n$, chamaremos de parâmetros do código linear C os inteiros (n, k, d), em que k é a dimensão de C sobre $\mathbb{F}_q$, d representa a distância mínima de C e n é denominado o comprimento do código C.*

Definição 4.10. *Seja $\beta = \{w_1, w_2, ..., w_k\}$ uma base ordenada de C e considere a matriz G cujas linhas são os vetores $w_i = (w_{i1}, w_{i2}, ..., w_{in})$; $i = 1, 2, ..., k$, isto é,*

$$G = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_k \end{pmatrix} = \begin{pmatrix} w_{11} & w_{12} & \cdots & w_{1n} \\ w_{21} & w_{22} & \cdots & w_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ w_{k1} & w_{k2} & \cdots & w_{kn} \end{pmatrix}.$$

A matriz G é chamada de ***matriz geradora*** *de C associada à base β. A matriz geradora na forma padrão será a matriz: $G^* = (Id_k|A)$, onde Id_k é a matriz identidade $k \times k$ e A, uma matriz $k \times (n-k)$.*

Teorema 4.11. *Dado um código C, existe um código equivalente C' com matriz geradora na forma padrão.*

Demonstração. Seja G uma matriz geradora de C associada à base $\beta = \{g_1, \ldots, g_i \ldots, g_j, \ldots, g_k\}$, onde $g_r = (g_{r1}, \ldots, g_{ri}, \ldots, g_{rj}, \ldots, g_{rn})$, para cada $r = 1, \ldots, k$. Mostraremos que com uma sequência de operações do tipo $(L_1), (L_2), (L_3)$ e (C_1) podemos colocar G na forma padrão, onde:

(L_1) Permutações de linhas.

(L_2) Multiplicação de uma linha por um escalar não nulo.

(L_3) Adição de um múltiplo escalar de uma linha a outra.

(C_1) Permutações de colunas.

Vejamos inicialmente que as operações L_1, L_2 e L_3 não alteram o código. De fato, se $\beta = \{g_1, \ldots, g_i \ldots, g_j, \ldots, g_k\}$ é uma base de C, então $\beta_1 = \{g_1, \ldots, g_j \ldots, g_i, \ldots, g_k\}$, $\beta_2 = \{g_1, \ldots, \alpha g_i, \ldots, g_k\}$ e $\beta_3 = \{g_1, \ldots, g_i \ldots, g_j + \alpha g_i, \ldots, g_k\}$ também são bases do código C, onde $\alpha \in \mathbb{F}_q$. Assim, ao realizar a operação L_p em G, obtém-se a matriz G_p, que é a matriz geradora do código C associada à base β_p, para cada $p = 1, 2$ ou 3. Logo, realizar estas operações em G não alteram o código C.

Agora, notemos que ao aplicar a operação C_1 em G, obtemos uma matriz G' que gera um código C' equivalente a C.

Suponhamos que

$$G = \begin{pmatrix} g_{11} & \cdots & g_{1i} & \cdots & g_{1j} & \cdots & g_{1n} \\ & & & \vdots & & & \\ g_{k1} & \cdots & g_{ki} & \cdots & g_{kj} & \cdots & g_{kn} \end{pmatrix}$$

e que a operação C_1 permuta as colunas i e j da matriz G. Assim, obtemos a matriz

$$G' = \begin{pmatrix} g_{11} & \cdots & g_{1j} & \cdots & g_{1i} & \cdots & g_{1n} \\ & & & \vdots & & & \\ g_{k1} & \cdots & g_{kj} & \cdots & g_{ki} & \cdots & g_{kn} \end{pmatrix}.$$

Claramente, temos que as linhas da matriz G' são linearmente independentes, já que as linhas de G são. Podemos então considerar o código C' gerado por esta matriz. Vejamos que C' é equivalente a C, para isto, consideremos a seguinte transformação linear $T : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$, definida por

$$T(g_{r1}, \ldots, g_{ri}, \ldots, g_{rj}, \ldots, g_{rn}) = (g_{r1}, \ldots, g_{rj}, \ldots, g_{ri}, \ldots, g_{rn}).$$

Assim, $\beta' = \{T(g_1), \ldots, T(g_k)\}$ é base de $T(C)$ e de C', logo $T(C) = C'$. Ainda, para $a = (a_1, \ldots, a_i, \ldots, a_j, \ldots, a_n), b = (b_1, \ldots, b_i, \ldots, b_j, \ldots, b_n) \in \mathbb{F}_q^n$, temos

$$d(a,b) = d((a_1, \ldots, a_i, \ldots, a_j, \ldots, a_n), (b_1, \ldots, b_i, \ldots, b_j, \ldots, b_n))$$
$$d((a_1, \ldots, a_j, \ldots, a_i, \ldots, a_n), (b_1, \ldots, b_j, \ldots, b_i, \ldots, b_n)) = d(T(a), T(b)).$$

Portanto T é uma isometria linear entre C e C', ou seja, estes códigos são equivalentes. Além disso, segue que a composição de operações L_1, L_2, L_3 e C_1 continua resultando em um código equivalente a C.

Agora, vejamos como obter um código C' equivalente a C cuja matriz geradora está na forma padrão. Como a primeira linha de G não é nula (os vetores linhas de G são linearmente independentes), por meio de (C_1), podemos supor $g_{11} \neq 0$. Agora, multiplicando a primeira linha por g_{11}^{-1},pela operação (L_2), substituímos g_{11} por 1.

Somando à segunda, terceira, etc. linhas, respectivamente, a primeira linha multiplicada respectivamente por $(-1)g_{21}, (-1)g_{31}, ..., (-1)g_{k1}$, pela operação (L_3) obtemos a matriz

$$\begin{pmatrix} 1 & b_{12} & \cdots & b_{1n} \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{k2} & \cdots & b_{kn} \end{pmatrix}.$$

Agora, na segunda linha dessa matriz, temos certamente um elemento não nulo que por meio da operação (C_1), pode ser colocado na segunda linha e segunda coluna. Multiplicando a segunda linha pelo inverso desse elemento, a matriz se transforma em

$$\begin{pmatrix} 1 & c_{12} & \cdots & c_{1n} \\ 0 & 1 & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{k2} & \cdots & c_{kn} \end{pmatrix}.$$

Novamente, usando a operação (L_3), obtemos a matriz

$$\begin{pmatrix} 1 & 0 & \cdots & d_{1n} \\ 0 & 1 & \cdots & d_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_{kn} \end{pmatrix},$$

e assim sucessivamente, até encontrarmos uma matriz na forma padrão

$$G' = (Id_k | A).$$

□

4.2 Código duais

Sejam $\boldsymbol{u} = (u_1, ..., u_n)$ e $\boldsymbol{v} = (v_1, ..., v_n)$ elementos de $\mathbb{F}_q^n$, define-se produto interno de $\boldsymbol{u}$ e $\boldsymbol{v}$ como sendo

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle = u_1 v_1 + \cdots + u_n v_n.$$

Notemos que esta operação coincide com o produto interno usual. Assim, são válidas as propriedades de produto interno, como simetria e bilinearidade.

Seja $C \subset \mathbb{F}_q^n$ um código linear, define-se

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

Lema 4.12. *Se $C \subset \mathbb{F}_q^n$ é um código linear, com matriz geradora G, então*

(*i*) *$C^{\perp}$ é um subespaço vetorial de $\mathbb{F}_q^n$.*

(*ii*) *$\boldsymbol{v} \in C^{\perp}$ se, e somente se, $G\boldsymbol{v}^t = 0$.*

Demonstração. (*i*) Dados $\boldsymbol{u}, \boldsymbol{v} \in C^{\perp}$ e $\lambda \in \mathbb{F}_q$.Temos $\forall \boldsymbol{w} \in C$, que

$$\langle \boldsymbol{u} + \lambda \boldsymbol{v}, \boldsymbol{w} \rangle = \langle \boldsymbol{u}, \boldsymbol{w} \rangle + \lambda \langle \boldsymbol{v}, \boldsymbol{w} \rangle = 0 + \lambda 0 = 0.$$

e, portanto, $u + \lambda v \in C^{\perp}$, provando que $C^{\perp}$ é um subespaço vetorial de $\mathbb{F}_q^n$.

(*ii*) Digamos que G é a matriz geradora a partir da base $\beta = \{w_1, \ldots, w_k\}$. Ao multiplicarmos G por $\boldsymbol{v}^t$, obtemos uma matriz coluna, onde a linha i é obtida multiplicando a linha i de G (que é o vetor w_i) pelo vetor coluna $\boldsymbol{v}^t$, para todo $i = 1, \ldots, k$. Note que esta multiplicação, é exatamente a definição do produto interno entre $w_i \in C$ e $\boldsymbol{v}^t$. Assim, $\boldsymbol{v} \in C^{\perp}$ se, e somente se, $\langle \boldsymbol{v}^t, w_i \rangle = 0$, para todo $i = 1, \ldots, k$, que por sua vez é equivalente à $G\boldsymbol{v}^t = 0$.

□

O subespaço vetorial $C^{\perp}$ de $\mathbb{F}_q^n$, ortogonal a C, é também um código linear que será chamado de código dual de C.

Proposição 4.13. *Seja $C \subset \mathbb{F}_q^n$ um código de dimensão k com matriz geradora na forma padrão $G = (Id_k|A)$. Então:*

(*i*) *$\dim C^{\perp} = n - k$.*

(*ii*) *$H = (-A^t|Id_{n-k})$ é uma matriz geradora de $C^{\perp}$.*

Demonstração. (*i*) Temos que $\boldsymbol{v} \in C^{\perp}$ se, e somente se, $G\boldsymbol{v}^t = 0$. Se $v = (v_1, v_2, \ldots, v_n)$ temos o seguinte sistema:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \vdots & a_{1,k+1} & \cdots & a_{1,n} \\ 0 & 1 & \cdots & 0 & \vdots & a_{2,k+1} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & \vdots & a_{k,k+1} & \cdots & a_{k,n} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

Daí:

$$\begin{cases} v_1 + a_{1,k+1}v_{k+1} + \ldots + a_{1,n}v_n &= 0 \\ v_2 + a_{2,k+1}v_{k+1} + \ldots + a_{2,n}v_n &= 0 \\ \vdots & \\ v_k + a_{k,k+1}v_{k+1} + \ldots + a_{k,n}v_n &= 0 \end{cases}$$

Então:

$$\begin{cases} v_1 &= -(a_{1,k+1}v_{k+1} + \ldots + a_{1,n}v_n) \\ v_2 &= -(a_{2,k+1}v_{k+1} + \ldots + a_{2,n}v_n) \\ \vdots & \\ v_k &= -(a_{k,k+1}v_{k+1} + \ldots + a_{k,n}v_n) \end{cases}$$

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix} = -A \cdot \begin{pmatrix} v_{k+1} \\ v_{k+2} \\ \vdots \\ v_n \end{pmatrix}$$

Logo, temos que $\boldsymbol{v}$ é dado por

$$\begin{aligned} &(-(a_{1,k+1}v_{k+1} + \ldots + a_{1,n}v_n), \ldots, -(a_{k,k+1}v_{k+1} + \ldots + a_{k,n}v_n), v_{k+1}, \ldots, v_n) \\ &= v_{k+1}(-a_{1,k+1}, -a_{2,k+1}, \ldots, -a_{k,k+1}, 1, 0, \ldots, 0) + \\ &+ \ldots + v_n(-a_{1,n}, -a_{2,n}, \ldots, -a_{k,n}, 0, 0, \ldots, 1) \end{aligned}$$

em que $v_{k+1}, v_{k+2}, \ldots, v_n \in \mathbb{F}_q$. Como $\mathbb{F}_q$ possui q elementos, existem $q^{n-(k+1)+1} = q^{n-k}$ possibilidades para $\boldsymbol{v}$, ou seja, $C^\perp$ possui q^{n-k} elementos, o que significa que sua dimensão é $n-k$

(ii) É evidente que as linhas de H são linearmente independentes, por causa do bloco Id_{n-k}, portanto, geram um subespaço vetorial de dimensão $n-k$. Como as linhas de H são ortogonais às linhas de G, temos que o espaço gerado pelas linhas de H está contido em $C^\perp$ e como esses dois subespaços têm a mesma dimensão, eles coincidem, provando assim que $H = (-A^t | Id_{n-k})$ é uma matriz geradora de $C^\perp$.

□

Proposição 4.14. *Suponha que C seja um código de dimensão k em $\mathbb{F}_q^n$ com matriz geradora G. Uma matriz H de ordem $(n-k) \times n$, com coeficientes em $\mathbb{F}_q$ e com linhas linearmente independentes, é uma matriz geradora de $C^\perp$ se, e somente se,*

$$G \cdot H^t = 0.$$

Demonstração. As linhas de H geram um subespaço vetorial de $\mathbb{F}_q^n$ de dimensão $n-k$, portanto, igual, à dimensão de $C^\perp$. Por outro lado, representando por $h_1, ..., h_{n-k}$ e por $g_1, ..., g_k$, respectivamente, as linhas de H e de G, temos que

$$(GH^t)_{i,j} = \langle g_i, h_j \rangle.$$

Portanto, $GH^t = 0$ é equivalente a dizer que todos os vetores do subespaço gerado pelas linhas de H estão em $C^\perp$. Por outro lado, esse subespaço tem a mesma dimensão de $C^\perp$, logo:

$$GH^t = 0 \Leftrightarrow C^\perp \text{ é gerado pelas linhas de } H \ .$$

□

Corolário 4.15. $(C^{\perp})^{\perp} = C$

Demonstração. Sejam G e H respectivamentes matrizes geradoreas de C e $C^{\perp}$. Logo, $G \cdot H^t = 0$. Tomando transpostas nessa última igualdade, temos que $H \cdot G^t = 0$, logo, G é a matriz geradora de $(C^{\perp})^{\perp}$, daí seguindo o resultado. □

Proposição 4.16. *Seja C um código linear e suponhamos que H seja uma matriz geradora de $C^{\perp}$. Temos então que*

$$\boldsymbol{v} \in C \Leftrightarrow H\boldsymbol{v}^t = 0.$$

Demonstração. Temos, pelo Corolário acima e pelo Lema 4.12 (ii), $v \in C$ se, e somente se, $v \in (C^{\perp})^{\perp}$. E isto equivale a $Hv^t = 0$. □

A proposição acima nos permite caracterizar os elementos de um código C por uma condição de anulamento. A matriz geradora H de $C^{\perp}$ é chamada de *matriz teste de paridade* de C.

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

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

Como G está na forma padrão, é fácil calcular uma matriz teste de paridade H. Pela Proposição 4.13, temos que

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

Dados $\boldsymbol{v} = (100111)$ e $\boldsymbol{v}' = (010101)$, como

$$H\boldsymbol{v}^t = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{e} \quad H(\boldsymbol{v}')^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \neq 0,$$

temos que $\boldsymbol{v} \in C$ e $\boldsymbol{v}' \notin C$.

Proposição 4.17. *Seja H a matriz teste de paridade de um código C. Temos que o peso de C é maior do que ou igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

Demonstração. ($\Leftarrow$) Suponhamos que cada conjunto de $s-1$ colunas de H é linearmente independente. Seja $\boldsymbol{c} = (c_1, \ldots, c_n)$ uma palavra não nula de C, e sejam $h^1, \ldots, h^n$ as colunas de H. Como $H\boldsymbol{c}^t = 0$, temos que

$$0 = H \cdot \boldsymbol{c}^t = \sum c_i h^i$$

Visto que $\omega(\boldsymbol{c})$ é o número de componentes não nulas de $\boldsymbol{c}$, segue que se $\omega(\boldsymbol{c}) < s-1$, teríamos uma combinação nula de um número t, com $1 \leq t < s-1$, de colunas de H, o que é contraditório. Logo, $\omega(\boldsymbol{c}) \geq s$ e, portanto, $\omega(C) \geq s$.

($\Rightarrow$) Suponhamos que $\omega(C) \geq s$ e que H teria $s-1$ colunas linearmente dependentes, digamos $h^{i_1}, \ldots, h^{i_{s-1}}$. Logo, existiriam $c_{i_1}, \ldots, c_{i_{s-1}}$, no corpo, nem todos nulos, tais que

$$c_{i_1} h^{i_1} + \cdots + c_{i_{s-1}} h^{i_{s-1}} = 0$$

Portanto, $\boldsymbol{c} = (0, \ldots, c_{i_1}, 0, \ldots, c_{i_{s-1}}, 0 \ldots, 0) \in C$, com $\omega(\boldsymbol{c}) \leq s-1 < s$. Absurdo. □

Teorema 4.18. *Seja H a matriz teste de paridade de um código C. Temos que o peso de C é igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Demonstração. ($\Rightarrow$) Suponhamos que $\omega(C) = s$, logo, todo conjunto de $s-1$ colunas de H são linearmente independentes. Por outro lado, existem s colunas de H linearmente dependentes, pois caso contrário, pela proposição anterior, teríamos $\omega(C) \geq s+1$.

($\Leftarrow$) Suponhamos que todo conjunto de $s-1$ vetores colunas de H é linearmente independente e existem s colunas linearmente dependentes. Logo, da proposição anterior, temos que $\omega(C) \geq s$. Mas $\omega(C)$ não pode ser maior do que s, pois, neste caso, novamente a proposição anterior, nos diria que todo conjunto com s colunas e H é linearmente independente, o que é uma contradição. □

Corolário 4.19 (Cota de Singleton)**.** *Os parâmetros (n, k, d) de um código linear satisfazem a desigualdade*

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

Demonstração. Se H é uma matriz teste de paridade, ela tem posto $n-k$. Como, pelo Teorema 4.18, $d-1$ é menor ou igual ao posto de H, segue a desigualdade. □

Um código será chamado de MDS (Maximum Distance Separable) se vale a igualdade $d = n - k + 1$.

CAPÍTULO 5

GRAFOS

Definição 5.1. *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.

Definição 5.2. *Um grafo G é dito bipartido se existe um 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 o outro em Y. Os conjuntos X e Y são chamados de conjunto partição.*

Considere o grafo a seguir, cujos vértices sao $V = \{a, b, c, d, e, f\}$.

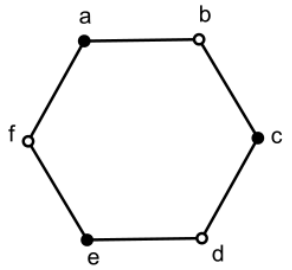

Figura 5.1: Grafo Bipartido

Notemos que podemos particionar o conjunto V em $X = \{a, c, e\}$ e $Y = \{b, d, f\}$. Assim, cada aresta deste grafo possui um vértice em X e um vértice em Y, ou seja, este grafo é bipartido.

Definição 5.3. *Seja G um grafo,$V_G = \{v_1, \ldots, v_m\}$ o conjunto ordenado de seus vértices e $A_G = \{a_1, \ldots, a_n\}$ o conjunto ordenado de suas arestas. Definimos a matriz $M = (m_{ij})$, denominada 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 $i = 1, \ldots, m$ e todo $j = 1, \ldots, n$.

Notemos que a coluna j possui 1 nas duas linhas que indicam os vértices que a compõem e 0 nas demais linhas. Assim, a soma dos elementos de cada coluna da matriz M é constante igual a 2.

Exemplo 5.4. *Seja G o grafo dado na Figura 5.2, onde $V(G) = \{v_1, v_2, v_3, v_4, v_5\}$ é seu conjunto de vértices e $A(G) = \{a_1, a_2, a_3, a_4, a_5, a_6\}$ seu conjunto de arestas.*

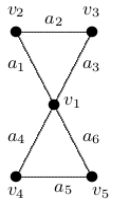

Figura 5.2: Grafo G

A matriz de incidência de G é a matriz 5×6 dada por

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

CAPÍTULO 6

PARÂMETROS DE UM CÓDIGO PROJETIVO PARAMETRIZADO

6.1 Código projetivo parametrizado por conjunto tórico algébrico

Seja $\mathbb{F}_q$ um corpo finito com q elementos e $L = \mathbb{F}_q[Z_1, \ldots, Z_n]$ um anel de polinômios sobre o corpo $\mathbb{F}_q$. Sejam $Z^{a_1}, \ldots, Z^{a_m}$ um conjunto finito de monômios, onde

$$Z^{a_i} = Z_1^{a_{i1}}.\cdots.Z_n^{a_{in}}, \text{ para todo } i = 1, \ldots, m$$

Consideramos agora um conjunto parametrizado por estes monômios

$$X = \{(t_1^{a_{11}}.\cdots.t_n^{a_{1n}} : \cdots : t_1^{a_{m1}}.\cdots.t_n^{a_{mn}}) \in \mathbb{P}^{m-1} | t_i \in \mathbb{F}_q^*\} \tag{6.1}$$

onde $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ e $\mathbb{P}^{m-1}$ é um espaço projetivo sobre o corpo $\mathbb{F}_q$. Chamamos X de *conjunto tórico algébrico* parametrizado por $Z^{a_1}, \ldots, Z^{a_m}$. Este conjunto forma um grupo multiplicativo, considerando a multiplicação componente a componente.

Seja A a matriz $n \times m$ dada por

$$A = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}. \tag{6.2}$$

Dizemos que o conjunto definido em (6.1) é um conjunto tórico algébrico associado à matriz A. Notemos que

$$\begin{aligned}(t_1^{a_{11}}.\cdots.t_n^{a_{1n}} : \cdots : t_1^{a_{m1}}.\cdots.t_n^{a_{mn}}) &= (t_1^{a_{11}}.\cdots.t_n^{a_{1n}})^{-1}(t_1^{a_{11}}.\cdots.t_n^{a_{1n}} : \cdots : t_1^{a_{m1}}.\cdots.t_n^{a_{mn}}) \\ &= (1 : t_1^{a_{21}-a_{11}}.\cdots.t_n^{a_{2n}-a_{1n}} : \cdots : t_1^{a_{m1}-a_{11}}.\cdots.t_n^{a_{mn}-a_{1n}})\end{aligned}$$

Tomando $b_{ij} = a_{ij} - a_{1j} \in \mathbb{Z}$ para todo $i = 2, \ldots, m$ e $j = 1, \ldots, n$, obtemos

$$X = \{(1 : t_1^{b_{21}} \cdot \cdots \cdot t_n^{b_{2n}} : \cdots : t_1^{b_{m1}} \cdot \cdots \cdot t_n^{b_{mn}}) \in \mathbb{P}^{m-1} | t_i \in \mathbb{F}_q^*\} \tag{6.3}$$

Usaremos qualquer uma das representações (6.1) ou (6.3) para referirmos ao conjunto tórico parametrizado pelos monômios $Z^{a_1}, \ldots, Z^{a_m}$ ou, de modo equivalente, para representar um conjunto tórico associado à matriz (6.2).

Considere agora $S = \mathbb{F}_q[X_1, \ldots, X_m] = \bigoplus_{d=0}^{\infty} S_d$, onde S_d é o conjunto dos polinômios homogêneos de grau d em $\mathbb{F}_q[X_1, \ldots, X_m]$, com a graduação padrão, juntamente com o polinômio nulo. Claramente S_d é um espaço vetorial com a soma de polinômios e multiplicação por escalar usuais. Sejam $P_1, \ldots, P_{|X|}$ os pontos de X e $f_0(X_1, \ldots, X_m) = X_1^d$. Assim, a aplicação de avaliação

$$\begin{aligned} ev_d : S_d &\longrightarrow \mathbb{F}_q^{|X|} \\ f &\longmapsto \left(\frac{f(P_1)}{f_0(P_1)}, \ldots, \frac{f(P_{|X|})}{f_0(P_{|X|})} \right) \end{aligned} \tag{6.4}$$

define uma transformação linear entre $\mathbb{F}_q$-espaços vetoriais, cuja imagem é um subespaço vetorial de $\mathbb{F}_q^{|X|}$.

Definição 6.1. *Definimos o código projetivo parametrizado de ordem d a partir do conjunto tórico X como sendo $C_X(d) = \mathrm{Im}(ev_d)$.*

Neste trabalho, nosso objetivo é estimar os parâmetros deste código linear: comprimento, dimensão e distância mínima. Claramente, o comprimento de $C_X(d)$ é dado por $|X|$, já que $C_X(d) \subseteq \mathbb{F}_q^{|X|}$. Notemos também que como $C_X(d) = \mathrm{Im}(ev_d)$, segue que

$$C_X(d) \cong S_d / \ker(ev_d).$$

Definição 6.2. *O ideal anulador de X, denotado por I_X, é o ideal gerado pelos polinômios homogêneos que se anulam em todos os pontos de X. Definimos também o subespaço vetorial $I_X(d)$ de S_d formado pelos polinômios homogêneos de grau d que se anulam em X, ou seja, $I_X(d) := I_X \cap S_d$.*

Temos que $\ker(ev_d) = I_X(d)$. De fato, se $f \in \ker(ev_d)$, então $f \in S_d$ e

$$\left(\frac{f(\boldsymbol{P}_1)}{f_0(\boldsymbol{P}_1)}, \ldots, \frac{f(\boldsymbol{P}_{|X|})}{f_0(\boldsymbol{P}_{|X|})} \right) = (0, \ldots, 0),$$

logo $f(\boldsymbol{P}_1) = \cdots = f(\boldsymbol{P}_{|X|}) = 0$, ou seja, $f \in I_X(d)$. Reciprocamente, se $f \in I_X(d)$, então $f \in S_d$ e $f(\boldsymbol{P}_1) = \cdots = f(\boldsymbol{P}_{|X|}) = 0$, logo $ev_d(f) = (0, \ldots, 0)$. Portanto, $f \in \ker(ev_d)$.

Para calcular a dimensão do código, precisamos estudar $\dim_k(S_d/I_X(d))$. Esta dimensão é dada pela função de Hilbert de I_X, definida por

$$\begin{array}{rccc} H_X: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & d & \longmapsto & H_X(d) = \dim_k(S_d/I_X(d)) \end{array}$$

Para d suficientemente grande, a função de Hilbert é dada por um polinômio, $h_X(d)$, denominado *polinômio de Hilbert*. Assim, existe um natural r, tal que $H_X(d) = h_X(d) = \sum_{i=0}^{k} c_i d^i$, para todo $d \geq r$. O menor número natural que satisfaz esta condição é denotado por r_X e é chamado de *índice de regularidade* de I_X. Ainda, definimos a dimensão de uma variedade projetiva $V \subset \mathbb{P}^n$ como sendo o grau do polinômio de Hilbert de seu correspondente ideal homogêneo $\boldsymbol{I}(V)$. No caso do conjunto tórico algébrico X, o próximo resultado mostra que sua dimensão é zero, pois o polinômio de Hilbert é constante e igual à cardinalidade de X.

Proposição 6.3. *$H_X(d) = |X|$ para todo $d \geq |X| - 1$.*

Demonstração. Seja $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{|X|}\}$ a base canônica de $\mathbb{F}_q^{|X|}$ e seja $d \geq |X| - 1$. Vamos construir um polinômio $f_1 \in S_d$ tal que $ev_d(f_1) = \boldsymbol{e}_1$. Denotaremos $X = \{\boldsymbol{P}_1, \ldots, \boldsymbol{P}_{|X|}\}$, onde $\boldsymbol{P}_j = (1 : P_{j2} : \cdots : P_{jm})$. Como $\boldsymbol{P}_1 \neq \boldsymbol{P}_2$, segue que para algum $k \in \{2, \ldots, m\}$ temos $P_{1k} \neq P_{2k}$. Defina

$$h_2 = \frac{X_k - P_{2k}X_1}{P_{1k} - P_{2k}} \in \mathbb{F}_q[X_1, \ldots, X_m].$$

Observe que h_2 é homogêneo de grau 1 e $h_2(\boldsymbol{P}_1) = 1$ e $h_2(\boldsymbol{P}_2) = 0$. Analogamente, definimos $h_3, \ldots, h_{|X|} \in \mathbb{F}_q[X_1, \ldots, X_m]$, tais que, para todo $i = 2, \ldots, |X|$, temos

$$h_i(\boldsymbol{P}_j) = \begin{cases} 0, & \text{se } j = i \\ 1, & \text{se } j = 1 \end{cases}.$$

Considere

$$f_1 := X_1^{d-|X|+1} h_2 . \cdots . h_{|X|}.$$

Observe que f_1 é um polinômio homogêneo de grau $(d - |X| + 1) + (|X| - 1) = d$, isto é, $f_1 \in S_d$. Mais ainda, $f_1(\boldsymbol{P}_1) = 1$ e $f_1(\boldsymbol{P}_j) = 0$, para todo $j \in \{2, \ldots, |X|\}$. Portanto,

$$ev_d(f_1) = \left(\frac{f_1(\boldsymbol{P}_1)}{f_0(\boldsymbol{P}_1)}, \ldots, \frac{f_1(\boldsymbol{P}_{|X|})}{f_0(\boldsymbol{P}_{|X|})}\right) = (1, 0, \ldots, 0) = \boldsymbol{e}_1$$

De modo análogo, podemos construir $f_2, \ldots, f_{|X|} \in S_d$ tais que $ev_d(f_j) = \boldsymbol{e}_j$, para todo $2 \leq j \leq |X|$. Isso prova que ev_d é sobrejetora para $d \geq |X| - 1$. Portanto,

$$H_X(d) = \dim S_d/I_X(d) = \dim ev_d(S_d) = \dim \mathbb{F}_q^{|X|} = |X|,$$

para todo $d \geq |X| - 1$.

□

Pela proposição anterior, para $d \geq |X| - 1$, temos $H_X(d) = |X|$, ou seja, a função de Hilbert é dado pelo polinômio constante $|X|$. Portanto, podemos concluir que $r_X \leq |X|-1$ e

$$h_X(d) = H_X(d) = |X|, \text{ para } d \geq r_X.$$

Ainda, $\dim(C_X(d)) = |X|$, o que implica $C_X(d) = \mathbb{F}_q^{|X|}$ para $d \geq r_X$. Por este motivo, podemos considerar sempre $0 \leq d < r_X$.

6.2 Os Parâmetros de $C_X(d)$

Estudaremos agora o conjunto tórico X para estimar os parâmetros do código $C_X(d)$, que acabamos de descrever.

6.2.1 Comprimento

Para computar o comprimento do código projetivo parametrizado gerado pelo conjunto tórico X, introduzimos os seguintes subgrupos multiplicativos de X. Para cada $i = 1, \ldots, n$, consideremos

$$Y_i := \{(1 : t_i^{b_{2i}} : \cdots : t_i^{b_{mi}}) \in \mathbb{P}^{m-1} : t_i \in \mathbb{F}_q^*\},$$

com a multiplicação coordenada a coordenada. Vejamos que $|Y_i| = \dfrac{q-1}{(q-1, b_{2i}, \ldots, b_{mi})} = d_i$, para todo $i = 1, \ldots, n$, onde $(q-1, b_{2i}, \ldots, b_{mi})$ representa o máximo divisor comum entre estes inteiros. De fato, como $\mathbb{F}_q$ tem q elementos, existe $\beta \in \mathbb{F}_q^*$ tal que $\mathbb{F}_q^* = \{1, \beta, \beta^2, \ldots, \beta^{q-2}\}$, vejamos que

$$\begin{aligned} Y_i = &\{(1 : 1 : \cdots : 1), (1 : \beta^{b_{2i}} : \cdots : \beta^{b_{mi}}), (1 : (\beta^2)^{b_{2i}} : \cdots : (\beta^2)^{b_{mi}}), \ldots, \\ &(1 : (\beta^{d_i-1})^{b_{2i}} : \cdots : (\beta^{d_i-1})^{b_{mi}})\}. \end{aligned}$$

Note que para $k, l < d_i \leq q-2$, temos

$$\begin{aligned} k \neq l \Rightarrow \beta^k \neq \beta^l \Rightarrow (\beta^k)^{b_{ji}} \neq (\beta^l)^{b_{ji}}, \forall j = 2, \ldots, m \\ \Rightarrow (1 : (\beta^k)^{b_{2i}} : \cdots : (\beta^k)^{b_{mi}}) \neq (1 : (\beta^j)^{b_{2i}} : \cdots : (\beta^j)^{b_{mi}}) \end{aligned}$$

Por outro lado, para $d_i \leq k \leq q-2$, temos $k = td_i + k'$, com $k' = 0$ ou $k' < d_i$. Quando $k' = 0$, temos que kb_{ji} é um múltiplo de $q-1$, para $j = 2, \ldots, m$, donde $\beta^k = 1$. Logo, $(1 : (\beta^k)^{b_{2i}} : \cdots : (\beta^k)^{b_{mi}}) = (1 : \cdots : 1)$. Caso $0 < k' < d_i$, segue que

$$\begin{aligned} (1 : (\beta^k)^{b_{2i}} : \cdots : (\beta^k)^{b_{mi}}) &= (1 : (\beta^{pd_i+k'})^{b_{2i}} : \cdots : (\beta^{pd_i+k'})^{b_{mi}}) \\ &= (1 : \beta^{pd_ib_{2i}+k'b_{2i}} : \cdots : \beta^{pd_ib_{mi}+k'b_{mi}}) \\ &= (1 : (\beta^{k'})^{b_{2i}} : \cdots : (\beta^{k'})^{b_{mi}}). \end{aligned}$$

Com isso, segue que Y_i possui $d_i = \dfrac{q-1}{(q-1, b_{2i}, \ldots, b_{mi})}$ elementos distintos.

Teorema 6.4. *O comprimento do código projetivo parametrizado de ordem d, $C_X(d)$, é dado por*

$$|X| = \frac{1}{|M|}\prod_{i=1}^{n}|Y_i|, \tag{6.5}$$

onde M é o conjunto de n-uplas $(i_1, \ldots, i_n)$ tais que

$$1 \leq i_j \leq \frac{q-1}{(q-1, b_{2j}, \ldots, b_{mj})}, \text{ para todo } j = 1, \ldots, n$$

e

$$\begin{aligned} i_1b_{21} + i_2b_{22} + \cdots + i_nb_{2n} &\equiv 0 \mod (q-1) \\ i_1b_{31} + i_2b_{32} + \cdots + i_nb_{3n} &\equiv 0 \mod (q-1) \\ &\vdots \\ i_1b_{m1} + i_2b_{m2} + \cdots + i_nb_{mn} &\equiv 0 \mod (q-1) \end{aligned} \tag{6.6}$$

Demonstração. Consideremos os grupos multiplicativos $Y_1 \times \cdots \times Y_n$ e X, munidos com a multiplicação coordenada a coordenada. Dessa forma, é fácil ver que a aplicação $\phi : Y_1 \times \cdots \times Y_n \longrightarrow X$, onde

$$\phi\left((1 : t_1^{b_{21}} : \cdots : t_1^{b_{m1}}), \ldots, (1 : t_n^{b_{2n}} : \cdots : t_n^{b_{mn}})\right) = \left(1 : t_1^{b_{21}}.\cdots.t_n^{b_{2n}} : \cdots : t_1^{b_{m1}}.\cdots.t_n^{b_{mn}}\right)$$

é um homomorfismo sobrejetor. Assim, temos que

$$(Y_1 \times \cdots \times Y_n)/\ker(\phi) \cong X,$$

e, portanto,

$$|X| = \frac{|Y_1 \times \cdots \times Y_n|}{|\ker(\phi)|} = \frac{1}{|\ker(\phi)|}\prod_{i=1}^{n}|Y_i|.$$

Se β é um gerador de $\mathbb{F}_q^*$, então pelo que vimos, os elementos de Y_j são $(1 : (\beta^{i_j})^{b_{2j}} : \cdots : (\beta^{i_j})^{b_{mj}})$, onde $1 \leq i_j \leq \frac{q-1}{(q-1, b_{2j}, \ldots, b_{mj})}$. Notemos agora que

$$\begin{aligned} \ker(\phi) = \{&(1 : \beta^{i_1b_{21}} : \cdots : \beta^{i_1b_{m1}}), \ldots, (1 : \beta^{i_nb_{2n}} : \cdots : \beta^{i_nb_{mn}}) \in Y_1 \times \cdots \times Y_n : \\ &(1 : \beta^{i_1b_{21}+i_2b_{22}\ldots i_nb_{2n}} : \cdots : \beta^{i_1b_{m1}+i_2b_{m2}\ldots i_nb_{mn}}) = (1 : 1 : \cdots : 1)\}. \end{aligned}$$

No entanto, para cada $j = 2, \ldots, m$, temos $\beta^{i_1b_{j1}+i_2b_{j2}\ldots i_nb_{jn}} = 1$ quando $i_1b_{j1} + i_2b_{j2}\cdots + i_nb_{jn}$ é um múltiplo de $q-1$, ou seja, $i_1b_{j1} + i_2b_{j2}\ldots i_nb_{jn} \equiv 0 \mod (q-1)$. Dessa forma, $|\ker(\phi)|$ é exatamente o número de n-uplas $(i_1, \ldots, i_n)$ tais que $1 \leq i_j \leq$

$\frac{q-1}{(q-1,b_{2j},\ldots,b_{mj})}$, para todo $j=1,\ldots,n$ e satisfazendo (6.6), ou seja, $|\ker(\phi)|=|M|$.
Portanto

$$|X|=\frac{1}{|M|}\prod_{i=1}^{n}|Y_i|,$$

□

Definimos agora o *toro projetivo* de dimensão $m-1$ como sendo

$$\mathbb{T}_{m-1}=\{(c_1:\cdots:c_m)\in\mathbb{P}^{m-1}:c_i\in\mathbb{F}_q^*\text{ para todo }i\}. \tag{6.7}$$

Notemos que $\mathbb{T}_{m-1}$ é conjunto tórico particular, parametrizado pelos monômios $Z_1,\ldots,Z_m$.

Claramente, $X\subseteq\mathbb{T}_{m-1}$. O seguinte corolário nos diz sobre quais condições temos a igualdade entre esses conjuntos.

Corolário 6.5. *Assuma que $n=m$. Então $X=\mathbb{T}_{m-1}$ se e somente se $|M|=q-1$ e $(q-1,b_{2j},\ldots,b_{mj})=1$, para todo $j=1,\ldots,m$.*

Demonstração. Seja $X=\mathbb{T}_{m-1}$, isto é, $X=\{(t_1:\cdots:t_m)\in\mathbb{P}^{m-1}:t_i\in\mathbb{F}_q^*\text{ para todo }i\}$. Assim, $|X|=(q-1)^{m-1}$, e de $(t_1:t_2:\cdots:t_m)=(1:t_1^{-1}t_2:\cdots:t_1^{-1}t_m)$ temos $(q-1,b_{2j},\ldots,b_{mj})=1$ para todo $j=1,\ldots,m$ pois $b_{21}=-1$ e $b_{ii}=1$ para $i=2,\ldots,m$. Mais ainda, de

$$(q-1)^{m-1}=\frac{1}{|M|}\prod_{j=1}^{m}|Y_j|=\frac{1}{|M|}\prod_{j=1}^{m}\frac{q-1}{(q-1,b_{2j},\ldots,b_{mj})}=\frac{1}{|M|}(q-1)^m$$

temos $|M|=q-1$.

Reciprocamente, se $|M|=q-1$ e $(q-1,b_{2j},\ldots,b_{mj})=1$, para todo $j=1,\ldots,m-1$, então

$$|X|=\frac{1}{q-1}\prod_{i=1}^{m}\frac{q-1}{1}=(q-1)^{m-1}=|\mathbb{T}_{m-1}|.$$

Como $X\subset\mathbb{T}_{m-1}$ temos que $X=\mathbb{T}_{m-1}$. □

Corolário 6.6. *Se a soma dos elementos de cada coluna da matriz A definida em (6.2) é uma constante ou, equivalentemente, se os monômios que parametrizam o conjunto tórico X possuem o mesmo grau, então $|X|\leq(q-1)^{n-1}$.*

Demonstração. Seja $\sum_{j=1}^{n}a_{ij}=\alpha$ (inteiro positivo), para todo $i=1,\ldots m$. Notemos que $|Y_i|\leq q-1$, para todo $i=1,\ldots,m$. Além disso,

$$\sum_{j=1}^{n}b_{ij}=\sum_{j=1}^{n}a_{ij}-\sum_{i=1}^{n}a_{1j}=\alpha-\alpha=0,\text{ para todo }i=2,\ldots,m.$$

Assim, considerando $(i_1, i_2, \ldots, i_n) = (1, 1, \ldots, 1)$, temos que $1 \leq i_j \leq \dfrac{q-1}{(q-1, b_{2j}, \ldots, b_{mj})}$ e esta n-upla satisfaz (6.6). Logo $(1, \ldots, 1) \in M$. Seja $\gamma = min\{|Y_1|, \ldots, |Y_n|\}$. Então $(k, \ldots, k) \in M$, para todo $1 \leq k \leq \gamma$, pois

$$kb_{i1} + kb_{i2} + \cdots + kb_{in} = k(b_{i1} + b_{i2} + \cdots + b_{in}) \equiv 0 \mod (q-1), \forall i = 2, \ldots, m,$$

ou seja, $(k, \ldots, k)$ satisfaz (6.6). Com isso, temos que $|M| \geq \gamma$. Assim,

$$|X| = \frac{1}{|M|} \prod_{i=1}^{n} |Y_i| \leq \frac{1}{\gamma} \gamma (q-1)^{n-1} = (q-1)^{n-1}.$$

□

Observe que se G é um grafo e X o conjunto tórico algébrico associado à matriz de incidência de G, então a soma dos elementos de cada coluna de sua matriz é $\alpha = 2$ e o resultado do corolário anterior é válido. Na realidade, nesta situação, $|Y_i| = q - 1$ para todo $i = 1, \ldots, n$, pois b_{ji} é 0, 1 ou -1. Logo $(q-1, b_{2i}, \ldots, b_{mi}) = 1$. Portanto, em qualquer grafo, $|X| = \dfrac{(q-1)^n}{|M|}$. Além disso, em [6, Corolário 3.8], foi encontrado o valor exato de $|X|$ se G é um grafo conexo. A saber,

$$|X| = \begin{cases} (q-1)^{n-2} & \text{se} \quad G \text{ é bipartido} \\ (q-1)^{n-1} & \text{se} \quad G \text{ não é bipartido.} \end{cases} \tag{6.8}$$

Por meio deste resultado, obtemos que

$$|M| = \begin{cases} (q-1)^2 & \text{se} \quad G \text{ é bipartido} \\ q-1 & \text{se} \quad G \text{ não é bipartido.} \end{cases}$$

6.2.2 Dimensão

Como mencionado anteriormente, a dimensão do código de avaliação de grau d parametrizado pelo conjunto tórico X é dada pela função de Hilbert de I_X, que é denotada por $H_X(d)$.

No seguinte teorema, calcularemos a dimensão do código gerado pelo conjunto tórico X em função da dimensão do código projetivo parametrizado gerado pelo toro projetivo $\mathbb{T}_{m-1}$.

Teorema 6.7. *A dimensão do código projetivo parametrizado de ordem d, $C_X(d)$, é dado por*

$$H_X(d) = H_{\mathbb{T}_{m-1}} - \overline{H}(d) \tag{6.9}$$

para todo $d \geq 0$ e onde $\overline{H}$ é a função de Hilbert de $I_X/I_{\mathbb{T}_{m-1}}$, isto é,

$$\overline{H}(d) = \dim(I_X(d)/I_{\mathbb{T}_{m-1}}(d))$$

Demonstração. Sabemos que $X \subseteq \mathbb{T}_{m-1}$, o que implica $I_X \supseteq I_{\mathbb{T}_{m-1}}$. Seja ψ a seguinte transformação linear

$$\begin{aligned} \psi : S_d/I_{\mathbb{T}_{m-1}(d)} &\longrightarrow S_d/I_X(d), \\ f + I_{\mathbb{T}_{m-1}}(d) &\longmapsto f + I_X(d). \end{aligned}$$

Vejamos que ψ está bem definida. Sejam $\overline{f} = \overline{g}$. Assim,

$$\begin{aligned} f + I_{\mathbb{T}_{m-1}}(d) = g + I_{\mathbb{T}_{m-1}}(d) &\Rightarrow f - g \in I_{\mathbb{T}_{m-1}}(d) \subseteq I_X(d) \\ &\Rightarrow f - g \in I_X(d) \Rightarrow f + I_X(d) = g + I_X(d). \end{aligned}$$

Além disso, claramente ψ é sobrejetivo. Mais ainda, $\ker(\psi) = I_X(d)/I_{\mathbb{T}_{m-1}}(d)$. De fato,

$$f \in \ker(\psi) \iff \psi(f) = f + I_X(d) = 0 + I_X(d) \iff f \in I_X(d).$$

Logo $\ker(\psi) = \{f + I_{\mathbb{T}_{m-1}}(d) : f \in I_X(d)\} = I_X(d)/I_{\mathbb{T}_{m-1}}(d)$. Assim, temos que

$$\frac{S_d/I_{\mathbb{T}_{m-1}}(d)}{I_X(d)/I_{\mathbb{T}_{m-1}}(d)} \cong S_d/I_X(d) \cong C_X(d).$$

Daí, segue que

$$\begin{aligned} \dim(S_d/I_X(d)) = \dim\left(\frac{S_d/I_{\mathbb{T}_{m-1}}(d)}{I_X(d)/I_{\mathbb{T}_{m-1}}(d)}\right) &= \dim(S_d/I_{\mathbb{T}_{m-1}}(d)) - \dim(I_X(d)/I_{\mathbb{T}_{m-1}}(d)) \\ \Rightarrow H_X(d) = H_{\mathbb{T}_{m-1}}(d) - \overline{H}(d) &= \dim C_X(d) \end{aligned}$$

O seguinte corolário relaciona os índices de regularidade de I_X, $I_{\mathbb{T}_{m-1}}$ e $I_X/I_{T_{m-1}}$, os quais são denotados por r_X, $r_{\mathbb{T}_{m-1}}$ e $r_{\overline{H}}$. □

Corolário 6.8. $r_{\mathbb{T}_{m-1}} = \max\{r_X, r_{\overline{H}}\}$.

Demonstração. Seja

$$\begin{aligned} \theta : I_X(d)/I_{\mathbb{T}_{m-1}}(d) &\longrightarrow I_X(d+1)/I_{\mathbb{T}_{m-1}}(d+1), \\ f + I_{\mathbb{T}_{m-1}}(d) &\longmapsto X_1 f + I_{\mathbb{T}_{m-1}}(d+1). \end{aligned}$$

Vejamos que θ está bem definido. Sejam $f, g \in I_X(d)$, então

$$f + I_{\mathbb{T}_{m-1}}(d) = g + I_{\mathbb{T}_{m-1}}(d) \Rightarrow (f-g) \in I_{\mathbb{T}_{m-1}}(d) \Rightarrow X_1(f-g) \in I_{\mathbb{T}_{m-1}}(d+1)$$

$$\Rightarrow X_1 f - X_1 g \in I_{\mathbb{T}_{m-1}}(d+1) \Rightarrow X_1 f + I_{\mathbb{T}_{m-1}}(d+1) = X_1 g + I_{\mathbb{T}_{m-1}}(d+1)$$

Portanto θ está bem definido e facilmente podemos ver que é uma transformação linear. Mostremos que $\ker(\theta) = \{0 + I_{\mathbb{T}_{m-1}}(d)\}$, isto é, θ é injetora. Se $f + I_{\mathbb{T}_{m-1}}(d) \in \ker(\theta)$, então $X_1 f \in I_{\mathbb{T}_{m-1}}(d+1)$, ou seja, para todo $P = (c_1 : \cdots : c_m) \in \mathbb{T}_{m-1}$, temos que $(X_1 f)(P) = c_1 f(P) = 0$. Como $c_1 \neq 0$, segue que $f(P) = 0$. Assim, para todo $P \in \mathbb{T}_{m-1}$, $f(P) = 0$ e f tem grau d, ou seja, $f \in I_{\mathbb{T}_{m-1}}(d)$. Portanto $f + I_{\mathbb{T}_{m-1}}(d) = 0 + I_{\mathbb{T}_{m-1}}(d)$.

Assim, temos que $I_X(d)/I_{\mathbb{T}_{m-1}}(d)$ é isomorfo à $Im(\theta) \subseteq I_X(d+1)/I_{\mathbb{T}_{m-1}}(d+1)$. Logo, $dim(I_X(d)/I_{\mathbb{T}_{m-1}}(d)) \leq dim(I_X(d+1)/I_{\mathbb{T}_{m-1}}(d+1))$, ou seja, $\overline{H}(d) \leq \overline{H}(d+1)$. Para todo $d \geq 0$, pelo teorema anterior,

$$H_{\mathbb{T}_{m-1}}(d) = H_X(d) + \overline{H}(d).$$

Assim, para $d \geq r_{\overline{H}}$, temos $\overline{H}(d) = h_{\overline{H}}(d)$ e para $d \geq r_X$, temos $H_X(d)) = h_X(d)$. Portanto, para $d \geq \max\{r_{\overline{H}}, r_X\}$, temos

$$H_{\mathbb{T}_{m-1}} = H_X(d) + \overline{H}(d) = h_X(d) + h_{\overline{H}}(d) = h_{\mathbb{T}_{m-1}},$$

isto é, $r_{\mathbb{T}_{m-1}} = \max\{r_{\overline{H}}, r_X\}$.

□

Assim, deste corolário, segue que $r_X \leq r_{\mathbb{T}_{m-1}}$. Mas em [3] (veja também em [2, Teorema 5.2.2]), foi provado que $r_{\mathbb{T}_{m-1}} = (m-1)(q-2)$. Portanto,

$$r_X \leq (m-1)(q-2) \tag{6.10}$$

Como foi observado na seção 1, se $d \geq (m-1)(q-2)$ então $H_X(d) = |X|$ e assim $C_X(d) = K^{|X|}$. Portanto, de agora em diante, iremos considerar $d < (m-1)(d-2)$.

6.2.3 Distância Mínima

Seja $Y := \mathbb{T}_{m-1} \backslash X$, digamos $Y = \{Q_1, \ldots, Q_{|Y|}\}$. Defina $C_Y(d)$ de modo análogo ao feito em (6.1), ou seja, $C_Y(d)$ é a imagem da transformação linear

$$\begin{aligned} \phi_d : S_d &\longrightarrow \mathbb{F}_q^{|Y|} \\ f &\longmapsto \left(\frac{f(Q_1)}{f_0(Q_1)}, \ldots, \frac{f(Q_{|Y|})}{f_0(Q_{|Y|})} \right), \end{aligned}$$

onde $f_0(X_1, \ldots, X_m) = X_1^d$. Denotemos por $\delta_X(d)$, $\delta_Y(d)$ e $\delta_{\mathbb{T}_{m-1}}(d)$ as distâncias mínimas de $C_X(d)$, $C_Y(d)$ e $C_{\mathbb{T}_{m-1}}(d)$, respectivamente. O seguinte teorema as relaciona.

Teorema 6.9. *Seja* $0 \leq d \leq (m-1)(q-2)$. *Então*

$$\delta_X(d) \leq \delta_{\mathbb{T}_{m-1}}(d) - \delta_Y(d) \tag{6.11}$$

Demonstração. Seja $X = \{P_1, \ldots, P_{|X|}\}$ e $Y = \{Q_1, \ldots, Q_{|Y|}\}$. Podemos escrever

$$\mathbb{T}_{m-1} = \{P_1, \ldots, P_{|X|}, Q_1, \ldots, Q_{|Y|}\}.$$

Considere

$$\Lambda = \left(\frac{f(P_1)}{X_1^d(P_1)}, \ldots, \frac{f(P_{|X|})}{X_1^d(P_{|X|})}, \frac{f(Q_1)}{X_1^d(Q_1)}, \ldots, \frac{f(Q_{|Y|})}{X_1^d(Q_{|Y|})} \right) \in C_{\mathbb{T}_{m-1}}(d),$$

com $\omega(\Lambda) = \delta_{\mathbb{T}_{m-1}}(d)$, onde $\omega(\Lambda)$ é o peso de Hamming da palavra código Λ, isto é, o número de entradas não nulas de Λ. Então

$$\Lambda_1 := \left(\frac{f(P_1)}{X_1^d(P_1)}, \ldots, \frac{f(P_{|X|})}{X_1^d(P_{|X|})} \right) \in C_X(d)$$

e

$$\Lambda_2 := \left(\frac{f(Q_1)}{X_1^d(Q_1)}, \ldots, \frac{f(Q_{|Y|})}{X_1^d(Q_{|Y|})} \right) \in C_Y(d)$$

Logo, $\delta_{\mathbb{T}_{m-1}}(d) = \omega(\Lambda) = \omega(\Lambda_1) + \omega(\Lambda_2) \geq \delta_X(d) + \delta_Y(d)$. Daí segue a desigualdade (6.11).

□

Como $X \subset \mathbb{T}_{m-1}(d)$, segue que $\delta_Y(d) \geq 1$. Logo, de (6.11), obtemos que $\delta_X(d) \leq \delta_{\mathbb{T}_{m-1}}(d) - 1$, para todo $0 \leq d < (m-1)(q-2)$. Mas $\delta_{\mathbb{T}_{m-1}}(d)$ foi computado em [7]. Assim, neste caso,

$$\delta_X(d) \leq (q-1)^{m-(k+2)}(q-1-l) - 1, \tag{6.12}$$

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

A partir de agora, consideremos o caso em que os monômios que parametrizam o conjunto tórico X possem o mesmo grau, isto é, $Z^{a_i} = Z_1^{a_{i1}} . \cdots . Z_n^{a_{in}}$ satisfaz $\sum_{j=1}^{n} a_{ij} = \alpha$, para todo $i = 1, \ldots, m$. Equivalentemente, vamos considerar os casos em que a soma dos elementos de cada coluna da matriz A, definida em (6.2), é uma constante. A seguinte aplicação nos ajudará a encontrar uma cota inferior para a distância mínima do código projetivo parametrizado correspondente. Seja

$$\begin{array}{rccl} \mu : & \mathbb{T}_{n-1} & \longrightarrow & X \\ & (t_1 : \cdots : t_n) & \longmapsto & (t_1^{a_{11}} . \cdots . t_n^{a_{1n}} : \cdots : t_1^{a_{m1}} . \cdots . t_n^{a_{mn}}). \end{array}$$

Vejamos que μ está bem definido. De fato,

$$(t_1 : \cdots : t_n) = (s_1 : \cdots : s_n) \iff (t_1 : \cdots : t_n) = \lambda(s_1 : \cdots : s_n), \text{ para algum } \lambda \in \mathbb{F}_q^*.$$

Assim,

$$\mu(t_1 : \cdots : t_n) = (t_1^{a_{11}} . \cdots . t_n^{a_{1n}} : \cdots : t_1^{a_{m1}} . \cdots . t_n^{a_{mn}})$$

$$
\begin{aligned}
&= ((\lambda s_1)^{a_{11}}.\cdots.(\lambda s_n)^{a_{1n}} : \cdots : (\lambda s_1)^{a_{m1}}.\cdots.(\lambda s_n)^{a_{mn}}) \\
&= (\lambda^{\alpha} s_1^{a_{11}}.\cdots.s_n^{a_{1n}} : \cdots : \lambda^{\alpha} s_1^{a_{m1}}.\cdots.s_n^{a_{mn}}) \\
&= \lambda^{\alpha}(s_1^{a_{11}}.\cdots.s_n^{a_{1n}} : \cdots : s_1^{a_{m1}}.\cdots.s_n^{a_{mn}}) \\
&= (s_1^{a_{11}}.\cdots.s_n^{a_{1n}} : \cdots : s_1^{a_{m1}}.\cdots.s_n^{a_{mn}}) = \mu(s_1 : \cdots : s_n).
\end{aligned}
$$

Além disso, μ é claramente um homomorfismo sobrejetor entre os grupos multiplicativos $\mathbb{T}_{n-1}$ e X. Definindo $N := \ker(\mu)$, temos

$$
\mathbb{T}_{n-1}/N \cong X \Rightarrow \frac{|\mathbb{T}_{n-1}|}{|N|} = |X| \Rightarrow |N| = \frac{|\mathbb{T}_{n-1}|}{|X|} = \frac{(q-1)^{n-1}}{|X|}.
$$

Ainda temos,

$$
\mathbb{T}_{n-1} = \bigcup_{i=1}^{|X|} N.T_i
$$

(união disjunto das correspondentes classes de equivalências) para certos $T_i \in \mathbb{T}_{n-1}$. Se considerarmos $P_i = \mu(T_i) \in X$, para todo $i = 1, \ldots, |X|$, e $N = \{R_1, \ldots, R_{|N|}\}$, então temos $X = \{P_1, \ldots, P_{|X|}\}$ e

$$
\begin{aligned}
\mathbb{T}_{n-1} = \bigcup_{i=1}^{|X|} N.T_i &= N.T_1 \cup N.T_2 \cup \cdots \cup N.T_{|X|} = \\
&= \{R_1T_1, \ldots, R_{|N|}T_1\} \cup \{R_1T_2, \ldots, R_{|N|}T_2\} \cup \cdots \cup \{R_1T_{|X|}, \ldots, R_{|N|}T_{|X|}\} = \\
&= \{R_1T_1, \ldots, R_{|N|}T_1, \ldots, R_1T_{|X|}, \ldots, R_{|N|}T_{|X|}\}.
\end{aligned}
$$

Como na introdução, seja $L = \mathbb{F}_q[Z_1, \ldots, Z_n]$. Definimos outra aplicação

$$
\begin{array}{rccl}
\tau : & S_d = \mathbb{F}_q[X_1, \ldots, X_m]_q & \longrightarrow & L_{\alpha d} \\
& f(X_1, \ldots, X_m) & \longmapsto & f(Z_1^{a_{11}}.\cdots.Z_n^{a_{1n}}, \ldots, Z_1^{a_{m1}}.\cdots.Z_n^{a_{mn}}),
\end{array}
$$

que claramente é uma transformação linear entre os espaços vetoriais S_d e $L_{\alpha d}$. Assim, podemos demonstrar o seguinte teorema que nos dá uma cota inferior para a distância mínima do correspondente código projetivo parametrizado.

Teorema 6.10. *Se a soma dos elementos de cada coluna de uma matriz A, definida em (6.2), é uma constante α. Então*

$$
\delta_X(d) \geq \left\lceil \frac{|X|.\delta_{\mathbb{T}_{n-1}}(\alpha d)}{(q-1)^{n-1}} \right\rceil, \tag{6.13}
$$

onde $\delta_{\mathbb{T}_{n-1}}(\alpha d)$ é a distância mínima do código projetivo parametrizado de ordem αd gerado pelo toro projetivo $\mathbb{T}_{n-1}$ e $\delta_X(d)$ é a distância mínima do código projetivo parametrizado associado ao conjunto tórico X, definido em (6.1). Também, $\lceil x \rceil$ é a função teto de x, isto é, $\lceil x \rceil = \min\{y \in \mathbb{Z} : y \geq x\}$.

Demonstração. Seja

$$\Gamma = \left(\frac{f(P_1)}{X_1^d(P_1)}, \ldots, \frac{f(P_{|X|})}{X_1^d(P_{|X|})} \right) \in C_X(d).$$

de tal maneira que $\omega(\Gamma) = \delta_X(d)$. Por outro lado, seja $f \in S_d$ e

$$\Omega = \left(\frac{\tau(f)(R_1T_1)}{Z_1^{\alpha d}(R_1T_1)}, \ldots, \frac{\tau(f)(R_{|N|}T_1)}{Z_1^{\alpha d}(R_{|N|}T_1)}, \ldots, \frac{\tau(f)(R_1T_{|X|})}{Z_1^{\alpha d}(R_1T_{|X|})}, \ldots, \frac{\tau(f)(R_{|N|}T_{|X|})}{Z_1^{\alpha d}(R_{|N|}T_{|X|})} \right).$$

Temos que $\Omega \in C_{\mathbb{T}_{n-1}}(\alpha d)$ e se $f(P_i) \neq 0$ para algum $P_i \in X$, então devido ao fato de que $\mu(R_jT_i) = \mu(R_j)\mu(T_i) = (1 : \cdots : 1)\mu(T_i) = P_i$, obtemos

$$\tau(f)(R_jT_i) = f(\mu(R_jT_i)) = f(P_i) \neq 0, \text{ para todo } j = 1, \ldots, |N|.$$

Assim, $\omega(\Omega) = |N|\omega(\Gamma) = |N|\delta_X(d)$ e, portanto

$$\delta_{\mathbb{T}_{n-1}}(\alpha d) \leq \omega(\Omega) = |N|\delta_X(d),$$

logo

$$\delta_X(d) \geq \frac{\delta_{\mathbb{T}_{n-1}}(\alpha d)}{|N|} = \frac{\delta_{\mathbb{T}_{n-1}}(\alpha d)}{(q-1)^{n-1}}|X|.$$

□

Se X é um conjunto tórico algébrico a partir de uma matriz de incidência de algum grafo, então $\alpha = 2$ e então podemos aplicar o teorema anterior. Ainda, se tivermos um grafo conexo, usando [3, Corolário 3.8] obtemos o seguinte resultado geral.

Corolário 6.11. *Seja X o conjunto tórico algébrico a partir da matriz de incidência de algum grafo conexo G. Então*

$$\delta_X(d) \geq \begin{cases} \left\lceil \dfrac{\delta_{\mathbb{T}_{m-1}}(2d)}{q-1} \right\rceil & \text{se} \quad G \text{ é bipartido} \\ \delta_{\mathbb{T}_{m-1}}(2d) & \text{se} \quad G \text{ não é bipartido.} \end{cases} \tag{6.14}$$

Para verificar esta desigualdade, basta utilizar (6.8) e (6.13).

CAPÍTULO 7

APLICAÇÃO DOS RESULTADOS APRESENTADOS

Nesta seção iremos apresentar três exemplos diferentes. Começaremos com um exemplo cujo código projetivo parametrizado é gerado a partir da matriz de incidência de um grafo não bipartido. Em seguida, definiremos clutters como casos particulares de hipergrafos e será dado um exemplo específico de códigos projetivos parametrizados por clutters uniformes. Por fim, computaremos os parâmetros de um código projetivo parametrizado associado a uma matriz que não representa um clutter, logo não representa um grafo. Nestes exemplos, usaremos δ'_d para representar a cota inferior para a distância mínima de $C_X(d)$ apresentada em (6.13) e b_d representará a cota de Singleton, isto é,

$$\left\lceil \frac{|X|.\delta_{\mathbb{T}_{n-1}}(\alpha d)}{(q-1)^{n-1}} \right\rceil = \delta'_d \leq \delta_X(d) \leq b_d = |X| - H_X(d) + 1.$$

7.1 Códigos projetivos parametrizados pela matriz de incidência de um grafo

Consideremos $\mathbb{F}_7$ um corpo finito com 7 elementos e o grafo dado no exemplo (5.4), cuja matriz de incidência é

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

O conjunto tórico gerado pela matriz A (ou associado ao grafo G da Fig. 1), é dado por

$$X = \{(t_1t_2 : t_2t_3 : t_1t_3 : t_1t_4 : t_4t_5 : t_1t_5) \in \mathbb{P}^5 : t_i \in \mathbb{F}_7^*\},$$

ou ainda,

$$X = \{(1 : t_1^{-1}t_3 : t_2^{-1}t_3 : t_2^{-1}t_4 : t_1^{-1}t_2^{-1}t_4t_5 : t_2^{-1}t_5) \in \mathbb{P}^5 : t_i \in \mathbb{F}_7^*\}.$$

Neste caso, teremos os subconjuntos Y_1, Y_2, Y_3, Y_4 e Y_5, e tais que, para cada $i = 1, 2, 3, 4, 5$,

$$|Y_i| = \frac{6}{(6, b_{2i}, b_{3i}, b_{4i}, b_{5i}, b_{6i})} = 6,$$

pois b_{ji} é igual a 1 ou -1 para algum $j \in \{2, \ldots, 6\}$. Vamos agora identificar o conjunto M do Teorema (6.4), que é dado pelas 5-uplas $(i_1, i_2, i_3, i_4, i_5)$, tais que $1 \leq i_j \leq |Y_j| = 6$, para todo $j = 1, \ldots, 5$, e satisfazendo

$$\begin{aligned}
&i_1.(-1) + i_2.0 + i_3.1 + i_4.0 + i_5.0 \equiv 0 \mod 6\\
&i_1.0 + i_2.(-1) + i_3.1 + i_4.0 + i_5.0 \equiv 0 \mod 6\\
&i_1.0 + i_2.(-1) + i_3.0 + i_4.1 + i_5.0 \equiv 0 \mod 6\\
&i_1(-1) + i_2.(-1) + i_3.0 + i_4.1 + i_5.1 \equiv 0 \mod 6\\
&i_1.0 + i_2.(-1) + i_3.0 + i_4.0 + i_5.1 \equiv 0 \mod 6.
\end{aligned} \tag{7.1}$$

Portanto, destas congruências, concluímos que $i_1 = i_2 = i_3 = i_4 = i_5$. Logo

$$M = \{(i, i, i, i, i) : i = 1, \ldots, 6\}.$$

Assim, usando o Teorema (6.4), temos

$$|X| = \frac{1}{|M|}\prod_{i=1}^{5}|Y_i| = \frac{1}{6}6^5 = 1296$$

Notemos ainda que, pelo Corolário (6.11), $\delta'_d = \delta_{\mathbb{T}_4}(2d)$. Usando Macaulay2, computamos os seguintes valores.

d	1	2	3	4	5	6	7	8	9	10
$H_X(d)$	6	21	55	120	231	401	627	885	1130	1296
$H_{\mathbb{T}_5}(d)$	6	21	56	126	252	457	762	1182	1722	2373
$\overline{H}(d)$	0	0	1	6	21	56	135	297	592	1077
δ'_d	864	432	180	108	36	24	12	5	3	1
b_d	1291	1276	1242	1177	1066	896	670	412	167	1

Logo, a partir desta tabela, podemos concluir que $r_X = 10$.

7.2 Código projetivo parametrizado pela matriz de incidência de um clutter

Definição 7.1. *Um clutter $\mathcal{C}$ é uma familia E de subconjuntos de um conjunto base finito $Z = \{Z_1, \ldots, Z_n\}$ tal que, se $A, B \in E$,$A \neq B$, então $A \not\subset B$. O conjunto base Z é chamado conjunto de vértices e E é chamado conjunto de arestas de $\mathcal{C}$ e são denotados por $V_{\mathcal{C}}$ e $E_{\mathcal{C}}$, respectivamente.*

Um exemplo de clutter é um grafo com os vértices e arestas definido da maneira usual para grafos.

Definição 7.2. *Seja $\mathcal{C}$ um clutter com o conjunto de vértices $V_{\mathcal{C}} = \{Z_1, \ldots, Z_n\}$ e seja A uma aresta de E. O vetor característico de A é o vetor $a = \sum_{Z_i \in A} e_i$, onde e_i é o i-ésimo vetor unitário de $\mathbb{R}^n$.*

Escrevemos $\{a_1, \ldots, a_m\}$ para o conjunto de todos os vetores característicos de arestas de $\mathcal{C}$. Neste caso, para cada $i \in \{1, \ldots, m\}$, escrevendo o vetor a_i como $a_i = \sum_{j=1}^{n} a_{ij} e_j$, com $a_{ij} \in \{0, 1\}$, para todo $j = 1, \ldots, n$ a matriz A obtida dispondo estes vetores em colunas é conhecida como matriz de incidência do clutter $\mathcal{C}$, isto é,

$$A = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}.$$

O conjunto X definido

$$X = \{(t_1^{a_{11}} \cdot \cdots \cdot t_n^{a_{1n}} : \cdots : t_1^{a_{m1}} \cdot \cdots \cdot t_n^{a_{mn}}) \in \mathbb{P}^{m-1} | t_i \in \mathbb{F}_q^*\}$$

é o conjunto tórico associado ao clutter $\mathcal{C}$. O clutter $\mathcal{C}$ é dito uniforme se a soma dos elementos de cada coluna de sua matriz de incidência é uma constante.

Percebemos que em qualquer clutter, como em grafos, $|X| = \dfrac{(q-1)^n}{|M|}$, já que $|Y_i| = q - 1$, para todo $n = 2, \ldots, n$.

Consideremos $\mathbb{F}_9$ um corpo finito com 9 elementos e X o conjunto tórico associado ao clutter uniforme ($\alpha = 3$) cuja matriz de incidência é a matriz 6×6 dada por

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \tag{7.2}$$

O conjunto tórico X associado a (7.2) é

$$X = \{(t_1t_2t_3 : t_2t_3t_4 : t_3t_4t_5 : t_4t_5t_6 : t_1t_5t_6 : t_1t_2t_6) \in \mathbb{P}^5 : t_i \in \mathbb{F}_9^*\},$$

ou ainda,

$$X = \{(1 : t_1^{-1}t_4 : t_1^{-1}t_2^{-1}t_4t_5 : t_1^{-1}t_2^{-1}t_3^{-1}t_4t_5t_6 : t_2^{-1}t_3^{-1}t_5t_6 : t_3^{-1}t_6) \in \mathbb{P}^5 : t_i \in \mathbb{F}_9^*\}.$$

Assim, os conjuntos Y_1, Y_2, Y_3, Y_4 e Y_5, são tais que para cada $i = 1, \ldots, 5$, temos

$$|Y_i| = \frac{8}{(8, b_{2i}, b_{3i}, b_{4i}, b_{5i}, b_{6i})} = 8,$$

pois $b_{ji} = 0, 1$, ou -1, para todo $j = 2, \ldots, 6$. Como fizemos no exemplo anterior, vamos identificar $|M|$, onde M é o conjunto das 5-uplas $(i_1, i_2, i_3, i_4, i_5)$, tais que $1 \leq i_j \leq |Y_j| = 8$, para todo $j = 1, \ldots, 5$, e satisfazendo

$$\begin{aligned}
i_1.(-1) + i_2.(-1) + i_3.(-1) + i_4.0 + i_5.0 &\equiv 0 \mod 8\\
i_1.0 + i_2.(-1) + i_3.(-1) + i_4.(-1) + i_5.0 &\equiv 0 \mod 8\\
i_1.0 + i_2.0 + i_3.(-1) + i_4.(-1) + i_5.(-1) &\equiv 0 \mod 8\\
i_1.1 + i_2.1 + i_3.1 + i_4.0 + i_5.0 &\equiv 0 \mod 8\\
i_1.0 + i_2.1 + i_3.1 + i_4.1 + i_5.0 &\equiv 0 \mod 8.\\
i_1.0 + i_2.0 + i_3.1 + i_4.1 + i_5.1 &\equiv 0 \mod 8.
\end{aligned} \tag{7.3}$$

Portanto, destas congruências, concluímos que $i_1 = i_4$ e $i_2 = i_5$, ou seja, $|M| = 8^3 = 512$. Logo, pelo Teorema (6.4), temos

$$|X| = \frac{1}{|M|}\prod_{i=1}^{6}|Y_i| = 8^3 = 512$$

Assim, da mesma forma que o exemplo anterior, e usando Macaulay2, obtemos os seguintes valores.

d	1	2	3	4	5	6	7	8	9	10	11	12
$H_X(d)$	6	19	44	85	146	231	344	442	492	510	512	512
$H_{\mathbb{T}_5}(d)$	6	21	56	126	252	462	792	1282	1972	2898	4088	5558
$\overline{H}(d)$	0	2	12	41	106	231	448	840	1480	2388	3576	5046
δ'_d	320	128	48	24	7	4	1	1	1	1	1	1
b_d	507	494	469	428	367	282	169	71	21	3	1	1

Logo, a partir desta tabela, podemos concluir que $r_X = 11$.

7.3 Código projetivo parametrizado por uma matriz que não representa um clutter

Neste exemplo, analisaremos os parâmetros de códigos projetivos parametrizados a partir de uma matriz que não representa um clutter.

Seja $\mathbb{F}_{11}$ um corpo finito com 11 elementos e X o conjunto tórico associado a matriz 3×4 dada por

$$A = \begin{pmatrix} 3 & 1 & 0 & 1 \\ 0 & 4 & 2 & 2 \\ 3 & 1 & 4 & 3 \end{pmatrix}.$$

Neste caso $\alpha = 6$. Assim,

$$X = \{(t_1^3 t_3^3 : t_1 t_2^4 t_3 : t_2^2 t_3^4 : t_1 t_2^2 t_3^3) \in \mathbb{P}^3 : t_i \in \mathbb{F}_{11}^*\}.$$

ou ainda,

$$X = \{(1 : t_1^{-2} t_2^4 t_3^{-2} : t_1^{-3} t_2^2 t_3 : t_1^{-1} t_2^2) \in \mathbb{P}^3 : t_i \in \mathbb{F}_{11}^*\}$$

Logo, temos que

$$\begin{aligned} Y_1 = \{(1 : t_1^{-2} : t_1^{-3} : t_1^{-2}) \in \mathbb{P}^3 : t_1 \in \mathbb{F}_q^*\} \Rightarrow |Y_1| = \frac{10}{(10, -2, -3, -2)} = 10, \\ Y_2 = \{(1 : t_2^4 : t_2^2 : t_2^2) \in \mathbb{P}^3 : t_2 \in \mathbb{F}_q^*\} \Rightarrow |Y_2| = \frac{10}{(10, 4, 2, 2)} = 5, \\ Y_3 = \{(1 : t_3^{-2} : t_1 : 1) \in \mathbb{P}^3 : t_3 \in \mathbb{F}_q^*\} \Rightarrow |Y_3| = \frac{10}{(10, -2, 1, 0)} = 10. \end{aligned}$$

O correspondente conjunto M de ternos (i_1, i_2, i_3), tais que $1 \leq i_1, i_3 \leq 10$ e $1 \leq i_2 \leq 5$, e satisfazendo

$$\begin{aligned} i_1.(-2) + i_2.4 + i_3.(-2) &\equiv 0 \mod 10 \\ i_1.(-3) + i_2.2 + i_3.1 &\equiv 0 \mod 10 \\ i_1.(-2) + i_2.2 + i_3.0 &\equiv 0 \mod 10. \end{aligned} \tag{7.4}$$

Destas congruências, concluímos que $i_1 \equiv i_2 \mod 5$, $i_3 \equiv i_2 \mod 5$ e $i_1 \equiv i_3 \mod 10$. Daí, segue que

$$M = \{(1,1,1), (2,2,2), (3,3,3), (4,4,4), (5,5,5), (6,1,6), (7,2,7), (8,3,8), (9,4,9), (10,5,10)\},$$

ou seja, M tem 10 elementos e, pelo Teorema (6.4), segue que

$$|X| = \frac{1}{|M|}\prod_{i=1}^{3}|Y_i| = 50.$$

Assim, analogamente aos exemplos anteriores, obtemos os seguintes valores

d	1	2	3	4	5	6
$H_X(d)$	4	10	20	32	44	50
$H_{\mathbb{T}_3}(d)$	4	10	20	35	56	84
$\overline{H}(d)$	0	0	0	3	12	34
δ'_d	20	3	1	1	1	1
b_d	47	41	31	19	7	1

Podemos concluir que $r_X = 6$.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Cox, D.; Little, J. e O'Shea, D. *Ideals, Varieties, and Algorithms*, Springer-Verlag, 2010 (3a. ed.).

[2] Cunha, G.D. - A distância mínima de códigos parametrizados no toro projetivo, tese de Mestrado, UFU 2014.

[3] González-Sarabia, M., Rentería, C. e Hernández de la Torre, M., *Minimum distance and second generalized Hamming weight of two particular linear codes*, Congr. Numer. **161** (2003) 105-116.

[4] González-Sarabia, M., Rentería, C. e Sarminento, E., *Projective parameterized linear codes*, Analele Stiintifice ale Universitatii Ovidius Constanta, **223** (2015), fascicola 3.

[5] Hefez, A. e Vilela, M. L. *Códigos Corretores de Erros*. IMPA, 2002.

[6] Rentería, C., Simis, A. e Villarreal, R. H., *Algebraic methods for parametrized codes and invariants of vanishing ideals over finite fields*, Finite Fields Appl. **17** (2011) 81-104.

[7] Sarminento, E., Vaz Pinto, M. e Villarreal, R.H. *The minimum distance of parametrized codes on projective tori*, Appl. Algebra Engrg. Comm. Comput. **22** (4) (2011) 249-264.