THIAGO RODRIGUES DA SILVA

Bases de Gröbner e a Geometria Algébrica na Teoria de Códigos Corretores de Erros

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2015

THIAGO RODRIGUES DA SILVA

Bases de Gröbner e a Geometria Algébrica na Teoria de Códigos Corretores de Erros

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

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Algébrica e Diferencial.

Orientador: Prof. Dr. Guilherme Chaud Tizziotti.

UBERLÂNDIA - MG
2015

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

S586b 2015

Silva, Thiago Rodrigues da, 1985-

Bases de Gröbner e a geometria algébrica na teoria de códigos corretores de erros / Thiago Rodrigues da Silva. - 2015.

56 f. : il.

Orientador: Guilherme Chaud Tizziotti.

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

Inclui bibliografia.

1. Matemática - Teses. 2. Curvas algébricas - Teses. 3. Códigos de Goppa - Teses. 4. Bases de Gröbner - Teses. I. Tizziotti, Guilherme Chaud. 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: Thiago Rodrigues da Silva.

NÚMERO DE MATRÍCULA: 11312MAT011.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica e Diferencial.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Bases de Gröbner e a Geometria Algébrica na Teoria de Códigos Corretores de Erros.

ORIENTADOR: Prof. Dr. Guilherme Chaud Tizziotti.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 04 de março de 2015, às 10h00min, pela seguinte Banca Examinadora:

NOME	ASSINATURA
Prof. Dr. Guilherme Chaud Tizziotti UFU - Universidade Federal de Uberlândia	
Prof. Dr. Alonso Sepúlveda Castellanos UFU - Universidade Federal de Uberlândia	
Prof. Dr. Fernando Eduardo Torres Orihuela UNICAMP - Universidade Estadual de Campinas	

Uberlândia-MG, 04 de março de 2015.

Dedicatória

Dedico esse trabalho primeiramente a Deus, pois só Ele pode me dar a força que eu precisava para chegar até aqui. Dedico a minha mãe Virgínia, minha irmã Aline, meu sobrinho Alex Jr. e a meu cunhado Alex pelo amor, carinho, incentivo, apoio e paciência durante meus estudos. E dedico também a todos os meus familiares e amigos que me apoiaram e sempre acreditaram em mim, em especial Fernanda, Tânia, Déborah, Renata, Rogério, Pedro Paulo, Thiago Macedo e Carlos. Sem vocês, jamais conseguiria realizar esse sonho...

Agradecimentos

Agradeço primeiramente a Deus, por me permitir realizar este sonho. Agradeço ao meu orientador e amigo Prof. Guilherme Chaud Tizziotti pelos ensinamentos e pela paciência nos momentos mais difíceis. Agradeço aos meus grandes mestres Dulce Mary de Almeida, Edson Agustini, Luiz Alberto Duran Salomão, Ednaldo Carvalho Guimarães, Fabiana Fiorezi de Marco Matos, Maria Teresa Menezes Freitas, Douglas Marin e Ana Carla Piantella pelos ensinamentos e por sempre me incentivarem e acreditarem na minha capacidade. Agradeço também aos meus amigos do mestrado pelo companheirismo, e aos professores Alonso Sepúlveda Catellanos e Fernando Eduardo Torres Orihuela por terem aceitado o convite para participarem da minha banca.

Obrigado a todos! Por vocês tenho total admiração e respeito.

SILVA, T. R. *Bases de Gröbner e a Geometria Algébrica na Teoria de Códigos Corretores de Erros*. 2015. 48 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho estudamos como podemos relacionar códigos a diferentes estruturas matemáticas e como podemos usar tais ferramentas para obtermos diferentes sistemáticas de codificação e relações entre seus parâmetros.

Palavras-chave: Códigos lineares, curvas algébricas, grupo de automorfismos, códigos de Goppa geométricos, bases de Gröbner.

SILVA, T. R. *Gröbner Basis and The Algebraic Geometry at The Theory of Codes of Errors Correctors*. 2015. 48 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

We study how we can relate codes to different mathematical structures and how we can use such tools to obtain different systematic coding and relations between its parameters.

Keywords: Linear codes, algebraic curves, automorphism group, AG codes, Gröbner basis.

Sumário

Introdução

Com vasta aplicação na área da tecnologia, os códigos corretores de erros são usados para enviar uma mensagem pelo celular, ouvir uma música ou até digitar um texto no computador. Todavia, manter as informações enviadas e recebidas entre os usuários na forma mais inalterada possível nem sempre é fácil quando se tem uma interferência.

Um idioma é o exemplo mais familiar de um código. Consideremos o conjunto $\mathcal{A}$, chamado "alfabeto", composto pelas 26 letras da língua portuguesa, as vogais acentuadas, o c cedilha (ç) e o espaço em branco que também será considerado como uma letra (que serão colocados sempre à direita de cada código, omitindo-os na escrita, para não haver repetições desnecessárias). Assim, todas as palavras da língua portuguesa são elementos de um subconjunto $\mathcal{P}$ de $\mathcal{A}^{47}$, onde 47 é o comprimento da maior palavra da língua portuguesa, supostamente a palavra *pneumoultramicroscopicossilicovulcanoconióticos*.

Tal código não é muito eficaz quando se deseja trocar informações via celular, por exemplo. Observamos que se uma palavra é digitada erroneamente pela sequência de letras "CATHORRO", nota-se que tal sequência não pertence a $\mathcal{P}$ e logo detectamos um erro, o qual é fácil corrigir, pois em $\mathcal{P}$ a palavra mais próxima de tal sequência é "CACHORRO". Entretanto, se a palavra "PATO"é digitada como "GATO", ou "MATO", não detectaríamos um erro, uma vez que todas essas palavras pertencem ao código.

Nosso objetivo neste trabalho é implementar diferentes estruturas matemáticas aos códigos, afim de obter novas relações entre seus parâmetros e construir novas sistemáticas de codificação.

No primeiro capítulo, definimos o que é um código e quais seus parâmetros. Começamos a enxergá-lo como um conjunto qualquer, depois como um espaço vetorial. Na sequência, nos restringimos a códigos cíclicos para associá-los a um ideal principal de um anel de polinômios e veremos como esta associação pode nos ajudar na construção de uma sistemática de codificação e na obtenção de seus parâmetros.

Já no segundo capítulo, apresentamos o conceito de módulos sobre aneis de polinômios, bem como associá-los a um código linear, afim de obtermos uma sistemática de codificação que usa a teoria de bases de Gröbner.

No terceiro capítulo, veremos como construir códigos sobre curvas algébricas e, usando um certo grupo de automorfismos, como dar uma estrutura de módulo para tais códigos.

Por fim, no quarto capítulo, apresentamos uma sistemática de codificação para certos códigos de Goppa geométricos, bem como exemplos que ilustram tal codificação.

Thiago Rodrigues da Silva
Uberlândia-MG, 04 de março de 2015.

Capítulo 1

Códigos Corretores de Erros

1.1 Introdução

Sejam $\mathcal{A}$ um conjunto finito qualquer e, para um inteiro $n \geq 1$, $\mathcal{A}^n = \{(a_1, \ldots, a_n) : a_i \in \mathcal{A}$, para cada $i = \{1, \ldots, n\}\}$. Para quaisquer u e v em $\mathcal{A}^n$, definimos a ***distância de Hamming*** entre u e v por

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

Em que, para um conjunto M qualquer, $|M|$ denota a cardinalidade de M. Não é difícil verificar que a distância de Hamming é uma métrica.

Um ***código*** $\mathcal{C}$ nada mais é do que um subconjunto não vazio de $\mathcal{A}^n$ e basicamente a teoria de códigos é aplicada na seguinte situação. Suponha que um emissor queira transmitir uma mensagem m, para um certo receptor, através de um canal (linha telefônica, *internet* ou um CD, por exemplo). Durante este processo de transmissão, m pode sofrer alterações e chegar modificada em seu destino. Estas alterações são chamadas de ***erros***. Aprofundando um pouco mais neste processo, temos o seguinte: o emissor codifica a mensagem m, utilizando um código $\mathcal{C}$, e a envia através de um canal, e o receptor decodifica a mensagem que chega até ele com a finalidade de obter a mensagem m. O esquema a seguir ilustra este processo.

$$\boxed{\textit{Emissor}} \ \rightarrow \ \boxed{\textit{Codificação}} \ \rightarrow \ \boxed{\textit{Canal}} \ \rightarrow \ \boxed{\textit{Decodificação}} \ \rightarrow \ \boxed{\textit{Receptor}}$$

Mais detalhes sobre este processo podem ser encontrados em [6] e [9].

Podemos fazer algumas perguntas sobre este processo. Por exemplo, qual código utilizar? Como fazer a codificação e a decodificação? É possível detectar e corrigir os erros? Vamos responder estas e outras perguntas a partir de agora.

O conjunto $\mathcal{A}$ é chamado ***alfabeto***, os elementos de um código $\mathcal{C} \subseteq \mathcal{A}^n$ são chamados ***palavras-código***, ou simplesmente ***palavras***, o número n é o ***comprimento*** do código $\mathcal{C}$ e a ***distância mínima*** de $\mathcal{C}$ é o inteiro não-negativo

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

Para $a \ \in \mathcal{A}^n$ e $t > 0$, os conjuntos

$$D(a, t) = \{u \ \in \ \mathcal{A}^n : \ d(u, a) \leqslant t\} \text{ e } S(a, t) = \{u \ \in \ \mathcal{A}^n : \ d(u, a) = t\},$$

são chamados, respectivamente, ***disco*** e ***esfera de Hamming*** de centro a e raio t.

Para um número real x, denotaremos o maior inteiro menor do que ou igual a x por $[x]$.

Lema 1.1.1 *Seja $\mathcal{C}$ um código com distância mínima d e seja $\widetilde{d} = \left[\frac{d-1}{2}\right]$. Se a e a' são palavras distintas de $\mathcal{C}$, então*

$$D(a, \widetilde{d}) \bigcap D(a', \widetilde{d}) = \emptyset.$$

Demonstração: De fato, suponhamos que um elemento u pertença a $D(a, \widetilde{d}) \bigcap D(a', \widetilde{d})$. Logo, $d(u, a) \leqslant \widetilde{d}$ e $d(u, a') \leqslant \widetilde{d}$ pela desigualdade triangular, o que implica $d(a, a') \leqslant d(a, u) + d(u, a')$. Por simetria e pela definição de maior inteiro, segue que $d(a, a') \leqslant 2\widetilde{d} \leqslant d - 1$, o que seria um absurdo, uma vez que $\mathcal{C}$ tem distância mínima d por hipótese.

■

O teorema a seguir ilustra a grande importância da distância mínima de um código.

Teorema 1.1.2 *Seja $\mathcal{C}$ um código e d sua distância mínima. Então $\mathcal{C}$ pode detectar no máximo $d - 1$ erros e pode corrigir no máximo $\widetilde{d} = \left[\dfrac{d-1}{2}\right]$ erros.*

Demonstração: Suponhamos que uma palavra u de $\mathcal{C}$ seja transmitida com t erros, $t \leqslant \widetilde{d}$, sendo recebida a palavra r. Segue então, que $d(u, r) = t \leqslant \widetilde{d}$. Agora, pelo Lema 1.1.1,

$$r \in D(u, \widetilde{d}) \;\Rightarrow\; r \notin D(a, \widetilde{d}),\; a \in \mathcal{C} \text{ e } a \neq u \;\Rightarrow\; d(a, r) > \widetilde{d}.$$

Logo, a palavra u é única a partir de r.

Por outro lado, dada uma palavra do código, podemos introduzir no máximo $d - 1$ erros de modo a não conseguirmos uma outra palavra do código. Logo, é possível detectarmos o erro e o resultado segue.

■

Observe que o teorema anterior nos diz que quanto maior for a distância mínima de um código, maior a sua capacidade de detecção e correção de erros.

Voltando ao processo de transmissão de uma mensagem. Se o receptor recebe uma palavra r, acontece uma das seguintes situações:

(i) $r \in D(a, \widetilde{d})$, para algum $a \in \mathcal{C}$.

(ii) $r \notin D(a, \widetilde{d})$, para todo $a \in \mathcal{C}$.

No primeiro caso, pelo Teorema 1.1.2, r é única e neste caso substituimos r por a. No segundo caso, não é possível decodificar r com precisão.

É importante observarmos que não há uma certeza absoluta de que "a" foi a palavra enviada pelo transmissor, uma vez que mais de $\widetilde{d}$ erros poderiam ser cometidos na transmissão.

1.2 Códigos Lineares

A partir de agora, o alfabeto $\mathcal{A}$ será um corpo finito com q elementos, denotado por $\mathbb{F}_q$. Para cada inteiro positivo n, $\mathbb{F}_q^n$ é um $\mathbb{F}_q$-espaço vetorial de dimensão n.

Definição 1.2.1 *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código. Dizemos que $\mathcal{C}$ é um **código linear** se for um subespaço vetorial de $\mathbb{F}_q^n$.*

A seguir, veremos como esta estrutura de espaço vetorial nos permite criar uma sistemática de codificação, além de outros fatos importantes relacionados aos chamados parâmetros de um código.

Sejam $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear e k a dimensão de $\mathcal{C}$ como $\mathbb{F}_q$-espaço vetorial. O comprimento n, a distância mínima d e a dimensão k formam um conjunto importante de parâmetros para $\mathcal{C}$. Um código com tais parâmetros é chamado de $[n, k, d]$-código ou código $[n, k, d]$. Vejamos por que eles são importantes. Seja $\mathcal{B} = \{v_1, v_2, \ldots, v_k\}$ uma de base de $\mathcal{C}$. Assim, se $v \in \mathcal{C}$, então existem (únicos) $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{F}_q$ tais que

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k.$$

Observe que $|\mathcal{C}| = q^k$, ou seja, o número de palavras em $\mathcal{C}$ é q^k. Assim, quanto maior for a dimensão k, maior será o número de palavras de $\mathcal{C}$. Além disso, já sabemos que quanto maior for a distância mínima d, maior será a capacidade de detectar e corrigir erros. Assim, quanto maiores forem d e k melhor. Porém, temos a seguinte relação entre eles:

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

Esta relação é chamada ***cota de Singleton*** e sua veracidade será mostrada mais adiante.

Outro parâmetro que envolve a distância entre palavras é o peso de um código. Para cada $v \in \mathbb{F}_q^n$, definimos o *peso* de v como sendo o inteiro $\omega(v) := |\{i : \ v_i \neq 0, \ 1 \leqslant i \leqslant n\}|$.

Note que $\omega(v) = |\{i : \ v_i \neq 0, \ 1 \leqslant i \leqslant n\}| = |\{i : \ v_i \neq 0_i, \ 1 \leqslant i \leqslant n\}| = d(v, 0)$.

Definição 1.2.2 *Definimos o **peso** de um código linear $\mathcal{C}$ como sendo o inteiro*

$$\omega(\mathcal{C}) := min\{\omega(v) : \ v \in \mathcal{C} \setminus \{0\}\}.$$

Proposição 1.2.3 *Se $\mathcal{C} \subseteq \mathbb{F}_q^n$ é um código linear com distância mínima d, então*

(i) $d(u, v) = \omega(u - v), \ \forall \ u, v \in \mathbb{F}_q{}^n$.

(ii) $d = \omega(\mathcal{C})$.

Demonstração: *(i)* De fato, para todos $u, v \in \mathbb{F}_q^n$, temos

$$\begin{aligned} \omega(u-v) &= |\{i:\ u_i - v_i \neq 0,\ 1 \leqslant i \leqslant n\}| \\ &= |\{i:\ u_i \neq v_i,\ 1 \leqslant i \leqslant n\}| \\ &= d(u,v). \end{aligned}$$

E o resultado segue.
Já em *(ii)*, para todos $u, v \in \mathcal{C}$, com $u \neq v$, segue que $z = u - v \in \mathcal{C} \setminus \{0\}$. Logo,

$$\begin{aligned} d &= \min\{i:\ u_i \neq v_i,\ 1 \leqslant i \leqslant n\} \\ &= \min\{i:\ u_i - v_i \neq 0,\ 1 \leqslant i \leqslant n\} \\ &= \min\{i:\ z_i \neq 0,\ 1 \leqslant i \leqslant n\} \\ &= \min\{\omega(z):\ z \in \mathcal{C} \setminus \{0\}\} \\ &= \omega(\mathcal{C}). \end{aligned}$$

■

Observação 1.2.4 *Observe que, agora, podemos encontrar d a partir $q^k - 1$ cálculos de distância, em vez de $\binom{q^k}{2}$ que é o número de cálculos que devemos fazer comparando palavra por palavra de um código linear. Na prática, para grandes valores de q^k, esse método para o cálculo de d é inviável por respresentar um custo computacional muito elevado. Por isso, temos que desenvolver outros métodos para determinar ou ao menos estimar a distância mínima de um código.*

Vejamos como encontrar um método de codificação para códigos lineares. Para cada $i = 1, \ldots, k$, tomemos $v_i = (v_{i1}, \ldots, v_{in}) \in \mathcal{B}$ e consideremos a seguinte matriz.

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

Chamaremos tal matriz de ***matriz geradora*** *do código $\mathcal{C}$ associada à base $\mathcal{B}$.*

• **Sistemática de codificação para códigos lineares:** Considere a transformação linear dada por

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ & x & \longmapsto & x \cdot G \end{array}$$

Logo, se $x \in \mathbb{F}_q^k$, então

$$T(\mathrm{x}) = x \cdot G = x_1 v_1 + \cdots + x_k v_k \in \mathcal{C}.$$

A partir de T, podemos associar, de maneira única, cada elemento de $\mathbb{F}_q^k$ a um elemento de $\mathcal{C}$, ou seja, podemos codificar qualquer elemento $x \in \mathbb{F}_q^k$. Observe que, neste processo de codificar um elemento de $\mathbb{F}_q^k$ temos que fazer $k(n-k)$ multiplicações e $(k-1)(n-k)$ somas.

Note que G não é determinada de forma única, uma vez que a base de $\mathcal{C}$ não é única. Além disso, se G e G' são duas matrizes que geram o mesmo código, então uma é obtida da outra por permutação de linhas, multiplicação de uma linha por um escalar não nulo e adição de um múltiplo escalar de uma linha à outra, ou seja, sequência de operações nas quais também uma base é obtida a partir de outra.

Para construir um código linear a partir de uma matriz geradora G, é necessário que suas linhas sejam linearmente independentes e que o código seja definido como imagem da transformação linear T definida anteriormente.

Logo, se $u \in \mathcal{C} = Im(T)$, então existe $v \in \mathbb{F}_q^k$ tal que

$$v \cdot G = u$$

Entretanto, nem sempre consguimos resolver um sistema como esse, pois G pode ser mais complexa. Entretanto, podemos escrever G de tal forma que o sistema acima seja mais fácil de ser resolvido. A definição a seguir, nos mostra como é esta G.

Definição 1.2.5 *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código com matriz geradora G. Dizemos que G está na* ***forma padrão*** *se*

$$G = [Id_k \mid A]_{k \times n} \quad ,$$

onde Id_k é a matriz identidade de ordem k e A, uma matriz de ordem $k \times (n-k)$.

Toda matriz G, geradora de um código $\mathcal{C}$ pode ser posta na foram padrão, basta efetuar sequências de operações como permutar colunas e/ou multiplicar uma coluna por um escalar não nulo. Todavia, efetuando tais sequências de operações em G, estaremos fazendo o mesmo em todas as palavras de $\mathcal{C}$. Logo, efetuar sequências de operações em G, matriz geradora de $\mathcal{C}$, é obter uma matriz G', na forma padrão, que será a geradora de um código $\mathcal{C}'$, equivalente a $\mathcal{C}$. Dizemos que $F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_{\shortparallel}^{\ltimes}$ é uma ***isometria*** se F preserva distâncias de Hamming, isto é, dados $u, v \in \mathbb{F}_q^n$, temos $d(F(u), F(v)) = d(u, v)$. Assim, dizemos que dois códigos $\mathcal{C}$ e $\mathcal{C}'$, ambos contidos em $\mathbb{F}_q^n$, são equivalentes se existe uma isometria F de $\mathbb{F}_q^n$ tal que $F(\mathcal{C}) = \mathcal{C}'$. Desta definição segue que códigos equivalentes possuem os mesmos parâmetros.

Teorema 1.2.6 *Todo código $\mathcal{C}$ possui um código equivalente $\mathcal{C}'$ gerado por uma matriz na forma padrão.*

Demonstração: Seja G a matriz geradora de um código $\mathcal{C}$ na forma

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ \vdots & \vdots & & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}.$$

O resultado segue apenas colocando G na forma padrão.

Notemos que as linhas de G são linearmente independentes. Suponhamos que $g_{11} \neq 0$. Multiplicando a primeira linha pelo inverso de g_{11} teremos o primeiro elemento da matriz igual a 1. Daí, multiplicando por $-g_{i1}$ a primeira linha e somando com a i-ésima, para todo $i = 2, 3, \ldots, k$, teremos a matriz

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

Certamente, pelo menos um elemento da segunda linha da matriz acima é não nulo. Assim, multiplicando a segunda linha pelo inverso desse elemento e permutando a coluna na qual ele está com a segunda, teremos uma nova matriz da forma

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

Multiplicando agora a segunda linha dessa matriz por $-c_{j2}$ e somando com a j-ésima linha, para todo $j = 1, 3, 4, \ldots, k$, teremos a matriz

$$\begin{bmatrix} 1 & 0 & d_{13} & \cdots & d_{1n} \\ 0 & 1 & d_{23} & \cdots & d_{2n} \\ 0 & 0 & d_{33} & \cdots & d_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & d_{k3} & \cdots & d_{kn} \end{bmatrix}.$$

Repetiremos essa sequência de operações à matriz acima até encontramos a seguinte matriz na forma padrão

$$\begin{aligned} G' &= \begin{bmatrix} 1 & 0 & \cdots & 0 & a_{1(k+1)} & \cdots & a_{1n} \\ 0 & 1 & \cdots & 0 & a_{2(k+1)} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & a_{k(k+1)} & \cdots & b_{kn} \end{bmatrix} \\ &= [Id_k \mid A_{k\times(n-k)}]. \end{aligned}$$

E o resultado segue.

■

Definição 1.2.7 *Seja $\mathcal{C} \in \mathbb{F}_q^n$ um código linear. Definimos o* ***código dual*** *de $\mathcal{C}$ por*

$\mathcal{C}^{\perp} = \{v \in \mathbb{F}_q^n : < u, v >= 0, \ \forall\ u \in \mathcal{C}\}$. *Em que $< u, v >$ é o produto interno entre u e v.*

Lema 1.2.8 *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear com matriz geradora G. Então,*

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

(ii) $x \in \mathcal{C}^\perp \iff G \cdot x^t = 0$.

Demonstração: *(i)* De fato, $0 \in \mathcal{C}^\perp$, pois $0 \in \mathcal{C}$ e $< u, 0 >= 0$.
Agora, se $u, v \in \mathcal{C}^\perp$, temos

$$< u + v, w >=< u, w > + < v, w >= 0 + 0 = 0, \forall\ w \in \mathcal{C}.$$

Logo, $u + v \in \mathcal{C}^\perp$.
E, se $\lambda \in \mathbb{F}_q$, temos

$$< \lambda u, w >= \lambda < u, w >= \lambda 0 = 0.$$

Ou seja, $\lambda u \in \mathcal{C}^\perp$.
Portanto, $\mathcal{C}^\perp$ é um subespaço vetorial de $\mathbb{F}_q^n$.
(ii) Sabemos que, $x \in \mathcal{C}^\perp$, se e somente se x é ortogonal a todos os elementos de $\mathcal{C}$, em particular a todos os elementos de uma base de $\mathcal{C}$. Como as linhas de G são bases de $\mathcal{C}$, segue que $G \cdot x^t = 0$.

■

Observe que $\mathcal{C}^\perp \subseteq \mathbb{F}_q^n$ é também um código linear.

Proposição 1.2.9 *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear de dimensão k e com matriz geradora $G = [Id_k \mid A]_{k \times n}$ na forma padrão. Então,*

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

(ii) $H = [-A^t \mid Id_{(n-k)}]$ *é a matriz geradora de* $\mathcal{C}^\perp$.

Demonstração: *(i)* De fato, pelo Lema 1.2.8 *(ii)*, um vetor $x = (x_1, \ldots, x_n) \in \mathcal{C}^\perp$ se, e somente se,

$$\begin{aligned}
G \cdot x^t \ = \ 0 \ &\iff \ (Id_k \mid A) \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \ = \ 0 \\
&\iff \ \left[\begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} \ + \ A \cdot \begin{bmatrix} x_{k+1} \\ \vdots \\ x_n \end{bmatrix} \right] \ = \ 0 \\
&\iff \ \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} + A \cdot \begin{bmatrix} x_{k+1} \\ \vdots \\ x_n \end{bmatrix} \ = \ 0 \\
&\iff \ \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} \ = \ -A \cdot \begin{bmatrix} x_{k+1} \\ \vdots \\ x_n \end{bmatrix}.
\end{aligned}$$

Observemos que $\begin{bmatrix} x_{k+1} \\ \vdots \\ x_n \end{bmatrix}$ há $n-k$ entradas e cada uma delas possui q possibilidades de escolha, uma vez que estão em $\mathbb{F}_q$. Logo, $\mathcal{C}^{\perp}$ possui $\underbrace{q \cdots q}_{n-k \text{ vezes}} = q^{n-k}$ elementos. Ou seja, $dim\mathcal{C}^{\perp} = n-k$.

(ii) Note que as linhas de H são linearmente independentes por $Id_{(n-k)}$. Além disso, as linhas de H são ortogonais às linhas de G.

De fato, calculando o produto interno entre os elementos da i-ésima linha de H pelos elementos da i-ésima linha de G, para $i = 1, \ldots, n$, temos

$$< (-a_{1j}, \ldots, -a_{ij}, \ldots, -a_{kj}, 0, \ldots, 0, 1, 0, \ldots, 0), (0, \ldots, 0, 1, 0, \ldots, 0, a_{i(k+1)}, \ldots, a_{ij}, \ldots, a_{in}) >$$

$$\begin{aligned} &= -a_{ij} + a_{ij} \\ &= 0 \end{aligned}$$

para $i = 1, \ldots, k$ e $j = k+1, \ldots, n$.

Logo, as linhas de H geram um espaço contido em $\mathcal{C}^{\perp}$ de dimensão $n-k$, a mesma de $\mathcal{C}^{\perp}$. Portanto, esses espaços são idênticos, provando que a matriz $H = [-A^t \mid Id_{(n-k)}]$ gera o código dual $\mathcal{C}^{\perp}$.

■

Lema 1.2.10 *Seja $\mathcal{C} \subseteq {\mathbb{F}_q}^n$ um código linear de dimensão k e matriz geradora G. Uma matriz H de ordem $(n-k) \times n$ com entradas em $\mathbb{F}_q$ e linhas linearmente independentes é geradora de $\mathcal{C}^{\perp}$ se, e somente se,*

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

Demonstração: Necessariamente, notemos que as linhas de H geram um espaço vetorial contido em $\mathbb{F}_q^n$ de dimensão $n-k$, igual a dimensão de $\mathcal{C}^{\perp}$. Agora, se $h_1, \ldots, h_{n-k}$ e $g_1, \ldots, g_k$ são, respectivamente, as representações das linhas de H e G, temos

$$(G \cdot H^t)_{i,j} =< g_i, h_j^t >,\ i = 1, \ldots, k \text{ e } j = 1, \ldots, n-k.$$

Logo,

$$G \cdot H^t = 0 \iff < g_i, h_j^t >= 0,\ i = 1, \ldots, k \text{ e } j = 1, \ldots, n-k.$$

Ou seja, todos os vetores do subespaço gerado pelas linhas de H pertencem a $\mathcal{C}^{\perp}$.

Reciprocamente, o subespaço gerado pelas linhas de H tem dimensão igual a dimensão de $\mathcal{C}^{\perp}$. Logo,

$$G \cdot H^t = 0 \iff \mathcal{C}^{\perp} \text{ é gerado pelas linhas de } H.$$

■

Corolário 1.2.11 *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear. Então, $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.*

Demonstração: De fato, sejam G e H as matrizes geradoras de $\mathcal{C}$ e $\mathcal{C}^{\perp}$, respectivamente. Sabemos, pelo Lema 1.2.10 que

$$G \cdot H^t = 0 \iff (G \cdot H^t)^t = 0 \iff H \cdot G^t = 0.$$

Provando que G^t é a matriz geradora de $(\mathcal{C}^{\perp})^{\perp}$.

■

Proposição 1.2.12 *Sejam $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear e H a matriz geradora de $\mathcal{C}^{\perp}$. Então,*

$$v \in \mathcal{C} \iff H \cdot v^t = 0.$$

Demonstração: Notemos que, pelo Corolário 1.2.11 e pelo Lema 1.2.8 *(ii)*, temos

$$v \in \mathcal{C} \iff v \in (\mathcal{C}^{\perp})^{\perp} \iff H \cdot v^t = 0.$$

E o resultado segue.

■

A matriz H, geradora de $\mathcal{C}^{\perp}$, é chamada de ***matriz de checagem*** ou ***matriz teste de paridade*** de $\mathcal{C}$.

Para cada $v \in \mathbb{F}_q^n$, o vetor $s = H \cdot v^t$ é chamado de ***síndrome*** de v.

Proposição 1.2.13 *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear e H sua matriz de checagem. Então, $\omega(\mathcal{C}) \geqslant s$ se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

Demonstração: ($\Longleftarrow$) Suponhamos que qualquer conjunto contendo quaisquer $s-1$ colunas de H seja linearmente independente. Seja $0 \neq c = (c_1, \ldots, c_n) \in \mathcal{C}$ e $h_1, \ldots, h_n$ as colunas de H. Como H é a matriz de checagem, de $\mathcal{C}$, então

$$0 = H \cdot c^t = \sum_{i=1}^{n} h_i \cdot c_i. \tag{1.1}$$

Como $\omega(\mathcal{C})$ é o número de componentes não nulas de c, suponha que $\omega(c) \leqslant s-1$, então (1.1) seria uma combinação linear de r colunas de H, com $1 \leqslant r \leqslant s-1$, o que é uma contradição. Logo, $\omega(c) \geqslant s$, e portanto, $\omega(\mathcal{C}) \geqslant s$.

($\Longrightarrow$) Suponhamos que $\omega(\mathcal{C}) \geqslant s$ e que H tenha $s-1$ colunas linearmente dependentes, a saber, $h_{i_1}, \ldots, h_{i_{s-1}}$. Então, existiriam $c_{i_1}, \ldots, c_{i_n} \in \mathbb{F}_q$ não todos nulos tais que

$$\sum_{j=1}^{s-1} c_{i_j} \cdot h_{i_j} = 0.$$

Ou seja, $c = (0, \ldots, 0, c_{i_1}, \ldots, c_{i_{s-i}}, 0, \ldots, 0) \in \mathcal{C}$ e logo, $\omega(c) \leqslant s-1 < s$, o que é uma contradição. Logo, $\omega(\mathcal{C}) \geqslant s$ suficientemente quando H tem $s-1$ colunas linearmente independentes.

■

Teorema 1.2.14 *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear e H sua matriz de checagem. Então, $\omega(\mathcal{C}) \geqslant s$ se, e somente se, qualquer conjunto contendo quaisquer $s-1$ colunas de H é linearmente independentes e existe um conjunto contendo quaisquer s colunas de H linearmente dependentes.*

Demonstração: ($\Longrightarrow$) Por hipótese, $\omega(\mathcal{C}) = s$. Logo, pela Proposição 1.2.13, segue que quaisquer $s-1$ colunas de H são linearmente independentes. Além disso, existem s colunas de H linearmente independentes, caso contrário, teríamos de ter $\omega(\mathcal{C}) \geqslant s+1$, o que seria um absurdo.

($\Longleftarrow$) Pela Proposição 1.2.13, temos, $\omega(\mathcal{C}) \geqslant s$. Suponhamos então que $\omega(\mathcal{C}) > s$. Logo, seguiria também da Proposição 1.2.13 que, qualquer conjunto contendo quaisquer s colunas de H seria linearmente independente, o que contradiz a hipótese. Portanto, $\omega(\mathcal{C}) = s$.

■

Corolário 1.2.15 ***(Cota de Singleton)*** *Se (n, k, d) são os parâmetros de um código linear $\mathcal{C}$, então vale*

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

Demonstração: Seja H a matriz de checagem de $\mathcal{C}$. Notemos que H tem posto $n-k$ e $d-1$ colunas linearmente independentes. Logo, H tem no máximo $n-k$ colunas linearmente independentes, isto é, $d-1 \leq n-k$. E o resultado segue.

■

1.3 Códigos Cíclicos

Relembremos que no início, começamos nosso estudo trabalhando com um código qualquer e em seguida passamos a enxergá-lo como um espaço vetorial, o que nos proporcionou obter relações entre seus parâmetros e construir uma sistemática de codificação. O que faremos a seguir é enxergar um código como um ideal de um anel e ver como esta nova estrutura pode nos ajudar na construção de uma nova sistemática de codificação, além da obtenção de resultados sobre os parâmetros do código.

Definição 1.3.1 *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear. Dizemos que $\mathcal{C}$ é um* ***código cíclico*** *se para todo $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, $(c_{n-1}, c_0, \ldots, c_{n-2})$ também está em $\mathcal{C}$.*

Seja $\mathbb{F}_q[X]$ o anel de polinômios na variável X e seja $R_n = \mathbb{F}_q[X]/(X^n - 1)$. Note que os elementos de R_n são da forma

$$\overline{r(X)} = \{r(X) + q(X)(X^n - 1) : \ q(X) \in \mathbb{F}_q[X]\}.$$

Não é difícil mostrar que R_n é um $\mathbb{F}_q$-espaço vetorial de base $\{1, \overline{X}, \overline{X^2}, \ldots, \overline{X^{n-1}}\}$ e dimensão n.

Definamos a transformação linear

$$\begin{array}{rccc} \psi: & \mathbb{F}_q^n & \longrightarrow & \dfrac{R_n}{a_0+a_1X+\cdots+a_{n-1}X^{n-1}}\ . \\ & (a_0,a_1,\ldots,a_{n-1}) & \longmapsto & \end{array} \tag{1.2}$$

Esta transformação será muito importante em nosso estudo, uma vez que ao provarmos que tal transformação é um isomorfismo, observaremos que ela levará qualquer código cíclico $\mathcal{C} \subseteq \mathbb{F}_q^n$ a um subconjunto de R_n que será um ideal.

Mostremos então, que ψ é um isomorfismo. Note que ψ claramente está bem definida. Agora, seja $v = (v_o, v_1, \ldots, v_{n-1}) \in \mathbb{F}_q^n$. Então,

$$\begin{aligned} Ker(\psi) &= \{v \in \mathbb{F}_q{}^n : \ \psi(v) = \overline{0}\} \\ &= \{v \in \mathbb{F}_q{}^n : \ \overline{v_0 + v_1X + \cdots + v_{n-1}X^{n-1}} = \overline{0}\} \\ &= \{v \in \mathbb{F}_q{}^n : \ \overline{v_0} + \overline{v_1X} + \cdots + \overline{v_{n-1}X^{n-1}} = 0 + 0\overline{X} + \cdots + 0\overline{X^{n-1}}\} \\ &= \{v \in \mathbb{F}_q{}^n : \ v_0 + v_1\overline{X} + \cdots + v_{n-1}\overline{X^{n-1}} = 0 + 0\overline{X} + \cdots + 0\overline{X^{n-1}}\}. \\ &= \{v \in \mathbb{F}_q{}^n : \ v_0 = v_1 = \cdots = v_n = 0\} \\ &= \{(0, 0 \ldots, 0)\}. \end{aligned}$$

Provando que ψ é injetora.

Por outro lado, dado $a_0 + a_1\overline{X} + \cdots + a_{n-1}\overline{X^{n-1}} \in R_n$, existe $a = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ tal que

$$\psi(a) = a_0 + a_1\overline{X} + \cdots + a_{n-1}\overline{X^{n-1}}.$$

Portanto, ψ é sobrejetora, logo isomorfismo.

■

Para $f(X) \in \mathbb{F}_q[X]$, seja $I(f(X)) = \{f(X) \cdot g(X) \ ; \ g(X) \in \mathbb{F}_q[X]\}$. Não é difícil ver que $I(f(X))$ é um ideal de $\mathbb{F}_q[X]$.

Proposição 1.3.2 *Todo ideal de $\mathbb{F}_q[X]$ é um ideal principal. Ou seja, todo ideal de $\mathbb{F}_q[X]$ é dado por $I(f(X))$, para algum $f(X) \in \mathbb{F}_q[X]$.*

Demonstração: De fato, se I um ideal do anel $\mathbb{F}_q[X]$.

Se $I = \{0\}$, basta tomarmos $f(X) = 0$ em $\mathbb{F}_q[X]$ e teremos $I = \{0\} = I(0) = I(f(X))$. Se $I \neq \{0\}$, então tomemos $f(X) \neq 0$ em I tal que $gr(f(X))$ seja o menor possível.

Provemos então que $I = I(f(X))$.

É claro que $f(X) \in I$. Logo, $I(f(X)) \subseteq I$, provando uma das inclusões.

Por outro lado, seja $g(X) \in I$. Então, pelo algorítmo da divisão, existem os polinômios $q(X)$ e $r(X)$ tais que

$$g(X) = f(X)q(X) + r(X)$$

Como $(-f(X))g(X)$ e $r(X) + (-f(X)g(X))$ pertencem a I, segue da definição de ideal que

$$r(X) = g(X) - f(X)q(X).$$

Observamos que se $r(X) \neq 0$, na expressão acima, então $r(X) \in I$ e teríamos $gr(r(X)) < gr(f(X))$ em I, o que é uma contradição, uma vez que $gr(f(X))$ é o menor possível. Logo, $r(X) = 0$ e, portanto, $g(X) = f(X)q(X) \in I$. Logo, $I \subseteq I(f(X))$, provando a outra inclusão.

Portanto, $I = I(f(X))$.

■

Definição 1.3.3 *Sejam $f(X), g(X) \in \mathbb{F}_q[X]$. Dizemos que $f(X)$ e $g(X)$ são* ***associados*** *se existe $c \in \mathbb{F}_q$ tal que $g(X) = cf(X)$ e são geradores de um mesmo ideal de $\mathbb{F}_q[X]$.*

Proposição 1.3.4 *Se dois polinômios são geradores de um mesmo ideal, então eles são associados, isto é, $f(X) = ag(X)$ e $g(X) = bf(X)$, onde $a, b \in \mathbb{F}_q$.*

Demonstração: De fato, se $f(X) = 0$, então temos $g(X) = 0$ (e vice versa) e o resultado segue.

Como $f(X) \in I(g(X))$, então temos $f(X) = a(X)g(X)$. Mas, $g(X) \in I(f(X))$, segue então que $g(X) = b(X)f(X)$ com $a(X), b(X) \in \mathbb{F}_q[X]$.

Suponhamos então que $f(X) \neq 0$. Então, temos $f(X) = a(X)g(X) = a(X)[b(X)f(X)] = [a(X)b(X)]f(X)$.

Como $\mathbb{F}_q[X]$ é um domínio, segue que $a(X)b(X) = 1$. Logo, $a(X) = a \in \mathbb{F}_q$ e $b(X) = b \in \mathbb{F}_q$.

Portanto, $f(X)$ e $g(X)$ são associados.

■

Corolário 1.3.5 *Se $I \neq \{0\}$ é um ideal de $\mathbb{F}_q[X]$, então existe um único polinômio mônico e de grau mínimo $f(X)$ em I, tal que $I = I(f(X))$.*

Demonstração: Suponhamos que existam dois polinômios mônicos $f(X)$ e $g(X)$ em I, de grau mínimo, tais que $I = I(f(X)) = I(g(X))$.

Como $f(X)$ e $g(X)$ geram o mesmo ideal, segue que eles são associados. Logo, existe $u \in \mathbb{F}_q$ tal que

$$f(X) = ug(X).$$

Além disso, como $f(X)$ e $g(X)$ são mônicos, segue que $u = 1$.

Portanto, $f(X) = g(X)$.

■

É claro que todo ideal de $\mathbb{F}_q[X]$ é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q[X]$. Todavia, se considerarmos o subanel $\mathbb{F}_q[X]_r$ de $\mathbb{F}_q$[X] dos polinômios de grau menor ou igual a r, que em particular é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q[X]$, a recíproca é falsa.

Por exemplo, $X^r \in \mathbb{F}_q[X]_r$, mas $X^{r+1} = X^r.X \notin \mathbb{F}_q[X]_r$.

Logo, $\mathbb{F}_q[X]_r$ não é um ideal de $\mathbb{F}_q[X]$.

Para $p(x) \in \mathbb{F}_q[X]$ seja $\mathbb{F}_q[X]_{p(X)} := \mathbb{F}_q[X]/p(x)$.

Proposição 1.3.6 *Todos os ideais de $\mathbb{F}_q[X]_{p(X)}$ são dados por $I(\overline{f(X)})$, onde $f(X)$ é um divisor de $p(X)$.*

Demonstração: Note que $\overline{f(X)} = \{f(X) + g(X)p(X) : g(X) \in \mathbb{F}_q[X]\}$.

Seja I um ideal de $\mathbb{F}_q[X]_{p(X)}$ e considere $J = \{g(X) \in \mathbb{F}_q[X] : \overline{g(X)} \in I\}$.

Mostremos que J é um ideal de $\mathbb{F}_q[X]$.

Seja $g_1(X),\ g_2(X) \in J$ e $h(X) \in \mathbb{F}_q[X]$.

Observe que $\overline{g_1(X)},\ \overline{g_2(X)} \in I$. Como I é ideal, segue que $\overline{g_1(X)}+\overline{g_2(X)} = \overline{g_1(X) + g_2(X)} \in I$. Logo, $g_1(X) + g_2(X) \in J$.

Agora, $\overline{g_1(X) \cdot h(X)} = \overline{g_1(X)} \cdot \overline{h(X)} \in I$, pois I é ideal. Assim, $g_1(X)h(X) \in J$, e portanto, J é um ideal.

Notemos agora que, $p(X) \in J$. Logo, $J \neq \{0\}$. Segue então da Proposição 1.3.2, que existe $f(X) \in \mathbb{F}_q[X]\backslash\{0\}$ tal que $J = I(f(X))$.

Como $p(X) \in I(f(X))$, concluímos que $p(X)$ é um múltiplo de $f(X)$, isto é, $f(X)$ divide $p(X)$.

Por outro lado, observe que

$$\begin{aligned} I &= \{\overline{g(X)} \in \mathbb{F}_q[X]/p(X) :\ g(X) \in J\} \\ &= \{\overline{f(X) \cdot g(X)} = \overline{f(X)} \cdot \overline{g(X)} :\ \overline{g(X)} \in \mathbb{F}_q[X]/p(X)\} \\ &= I(\overline{f(X)}). \end{aligned}$$

■

Seja S_n o grupo simétrico. Para $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ e $\sigma \in S_n$, consideremos a aplicação linear dada por $T_\sigma(a_1, \ldots, a_n) := (a_{\sigma(1)}, \ldots, a_{\sigma(n)})$ e a permutação $\pi(i) = \begin{cases} i-1, & \text{se } i \geqslant 1, \\ n-1, & \text{se } i = 0 \end{cases}$

Observemos, primeiramente, que a transformação linear $T_\pi : \mathcal{C} \longrightarrow \mathbb{F}_q^n$, definida por $T_\pi(v) = (c_{n-1}, c_0, \ldots, c_{n-2})$, para todo $v = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, sofre a seguinte ação por meio de ψ, definida em (1.2).

$$\begin{aligned} \psi(T_\pi(v)) &= \psi((c_{n-1}, c_0, \ldots, c_{n-2})) \\ &= \overline{c_{n-1} + c_0X + \cdots + c_{n-2}X^{n-1}} \\ &= \overline{c_{n-1}X^n + c_0X + \cdots + c_{n-2}X^{n-1}} \\ &= \overline{X} \cdot (\overline{c_o + c_1X + \cdots + c_{n-1}X^{n-1}}) \\ &= \overline{X} \cdot \psi(v). \end{aligned}$$

Ou seja, ψ se caracteriza na multiplicação por $\overline{X}$ em R_n.

Tal operação nos leva ao seguinte lema.

Lema 1.3.7 *Seja V um subespaço vetorial de R_n. Então, V é um ideal de R_n se, e somente se, V é fechado pela multiplicação por $\overline{X}$.*

Demonstração: ($\Longrightarrow$) Notemos que V é fechado pela adição, pois é subespaço vetorial de R_n.

Agora, para todo $\overline{X} \in R_n$, temos $\overline{X}.\overline{f(X)} \in V$, para todo $\overline{f(X)} \in V$, pois V é ideal de R_n por hipótese.

Logo, V é fechado pela multiplicação por $\overline{X}$.

($\Longleftarrow$) É claro que $\overline{f(X)} + \overline{g(X)} = \overline{f(X) + g(X)} \in V$, para todos $f(X), g(X) \in V$. Mostremos então que vale a segunda condição da definição de um ideal.

Seja $a \in \mathbb{F}_q$. Como V é subespaço vetorial de R_n, segue que $a.\overline{f(X)} \in V$, para todo $\overline{f(X)} \in V$.

Por outro lado, como por hipótese, V é fechado pela multiplicação por $\overline{X}$, temos

$$\overline{X \cdot f(X)} = \overline{X} \cdot \overline{f(X)} \in V.$$

Além disso,

$$\overline{X^2 \cdot f(X)} = \overline{X \cdot X \cdot f(X)} = \overline{X} \cdot \overline{X \cdot f(X)} = \overline{X} \cdot \overline{X} \cdot \overline{f(X)} = \overline{X \cdot X} \cdot \overline{f(X)} = \overline{X^2} \cdot \overline{f(X)} \in V.$$

Assim, para todo $m \in \mathbb{N}$, é claro que

$$\overline{X^m \cdot f(X)} = \overline{X^m} \cdot \overline{f(X)} \in V$$

Seja agora, $\overline{g(X)} = \overline{a_0 + a_1X + \cdots + a_{n-1}X^{n-1}} \in R_n$. Logo, para todo $\overline{f(X)} \in V$, temos

$$\begin{aligned}
\overline{g(X)} \cdot \overline{f(X)} &= \overline{g(X) \cdot f(X)} \\
&= \overline{(a_0 + a_1X + \cdots + a_{n-1}X^{n-1}) \cdot f(X)} \\
&= \overline{a_0f(X) + a_1Xf(X) + \cdots + a_{n-1}X^{n-1}f(X)} \\
&= \overline{a_0f(X)} + \overline{a_1Xf(X)} + \cdots + \overline{a_{n-1}X^{n-1}f(X)} \\
&= a_0\overline{f(X)} + a_1\overline{Xf(X)} + \cdots + a_{n-1}\overline{X^{n-1}f(X)} \\
&= a_0\overline{f(X)} + a_1\overline{X} \cdot \overline{f(X)} + \cdots + a_{n-1}\overline{X^{n-1}} \cdot \overline{f(X)} \in V,
\end{aligned}$$

pois, como vimos anteriormente, que cada parcela desta soma pertence a V. O resultado segue, pois V é subespaço vetorial.

■

O seguinte resultado a seguir nos mostra como dar a estrutura de ideal a um código cíclico.

Teorema 1.3.8 *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$. Então, $\mathcal{C}$ é um código cíclico se, e somente se, $\psi(\mathcal{C})$ é um ideal de R_n.*

Demonstração: ($\Longrightarrow$) De fato, por definição, para todo $v \in \mathcal{C}$, temos $\psi(T_\pi(v)) = \overline{X} \cdot \psi(v)$. Logo,

$$\psi(T_\pi(\mathcal{C})) = \overline{X} \cdot \psi(\mathcal{C}).$$

Como $\psi(T_\pi(\mathcal{C})) \subseteq R_n$, segue do Lema 1.3.7 que $\psi(\mathcal{C})$ é um ideal de R_n.
($\Longleftarrow$) Seja $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$. Como $\psi(\mathcal{C})$ é ideal de R_n, temos

$$\begin{aligned}
\psi(T_\pi(c_0, c_1, \ldots, c_{n-1})) &= \overline{X} \cdot \psi(c_0, c_1, \ldots, c_{n-1}) \\
&= \overline{X} \cdot (c_0 + c_1\overline{X} + \cdots + c_{n-1}\overline{X^{n-1}}) \\
&= c_0\overline{X} + c_1\overline{X^2} + \cdots + c_{n-1}\overline{X^n} \\
&= c_{n-1} + c_0\overline{X} + \cdots + c_{n-2}\overline{X^{n-1}} \\
&= \psi(c_{n-1}, c_0, \ldots, c_{n-2}).
\end{aligned}$$

Assim, $\psi(c_{n-1}, c_0, \ldots, c_{n-2}) \in \psi(\mathcal{C})$. Como ψ é bijetora, temos $T_\pi(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$.
Portanto, $\mathcal{C}$ é cíclico.

■

Logo, da Proposição 1.3.6, segue que um código $\mathcal{C} \subseteq \mathbb{F}_q^n$ é cíclico se, e somente se $\psi(\mathcal{C}) = I(\overline{g(X)})$, onde $g(X) \in \mathbb{F}_q[X]$ é um divisor de $X^n - 1$. O polinômio $g(x)$ é chamado de gerador de $\mathcal{C}$. Note que, se $\mathcal{C}$ é cíclico, podemos associar a palavra $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ ao polinômio $c_0 + c_1X + \ldots + c_{n-1}X^{n-1}$ em R_n.

A seguir, veremos como encontrar a dimensão de um código cíclico $\mathcal{C}$ a partir do grau de seu polinômio gerador.

Se p é a característica de $\mathbb{F}_q$ e se $n = mp^s$, com $mdc(m, p) = 1$, segue que

$$\begin{aligned}
X^n - 1 &= X^{mp^s} - 1^{mp^s} \\
&= (X^m)^{p^s} - 1^{p^s} \\
&= (X^m - 1)^{p^s}.
\end{aligned}$$

Note que a derivada $(X^m - 1)' = mX^{m-1} \neq 0$. Logo, $X^m - 1$ não tem fator em comum com sua derivada, pois se $mdc(X^m - 1, mX^{m-1}) = p(X) \neq 1$, então $X \mid p(X)$ e portanto, $X \mid X^m - 1$. Assim, 0 seria raiz de $X^m - 1$, o que é um absurdo.
Além disso, suponhamos que $X^m - 1 = (p(X))^k \cdot q(X)$, com $k > 2$. Então, derivando a igualdade, temos

$$mX^{m-1} = k(p(X))^{k-1}.p'(X).q(X) + (p(X))^k.q'(X).$$

Logo, $X^m - 1$ teria fator em comum com sua derivada, o que também é um absurdo.
Assim, $X^m - 1$ admite decomposição da forma

$$X^m - 1 = g_1 \cdots g_r,$$

onde $g_1, \ldots, g_r$ são polinômios mônicos, irredutíveis e distintos dois a dois.
Logo,

$$\begin{aligned} X^n - 1 &= (X^m - 1)^{p^s} \\ &= (g_1 \cdots g_r)^{p^s} \\ &= g_1^{p^s} \cdots g_r^{p^s}. \end{aligned}$$

Como os polinômios $1,\ g_i,\ g_i^2,\ g_i^3,\ g_i^4, \ldots,\ g_i^{p^s}$, para $i = 1, \ldots, r$, também são divisores de $X^n - 1$, segue que $X^n - 1$ tem exatos $(p^s + 1)^r$ divisores mônicos.

Além disso, como há bijeções entre os ideais de $\mathbb{F}_q[X]/(X^n - 1)$ com os divisores de $X^n - 1$, concluímos que R_n possui exatamente $(p^s + 1)^r$ ideais.

Agora, se $mdc(n, p) = 1$, segue que $s = 0$ e, portanto, R_n terá $(p^0 + 1)^r = 2^r$ ideais.

Por outro lado, R_n não é um domínio de integridade, pois se $X^n - 1 = (X - 1) \cdot (X^{n-1} + X^{n-2} + \cdots + X + 1)$, segue que

$$\overline{(X - 1) \cdot (X^{n-1} + X^{n-2} + \cdots + X + 1)} = \overline{X^n - 1} = \overline{X^n} - \overline{1} = \overline{1} - \overline{1} = \overline{0}.$$

Ou seja, existem dois elementos de R_n cujo produto é nulo.

Assim, denotando por $g(X)$ um divisor de $X^n - 1$, temos

$$\frac{X^n - 1}{g(X)} = h(X).$$

Teorema 1.3.9 *Seja $I = I(\overline{g(X)})$ um ideal, onde $g(X)$ é um divisor de $X^n - 1$, tal que $gr(g(X)) = s < n$. Então, o conjunto $B = \{\overline{g(X)},\ \overline{Xg(X)}, \ldots,\ \overline{X^{n-s-1}g(X)}\}$ é uma base de I como $\mathbb{F}_q$-espaço vetorial.*

Demonstração: Mostremos primeiramente que os elementos de B são linearmente independentes. Sejam $a_0, \ldots, a_{n-s-1} \in \mathbb{F}_q$, tais que

$$\begin{aligned} a_0\overline{g(X)} + a_1\overline{Xg(X)} + \cdots + a_{n-s-1}\overline{X^{n-s-1}g(X)} &= \overline{0} \implies \\ \overline{g(X)} \cdot (a_0 + a_1\overline{X} + \cdots + a_{n-s-1}\overline{X^{n-s-1}}) &= \overline{0} \end{aligned}$$

Logo, $g(X)$ é um divisor de $a_0 + a_1X + \cdots + a_{n-s-1}X^{n-s-1}$. Segue então que existe $d(X) \in \mathbb{F}_q[X]$ tal que

$$\begin{aligned} g(X) \cdot (a_0 + a_1X + \cdots + a_{n-s-1}X^{n-s-1}) &= d(X) \cdot (X^n - 1) \implies \\ a_0 + a_1X + \cdots + a_{n-s-1}X^{n-s-1} &= d(X) \cdot \frac{X^n - 1}{g(X)} \implies \\ a_0 + a_1X + \cdots + a_{n-s-1}X^{n-s-1} &= d(X) \cdot h(X). \end{aligned}$$

Note que $gr(h(X)) = n - s$. Logo, $gr(d(X)) = -1$, o que é um absurdo.

Portanto, $a_0 + a_1X + \cdots + a_{n-(s+1)}X^{n-s-1} = 0$, o que implica $a_0 = a_1 = \cdots = a_{n-s-1} = 0$, provando que os elementos de B são linearmente independentes.

Basta mostrarmos agora que qualquer elemento de I é gerado por elementos de B.

De fato, seja $\overline{f(X)} \in I$. Como $I = I(\overline{g(X)})$ é $g(X)$ é um divisor de $X^n - 1$, temos

$$f(X) \equiv d(X)g(X) \mod (X^n - 1).$$

Agora pelo algoritmo da divisão, segue que $d(X) = c(X)h(X) + r(X)$, com $r(X) = a_0 + a_1 + \cdots + a_{n-s-1}X^{n-s-1}$. Logo,

$$\begin{aligned} f(X) &\equiv d(X)g(X) \mod (X^n - 1) \\ &\equiv [c(X)h(X) + r(X)]g(X) \mod (X^n - 1) \\ &\equiv [c(X)h(X)g(X) + r(X)g(X)] \mod (X^n - 1). \end{aligned}$$

Assim,

$$\begin{aligned} f(X) &\equiv [c(X)(X^n - 1) + r(X)g(X)] \mod (X^n - 1) \\ &\equiv [0 + r(X)g(X)] \mod (X^n - 1) \\ &\equiv r(X)g(X) \mod (X^n - 1). \end{aligned}$$

Portanto,

$$\begin{aligned} \overline{f(X)} &= (\overline{a_0 + a_1X + \cdots + a_{n-s-1}X^{n-s-1}}) \cdot \overline{g(X)} \\ &= a_0\overline{g(X)} + a_1\overline{Xg(X)} + \cdots + a_{n-s-1}\overline{X^{n-s-1}g(X)}. \end{aligned}$$

Ou seja, $\overline{f(X)}$ é gerado por elementos de B. Concluímos então que B é base de I como $\mathbb{F}_q$-espaço vetorial.

■

Corolário 1.3.10 *Se $\mathcal{C} \subset \mathbb{F}_q^n$ é um código cíclico e $g(x)$, com $gr(g(x)) = r$, é seu polinômio gerador, então a dimensão k de $\mathcal{C}$ é $n-r$. Consequentemente, sua distância mínima é $d \leq r+1$.*

• **Sistemática de codificação para códigos cíclicos:** Seja $\mathcal{C}$ um código cíclico com polinômio gerador $g(x) = x^r + a_{r-1}x^{r-1} + \ldots + a_1x + a_0$. Dado $w = (w_1, \ldots, w_k) \in \mathbb{F}_q^k$, construímos o polinômio $w(x) = w_1x^{n-1} + w_2x^{n-2} + \ldots + w_kx^{n-k}$, em que $n-k = r$. Dividimos o polinômio $w(x)$ por $g(x)$ e obtemos $w(x) = q(x).g(x) + r(x)$, onde o grau de $r(x)$ é menor do que r. Logo, $w(x) - r(x) = q(x).g(x)$ e podemos associar $w(x) - r(x)$ a uma palavra de $\mathcal{C}$, já que $g(x)$ é o polinômio gerador de $\mathcal{C}$. É importante observar que a forma como $w(x)$ foi construído nos garante uma bijetividade entre $w(x) - r(x)$ e a palavra em $\mathcal{C}$ a ele correspondida. De fato, suponha que existam $w_1, w_2 \in \mathbb{F}_q^k$, com $w_1 \neq w_2$, tais que $w_1(x) - r_1(x) = w_2(x) - r_2(x)$. Daí, $w_1(x) - w_2(x) = r_2(x) - r_1(x)$, que é um absurdo, pois como $w_1 \neq w_2$, então $gr(w_1(x) - w_2(x)) \geq n - k = r$, e, por outro lado, $gr(r_2(x) - r_1(x)) < r$.

Assim, vimos que um código cíclico possui uma estrutura algébrica, de um ideal, que nos ajuda na obtenção de seus parâmetros e na construção de uma sistemática de codificação. Uma pergunta que podemos fazer é: e se $\mathcal{C}$ não é cíclico, será que podemos encontrar outro tipo

de estrutura algébrica que nos ajude na obtenção de seus parâmetros e na construção de uma sistemática de codificação? Utilizando os conceitos e resultados de automorfismo de códigos e de bases de Gröbner para módulos, veremos que a resposta é sim.

A seguir introduziremos o conceito de automorfismo para um código $\mathcal{C} \subseteq \mathbb{F}_q^n$. Conceitos e resultados ligados à bases de Gröbner podem ser vistos no Apêndice A.

Sejam $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$ e S_n o grupo simétrico cujos elementos são as permutações do conjunto $\{1, 2, \ldots, n\}$.

Para $\pi \in S_n$, S_n age sobre $\mathbb{F}_q^n$ via: $\pi(c_1, c_2, \ldots, c_n) = (c_{\pi(1)}, c_{\pi(2)}, \ldots, c_{\pi(n)})$.

Então, o grupo de automorfismos de $\mathcal{C} \subseteq \mathbb{F}_q^n$ é dado por:

$$\mathbf{Aut}(\mathcal{C}) = \{\pi \in S_n \ ; \ \pi(\mathcal{C}) = \mathcal{C}\} = \{\pi \in S_n \ ; \ \pi(c) \in \mathcal{C} \ , \ \forall \ c \in \mathcal{C}\}.$$

Consideremos $\mathcal{C}$ com um $\sigma \in Aut(\mathcal{C})$. O fato de $\sigma \in S_n$, nos diz que ele divide o conjunto $\{1, 2 \ldots, n\}$ em r blocos (ou órbitas cíclicas), onde r pode variar de 1 (como no caso dos códigos cíclicos) a n. Denotaremos tais órbitas por $O_1, \ldots, O_r$.

Fixemos um elemento $c_{i,0} \in O_i$, para $j = 0, 1, \ldots, |O_i| - 1$, que é um abuso de notação, já que $O_i \subseteq \{1, \ldots, n\}$. Definimos $c_{i,j} = \sigma^j(c_{i,0})$. Logo, vemos que $c_{i,|O_i|} = c_{i,0}$ e, por convenção, escrevemos $c_{i,-1} = \sigma^{-1}(c_{i,0}) = c_{i,|O_i|-1}$.

Portanto, dada $\overrightarrow{c} = (c_1, \ldots, c_n) \in \mathcal{C}$ e rearranjando, se necessário, as componentes de $\overrightarrow{c}$ vemos que se pode representar as palavras de $\mathcal{C}$ como r-uplas de polinômios em uma variável $(h_1(t), \ldots, h_r(t))$, onde

$$h_i(t) = \sum_{j=0}^{|O_i|-1} c_{i,j} t^j.$$

Podemos ver as r-uplas $(h_1(t), \ldots, h_r(t))$ como elementos do $\mathbb{F}_q[t]$-módulo

$$M = \bigoplus_{i=1}^{r} \frac{\mathbb{F}_q[t]}{\langle t^{|O_i|} - 1 \rangle}.$$

O $\mathbb{F}_q[t]$-submódulo $\overline{\mathcal{C}} \subseteq \mathbb{F}_q[t]^r$ gerado pelas palavras código de $\mathcal{C}$ e por $q_i = (t^{|O_i|} - 1)e_i$, onde para $i = 1, \ldots, r$, e_i é o i-ésimo vetor da base padrão de $\mathbb{F}_q[t]^r$ é dito associado a $\mathcal{C}$. Também podemos ver $\overline{\mathcal{C}}$ como sendo a imagem inversa $\pi^{-1}(\mathcal{C})$ da sobrejeção

$$\pi : \mathbb{F}_q[t]^r \to \bigoplus_{i=1}^{r} \frac{\mathbb{F}_q[t]}{\langle t^{|O_i|} - 1 \rangle}.$$

Portanto, vimos como um $[n, k, d]$-código linear $\mathcal{C}$ com um automorfismo σ pode ser associado a um submódulo $\overline{\mathcal{C}}$ do módulo livre $\mathbb{F}_q[t]^r$. Com essa estrutura de módulos, resumidamente, temos a seguinte sistemática de codificação muito semelhante à feita no caso de códigos cíclicos, que utiliza a teoria de bases de Gröbner e que será detalhada mais adiante. Dado $w \in \mathbb{F}_q^k$, construímos $w(t) \in \mathbb{F}_q[t]^r$, e como $\mathcal{C}$ é um $\mathbb{F}_q[t]$-módulo, terá uma base de Gröbner $\{f_1, \ldots, f_r\}$ e utilizando um algoritmo semelhante ao da divisão de polinômios podemos escrever $w(t) = a_1 f_1 + \ldots + a_r f_r + \widetilde{f} \Rightarrow w(t) - \widetilde{f} = a_1 f_1 + \ldots + a_r f_r \in \mathcal{C}$, e codificamos w.

Observamos que encontrar um automorfismo para um código qualquer não é simples. Por isso, o tratamento com códigos de Goppa geométricos, que são códigos construídos utilizando curvas, será interessante, já que os automorfismos destes códigos podem ser obtidos pelos automorfismos das curvas em que estão definidos. Veremos mais detalhes no próximo capítulo.

Capítulo 2

Códigos Sobre Curvas Algébricas

2.1 Preliminares

No início da década de 1980, V. D. Goppa introduziu a geometria algébrica na teoria de códigos com a construção de códigos sobre curvas. Esta nova construção foi muito relevante, com grande impacto tanto na análise dos parâmetros quanto nos processos de codificação e decodificação desses códigos. Neste capítulo veremos como construir tais códigos, chamados de Goppa geométricos.

A partir de agora, k será um corpo algebricamente fechado, mais especificamente o fecho algébrico do corpo $\mathbb{F}_q$, isto é, $k = \overline{\mathbb{F}}_q$. Denotaremos o ***espaço afim*** de dimensão n, com coordenadas $x_1, \ldots, x_n$, por $\mathbb{A}^n$, e o espaço projetivo de dimensão n, com coordenadas $x_0, x_1, \ldots, x_n$, será denotado por $\mathbb{P}^n$. Em um primeiro momento, discutiremos sobre o espaço afim, para na sequência estudarmos o caso projetivo, que é um pouco mais complicado, já que usamos coordenadas homogêneas.

No espaço $\mathbb{A}^n$, introduzimos a topologia de Zariski. Os conjuntos fechados são os conjuntos de zeros de ideais I de $k[x_1, \ldots, x_n]$, ou seja,

$$V(I) := \{(x_1, \ldots, x_n) \in \mathbb{A}^n : \ f(x_1, \ldots, x_n) = 0, \ \forall \ f \in I\}.$$

O conjunto $V(I)$ é dito ***irredutível*** se não pode ser escrito como união de quaisquer dois de seus subconjuntos próprios e fechados. O conjunto $V(I)$ é irredutível se, e somente se, I é um ideal primo. A demonstração deste fato pode ser vista na Proposição 3 do Capítulo 4 de [3].

Um aberto será o complemento de um conjunto fechado.

Definição 2.1.1 *Seja I_P um ideal primo de $k[x_1, \ldots, x_n]$. O conjunto $\mathcal{X}$ de zeros do ideal I_P é chamado de* ***variedade afim****.*

Como exemplo, podemos tomar em $\mathbb{A}^3$ a esfera unitária $x^2+y^2+z^2 = 1$. Então, a variedade afim $\mathcal{X}$ será o conjunto formado pelos zeros do ideal $I = \langle x^2 + y^2 + z^2 - 1 \rangle$.

Definição 2.1.2 *Seja I_P um ideal primo de $k[x_1, \ldots, x_n]$. O anel $k[\mathcal{X}] := k[x_1, \ldots, x_n]$ / I_P é chamado de* ***anel de coordenadas*** *da variedade afim $\mathcal{X}$.*

Como I_P é primo, segue que $k[\mathcal{X}]$ é um domínio.

Definição 2.1.3 *O corpo quociente de $k[\mathcal{X}]$, denotado por $k(\mathcal{X})$, é chamado de* ***corpo de funções*** *da variedade $\mathcal{X}$. A dimensão da variedade $\mathcal{X}$ é o grau de transcendência de $k(\mathcal{X})$ sobre k. Se tal dimensão for igual a 1, então dizemos que $\mathcal{X}$ é uma* ***curva algébrica****.*

Vamos definir a seguinte relação de equivalência $\sim$ em $\mathbb{A}^{n+1} \setminus \{0\}$:

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \iff \exists\ \lambda \in \mathbb{F}_q^*, \text{ tal que } (x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n).$$

Definição 2.1.4 *Definimos o* ***espaço projetivo*** *n-dimensional sobre $\mathbb{F}_q$, como sendo*

$$\mathbb{P}^n := (\mathbb{A}^{n+1} \setminus \{0\}) \ / \ \sim$$

Denotaremos um ponto P de $\mathbb{P}^n$ por

$$P = (x_0 : \ldots : x_n) = \{(y_0, \ldots, y_n)\ ;\ (y_0, \ldots, y_n) \sim (x_0, \ldots, x_n)\},$$

e diremos que $(x_0 : \ldots : x_n)$ são as ***coordenadas projetivas*** *de P.*

Geometricamente, podemos pensar nos pontos de $\mathbb{P}^n$ como o conjunto das retas que passam pela origem em $\mathbb{A}^{n+1}$.

Exemplo 2.1.5 *Considere em $\mathbb{A}^3$ a relação de equivalência*

$$(x_1,\ y_1,\ z_1) \sim (x_2,\ y_2,\ z_2) \iff \exists\ \lambda \in \mathbb{F}_q{}^*,\ \textit{tal que } (x_1,\ y_1,\ z_1) = \lambda(x_2,\ y_2,\ z_2).$$

É fácil ver que

$$\begin{array}{ccc} \mathbb{A}^2 & \longrightarrow & (\pi : z = 1) \subset \mathbb{A}^3 \\ (x, y) & \longmapsto & (x, y, 1) \end{array} \quad e \quad \pi \longrightarrow \begin{cases} \textit{retas } r \subset \mathbb{A}^3 \textit{ que passam} \\ \textit{pela origem e tais que } r \not\subset \pi \end{cases}$$

são bijeções.

Assim, dada uma reta $s \in \pi$, o espaço (plano) projetivo $\mathbb{P}^2$ será o conjunto dos pontos das retas r, que passam pela origem de $\mathbb{A}^3$ e intersectam s, isto é, $\mathbb{P}^2 = (\mathbb{A}^3 \setminus \{(0,0,0)\}) \ / \ \sim$. A figura a seguir ilustra o plano projetivo.

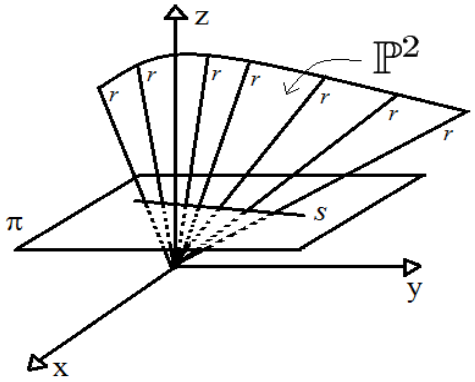

Figura 2.1: Plano Projetivo

Vejamos como podemos relacionar espaço afim e espaço projetivo.

Proposição 2.1.6 *Seja* $\mathcal{U} = \{(x_0 : \ldots : x_n) \in \mathbb{P}^n : x_0 \neq 0\}$ *e considere a aplicação*

$$\begin{array}{rccc} \varphi: & \mathbb{A}^n & \longrightarrow & \mathbb{P}^n \\ & (a_1, \ldots, a_n) & \longmapsto & (1 : a_1 : \ldots : a_n) \end{array}.$$

Então, φ *é injetora e* $Im(\varphi) = \mathcal{U}$.

Demonstração: De fato, observemos que $\varphi(a_1, \ldots, a_n) = (1 : a_1 : \ldots : a_n) \in \mathcal{U}$. Logo, podemos escrever

$$\varphi: \ \mathbb{A}^n \longrightarrow \mathcal{U}$$

Definamos

$$\begin{array}{rccc} \psi: & \mathcal{U} & \longrightarrow & \mathbb{A}^n \\ & (a_0 : a_1 : \ldots : a_n) & \longmapsto & \left(\dfrac{a_1}{a_0}, \ldots, \dfrac{a_n}{a_0}\right) \end{array}.$$

Notemos que ψ está bem definida, pois dado $(a_0, \ldots, a_n) = (b_0, \ldots, b_n)$ em $\mathcal{U}$, existe $\lambda \in \mathbb{F}_q^*$, tal que $(b_0, \ldots, b_n) = \lambda(a_0, \ldots, a_n)$, ou seja, $b_i = \lambda a_i$, para $i = 0, \ldots, n$. Assim,

$$\left(\frac{b_1}{b_0}, \ldots, \frac{b_n}{b_0}\right) = \left(\frac{\lambda a_1}{\lambda a_0}, \ldots, \frac{\lambda a_n}{\lambda a_0}\right) = \left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right).$$

Por outro lado, observemos que

$$(\psi \circ \varphi)(a_1, \ldots, a_n) = \psi(1 : a_1 : \ldots : a_n) = \left(\frac{a_1}{1}, \ldots, \frac{a_n}{1}\right) = (a_1, \ldots, a_n)$$

e

$$(\varphi \circ \psi)(a_0 : \ldots : a_n) = \varphi\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) = \left(1 : \frac{a_1}{a_0} : \ldots : \frac{a_n}{a_0}\right) = (a_0 : a_1 : \ldots : a_n).$$

Portanto, $\psi \circ \varphi = Id_{\mathbb{A}^n}$ e $\varphi \circ \psi = Id_{\mathcal{U}}$. Provando que φ é injetora e $Im(\varphi) = \mathcal{U}$.

■

Diante disso, temos $\mathbb{P}^n = \mathcal{U} \cup \{p \in \mathbb{P}^n : P = (0 : x_1 : \ldots : x_n)\}$. E pela Proposição 2.1.6, podemos identificar $\mathcal{U}$ com $\mathbb{A}^n$.

E observando que,

$$\begin{array}{ccc} \mathbb{P}^{n-1} & \longrightarrow & \{p \in \mathbb{P}^n : P = (0 : x_1 : \ldots : x_n)\} \\ (x_1 : \ldots : x_n) & \longrightarrow & (0 : x_1 : \ldots : x_n) \end{array}$$

é claramente uma bijeção, podemos identificar $\{P \in \mathbb{P}^n : P = (0 : x_1 : \ldots : x_n)\}$ com $\mathbb{P}^{n-1}$.

Logo, temos

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

Assim, para o caso $n = 1$, temos $\mathbb{P}^1 = \mathbb{A}^1 \cup \mathbb{P}^0$. Podemos então identificar $\mathbb{P}^0$ com o conjunto $\{(0 : y) : y \in \mathbb{F}_q\} = \{(0 : 1)\}$. Logo, $\mathbb{P}^0$ tem um único ponto que chamaremos de ***ponto no infinito*** e o denotaremos por P_∞.

Assim, definimos a ***reta projetiva*** por

$$\mathbb{P}^1 = \mathbb{A}^1 \cup \{P_\infty\}.$$

A seguir, estudaremos o comportamento de variedades no espaço projetivo. Todavia, devemos restringir alguns conceitos para conseguir nosso objetivo. Vejamos o porquê no exemplo que segue.

Exemplo 2.1.7 *Considere o polinômio* $f = 2y - z^3 \in \mathbb{R}[x, y, z]$.

Queremos determinar o conjunto $V(f) = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : f(x_0, x_1, x_2) = 0\}$ *contido em* $\mathbb{P}^2_{\mathbb{R}}$.

Observe que $P = (1 : 36 : 4) \in V(f)$, *pois* $f(1, 36, 4) = 0$, *mas* $P' = 2P = (2 : 72 : 8) \notin V(f)$, *uma vez que* $f(2, 72, 8) = -368$.

Ou seja, as coordenadas projetivas $(1 : 36 : 4)$ *e* $(2 : 72 : 8)$ *não são homogêneas. Isso se deve ao fato dos termos dos polinômios* f, $(2x)$ *e* $(-z^3)$, *não terem o mesmo grau.*

Para não nos depararmos com tal situação, iremos trabalhar apenas com polinômios homogêneos. De forma análoga ao que foi estudado no caso afim, trabalharemos com polinômios homogêneos de um ideal primo I_P de $k[x_0, x_1, \ldots, x_n]$.

Definição 2.1.8 *Seja* I_P *um ideal primo de* $k[x_0, x_1, \ldots, x_n]$. *Uma* ***variedade projetiva*** $\mathcal{X}$ *é o conjunto de zeros em* $\mathbb{P}^n$ *de polinômios homogêneos de* I_P.

Para simplificar as notações, denotaremos pelo mesmo símbolo $\mathcal{X}$ tanto a variedade afim quanto projetiva e mencionaremos sempre quais delas especificamente estaremos trabalhando.

Além disso, podemos tornar um polonômio homogêneo pela inclusão e exclusão de variáveis. Em nosso trabalho, trabalharemos apenas com a inclusão de variáveis, como definido a seguir.

Definição 2.1.9 *Seja $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ um polinômio de grau m. Definimos a* ***homogeneização*** *de f em respeito a x_{n+1}, por*

$$f_h = x_{n+1}^m \cdot f\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right).$$

Exemplo 2.1.10 *Considere $f(x, y) = x^5 + 3x^2y^2 - 7y^3$ em $\mathbb{F}_q[x, y]$.*

Note que $gr(f) = 5$, todavia não é um polinômio homogêneo. Assim, homogeneizando f em respeito a z, temos

$$f_h(x, y, z) = x^5 + 3x^2y^2z - 7y^3z^2.$$

Já vimos que no espaço projetivo $\mathbb{P}^n$ precisamos trabalhar com coordenadas homogêneas. Isto significa que necessariamente, temos de estudar funções racionais tais que tanto o numerador e o denominador sejam polinômios homogêneos e de mesmo grau.

Se considerarmos agora o subanel $R(\mathcal{X})$ de $k(x_0, x_1, \ldots, x_n)$, que consiste das funções racionais $\dfrac{f}{g}$, em que f e g são polinômios homogêneos de mesmo grau e $g \notin I_P$, onde I_P é um ideal primo. Veremos que $R(\mathcal{X})$ tem um único ideal maximal $M(\mathcal{X}) \subsetneqq I_P$, consistindo das funções racionais $\dfrac{f}{g}$, com $f \in I_P$ e o corpo de funções $k(\mathcal{X})$ é por definição o quociente $k(\mathcal{X})$ / $M(\mathcal{X})$.

De fato, notemos que $R(\mathcal{X}) = \left\{\dfrac{f}{g} \in k(\mathcal{X}) : g \notin I_P\right\}$.

Seja $M(\mathcal{X}) = \left\{\dfrac{f}{g} \in R(\mathcal{X}) : f \in I_P\right\}$. Mostremos que $M(\mathcal{X})$ de fato é um ideal.

Sejam $\dfrac{f_1}{g_1}, \dfrac{f_2}{g_2} \in M(\mathcal{X})$. Logo, $\dfrac{f_1}{g_1} + \dfrac{f_2}{g_2} = \dfrac{f_1g_2 + g_1f_2}{g_1g_2} \in M(\mathcal{X})$, pois $f_1g_2,\ g_1f_2 \in I_P$ e, como I_P é um ideal primo, $g_1g_2 \notin I_P$.

Sejam agora $\dfrac{f}{g} \in M(\mathcal{X})$ e $h = \dfrac{f_1}{g_1} \in R(\mathcal{X})$, com $g_1 \notin I_P$. Assim, $\dfrac{f}{g} \cdot h = \dfrac{ff_1}{gg_1} \in M(\mathcal{X})$, pois I_P é ideal primo e portanto, $gg_1 \notin I_P$.

Logo, $M(\mathcal{X})$ é um ideal.

Mostremos agora que $M(\mathcal{X})$ é maximal.

Suponha que exista um ideal J de $R(\mathcal{X})$ tal que $M(\mathcal{X}) \subsetneqq J \subseteq R(\mathcal{X})$.

Logo, existe $\dfrac{f}{g} \in J$, tal que $\dfrac{f}{g} \in M(\mathcal{X})$.

Daí, $f \notin J$ e $\dfrac{g}{f} \in R(\mathcal{X})$. Temos então

$$\frac{f}{g} \cdot \frac{g}{f} \in J \implies 1 \in J \implies J = R(\mathcal{X})$$

Finalmente, suponha que exista $M'(\mathcal{X}) := \left\{\dfrac{f'}{g'} \in k(\mathcal{X}) : f' \in I_P\right\}$ maximal, tal que $M'(\mathcal{X}) \subsetneqq R(\mathcal{X})$.

Como mostrado anteriormente, temos também $M(\mathcal{X}) \subsetneqq R(\mathcal{X})$.

Seja $\frac{f}{g} \in M(\mathcal{X})$. Como $M'(\mathcal{X})$ também é maximal, segue que $\frac{f}{g} \in M'(\mathcal{X})$. Logo, $M(\mathcal{X}) \subseteq M'(\mathcal{X})$.

De modo análogo, temos $M'(\mathcal{X}) \subseteq M(\mathcal{X})$, e portanto, $M(\mathcal{X}) = M'(\mathcal{X})$.

Assim, $M(\mathcal{X})$ é o único ideal maximal nas condições acima.

Definição 2.1.11 *Sejam $\mathcal{X}$ uma variedade projetiva, P um ponto em $\mathcal{X}$, U_P uma vizinhança de P e, f e g polinômios homogêneos de mesmo grau, com $g(P) \neq 0$. O quociente $\varphi := \frac{f}{g}$, definido em U_P, é chamado **regular** no ponto P, se $\varphi(P) = 0$.*

As funções que são regulares em todo ponto de U_P formam um anel que será denotado por $k[U_P]$.

Definição 2.1.12 *Seja $\mathcal{X}$ uma variedade projetiva e $P \in \mathcal{X}$. Definimos o **anel local** $O_P(\mathcal{X})$ do ponto P sobre $\mathcal{X}$ como sendo o conjunto das funções racionais que regulares em P, isto é,*

$$O_P(\mathcal{X}) = \left\{ \varphi = \frac{f}{g} : \ \varphi(P) = 0, \ P \in \mathcal{X} \right\}.$$

Tal anel tem um único ideal maximal, o qual denotaremos por M_P, que consiste das funções regulares em O_P que se anulam em P.

Em 2.1.6, vimos como podemos relacionar os espaços afim e projetivo. Nosso interesse agora é estender uma variedade afim para uma variedade projetiva de forma análoga. Considere então, um polinômio f em $k[x_1, \ldots, x_n]$. Seja f^* um polinômio homogêneo, associado à f, definido da seguinte forma

$$f^*(x_0, \ldots, x_n) := x_{n+1}^m \cdot f\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right),$$

onde $m = gr(f)$.

Seja $\mathcal{X}$ uma variedade afim em $\mathbb{A}^n$ definida pelo ideal primo I. Seja I^* o ideal primo gerado pelo conjunto $\{f^* : f \in I\}$. Então, I^* define uma variedade projetiva $\mathcal{X}^*$ em $\mathbb{P}^n$.

Definimos $\mathcal{X}^*_{x_0} := \{(x_0 : \ldots : x_n) \in \mathcal{X}^* : x_0 \neq 0\}$. Então, a aplicação

$$\begin{array}{rccc} h: & \mathcal{X} & \longrightarrow & \mathcal{X}^*_{x_0} \\ & (x_1, \ldots, x_n) & \longmapsto & (1 : x_1 : \ldots : x_n) \end{array},$$

é um isomorfismo.

Os pontos $(x_0 : \ldots : x_n) \in \mathcal{X}^*$ com $x_0 = 0$ são chamados de ***pontos no infinito*** da variedade afim $\mathcal{X}$.

Além disso, os corpos de funções $K(\mathcal{X})$ e $K(\mathcal{X}^*)$ são isomorfos por $\frac{f}{g} \longmapsto \frac{f^* x_0^m}{g^*}$, onde $m = gr(g) - gr(f)$.

Antes de ilustrarmos tais conceitos, vale observar que $\mathcal{X}^*_{x_0}$ pode ser definido para qualquer coordenada.

Exemplo 2.1.13 *Considere em $\mathbb{P}^2$ com coordenadas projetivas $(x : y : z)$ a variedade projetiva $\mathcal{X}$ dada por $xz - y^2 = 0$*

Note que o polinômio que define $\mathcal{X}$ é homogêneo. Todavia, o mesmo pode ter sido homogeneizado em respeito a x ou a z. Assim, quando $z = 0$, o polinômio $xz - y^2$ é zero se, e somente se, $y = 0$. Logo, se $x \neq 0$, o ponto $P = (1 : 0 : 0)$ é um ponto no infinito de $\mathcal{X}$. Quando $x = 0$, o polinômio $xz - y^2$ também se anula quando $y = 0$. Logo, se $z \neq 0$, o ponto $Q = (0 : 0 : 1)$ também é um ponto no infinito de $\mathcal{X}$.

Agora, observe que a função racional $\varphi = \dfrac{2xz + z^2}{y^2 + z^2}$ não é regular em Q, pois $\varphi(Q) = 1 \neq 0$.

Substituindo y^2 por xz em φ, temos $\varphi' = \dfrac{2x + z}{x + z}$ não regular em P, pois $\varphi'(P) = 2 \neq 0$.

Por outro lado, função $\psi = \dfrac{x^3 + y^3}{z^3}$ se anula em P e pode ser escrita como $\psi = \dfrac{y^3}{z^3} . \dfrac{y^3 + z^3}{y^3}$, pois

$$\frac{y^3}{z^3} \cdot \frac{y^3 + z^3}{z^3} = \frac{(y^2)^3 + y^3z^3}{z^6} = \frac{x^3z^3 + y^3z^3}{z^6} = \frac{x^3 + z^3}{z^3}.$$

Entretanto, $\dfrac{y^3}{z^3}$ é zero em P, mas $\dfrac{y^3 + z^3}{z^3}$ não é regular em P.

Ou seja, se $k = \mathbb{C}$, para pontos na vizinhança de P, há na topologia usual, uma correspondência um para um com $\dfrac{y}{z}$, o que não é verdadeiro para $\dfrac{x}{z}$. Este é um exemplo onde trabalhamos com o chamado parâmetro local, que será definido mais adiante.

De maneira particular, considerando apenas curvas em $\mathbb{A}^2$, temos a seguinte definição.

Definição 2.1.14 *Considere uma curva em $\mathbb{A}^2$ definida por $f(x, y) = 0$. Seja $P = (a, b)$ um ponto desta curva. Se pelo menos uma das derivadas parciais f_x ou f_y não se anula em P, então dizemos que P é um ponto* ***não-singular*** *da curva. Uma curva em que todos os pontos são não-singulares é chamada de* ***suave*** *ou* ***não-singular****.*

A curva então tem uma tangente no ponto P de equação $f_x(P)(x - a) + f_y(P)(y - b) = 0$. Definindo

$$d_P f := f_X(P)(X - a) + f_Y(P)(Y - b),$$

a tangente T_P em P é definida por $d_P f = 0$.

Se $g \in k[\mathcal{X}]$, não faria sentido em definir $d_P g$ da mesma forma, pois g só é definida por múltiplos módulo f.

Dado P um ponto da curva, observamos que d_P mapeia um elemento de $k[\mathcal{X}]$ por uma função linear definida na tangente T_P, isto é, passa a ser um elemento de T_P^*, ou em outras palavras,

$$\begin{array}{ccc} T_P & \longrightarrow & T_P^* \\ w & \longmapsto & w^* \end{array}$$

é um mapeamento de w.

Desde que $d_P f = 0$, se f é constante, podemos nos restringir às funções racionais em $m_P = M_P \subseteq O_P$. Então, a partir da regra do produto para diferenciação de funções, observamos que m_P^2 está no núcleo deste mapeamento.

De fato, sejam $\frac{f_1}{g_1},\ \frac{f_2}{g_2} \in m_P$.

Logo, $\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} \in m_P^2$ e $\left(\frac{f_1}{g_1} \cdot \frac{f_2}{g_2}\right)' = \frac{f_1' g_1 - f_1 g_1'}{g_1^2} \cdot \frac{f_2}{g_2} + \frac{f_1}{g_1} \cdot \frac{f_2' g_2 - f_2 g_2'}{g_2^2} = 0$, pois, $\frac{f_1}{g_1}$ e $\frac{f_2}{g_2}$ se anulam em P.

Então, do Teorema dos Isomorfismos, segue que $\frac{m_P}{m_P^2}$ é isomorfo a T_P^* por um ponto não singular que define um espaço de dimensão um.

Isto significa que podemos definir um ponto não singular de uma curva, exigindo que a dimensão do $\mathbb{F}_q-$espaço vetorial $\frac{m_P}{m_P^2}$ seja um.

Às curvas cujos pontos são todos não-singulares daremos o nome de ***suaves***. Assim, nos res tringindo apenas a estas curvas, temos a seguinte consequência.

Dado P um ponto de $\mathcal{X}$ e lembrando que o ideal maximal m_P do anel local O_P consiste das funções que se anulam em P, vemos que os outros elementos de O_P são invertíveis, logo unidades.

Desde que a dimensão de $dim_{\mathbb{F}_q}\left(\frac{m_P}{m_P^2}\right) = 1$, há um elemento t, gerador deste espaço, isto é, $\frac{m_P}{m_P^2} = \langle t \rangle$. Usaremos t também para denotar um elemento correspondente em m_P.

Podemos então descrever cada elemento z de O_P de forma única, como $z = ut^m$, onde u é a unidade e $m \in \mathbb{N}_0$. A função t, de O_P é chamada de ***parâmetro local*** em P e a função f será o parâmetro local de P se $d_P f \neq 0$ em T_P.

Temos então as seguintes possibilidades:

(i) Se $m > 0$, então P é um zero de multiplicidade m de z e escrevemos

$$m = ord_P(z) = v_P(z).$$

Onde $ord_P(z)$ e $v_P(z)$ representam, respectivamente, a ***ordem*** e a ***valorização discreta*** de z em P.

Logo, O_P é um ***anel de valorização discreta*** e elementos t com $v_P(t) = 1$ são parâmetros locais.

Além disso, podemos estender a ordem da função para $K(\mathcal{X})$ definindo

$$v_P\left(\frac{f}{g}\right) := v_P(f) - v_P(g).$$

(ii) Se $v_P(z) = -m < 0$, então dizemos que z tem um ***polo*** de ordem m em P.

(iii) Se $z \in K(\mathcal{X})$ com $v_P(z) = m$, então podemos escrever $z = at^m + z'$, onde $a \in K,\ a \neq 0$ e $v_P(z') > m$.

Para a construção de códigos, que veremos mais adiante, estaremos interessados em pontos que têm suas coordenadas no alfabeto $\mathbb{F}_q$. Tais pontos recebem um nome especial.

Definição 2.1.15 *Se k é o fecho algébrico de $\mathbb{F}_q$ e $\mathcal{X}$ é uma curva sobre k, então os pontos de $\mathcal{X}$ cujas coordenadas estão em $\mathbb{F}_q$ são chamados de* ***pontos racionais****.*

O conceito que veremos a seguir, pode ser entendido como um mecanismo de contagem de polos e zeros de uma função f em uma curva $\mathcal{X}$, além da informação de onde eles se econtram e quais são suas multiplicidades. Consideremos $\mathcal{X}$ uma curva algébrica suave projetiva sobre k.

Definição 2.1.16 *Um* ***divisor*** *é uma soma formal*

$$D = \sum_{P \in \mathcal{X}} n_P P,$$

em que $n_p \in \mathbb{Z}$ e é igual a zero a menos de um número finito de pontos P.

O conjunto dos divisores de $\mathcal{X}$, denotado por $Div(\mathcal{X})$, é um grupo aditivo com a adição formal. em $\mathcal{X}$.

Definição 2.1.17 *Um divisor D é chamado* ***divisor efetivo****, e o denotamos por $D \succcurlyeq 0$, se todos os coeficientes n_p são não-negativos.*

Definição 2.1.18 *Definimos o* ***grau*** *de um divisor D por $\sum n_P$.*

Lembrando que $v_P = ord_P$ é a valorização discreta de uma função, temos a seguinte definição

Definição 2.1.19 *Se f é uma função racional, não identicamente nula em $\mathcal{X}$, definimos o* ***divisor de*** *f por*

$$(f) := \sum_{P \in \mathcal{X}} v_P(f) P.$$

Em certo sentido, o divisor de f é um dispositivo que nos diz quais são seus zeros e polos com suas respectivas multiplicidades. Como f é uma função racional, em que numerador e denominador têm o mesmo grau, e como k é algebricamente fechado, segue que f possui o mesmo número de zeros e polos. Assim, o grau de um divisor de uma função racional é sempre zero.

Chamaremos o divisor (f) de uma função racional de ***divisor principal***. Os divisores $(f)_0 := \sum_{v_P(f)>0} v_P(f)P$ e $(f)_\infty := \sum_{v_P(f)<0} v_P(f)P$ são chamados, respectivamente, ***divisor de zeros*** e ***divisor de polos*** de f.

Dizemos que dois divisores D e D' são ***linearmente equivalentes***, e denotaremos por $D \equiv D'$, se $D - D'$ é um divisor principal.

Note que, tal relação é uma relação de equivalência.

Definição 2.1.20 *Seja D um divisor em uma curva $\mathcal{X}$. Definimos o espaço vetorial $\mathcal{L}(D)$ sobre $\mathbb{F}_q$ por*

$$\mathcal{L}(D) = \{f \in \mathbb{F}_q(\mathcal{X})^* : (f) + D \succcurlyeq 0\} \cup \{0\}.$$

Observe que, se $D = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j,\ \forall\ n_i, m_j > 0$, então $\mathcal{L}(D)$ é composto por 0 mais as funções que tem zeros de multiplicidade, no mínimo m_j, em Q_j $(1 \leqslant j \leqslant s)$ e que não tem polos, exceto possivelmente, nos pontos P_i com ordem máxima n_i $(1 \leqslant i \leqslant r)$.

Mostremos então, que este espaço tem dimensão finita. Antes, note que se $D \equiv D'$ e g é uma função racional tal que $(g) = D' - D$, então a aplicação $f \mapsto f \cdot g$ e o fato de que $(f.g) = (f) + (g)$ nos diz que $\mathcal{L}(D)$ e $\mathcal{L}(D')$ são isomorfos.

Teorema 2.1.21 *Seja $\mathcal{L}(D)$ como em 2.1.20. Então,*

(i) $\mathcal{L}(\mathcal{D}) = 0$, *se* $gr(D) < 0$;

(ii) $l(D) := dim_k \mathcal{L}(D) \geqslant 1 + gr(D)$.

Demonstração: *(i)* Por hipótese $gr(D) < 0$, então para qualquer função $f \in k(\mathcal{X})^*$ temos que $gr((f) + D) < 0$, ou seja, $f \notin \mathcal{L}(D)$, o que implica que $\mathcal{L}(D) = \{0\}$.

(ii) Suponhamos que $f \in \mathcal{L}(D)$ com $f \neq 0$. Logo, $D' := D + (f)$ é um divisor efetivo e, pelo que vimos anteriormente, $\mathcal{L}(D')$ tem a mesma dimensão de $\mathcal{L}(D)$. Logo, podemos assumir que D é efetivo e da forma $D = \sum_{i=1}^{r} n_i P_i,\ (n_i \geqslant 0,\ 1 \leqslant i \leqslant r)$. Agora, no ponto P_i, podemos fazer uma correspondência entre f e um elemento do espaço vetorial $(t_i^{-n_i} O_{P_i})/O_{P_i}$ de dimensão n_i, em que t_i é um parâmetro local em P_i. Assim, obtemos uma aplicação de f na soma direta desses espaços vetoriais (no caso de $f = 0$, levamos 0 no espaço nulo). Esta aplicação é linear e se f está no núcleo desta aplicação significa que f não possui nenhum pólo em qualquer um dos pontos P_i, ou seja, f é constante. Daí, segue que $dim_k \mathcal{L}(D) \leq 1 + \sum_{i=1}^{r} n_i = 1 + gr(D)$. ■

Considere $\mathcal{X}$ em $\mathbb{A}^2$ uma curva suave afim definida por $f(X, Y) = 0$, $P = (a, b)$ um ponto de $\mathcal{X}$, T_P a tangente em P, definida por $d_P f = f_x(a, b)(X - a) + f_y(a, b)(Y - b) = 0$ e $\Phi[\mathcal{X}]$ o conjunto de todos os mapeamentos que associam cada ponto $P \in \mathcal{X}$ a um elemento de T_P^*, isto é, o conjunto de todas as funções lineares da forma

$$\begin{array}{rccc} \varphi\ : & \mathcal{X} & \longrightarrow & k[\mathcal{X}] \\ & P & \longmapsto & d_P\varphi \in T_P^* \end{array}$$

Definição 2.1.22 *Um elemento φ de $\Phi[\mathcal{X}]$ é chamado de* ***forma diferencial regular*** *em $\mathcal{X}$, se todo ponto $P \in \mathcal{X}$ tem uma vizinhança U_P tal que nesta vizinhança, φ pode ser representado por*

$$\varphi = \sum_{i=1}^{n} f_i . dg_i,$$

onde f_i e g_i são funções regulares em U_P.

Para o nosso caso, as formas diferenciais em $\mathcal{X}$ formam um $k[\mathcal{X}]$-módulo, denotado por $\Omega[\mathcal{X}]$. Tal módulo é gerado por elementos df, com $f \in k[\mathcal{X}]$ munido das relações

(i) $d(f+g) = df + dg$;

(ii) $d(f.g) = g.df + f.dg$;

(iii) $d(a) = 0,\ \forall\ a \in \mathbb{F}_q$.

Todavia, para as formas diferenciais racionais, temos a relação

(iv) $d\left(\dfrac{f}{g}\right) = \dfrac{g\ df - f\ dg}{g^2}$.

Vamos agora extender a definição de forma diferencial racional para curvas projetivas suaves $\mathcal{X}$. Para tanto, consideremos o par (U, ω), onde $\emptyset \neq U \subseteq \mathcal{X}$ e $\omega = g\ df$ em U. Dados os pares (U, ω) e (V, η), dizemos que eles são equivalentes se $\omega = \eta$ em $U \cap V$.

Definição 2.1.23 *Definimos a* ***forma diferencial racional*** *para uma curva projetiva suave $\mathcal{X}$ como sendo a classe de equivalência para a relação acima.*

Para simplificarmos as notações, chamaremos as formas diferenciais racionais em $\mathcal{X}$ apenas por ***diferenciais*** e denotaremos o espaço dos diferenciais em $\mathcal{X}$ por $\Omega(\mathcal{X})$.

Teorema 2.1.24 *[[8], Teorema 10.4.2] O espaço $\Omega(\mathcal{X})$ tem dimensão 1 sobre $k(\mathcal{X})$; em uma vizinhança de um ponto P com parâmetro local t, um diferencial ω pode ser representado como $\omega = f.dt$, onde f é uma função racional.*

Definição 2.1.25 *Definimos o* ***divisor*** (ω) *do diferencial ω em uma curva projetiva suave $\mathcal{X}$ por*

$$(\omega) := \sum_{P \in \mathcal{X}} v_P(f_P)P,$$

onde $\omega = f_P dt_P$ é a representação local de ω e v_P é a ***valorização*** *em O_P.*

Se ω é um diferencial, o divisor $W = (\omega)$ é chamado de ***divisor canônico***. Se ω' é outro diferencial não-nulo, então $\omega' = f\omega$ para alguma função racional f. Assim, $(\omega') = W' = W$ e, portanto, divisores canônicos formam uma classe de equivalência, que também é denotada por W.

No que se segue, denotaremos, para um divisor D, $\ell(D) := dim_k \mathcal{L}(D)$.

Definição 2.1.26 *Seja $\mathcal{X}$ uma curva projetiva suave sobre $\mathbb{F}_q$. Definimos o* ***gênero*** *g de $\mathcal{X}$ por $g = \ell(W)$.*

Para uma curva projetiva não-singular temos a chamada fórmula de Plücker.

Teorema 2.1.27 *[[8], Teorema 10.4.6] Seja $\mathcal{X}$ uma curva projetiva não-singular de grau d em $\mathbb{P}^2$. Então,*

$$g = \frac{1}{2}(d-1)(d-2).$$

Definição 2.1.28 *Seja D um divisor em uma curva algébrica projetiva não-singular $\mathcal{X}$. Definimos o conjunto*

$$\Omega(D) := \{\omega \in \Omega(\mathcal{X}) : (\omega) - D \succcurlyeq 0\}$$

*e denotamos $\delta(D) = \dim_k \Omega(D)$ o chamado **índice de especialidade** do divisor D.*

A conecção com funções é estabelecida no seguinte teorema.

Teorema 2.1.29 *Seja D um divisor em uma curva algébrica suave projetiva $\mathcal{X}$. Então,*

$$\delta(D) = l(W - D).$$

Demonstração: Se $W = (\omega)$, definimos o seguinte mapeamento linear

$$\begin{array}{rccc} \varphi & : & \mathcal{L}(W-D) & \longrightarrow & \Omega(D) \\ & & f & \longmapsto & \varphi(f) = f\ \omega \end{array}.$$

Vejamos que φ é um isomorfismo.

De fato, claramente, φ é linear e para $f \in \mathcal{L}(W-D)$ temos que $(f\ w) = (f) + (w) \geq -(W-D) + W = D$. Assim, $f\ \omega \in \Omega(D)$. Agora, seja $f \in \mathcal{L}(W-D)$ tal que $\varphi(f) = f\ \omega = 0$. Logo, $f = 0$ e temos que $Ker(\varphi) = \{0\}$ e φ é injetora. Finalmente, temos que φ é sobrejetora, pois dado $\omega_1 \in \Omega(D)$, do Teorema 2.1.24 sabemos que $\Omega(\mathcal{X})$ tem dimensão 1 sobre $k(\mathcal{X})$ e, assim, $\omega_1 = f\ \omega$, para algum $f \in k(\mathcal{X})$. Agora, $(f) + W = (f) + (\omega) = (f\ \omega) = (\omega_1) \geq D$. Logo, $(f) \geq -(W-D) \Rightarrow f \in \mathcal{L}(W-D)$, e temos que φ é sobrejetora.

■

O resultado a seguir, é muito importante não só na geometria algébrica como para o tratamento de códigos sobre curvas algébricas. A demonstração deste resultado pode ser encontrada em [10].

Teorema 2.1.30 ***(Riemann-Roch)*** *Seja D um divisor em uma curva algébrica suave projetiva $\mathcal{X}$ de gênero g. Então, para qualquer divisor canônico W, temos*

$$l(D) - l(W-D) = gr(D) - g + 1.$$

Este teorema nos permite determinar o grau de um divisor canônico da seguinte maneira.

Corolário 2.1.31 *Para um divisor canônico W, temos*

$$gr(W) = 2g - 2.$$

Demonstração: Observemos, primeiramente, que todas as funções regulares em uma curva projetiva $\mathcal{X}$ são constantes. Logo, em particular para $W = 0$ para a diferencial nula, temos $\mathcal{L}(0) = \mathbb{F}_q$, isto é, $l(0) = dim_{\mathbb{F}_q}\mathcal{L}(W) = 1$.

Assim, fazendo $D = W$ no Teorema de Riemann-Rock e pela definição de gênero, segue que

$$\begin{aligned} l(W) - l(0) &= gr(W) - g + 1 \implies \\ l(W) &= gr(W) - g + 2 \implies \\ g &= gr(W) - g + 2 \implies \\ gr(W) &= 2g - 2. \end{aligned}$$

■

Corolário 2.1.32 *Seja D um divisor em uma curva algébrica suave projetiva $\mathcal{X}$ de gênero g tal que $gr(D) > 2g - 2$. Então,*

$$l(D) = gr(D) - g + 1.$$

Demonstração: Basta mostrarmos que $l(W - D) = 0$ no Teorema de Riemann-Roch.

Observemos pelo Corolário 2.1.31, que $gr(W - D) < 0$. Logo, pelo Teorema 2.1.21 *(i)*, temos $\mathcal{L}(W - D) = 0$, o que implica $l(W - D) = dim_{\mathbb{F}_q}\mathcal{L}(W - D) = 0$.

E o resultado segue.

■

2.2 Códigos Sobre uma Curva Algébrica $\mathcal{X}$

Seja $\mathcal{X}$ uma curva algébrica suave projetiva de gênero g sobre $\mathbb{F}_q$. Sejam $P_1, \ldots, P_n$ pontos racionais sobre $\mathcal{X}$, $D := P_1 + \cdots + P_n$ e G um divisor cujo suporte é disjunto do suporte de D.

Definimos o ***código de Goppa algébrico geométrico*** (ou simplesmente código de Goppa geométrico) $\mathcal{C}(D, G)$ como sendo a imagem da aplicação linear

$$\begin{array}{rccc} \alpha: & \mathcal{L}(G) & \longrightarrow & \mathbb{F}_q^n \\ & f & \longmapsto & \alpha(f) = (f(P_1), \ldots, f(P_n)) \end{array}.$$

Isto é, $\mathcal{C}(D,G) = Im(\alpha)$. No caso de $G = aP$ para algum ponto racional de $\mathcal{X}$ e D for a soma dos outros pontos racionais de $\mathcal{X}$, dizemos que o código de Goppa geométrico $\mathcal{C}_(D, aP)$ é um ***código pontual***.

Note que $\mathcal{C}(D,G)$ tem comprimento n. O teorema a seguir nos diz como encontrar sua dimensão e uma cota para sua distância mínima.

Teorema 2.2.1 *Seja $\mathcal{C}(D,G)$ um código de Goppa algébrico gemétrico. Então,*

(i) $dim\mathcal{C}(D,G) = k = dim\mathcal{L}(G) - dim\mathcal{L}(G-D)$;

(ii) $\mathcal{C}(D,G)$ *tem distância mínima* $d \geqslant n - gr(G)$.

Demonstração: *(i)* A aplicação α é sobrejetiva sobre sua imagem, é $\mathcal{C}(D,G)$. Note que, $Ker(\alpha) = \{f \in \mathcal{L}(G)\ ;\ v_{P_i}(f) > 0,\ i = 1,\ldots,n\} = \mathcal{L}(G-D)$. Então, $\mathcal{L}(G)/\mathcal{L}(G-D) \simeq \mathcal{C}(D,G)$ e, portanto, $k = dim\mathcal{L}(G) - dim\mathcal{L}(G-D)$.

(ii) Suponhamos que $\mathcal{C}(D,G) \neq 0$ e seja $d = \omega(\alpha(f))$ para algum $0 \neq f \in \mathcal{L}(G)$. Então, existem $n-d$ pontos $P_{i_1},\ldots,P_{i_{n-d}} \in Supp(D)$, tais que $f(P_{i_j}) = 0$, para $j = 1,\ldots,n-d$. Assim, $f \in \mathcal{L}(G-E)$, em que $E = P_{i_1} + \cdots + P_{i_{n-d}}$. Como $gr(G-E) \geq 0$, segue que $d \geq n - gr(G)$.

■

Corolário 2.2.2 *Se $gr(G) < n$, temos o seguinte.*

(i) α *é injetiva e* $\mathcal{C}(D,G)$ *é um* $[n,k,d]$ *código em que*

$$d \geq n - gr(G) \quad e \quad k = dim\mathcal{L}(G) \geq gr(G) + 1 - g,$$

donde segue que $k + d \geq n + 1 - g$.

(ii) Se $2g - 2 < gr(G) < n$, *então* $k = gr(G) + 1 - g$.

(iii) Se $\{f_1,\ldots,f_k\}$ *é uma base de* $\mathcal{L}(G)$, *então*

$$M = \begin{pmatrix} f_1(P_1) & \ldots & f_1(P_n) \\ \vdots & \vdots & \vdots \\ f_k(P_1) & \ldots & f_k(P_n) \end{pmatrix}$$

é uma matriz geradora do código $\mathcal{C}(D,G)$.

Demonstração: *(i)* Como $gr(G-D) < 0$, segue que $dim\mathcal{L}(G-D) = 0$ e como este é o núcleo da aplicação α, temos que α é injetiva.

(ii) Como $gr(G) < 2g-2$, segue que $dim\mathcal{L}(W-G) = 0$ e do Teorema de Riemann-Roch obtemos $k = gr(G) + 1 - g$.

■

Sejam P um ponto da curva $\mathcal{X}$ de gênero g, t um parâmetro local em P e $\omega = f\,dt$ a representação local de ω. Podemos escrever $f = \sum_i a_i t^i$. Definimos o ***resíduo*** $Res_P(\omega)$ de

ω no ponto P como sendo a_{-1}. É possível mostrar que este parâmetro independe da escolha do parâmetro local t. O resultado a seguir, é um resultado importante na teoria de curvas algébricas e é conhecido como Teorema dos Resíduos. Para um estudo sobre a teoria de curvas algébricas sobre corpos finitos veja [7].

Teorema 2.2.3 *Se ω é um diferencial em uma curva projetiva não-singular $\mathcal{X}$, então*

$$\sum_{P \in \mathcal{X}} Res_P(\omega) = 0.$$

Considere a aplicação

$$\begin{array}{rccc} \alpha^* : & \Omega(G-D) & \longrightarrow & \mathbb{F}_q^n \\ & \eta & \longmapsto & (Res_{P_1}(\eta), \ldots, Res_{P_n}(\eta)) \end{array}.$$

Definimos o código linear $\mathcal{C}^*(D,G)$ como sendo a imagem de α^*, isto é, $\mathcal{C}^*(D,G) = Im(\alpha^*)$.

Tal código tem comprimento n e os demais parâmetros são tratados no teorema a seguir.

Teorema 2.2.4 *(i)* $dim_{\mathbb{F}_q} \mathcal{C}^*(D,G) = k^* = n - gr(G) + g - 1$*;*

(ii) $\mathcal{C}^*(D,G)$ tem distância mínima $d^* \geqslant gr(G) - 2g + 2$.

Demonstração: Ver [8], Teorema 10.6.7.

■

Segue agora o teorema que relaciona os códigos de Goppa e Reed-Solomon generalizados.

Teorema 2.2.5 *Os códigos $\mathcal{C}(D,G)$ e $\mathcal{C}^*(D,G)$ são códigos duais.*

Demonstração: Notemos, pelos Teoremas 2.2.1 e 2.2.4, que $k + k^* = n$. Então, basta tomarmos duas palavras quaisquer, uma de cada código, e mostrar que o produto interno entre elas é igual a zero.

Sejam $f \in \mathcal{L}(G)$ e $\eta \in \Omega(G-D)$. Pelas definições de $\mathcal{C}(D,G)$ e $\mathcal{C}^*(D,G)$, o diferencial $f\eta$ não tem polos, exceto possivelmente polos de ordem 1, nos pontos $P_1, \ldots, P_n$.

Além disso, o resíduo de $f\eta$ em P_i é igual a $f(P_i)Res_{P_i}(\eta)$, para $i = 1, \ldots, n$. Pelo Teorema 2.2.3, a soma dos resíduos de $f\eta$ sobre todos os polos (isto é, sobre os pontos P_i) é igual a zero. Assim, temos que

$$< \alpha(f), \alpha^*(\eta) >= \sum_{i=1}^{n} f(P_i)Res_{P_i}(\eta) = 0.$$

■

2.3 Automorfismos e Estrutura de Módulo

Seja $\mathcal{C}(D,G)$ um código de Goppa geométrico sobre uma curva $\mathcal{X}$. O resultado a seguir nos mostra como associar automorfismos de $\mathcal{X}$ a automorfismos de $\mathcal{C}(D,G)$.

Proposição 2.3.1 *Seja $Aut(\mathcal{X})$ o grupo de automorfismos de $\mathcal{X}$ sobre $\mathbb{F}_q$ e considere o subgrupo*

$$Aut_{D,G}(\mathcal{X}) = \{\sigma \in Aut(\mathcal{X}) \,:\, \sigma(D) = D \text{ e } \sigma(G) = G\}\,.$$

Cada $\sigma \in \mathrm{Aut}_{D,G}(\mathcal{X})$ induz um automorfismo

$$\sigma(f(P_1),\ldots,f(P_n)) = (f(\sigma^{-1}(P_1)),\ldots,f(\sigma^{-1}(P_n))) \tag{2.1}$$

de $\mathcal{C}(D,G)$.

Demonstração: Veja [5], Lema II.A.1.

■

Corolário 2.3.2 *Sejam $\sigma \in \mathrm{Aut}_{D,G}(\mathcal{X})$ e $Supp(D) = O_1 \cup \ldots \cup O_r$ a decomposição do suporte de D em órbitas disjuntas obtidas pela ação de σ. Então, as coordenadas das palavras-código correspondentes aos pontos de cada órbita O_i são permutadas ciclicamente por σ.*

A seguir, veremos como um código de Goppa geométrico $\mathcal{C}(D,G)$ pode ser associado a um submódulo do módulo livre $\mathbb{F}_q[t]^r$.

Para $\sigma \in \mathrm{Aut}_{D,G}(\mathcal{X})$ os pontos do suporte de D se decompõem em órbitas disjuntas obtidas pela ação de σ, digamos que $Supp(D) = O_1 \cup \ldots \cup O_r$. Vamos denotar os pontos de D por $P_{i,j}$, em que $i = 1,\ldots,r$ e, para cada i, $j = 0,\ldots,|O_i|-1$.

Em cada uma das órbitas O_i, escolhemos um ponto P qualquer em O_i, que será denotado por $P_{i,0}$, e denotamos os demais pontos de O_i por

$$P_{i,j} = \sigma^j(P_{i,0}).$$

Assim, temos que $P_{i,|O_i|} = P_{i,0}$ e, por convenção, escreveremos $P_{i,-1} = \sigma^{-1}(P_{i,0}) = P_{i,|O_i|-1}$.

No Corolário 2.3.2, vimos que as coordenadas das palavras-código correspondentes aos pontos de cada órbita O_i são permutadas ciclicamente por σ. Reorganizando estas coordenadas, podemos representar as palavras-código como r-uplas de polinômios em uma variável

$$(h_1(t),\ldots,h_r(t)) \in \mathbb{F}_q[t]^r \tag{2.2}$$

em que, para cada $i = 1,\ldots,r$,

$$h_i(t) = \sum_{j=0}^{|O_i|-1} f(P_{i,j})t^j$$

e $f \in \mathcal{L}(G)$.

A maneira mais direta de incorporar as permutações cíclicas das entradas é ver as r-uplas de (2.2) como elementos do $\mathbb{F}_q[t]$-módulo:

$$M = \bigoplus_{i-1}^{r} \mathbb{F}_q[t]/\langle t^{|O-i|-1}\rangle. \tag{2.3}$$

Observação 2.3.3 *O conjunto C das r-uplas obtidas das palavras do código $\mathcal{C}(D,G)$ é fechado com relação à soma. Além disso, a mutiplicação de uma r-upla de polinômios, como em (2.2), por t nos dará*

$$\begin{aligned} t \cdot h_i(t) &= \sum_{j=0}^{|O_i|-1} f(P_{i,j})t^{j+1} \\ &\equiv \sum_{j=0}^{|O_i|-1} f(P_{i,j-1})t^{j} \quad \mod \langle t^{|O_i|}-1\rangle \\ &= \sum_{j=0}^{|O_i|-1} f(\sigma^{-1}(P_{i,j}))t^{j}. \end{aligned} \tag{2.4}$$

Comparando com (2.1), podemos observar que um elemento de C multiplicado por t é o mesmo que aplicar o automorfismo do código induzido por σ. Logo, C é fechado pela multiplicação por t.

Com estas observações, temos o seguinte resultado.

Proposição 2.3.4 *Seja C o $\mathbb{F}_q$-espaço vetorial do módulo M, dado em (2.3), formado pelas palavras do código $\mathcal{C}(D,G)$. Então, C é um $\mathbb{F}_q[t]$-submódulo de M com respeito à multiplicação por t, dada em (2.4).*

Demonstração: Segue da definição de submódulo e da Observação 2.3.3.

■

Consideremos o $\mathbb{F}_q[t]$-submódulo $\overline{C}$ do módulo livre $\mathbb{F}_q[t]^r$ gerado pelas palavras do código $\mathcal{C}(D,G)$. Em outras palavras, $\overline{C}$ é a imagem inversa $\pi^{-1}(C)$ da aplicação sobrejetiva

$$\pi \ : \ \mathbb{F}_q[t]^r \longrightarrow \bigoplus_{i=1}^{r} \mathbb{F}_q[t]/\langle t^{|O_i|}-1\rangle.$$

É neste sentido que o código $\mathcal{C}(D,G)$ pode ser associado a um submódulo de um módulo livre sobre $\mathbb{F}_q[t]$ e, assim, a teoria de bases de Gröbner para módulos pode ser aplicada.

Observação 2.3.5 *Não entraremos em detalhe, mas observamos que usando o Corolário 2.3.2, se pode fazer uma associação análoga ao dual do código $\mathcal{C}(D,G)$.*

Capítulo 3

Codificação de Certos Códigos de Goppa Geométricos

3.1 Sistemática de Codificação

Observamos que a palavra "certos"deve ser colocada pois, como vimos no final do capítulo anterior, a associação de um código de Goppa geométrico $\mathcal{C}(D,G)$ com um submódulo depende da existência de um automorfismo σ que fixa cada um dos divisores D e G.

Seja $C = \mathcal{C}(D,G)$ um código de Goppa geométrico de comprimento n e dimensão k, e que pode ser associado a um submódulo como no capítulo anterior. Vimos que as palavras de C podem ser associadas a r-uplas da forma $h = (h_1(t), \ldots, h_r(t))$. Usando a ordem POT tomamos, em uma ordem decrescente, k monômios não-padrões $m_l = t^{i_l}e_{j_l}$, $l = 1, \ldots, k$. Para cada $h = (h_1(t), \ldots, h_r(t))$ associada a uma palavra de C, seja $VC(h) \in \mathbb{F}_q^n$ o vetor dos coeficientes dos termos de h ordenados utilizando a ordem POT.

Sistemática de codificação: Sejam $C = \mathcal{C}(D,G)$ um código de Goppa gemétrico de comprimento n e dimensão k, $\overline{C} \subseteq \mathbb{F}_q[t]^r$ o submódulo associado a C e $\mathcal{G} = \{g_1, \ldots, g_r\}$ uma base de Gröbner de $\overline{C}$. Seja $\{m_1, \ldots, m_k\}$ os monômios não-padrões obtidos como no paragráfo anterior. Dado $w = (w_1, \ldots, w_k) \in \mathbb{F}_q^k$, defina $f := \sum_{i=1}^{k} w_i m_i$. Daí, escreva $f = a_1g_1 + \ldots a_rg_r + R$ e, como $f - R \in \overline{C}$, $VC(f-R) \in C$.

Para os dois exemplos a seguir, consideraremos o código pontual $C = \mathcal{C}(D, 19P_\infty)$ construído sobre a curva Hermitiana $\mathcal{H}_3$ definida sobre $\mathbb{F}_9$ pela equação

$$x^4 = y^3 + y.$$

Esta curva tem gênero $g = 3$ e possui 27 pontos $\mathbb{F}_9$-racionais mais o ponto no infinito $P_\infty = (0:1:0)$. Pelo Teorema de Riemman-Roch (Teorema 2.1.30) segue que

$$dim_{\mathbb{F}_9}\mathcal{L}(19P_\infty) \;=\; 19 + 1 - 3 \;=\; 17.$$

Assim, C tem comprimento $n = 27$ e dimensão $k = 17$.

Exemplo 3.1.1 *Seja α é um gerador de $\mathbb{F}_9\backslash\{0\}$ e considere σ dado por*

$$\sigma : \begin{cases} x & \longmapsto & \alpha x \\ y & \longmapsto & \alpha^4 y \end{cases}$$

Não é difícil ver que σ é um automorfismo de $\mathcal{H}_3$. O automorfismo σ fixa P_∞, já que $\sigma(P_\infty) = (0 : \alpha^4 : 0) = P_\infty$ e sob a ação de σ os outros 27 pontos racionais de $\mathcal{H}_3$ se dispõem nas seguintes 5 órbitas:

$O_1 = \{(1, \alpha^7), (\alpha, \alpha^3), (\alpha^2, \alpha^7), (\alpha^3, \alpha^3), (\alpha^4, \alpha^7), (\alpha^5, \alpha^3), (\alpha^6, \alpha^7), (\alpha^7, \alpha^3)\}$,
$O_2 = \{(1, \alpha^4), (\alpha, 1), (\alpha^2, \alpha^4), (\alpha^3, 1), (\alpha^4, \alpha^4), (\alpha^5, 1), (\alpha^6, \alpha^4), (\alpha^7, 1)\}$,
$O_3 = \{(1, \alpha^5), (\alpha, \alpha), (\alpha^2, \alpha^5), (\alpha^3, \alpha), (\alpha^4, \alpha^5), (\alpha^5, \alpha), (\alpha^6, \alpha^5), (\alpha^7, \alpha)\}$,
$O_4 = \{(0, \alpha^2), (0, \alpha^6)\}$ *e*
$O_5 = \{(0, 0)\}$

Usando tal decomposição, podemos associar C a um submódulo $\overline{C} \subseteq \mathbb{F}_9[t]^5$ e escrever as palavras do código $\mathcal{C}(D, 19P_\infty)$ como quíntuplas da forma

$$(h_1(t), h_2(t), h_3(t), h_4(t), h_5(t)) \in \mathbb{F}_9[t]^5$$

Note que, x tem polo de ordem 3 em P_∞, y tem polo de ordem 4 em P_∞ e

$$\{1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3, x^3y, x^2y^2, xy^3, y^4, x^3y^2, x^2y^3, xy^4\}$$

é uma base para $\mathcal{L}(19P_\infty)$.

Usando a ordem POT em $\mathbb{F}_9[t]^5$, calculamos, pelo Algoritmo de Buchberger a seguinte base de Gröbner $\mathcal{G} = \{g_1, g_2, g_3, g_4, g_5\}$ para o submódulo $\overline{C}$ de $\mathbb{F}_9[t]^5$.

$$\begin{aligned} g_1 &= (1, \alpha^6, \alpha t + \alpha t^4 + \alpha^6 t^3 + \alpha^2 t^2 + \alpha t + \alpha^2, \alpha t^2 + \alpha, 1) \\ g_2 &= (0, t + \alpha^5, t^5 + \alpha^5 t^4 + \alpha^7 t + \alpha^7 t + \alpha^7, \alpha^2 t + \alpha^4, 1) \\ g_3 &= (0, 0, t^6 + \alpha^6 t^5 + \alpha^2 t^4 + \alpha^7 t^3 + \alpha t^2 + \alpha^4 t + \alpha^5, \alpha^3 t + \alpha^3, \alpha^7) \\ g_4 &= (0, 0, 0, t^2 - 1, 0) \\ g_5 &= (0, 0, 0, 0, t - 1) \end{aligned}$$

A partir daí, tomamos

- $m_1 = t^7 e_1,\ m_2 = t^6 e_1,\ m_3 = t^5 e_1,\ m_4 = t^4 e_1,\ m_5 = t^3 e_1,\ m_6 = t^2 e_1,\ m_7 = t e_1,\ m_8 = 1 e_1$
- $m_9 = t^7 e_2,\ m_{10} = t^6 e_2,\ m_{11} = t^5 e_2,\ m_{12} = t^4 e_2,\ m_{13} = t^3 e_2,\ m_{14} = t^2 e_2,\ m_{15} = t e_2$
- $m_{16} = t^7 e_3,\ m_{17} = t^6 e_3$

Vamos codificar $\omega = (0, 0, 0, 0, 0, 0, \alpha, 0, 0, 0, 0, 0, 0, 0, 1, 0, \alpha^3) \in \mathbb{F}_9^{17}$.
Primeiramente, definimos

$$\begin{aligned} f &:= \sum_{i=1}^{17} \omega_i m_i \\ &= \alpha t e_1 + t e_2 + \alpha^3 t_3 \\ &= (\alpha t, t, \alpha^3 t^6, 0, 0) \ \in \ \mathbb{F}_9[t]^5. \end{aligned}$$

Usando o Algoritimo A.0.9 temos:

$$\alpha t g_1 \ = \ (\alpha t, \alpha^7 t, \alpha^2 t^6 + \alpha^2 t^5 + \alpha^7 t^4 + \alpha^3 t^3 + \alpha^2 t^2 + \alpha^3 t, \alpha^3 t^2 + \alpha^2 t, \alpha t).$$

Assim,

$$f - \alpha t g_1 \ = \ (0, 2\alpha t, -2t^6 - \alpha^2 t^5 - \alpha^7 t^4 - \alpha^3 t^3 - \alpha^2 t^2 - \alpha^3 t, -\alpha^3 t^2 - \alpha^2 t, -\alpha t).$$

Daí, dividindo $d_1 e_1 = f_1 = \alpha t$ por $g_{1_1} = 1$, temos o quociente αt e resto

$$R_1 = 0 e_1.$$

Dividindo $d_2 e_2 = (f - \alpha t g_1) e_2$ por g_{2_2}, temos o quociente 2α e resto

$$R_2 = (-2\alpha^6) e_2.$$

Segue então que $d_3 = f_\alpha t g_1 - 2\alpha g_2 - R_2 = (0, -4\alpha^6, -2t^6 - t^5 + t^4 + (-1 - 2\alpha)t^3 - \alpha^2 t^2 + (-1 - 2\alpha)t - 2\alpha, -\alpha^3 t^2 + t - 2\alpha^5, -2t - 2\alpha)$. Logo, dividindo $d_3 e_3$ por g_{3_3}, temos o quociente -2 e resto

$$R_3 = (-\alpha t^5 - 2\alpha t^4 - t^2 - 2\alpha t - \alpha) e_3.$$

Temos então $d_4 = f_\alpha t g_1 - 2\alpha g_2 - R_2 + 2g_3 - R_3 = (0, -4\alpha^6, 0, -\alpha^3 t^2 - \alpha^2 t - 2, -2t + 2)$. Daí, dividindo $d_4 e_4$ por g_{4_4}, temos $-\alpha^3$ como quociente

$$R_4 = (-\alpha^2 t - 2\alpha - 1) e_4.$$

como resto.

E por fim, $d_5 = f_\alpha t g_1 - 2\alpha g_2 - R_2 + 2g_3 - R_3 + \alpha^3 g_4 - R_4 = (0, -\alpha^6, 0, -2\alpha^2 t - 1, -2t + 2)$. E dividindo $d_5 e_5$ por g_{5_5}, temos o quociente -2 e resto

$$R_5 = 0 e_5.$$

Assim,

$$\begin{aligned} R &= (R_1, R_2, R_3, R_4, R_5) \\ &= (0, -2\alpha^6, -\alpha t^5 - 2\alpha t^4 - t^2 - 2\alpha t - \alpha, -\alpha^2 t - 2\alpha - 1, 0). \end{aligned}$$

Logo, $f - R = (\alpha t, t + 2\alpha^6, \alpha^3 t^6 - 2\alpha t^5 + 2\alpha t^4 + t^2 + 2\alpha t + \alpha, \alpha^2 t + 2\alpha + 1, 0) \in \overline{C}$.
Portanto,

$$VC(f - R) \;=\; (0,0,0,0,0,\alpha,0,0,0,0,0,0,0,1,2\alpha^6,0,\alpha^3,-2\alpha,2\alpha,0,1,2\alpha,\alpha,\alpha^2,2\alpha,1,0) \in C.$$

Exemplo 3.1.2 *Agora, considere* $\tau : \begin{cases} x \longmapsto \alpha^2 x \\ y \longmapsto y + \alpha^2 \end{cases}$ *Afirmamos que* τ *é um automorfismos de* $\mathcal{H}_3$.

De fato, observamos que $\mathbb{F}_9$ *pode ser representado por* $\mathbb{F}_3[\alpha]/\langle \alpha^2 + \alpha - 1 \rangle$ *e temos que*

$$\begin{aligned} (\alpha^2 x)^4 &= (y + \alpha^2)^3 + y + \alpha^2 \implies \\ \alpha^8 x^4 &= y^3 + 3y^2\alpha^2 + 3y\alpha^4 + \alpha^6 + y + \alpha^2 \end{aligned}$$

Como $\alpha^4 = -1$ *temos que* $\alpha^6 = -\alpha^2 \Rightarrow \alpha^6 + \alpha^2 = 0$, *e a afirmação segue.*
Notemos ainda que a ordem de τ *é 12, pois*

$$\begin{aligned} \tau(x) &= \alpha^2 x \\ \tau^2(x) &= \alpha^2(\alpha^2 x) \\ \tau^3(x) &= \alpha^2(\alpha^4 x) \\ &\vdots \\ \tau^{12}(x) &= \alpha^2(\alpha^{22} x) \;=\; \alpha^{24} x \;=\; x \end{aligned}$$

já que $\alpha^8 = 1$. *E* $\tau(y) = y + \alpha^2 \Rightarrow \tau^2(y) = y + 2\alpha^2 \Rightarrow \tau^3(y) = y + 3\alpha^2 = y$.
Além disso, τ *fixa* $P_\infty = (0 : 1 : 0)$, *já que* $\sigma(P_\infty) = (0 : 1 + \alpha^2 : 0) = P_\infty$ *e sob a ação de* τ *os outros* 27 *pontos racionais de* $\mathcal{H}_3$ *se decompõem nas seguintes 3 órbitas:*

$O_1 = \{(1, \alpha^4), (\alpha^2, \alpha^4{+}\alpha^2), (\alpha^4, \alpha^4{+}2\alpha^2), (\alpha^6, \alpha^4), (1, \alpha^4{+}\alpha^2), (\alpha^2, \alpha^4{+}2\alpha^2), (\alpha^4, \alpha^4), (\alpha^6, \alpha^4{+}\alpha^2), (1, \alpha^4 + 2\alpha^2), (\alpha^2, \alpha^4), (\alpha^4, \alpha^4 + \alpha^2), (\alpha^6, \alpha^4 + 2\alpha^2)\}$,
$O_2 = \{(\alpha, 1), (\alpha^3, 1 + \alpha^2), (\alpha^5, 1 + 2\alpha^2), (\alpha^7, 1), (\alpha, 1 + \alpha^2), (\alpha^3, 1 + 2\alpha^2), (\alpha^5, 1), (\alpha^7, 1 + \alpha^2), (\alpha, 1 + 2\alpha^2), (\alpha^3, 1), (\alpha^5, 1 + \alpha^2), (\alpha^7, 1 + 2\alpha^2)\}$ *e*
$O_3 = \{(0, 0), (0, \alpha^2), (0, 2\alpha^2)\}$.

Note que O_1 *e* O_2 *tem doze elementos cada e* O_3 *tem 3 elementos.*
Usando a base de $\mathcal{L}(19Q)$ *dada no exemplo anterior e a ordem POT em* $\mathbb{F}_9[t]^3$, *calculamos, com o auxílo do Algoritmo de Buchberger (A.0.14), a seguinte base de Gröbner do submódulo* $\overline{C}$ *de* $\mathbb{F}_9[t]^3$.

$$\begin{aligned} g_1 &= (1, \alpha^3 t^6 + \alpha^7 t^4 + \alpha^7 t^3 + t^2 + \alpha^6 t + \alpha, \alpha^5 t^2 + t + \alpha) \\ g_2 &= (0, t^7 + \alpha^3 t^6 + \alpha^5 t^5 + \alpha^4 t^4 + \alpha^4 t^3 + \alpha^7 t^2 + \alpha t + 1, \alpha^2 t + \alpha^6) \\ g_3 &= (0, 0, t^3 - 1), \end{aligned}$$

Além disso,

- $m_1 = t^{11}e_1,\ m_2 = t^{10}e_1,\ m_3 = t^9e_1,\ m_4 = t^8e_1,\ m_5 = t^7e_1,\ m_6 = t^6e_1,\ m_7 = t^5e_1,\ m_8 = t^4e_1,\ m_9 = t^3e_1,\ m_{10} = t^2e_1,\ m_{11} = te_1,\ m_{12} = 1e_1$
- $m_{13} = t^{11}e_2,\ m_{14} = t^{10}e_2,\ m_{15} = t^9e_2,\ m_{16} = t^8e_2,\ m_{17} = t^7e_2$.

Vamos codificar a palavra $\omega = (0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,\alpha,1) \in \mathbb{F}_9^{27}$.
Usando o Algoritimo A.0.9 temos:

$$\begin{aligned} f &= \sum_{i=1}^{17} \omega_1 m_i \\ &= te_1 + (\alpha t^8 + t^7)e_2 \\ &= (t, \alpha t^8 + t^7, 0). \end{aligned}$$

Agora, $tg_{1_1} = (1, \alpha^3t^7 + \alpha^7t^5 + \alpha^7t^4 + t^3 + \alpha^6t^2 + \alpha, \alpha^5t^3 + t^2 + \alpha)$.
Assim, $f_1 - tg_1 = (0, \alpha t^8 + \alpha^6t^7 + \alpha^3t^5 + \alpha^3t^4 - t^3 + \alpha^2t^2 + \alpha^5t, \alpha t^3 - t^2 - \alpha^5t)$, *e dividindo* $d_1e_1 = f_1$ *por* g_{1_1}, *temos o quociente* t *e resto* $R_1 = 0$.
Seguindo, temos $d_2e_2 = (f - tg_1)e_2$, *que dividido por* g_{2_2} *nos dá o quociente* $\alpha t + \alpha$ *e resto* $R_2 = (\alpha^3t^6 + \alpha^5t^5 + \alpha^6t^4 + \alpha^7t^3 - t^2 + \alpha^3t + \alpha^5)e_2$.
Finalmente, dividindo $d_3e_3 = [f - tg_1 - (\alpha t\alpha)g_2 - R_2]e_3$ *por* g_{3_3}, *temos o quociente* α *e resto* $R_3 = (\alpha t^2, \alpha^5t - 1)e_3$.
Logo,

$$\begin{aligned} R &= (R_1, R_2, R_3) \\ &= (0, \alpha^3t^6 + \alpha^5t^5 + \alpha^6t^4 + \alpha^7t^3 - t^2 + \alpha^3t + \alpha^5, \alpha t^2, \alpha^5t - 1). \end{aligned}$$

Portanto, $f - R = (t, \alpha t^8 + t^7 + \alpha^7t^6 - \alpha t^5 + \alpha^2t^4 + \alpha^3t^3 + t^2 + \alpha^7t + \alpha, \alpha^5t^2 + \alpha t + 1,) \in \overline{C}$ *e,*

$$VC(f - R) = (0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,\alpha,1,\alpha^7,-\alpha,\alpha^2,\alpha^3,1,\alpha^7,\alpha,\alpha^5,\alpha,1) \in C.$$

3.2 Conclusões e Perspectivas Futuras

Neste trabalho, observamos que associando códigos a diferentes estruturas matemáticas podemos obter novas sistemáticas de codificação e relações entre seus parâmetros. Este trabalho pode servir de motivação para o estudo dos processos de decodificarão dos tipos de códigos vistos aqui. Além disso, esperamos que o trabalho também sirva de motivação para um estudo de outros tipos de códigos, associados a outros tipos de estruturas matemáticas.

Apêndice A

Bases de Gröbner Para Módulos

A teoria de bases de Gröbner para ideais de anéis de polinômios, iniciada por B. Buchberger no início dos anos 1980, é uma ferramenta muito importante e que vem sendo utilizada, dentre outras áreas, também na teoria de códigos, veja por exemplo [2]. Sugerimos as referências [1] e [3] para um estudo sobre este assunto. A teoria para módulos sobre anéis de polinômios é completamente análoga, porém um tanto menos trabalhada. Para um estudo mais detalhado sobre esta parte da teoria sobre módulos sugerimos a referência [3] Capítulo 9. Aqui faremos um resumo, considerando apenas módulos sobre o anel de polinômios em uma variável e apresentando resultados que serão necessários no decorrer deste trabalho.

Começamos, com algumas definições básicas.

Definição A.0.1 *Sejam A um anel comutativo com unidade e M um grupo aditivo munido da multiplicação por escalar*

$$\begin{array}{ccc} A \times M & \longrightarrow & M \\ (a, m) & \longmapsto & a.m \end{array} .$$

Dizemos que M é um ***A-módulo*** *se as seguintes condições são satisfeitas.*

(i) $1.m = m, \ \forall \ m \in M;$

(ii) $(a_1 a_2).m = a_1.(a_2.m), \ \forall \ a_1, a_2 \in A, \ e \ \forall \ m \in M;$

(iii) $(a_1 + a_2).m = a_1.m + a_2.m, \ \forall \ a_1, a_2 \in A \ e \ \forall \ m \in M;$

(vi) $a.(m_1 + m_2) = a.m_1 + a.m_2, \ \forall \ a \in A \ e \ \forall \ m_1, m_2 \in M.$

Diremos simplesmente que M é um módulo, ao invés de A-módulo, se não for necessário explicitar o anel A.

Definição A.0.2 *Dizemos que um A-módulo M é um* ***módulo livre*** *se existe uma família $(m_i)_{i \in I}$ de elementos de M satisfazendo as seguintes condições:*

(i) a família $(m_i)_{i \in I}$ é linearmente independente;

(ii) todo elemento m de M é uma combinação linear de elementos da família $(m_i)_{i\in I}$.

Definição A.0.3 *Sejam A um anel e M um A-módulo. Dizemos que um subgrupo N de M é um A-**submódulo**, ou simplesmente um submódulo de M, se a multiplicação por escalar de M preserva N, isto é, se*

$$a \cdot n \in N, \ \forall\ a \in A \ e \ \forall\ n \in N.$$

Seja $B = \{e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, 0, \ldots, 0), \ldots, e_r = (0, \ldots, 0, 1)\}$ uma base de A^r, que é um módulo livre. Um ***monômio*** em A^r é um vetor da forma $m = t^i e_j$, em que $1 \leq j \leq r$ e $i \geq 0$.

Uma ***ordem monomial*** é uma ordem total $<$ sobre a coleção de monômios que, para quaisquer dois monômios m_1 e m_2, satisfaz as seguintes condições:

(i) se $m_1 > m_2$, então $t^i m_1 > t^i m_2$, para todo $i > 0$;

(ii) $t^i e_j > e_j$, para todo j e todo $i > 0$.

Neste trabalho, usaremos a ordem POT (Position Over Term ou posição sobre o termo), definida da seguinte maneira.

Definição A.0.4 *A ordem POT, denotada por $>_{POT}$, sobre A^r é definida por*

$$t^k e_i >_{POT} t^\ell e_j$$

se $i < j$, ou $i = j$ e $k > \ell$.

A seguir, veremos nomenclaturas importantes para o estudo de bases de Gröbner. Fixemos uma ordem $<$ qualquer sobre os monômios de A^r. Seja $f \neq 0$ um elemento de A^r. Então, podemos escrever

$$f = a_1 m_1 + a_2 m_2 + \cdots + a_l m_l$$

em que $a_i \in \mathbb{F}_q \setminus \{0\}$ e m_i é um monômio em A^r para todo $i = 1, 2, \ldots, l$, de tal modo que $m_1 > m_2 > \cdots > m_l$. O ***monômio líder*** de f é $Lm(f) = m_1$; o ***coeficiente líder*** de f $Lc(f) = a_1$; e o ***termo líder*** de f é $Lt(f) = a_1 m_1$.

Definição A.0.5 *Seja $\mathcal{G} = \{g_1, \ldots, g_t\}$ um conjunto de vetores não nulos contido em um submódulo $M \subset A^r$. Dizemos que $\mathcal{G}$ é uma **base de Gröbner** para M se para todo $f \in M$ existe $i \in \{1, \ldots, t\}$ tal que $Lm(g_i)$ divide $Lm(f)$.*

Para um submódulo M de A^r, seja $Lt(M)$ o conjunto formado por todos os termos líderes dos elementos de M. Um monômio em $Lt(M)$ será chamado de ***monômio não-padrão*** e um monômio em $M \setminus Lt(M)$ será chamado de ***monômio padrão*** para M.

Observação A.0.6 *Se $\mathcal{G} = \{g_1, \ldots, g_t\}$ é uma base de Gröbner para o submódulo M e se $Lm(g_i)$ divide $Lm(g_j)$, então o conjunto $\mathcal{G}' = \mathcal{G} \setminus \{g_j\}$ continua sendo uma base de Gröbner para M.*

Proposição A.0.7 *(i) Todo submódulo $M \neq \{0\}$ de A^r tem uma base de Gröbner.*

(ii) Se $\mathcal{G} = \{g_1, \ldots, g_t\}$ é uma base de Gröbner para o submódulo M de A^r, então $M = \langle g_1, \ldots, g_t \rangle$.

Demonstração:
Ver [3], Corolário 6, pp. 75.

■

Definição A.0.8 *Sejam $f, \widetilde{f}, g, h \in A^r$, com $g \neq 0$ e $\mathrm{F} = \{f_1, \ldots, f_s\} \subset A^r$.*

*1) Dizemos que f é **reduzido** a h módulo g, e escrevemos $f \to^g h$, se $Lt(g)$ divide um termo $\mathbf{X}$ que aparece em f e, além disso,*

$$h = f - \frac{\mathbf{X}}{Lt(g)} \cdot g.$$

*2) Dizemos que f é **reduzido** a h módulo F, e escrevemos $f \to_+^{\mathrm{F}} h$, se existe uma sequência de índices $i_1, \ldots, i_t \in \{1, \ldots, s\}$ e vetores $h_1, \ldots, h_{t-1} \in A^r$ tais que*

$$f \to^{f_{i_1}} h_1 \to^{f_{i_2}} h_2 \to^{f_{i_3}} \cdots \to^{f_{i_{t-1}}} h_{t-1} \to^{f_{i_t}} h.$$

*3) Dizemos que $\widetilde{f}$ é **reduzido** com respeito a F, se $\widetilde{f} = 0$ ou se nenhum dos monômios que aparecem em $\widetilde{f}$ é divisível por qualquer um dos $Lm(f_i)$, $i = 1, \ldots, s$.*

*Se $f \to_+^F \widetilde{f}$ e $\widetilde{f}$ é reduzido com respeito a F, escrevemos $f = a_1 f_1 + \ldots + a_s f_s + \widetilde{f}$, em que $a_1, \ldots, a_s \in A$, e dizemos que $\widetilde{f}$ é um **resto** para f com respeito a F.*

Como no caso da teoria de bases de Gröbner para ideais, há, também no caso de módulos, uma ***forma normal*** com respeito a uma base de Gröbner $\mathcal{G} = \{g_1, \ldots, g_s\}$, similar ao algoritmo da divisão, em que um elemento arbitrário $f \in \mathbb{F}_q[t]^r$ pode ser escrito como

$$f = a_1 g_1 + \cdots + a_s g_s + \overline{f}^{\mathcal{G}}$$

onde $a_1, \ldots, a_s \in \mathbb{F}_q$ e $\overline{f}^{\mathcal{G}} \in \mathbb{F}_q[t]^r$ é o resto. A forma normal é determinada unicamente por f e pela escolha da ordem utilizada. No que se segue, usaremos a ordem POT (poderíamos usar uma outra ordem).

Veremos a seguir, um algoritmo para encontrar a forma normal de $f \in \mathbb{F}_q[t]^r$ com respeito a ordem POT.

Pelo item *(i)* da Proposição A.0.7, qualquer submódulo $M \subseteq \mathbb{F}_q[t]^r$ possui uma base de Gröbner $\mathcal{G} = \{g_1, \ldots, g_s\}$, com $s \leqslant r$, em que os g_j estão ordenados de forma que seus termos líderes fiquem listados de forma decrescente com respeito a ordem POT. Sejam

$$f = \sum_{i=1}^{r} f_i e_i \ \text{ e } \ g_j = \sum_{i=1}^{r} g_{j_i} e_i \text{ para cada } j = 1, \ldots, s.$$

Para $p(t), q(t) \in \mathbb{F}_q[t]$, definimos $Quot(p(t), q(t))$ e $Rem(p(t), q(t))$ como sendo, respectivamente, o quociente e o resto da divisão de $p(t)$ por $q(t)$.

Com estas notações temos o seguinte algoritmo para encontrar $a_1, \ldots, a_s \in \mathbb{F}_q$ e $R \in \mathbb{F}_q[t]^r$ tais que $f = a_1 g_1 + \cdots + a_s g_s + R$.

Algorítimo A.0.9

Início: $d := f;\ R := 0; j := 1$
  Para $i = 1$ *até* r, *faça*
    Se $Lt(g_j)$ *contém* e_i ***então***
      $a_i := Quot(d_i, g_{j_i})$
      $R_i := Rem(d_i, g_{j_i})$
      $d_i := d - a_i g_j - R_i e_i$
      $R := R + R_i e_i$
      $j := j + 1$
    Caso contrário
      $a_i := 0$
      $R := R + d_i e_i$
      $d := d - d_i e_i$.

A veracidade do algoritimo segue do fato de se considerar os valores de d e R após cada passo ciclo **Para**. Vemos que o algoritmo vale para o caso $r = 1$ e usamos indução para os demais casos. Por exemplo, para $r = 1$, temos $i = 1$ e $g_1 = \sum d_{1_i} e_i$, e após a conclusão do primeiro passo através do ciclo se $Lt(g_1)$ contém e_1, usando o algoritmo da divisão temos:

$$f_1 = a_1 g_{1_1} + R_1,$$

onde R_1 é zero ou tem grau menor que g_{1_1}.

Subtraindo $a_1 g_{1_1} + R_1 e_1$ de f, e movendo $R_1 e_1$ para o primeiro membro, obtemos um dividendo intermediário d e o resto parcial R, como segue

$$d = \sum_{i=2}^{r} (f_i - a_1 g_{1_i}) e_i \ \text{ e } \ R = R_1 e_1,$$

$$f \ = \ d + a_1 g_1 + R.$$

O resultado a seguir nos garantirá um tipo especial de base de Gröbner.

Proposição A.0.10 *Se M é um submódulo do módulo livre $\mathbb{F}_q[t]^r$, então M possui uma base de Gröbner $\mathcal{G}$ com a seguinte propriedade: para cada $j = 1, \ldots, r$, existe no máximo um elemento de $\mathcal{G}$ cujo monômio líder é da forma $t^i e_j$. Ou seja, $\mathcal{G} = \{g^{(1)}, \ldots, g^{(r)}\}$ é uma base de Gröbner tal que*

$$\begin{aligned} g^{(1)} &= (g_1^{(1)}(t), g_2^{(1)}(t), \ldots, g_r^{(1)}(t)) \\ g^{(2)} &= (0, g_2^{(2)}(t), \ldots, g_r^{(2)}(t)) \\ &\vdots \\ g^{(r)} &= (0, \ldots, 0, g_r^{(r)}(t)), \end{aligned}$$

em que, para cada i, j, $g_i^{(j)}(t) \in \mathbb{F}_q[t]$ *Em particular,* M *possui uma base de Gröbner com no máximo* r *elementos.*

Demonstração:

A Proposição A.0.7 nos diz que todo submódulo de $\mathbb{F}_q[t]^r$ possui uma base de Gröbner. Seja $\widetilde{\mathcal{G}} = \{g^{(1)}, \ldots, g^{(s)}\}$ uma base de Gröbner qualquer de M.

Suponha que dentre os elementos de $\mathcal{G}$ existam dois, $g^{(i)}$ e $g^{(k)}$, com $Lt(g^{(i)}) = t^u e_j$ e $Lt(g^{(k)}) = t^v e_j$, para o mesmo j. Sem perda de generalidade, suponhamos $u \leqslant v$. Logo, $Lt(g^{(k)})$ é divisível por $Lt(g^{(i)})$ e os termos líderes de $\mathcal{G}_1 = \widetilde{\mathcal{G}} \setminus \{g^{(k)}\}$ geram o mesmo submódulo M gerado por $\widetilde{\mathcal{G}}$. Portanto, pela Observação A.0.6, $\mathcal{G}_1$ também é uma base de Gröbner de M.

Repetindo o mesmo argumento para $\mathcal{G}_1$ e assim, sucessivamente, conseguimos uma base de Grobner $\mathcal{G}$ com a propriedade desejada.

Em particular tal $\mathcal{G}$ possui no máximo r elementos, já que temos $e_1, \ldots, e_r$ fazendo parte dos geradores dos $Lt(g^{(i)})$.

■

Observação A.0.11 *Para nossas aplicações consideraremos, para* $i = 1, \ldots, r$, *os* $q_i = (t^{|O_i|-1})e_i$ *(já vistos no final do capítulo anterior) como geradores do submódulo associado ao código, o que implicará que a base de Gröbner terá exatemente* r *elementos.*

A seguir, descreveremos o algoritmo de Buchberger, que nos permite encontrar uma base de Gröbner para módulos.

Para descrevermos tal algoritmo necessitamos do conceito de S-polinômio.

Sejam $m_1 = t^k e_i$ e $m_2 = t^\ell e_j$ dois monômios em A^r. Definimos o ***mínimo múltiplo comum*** entre os monômios m_1 e m_2, como sendo

$$mmc(m_1, m_2) = \begin{cases} 0, \text{ se } i \neq j, \\ t^{min\{k,\ell\}} e_i, \text{ se } i = j \end{cases}.$$

Definição A.0.12 *Sejam* $f, g \in A^r$, *com* $f, g \neq 0$ *e* $\mathbb{L} = mmc(Lm(f), Lm(g))$. *Definimos o vetor*

$$S(f, g) = \frac{\mathbb{L}}{Lt(f)} \cdot f - \frac{\mathbb{L}}{Lt(g)} \cdot g$$

como sendo o ***S-polinômio*** *de* f *e* g.

Teorema A.0.13 *Seja $\mathcal{G} = \{g_1, \ldots, g_t\}$ um conjunto de vetores não nulos de A^r. Então, $\mathcal{G}$ é uma base de Gröbner para o submódulo $M = \langle g_1, \ldots, g_t \rangle$ de A^r se, e somente se, para todo $i \neq j$, temos $S(g_i, g_j) \to_+^{\mathcal{G}} 0$.*

Algorítimo A.0.14 (Algoritmo de Buchberger)

Entrada: F $= \{f_1, \ldots, f_s\} \subseteq A^r$, com $f_i \neq 0$, para $1 \leqslant i \leqslant s$
Saída: $\mathcal{G} = \{g_1, \ldots, g_t\}$ base de Gröbner para $\langle f_1, \ldots, f_s \rangle$
Início: $\mathcal{G} :=$ F, $\mathbf{G} := \{\{f_i, f_j\} : f_i \neq f_j \in \mathcal{G}\}$
Enquanto $\mathbf{G} \neq \emptyset$, faça
  escolha algum $\{f, g\} \in \mathbf{G}$
  $\mathbf{G} := \mathbf{G} \backslash \{\{f, g\}\}$
  $S(f, g) \to_+^{\mathcal{G}} h$
Se $h \neq 0$, **então**
$\mathbf{G} := \mathbf{G} \cup \{\{u, h\}, \ \forall\ u \in \mathcal{G}\}$
$\mathcal{G} := \mathcal{G} \cup \{h\}$.

As demonstrações dos resultados anteriores podem ser vistas em [3], Capítulo 2.

Vejamos então um exemplo que ilustra tais conceitos.

Exemplo A.0.15 *Considere os vetores $f_1 = (0, y, x)$ e $f_2 = (0, x, xy - x)$ de $\mathbb{Q}[x, y]^3$.*

Tomando $x > y$ em $\mathbb{Q}[x, y]$ e a ordem POT em $\mathbb{Q}[x, y]^3$ com $e_1 < e_2 < e_3$, vamos calcular uma base de Gröbner para o submódulo $M = \langle f_1, f_2 \rangle$ de $\mathbb{Q}[x, y]^3$ usando o Algoritmo A.0.14.

Seja $G = \{f_1, f_2\}$. Pela Definição A.0.12, temos

$$\begin{aligned} S(f_1, f_2) &= xf_1 - yf_2 \\ &= (0, 0, x^2 - xy^2 + xy). \end{aligned}$$

Mas, $S(f_1, f_2) \to_+^{\mathrm{G}} f_3 = (0, -x^2, 2x^2 - xy^2 - x^2y + xy)$. Assim, adicionamos o vetor f_3 a G. Agora, notemos que $S(f_1, f_3) = S(f_2, f_3) = 0$.
Concluímos então que $\mathcal{G} = \{f_1, f_2, f_3\}$ é uma base de Gröbner para M.

Referências Bibliográficas

[1] ADAMS, W. e LOUSTAUNAN, P., *An Introduction to Gröbner Bases*. Providence, RI: Amer. Math. Soc., 1994.

[2] CARVALHO, C., *Gröbner bases methods in coding theory*. Contemporary Mathematics, American Mathematical Society, a publicar.

[3] COX, D., LITTLE, J. e O'SHEA, D., *Ideals, Varieties and Algorithms*. Springer, New York, 1992.

[4] GARCIA, A. e LEQUAIN, Y., *Elementos de Álgebra*. 5ª edição. IMPA, Rio de Janeiro, 2010.

[5] HEEGARD, C., LITTLE, J. e SAINTS, K., *Systematic Encoding via Gröbner Bases for a Class of Algebraic-Geometric Goppa Codes*. IEEE trans. Infor. Theory 41(6) (1995), 1752-1761.

[6] HEFEZ, A. e VILLELA, M., *Códigos Corretores de Erros*. Série e Computação e Matemática, IMPA, Rio de Janeiro, 2008.

[7] HIRSCHFELD, J. W. P., KORCHMÁROS, G. e TORRER, F., *Algebraic Curves over a Finite Field*. Princeton University Press, 2008.

[8] van LINT, J. H. , *Introduction to Coding Theory*. New York, Springer, 1982.

[9] MUNUERA, C. e TENA, J., *Codificación de la Información*. Univ. de Valladolid, 1997.

[10] STICHTENOTH, H., *Algebraic Function Fields and Codes*. Berlim, Springer, 1993.

[11] TIZZIOTTI, G. C., *Codificação de Certos Códigos de Goppa Geométricos Utilizando a Teoria de Bases de Gröbner e Códigos Sobre a Curva Norma-traço*, (Tese de doutorado). Universidade Estadual de Campinas, 2008.