Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Programa de Pós-Graduação em Matemática

Mauro Rodrigues Rocha Junior

Bases de Gröbner aplicadas a Códigos Corretores de Erros

Juiz de Fora
2017

Mauro Rodrigues Rocha Junior

Bases de Gröbner aplicadas a Códigos Corretores de Erros

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Juiz de Fora, na área de concentração em Álgebra, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Beatriz Casulari da Motta Ribeiro

Juiz de Fora

2017

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Rodrigues Rocha Junior, Mauro.
Bases de Gröbner aplicadas a Códigos Corretores de Erros / Mauro Rodrigues Rocha Junior. – 2017.
69 f.

Orientadora: Beatriz Casulari da Motta Ribeiro
Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Pós-Graduação em Matemática, 2017.

1. Base de Gröbner. 2. Variedades afins. 3. Corpos de funções. 4. Códigos algébrico-geométricos. I. Ribeiro, Beatriz Casulari da Motta, orient. II. Título.

Mauro Rodrigues Rocha Junior

Bases de Gröbner aplicadas a Códigos Corretores de Erros

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Juiz de Fora, na área de concentração em Álgebra, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovada em:

BANCA EXAMINADORA

Profa. Dra. Beatriz Casulari da Motta Ribeiro
Orientadora
Universidade Federal de Juiz de Fora

Professor Dr. Guilherme Chaud Tizziotti
Universidade Federal de Uberlândia

Professor Dr. Frederico Sercio Feitosa
Universidade Federal de Juiz de Fora

AGRADECIMENTOS

Muitas pessoas para agradecer com poucas palavras, desde já peço desculpas aos não citados explicitamente.

Agradeço primeiramente a Deus, aos meus pais, Mauro e Joana, que sempre foram meus maiores conselheiros e amigos e que me motivaram a estudar, aos meus irmãos e a todos os meus familiares.

A todos os meus amigos que me ajudaram e me aguentaram nos momentos de chatura, em especial a minha grande amiga Sarah que me mostrou a vida boemia, Eli por sempre poder contar com ele, minha conselheira Maiara que sempre teve a paciência de me escutar e dar conselhos, Walberto que me aturou esses dois anos morando na mesma casa e a Naamã, Marcela, Julio Lanazca, Graciliano, Mario, Hugo, Oscar, Daniel, Jorge Luis, Anderson, Alberth, Andres, Giovana, Rodrigo, pela companhia, duvidas tiradas e pelos momentos descontraídos. Sei que faltam muitos aqui, mas considere a transitividade.

Ao coordenador Grigori, a secretária Paula e aos professores Lonardo, Flaviana, Joana, Sandro, Laura, Sérgio, Willian, Andrey, pois aprendi muito com eles. Agradeço em especial a professora Beatriz Casulari da Motta Ribeiro que aceitou me orientar e sempre teve a paciência e compreensão de tirar minhas duvidas. Aos professores Frederico Sercio Feitosa e Guilherme Chaud Tizziotti por aceitarem a participar da banca.

À CAPES e UFJF, pelo importante apoio financeiro concedido ao longo de todo o curso.

Por fim, só tenho a agradecer cada um de vocês que me ajudaram nessa conquista, eu não imaginava como iria ser incrível tudo isso.

RESUMO

O principal objetivo desse trabalho é estudar duas aplicações distintas das bases de Gröbner a códigos lineares. Com esse objetivo, estudamos como relacionar códigos a outras estruturas matemáticas, fazendo com que tenhamos novas ferramentas para a realização da codificação. Em especial, estudamos códigos cartesianos afins e os códigos algébrico-geométricos de Goppa.

Palavras-chave: Base de Gröbner. Variedades afins. Corpos de funções. Códigos algébrico-geométricos.

ABSTRACT

The main objective of this work is to study two different applications of Gröbner basis to linear codes. With this purpose, we study how to relate codes to other mathematical structures, allowing us to use new tools to do the coding. In particular, we study affine cartesian codes e algebraic-geometric Goppa codes.

Key-words: Gröbner basis. Affine varieties. Function fields. Algebraic-geometric codes.

SUMÁRIO

1 INTRODUÇÃO

O problema de transmitir informações de forma segura e correta existe desde o início da civilização. Na transmissão de dados podem ocorrem problemas, como interferências electromagnéticas ou erros humanos, que chamamos de ruído e que fazem com que a mensagem recebida seja diferente daquela que foi enviada. A teoria de códigos corretores de erro tem como objetivo desenvolver métodos que permitam detectar e corrigir a maior quantidade de erros possível.

Na década de 1940, os programas eram gravados em cartões perfurados cuja leitura pelo computador permitia detectar erros de digitação. Caso um erro fosse detectado, a leitura era interrompida. Inquietado pelo fato das máquinas conseguirem detectar um erro, mas não corrigí-lo, Hamming desenvolveu um código capaz de detectar até dois erros e corrigir um erro, se ele for o único. Ainda na mesma década, Shannon publicou "A Mathematical Theory of Communication", consolidando o início da teoria de códiigos em conjunto com o trabalho de Hamming.

Em particular, a teoria de códigos lineares utiliza ferramentas matemáticas sofisticadas e pode ser abordada a partir de diversas áreas, tais como Geometria Algébrica, Teoria dos Números e Teoria de Grupos. Nesse trabalho, nossa abordagem de códigos corretores de erros utiliza duas ferramentas como base: variedades afins e corpos de funções algébricas. A primeira abordagem deve-se a Lax e Fitzgerald em [9] e torna-se bastante interessante por utilizar resultados clássicos. Já a segunda, deve-se ao interesse de apresentar uma classe dos códigos lineares introduzida por Goppa em 1981 que tem sido tema de estudo desde então.

Nosso interesse em apresentar dois tipos de construção diferentes de códigos vem do fato de que as mesmas admitem o uso de uma ferramenta comum de formas distintas: as bases de Gröbner.

O conceito de bases de Gröbner apareceu pela primeira vez em 1965, na tese de Buchberger, orientada por Gröbner. O problema a ser resolvido parecia simples: dado um ideal de um anel de polinômios $K[x]$, como determinar uma base do anel $K[x]/I$ como K-espaço vetorial? Essa resposta era conhecida no caso de polinômios em uma só variável, mas muda quando temos várias variáveis. A ideia de Buchberger foi, então, fixar uma ordem monomial e determinar um conjunto especial $\mathscr{G}$ de geradores para I (que sabemos que é finita, pelo Teorema da base de Hilbert) com uma propriedade especial: as classes dos monômios que não são múltiplos de nenhum dos monômios líderes de $\mathscr{G}$ formam uma base para $K[x]/I$.

Dessa forma, no primeiro capítulo, fazemos uma breve introdução ao conceito de ordens monomiais e apresentamos as bases de Gröbner e o algoritmo de Buchberger.

No segundo capítulo, apresentamos uma primeira aplicação de bases de Gröbner a códigos. Para isso, começamos com conceitos e resultados básicos da teoria de códigos, mais especificamente de códigos lineares. Em seguida, estudamos a construção de códigos apresentada em [9] seguindo os passos de [3], os chamados códigos cartesianos afins, que utilizaram variedades afins e certa aplicação que depende dos pontos de tais variedades.

Em seguida, começamos o estudo da segunda aplicação de bases de Gröbner a códigos.

No terceiro capítulo, apresentamos as ferramentas que serão utilizadas no capítulo seguinte e são parte da teoria de corpos de funções, como lugares, valorização discreta e divisores, além de resultados importantes, como o teorema da aproximação fraca e o teorema de Riemann-Roch.

No quarto capítulo, apresentamos a construção de alguns códigos lineares, tendo como foco principal os códigos geométricos de Goppa. Em particular, vemos o exemplo dos códigos racionais.

Finalmente, no último capítulo, apresentamos um estudo de codificação de códigos lineares utilizando bases de Gröbner proposto por Little, Saints e Heegard. Nesse caso, é dada uma estrutura de submódulo de um módulo livre para os códigos de Goppa, um grande avanço na teoria de códigos, pois tal sistema de codificação é mais eficiente do que canônico, isto é, utilizando matriz geradora.

2 BASES DE GRÖBNER

2.1 ORDENS MONOMIAIS

Neste capítulo, K denotará um corpo e $K[x]$ será o anel de polinômios em n variáveis $x_1, ..., x_n$ com coeficientes em K.

Definição 2.1. O conjunto de todos os monômios de $K[x]$ é denotado por $\mathbb{M}_n$, ou seja,

$$\mathbb{M}_n = \left\{ \prod_{i=1}^{n} x_i^{\alpha_i}; \alpha_1, ..., \alpha_n \in \mathbb{N}. \right\}$$

O monômio $x_1^0 \cdot ... \cdot x_n^0$ é denotado por 1.

Definição 2.2. Uma relação de ordem, ou uma ordenação, sobre um conjunto C (não vazio) é uma relação $\leq$ satisfazendo:

1. $c \leq c$ para todo $c \in C$ (reflexiva).
2. Se $c_1, c_2 \in C$ são tais que $c_1 \leq c_2$ e $c_2 \leq c_1$ então $c_1 = c_2$ (anti-simétrica).
3. Sejam c_1, c_2 e $c_3 \in C$. Se $c_1 \leq c_2$ e $c_2 \leq c_3$ então $c_1 \leq c_3$ (transitiva).

Definição 2.3. Uma ordem monomial $\leq$ sobre $\mathbb{M}_n$ é uma relação de ordem total que satisfaz:

1. Seja $m_1, m_2 \in \mathbb{M}_n$ tais que $m_1 \leq m_2$, então $m_1 m_3 \leq m_2 m_3$ para todo $m_3 \in \mathbb{M}_n$.
2. Todo subconjunto não vazio de $\mathbb{M}_n$ admite um menor elementos em relação a $\leq$.

Definição 2.4. Definimos a ordem lexicográfica $\leq_L$ da seguinte maneira:
Dados dois monômios $\prod_{i=1}^{n} x_i^{\alpha_i}$ e $\prod_{i=1}^{n} x_i^{\beta_i}$ dizemos que

$$\prod_{i=1}^{n} x_i^{\alpha_i} \leq_L \prod_{i=1}^{n} x_i^{\beta_i}$$

se $\alpha_k = \beta_k$ para todo $k \in \{1, ..., n\}$, isto é, $\prod_{i=1}^{n} x_i^{\alpha_i} = \prod_{i=1}^{n} x_i^{\beta_i}$, ou existe $i \in \{1, ..., n\}$ tal que $\alpha_i < \beta_i$ e $\alpha_j = \beta_j$ para todo $j < i$.

Exemplo 2.1. Considerando a ordem lexicográfica e os monômios xy^3z^3, xy^2z^4, $x^2y^4z^2$, x^4y, $x^3y^2z^3 \in K[x, y, z]$, temos que:

$$xy^2z^4 \leq_L xy^3z^3 \leq_L x^2y^4z^2 \leq_L x^3y^2z^3 \leq_L x^4y.$$

Uma outra ordem que também utilizaremos é a ordem lexicográfica graduada.

Definição 2.5. Definimos a ordem lexicográfica graduada $\leq_{LG}$ da seguinte maneira: Dados dois monômios $\prod_{i=1}^{n} x_i^{\alpha_i}$ e $\prod_{i=1}^{n} x_i^{\beta_i}$ dizemos que

$$\prod_{i=1}^{n} x_i^{\alpha_i} \leq_{LG} \prod_{i=1}^{n} x_i^{\beta_i}$$

se:
$\deg\left(\prod_{i=1}^{n} x_i^{\alpha_i}\right) < \deg\left(\prod_{i=1}^{n} x_i^{\beta_i}\right)$ ou $\deg\left(\prod_{i=1}^{n} x_i^{\alpha_i}\right) = \deg\left(\prod_{i=1}^{n} x_i^{\beta_i}\right)$ e existe $k \in \{1, ..., n\}$ tal que $\alpha_k > \beta_k$ e $\alpha_j = \beta_j$ para todo $j > k$.

Outra ordem que utilizaremos nos últimos capítulos é a ordem POT.

Definição 2.6. Um monômio em $K[x]^m$ é um vetor do tipo Xe_i, onde e_i é o vetor canônico e $1 \leq i \leq m$ e X é um monômio em $K[x]$.

Definição 2.7. A ordem POT, denotada por $>_{POT}$, sobre $K[x]^r$ é definida por:

$$x^k e_i >_{POT} x^l e_j \,,$$

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

Exemplo 2.2. Sejam a e b pertencente a $K[x]^m$, com $a = (x, x^2, ..., x^r)$ e $b = (x^r, ..., x)$, então temos pela ordem POT que $ae_i >_{POT} be_j$ para $i < j$, $ae_i <_{POT} be_j$ para $i > j$ e quando tivermos $i = j$ teremos que dividir em dois casos
1º Caso: Se r for par, então se $i \leq \frac{r}{2}$, temos $ae_i <_{POT} be_j$, agora se $i > \frac{r}{2}$, então $ae_i >_{POT} be_j$.
2º Caso: Se r for ímpar, temos $ae_i =_{POT} be_j$ para $i = j = \frac{r+1}{2}$, $ae_i <_{POT} be_j$ para $i < \frac{r+1}{2}$ e $ae_i >_{POT} be_j$ se $i > \frac{r+1}{2}$.

Agora que já definimos as ordens monomiais que serão utilizadas ao longo desse trabalho, vamos falar um pouco sobre o algoritmo da divisão para n variáveis. Dados polinômios $f, f_1, ..., f_m$ em $K[x]$, de forma semelhante ao algoritmo da divisão de uma variável, queremos encontrar $q_1, ..., q_m, r \in K[x]$ tais que

$$f = q_1 f_1 + ... + q_m f_m + r.$$

Para isso temos o seguinte algoritmo

Algoritmo da Divisão de n variáveis

Entrada: $f, f_1, ..., f_m \in K[x]$;

Defina $q_1 = ... = q_m = r = 0$ e $h = f$;

Enquanto $h \neq 0$ faça

Se existe $i \in \{1, ..., m\}$ tal que $ml(f_i)|ml(h)$

Então

Escolha o menor tal índice i e faça

$$q_i = q_i + \frac{tl(h)}{tl(f_i)};$$

$$h = h - \frac{tl(h)}{tl(f_i)f_i};$$

Senão

$$r = r + tl(h);$$

$$h = h - tl(h);$$

Saída: $q_1, ..., q_m, r \in K[x]$ tais que$f = \sum_{j=1}^{s} q_j g_j + r$,

$ml(f_i) \nmid m$ para todo $m \in \mathbb{M}(r)$ e todo $i = 1, ..., s$.

O seguinte teorema nos garante a existência de $q_1, ..., q_m$ e r como no algoritmo anterior.

Teorema 2.1. Sejam $f, g_1, ..., g_m$ polinômios e $\leq$ uma ordem monomial fixada. Então existem $q_1, ..., q_m, r \in K[x]$, tais que

$$f = q_1 g_1 + ... + q_s g_m + r,$$

com $ml(g_i) \nmid m$ para todo $m \in \mathbb{M}(r)$ e todo $i = 1, ..., m$.

Demonstração. ver [8] teorema 3.30. □

Exemplo 2.3. Seja $f_1 = x^4y^2 + 1$ e $f_2 = 2y^5 - y$ e $f = 6x^6y^4 + 7x^5 + 8x^4y^7 + 1$, então fazendo a divisão de f por f_1 e f_2, temos pelo algoritmo da divisão
Iniciamos com

$$F = f = 6x^6y^4 + 7x^5 + 8x^4y^7 + 1;$$

$$r = 0;$$

$$q_1 = 0;$$

$$q_2 = 0.$$

Como $ml(f_1)$ divide $ml(F)$, obtemos

$$F = f - \frac{ml(f)}{ml(f_1)} f_1 = 7x^5 + 8x^4y^7 - 6x^2y^2 + 1;$$
$$r = 0;$$
$$q_1 = 6x^2y^2;$$
$$q_2 = 0.$$

Como $ml(f_1)$ não divide $ml(F)$ e $ml(f_2)$ não divide $ml(F)$, obtemos:

$$F = F - ml(F) = 8x^4y^7 - 6x^2y^2 + 1;$$
$$r = 7x^5;$$
$$q_1 = 6x^2y^2;$$
$$q_2 = 0.$$

Como $ml(f_1)$ divide $ml(F)$, obtemos

$$F = F - \frac{ml(F)}{ml(f_1)} f_1 = -6x^2y^2 - 8y^5 + 1;$$
$$r = 7x^5;$$
$$q_1 = 6x^2y^2 + 8y^5;$$
$$q_2 = 0.$$

Como $ml(f_1)$ não divide $ml(F)$ e $ml(f_2)$ não divide $ml(F)$, obtemos

$$F = -8y^5 + 1;$$
$$r = 7x^5 - 6x^2y^2;$$
$$q_1 = 6x^2y^2;$$
$$q_2 = 0.$$

Como $ml(f_2)$ divide $ml(F)$, temos

$$F = F - \frac{ml(F)}{ml(f_2)} f_2 = 4y + 1;$$
$$r = 7x^5 - 6x^2y^2;$$
$$q_1 = 6x^2y^2 + 8y^5;$$
$$q_2 = -4.$$

Como $ml(f_1)$ não divide $ml(F)$ e $ml(f_2)$ não divide $ml(F)$, obtemos

$$F = 1;$$
$$r = 7x^5 - 6x^2y^2 - 4y;$$
$$q_1 = 6x^2y^2 + 8y^5;$$
$$q_2 = -4.$$

Como $ml(f_1)$ não divide $ml(F)$ e $ml(f_2)$ não divide $ml(F)$, obtemos

$$\begin{aligned} F &= 0; \\ r &= 7x^5 - 6x^2y^2 - 4y + 1; \\ q_1 &= 6x^2y^2 + 8y^5; \\ q_2 &= -4. \end{aligned}$$

No próximo passo o algoritmo para. Portanto, temos

$$f = (6x^2y^2 + 8y^5)(x^4y^2 + 1) + (2y^5 - y)(-4) + 7x^5 - 6x^2y^2 - 4y + 1.$$

2.2 BASES DE GRÖBNER

A teoria de bases de Gröbner para ideais de anéis de polinômios é uma ferramenta muito utilizada na teoria de códigos, pois sua principal característica é determinar uma base para um ideal dado de modo que um polinômio pertença a esse ideal se, somente se, deixa resto zero na divisão pelos elementos da base. Nas seções 2.2 e 2.3 sempre que omitirmos a ordem utilizada, estaremos considerando a ordem lexicográfica.

Definição 2.8. Dado um polinômio $f \in K[x]$, denotaremos por $ml(f)$ o monômio líder de f e $tl(f)$ o termo líder.

Exemplo 2.4. Considere o polinômio $f(x) = 3x^4y^2 + 5x^2y + 3xy + 2x + y + 8$, então $ml(f) = x^4y^2$ e $tl(f) = 3x^4y^2$.

Definição 2.9 (Base de Gröbner). Sejam $I \subset K[x]$ um ideal e $\leq$ uma ordem monomial fixada. Um subconjunto não vazio e finito G de I é uma base de Gröbner para I com respeito a relação $\leq$, se para todo $f \in I$ existe $g \in G$ de modo que $ml(g)$ divide $ml(f)$. Denotaremos por $ml(G)$ o conjunto de todos os monômios líderes de todos os $g \in G$.

Exemplo 2.5. Considere o seguinte ideal $I = \langle f_1, f_2 \rangle$, com $f_1 = x^2$ e $f_2 = xy + y^2$, inicialmente poderíamos pensar que $\{f_1, f_2\}$ seria uma base de Gröbner para I, porém não é, pois se olharmos para $h = -xy^2 + yf_2 = y^3$, temos que $ml(f_1) \nmid ml(h)$ e $ml(f_2) \nmid ml(h)$ e $h \in I$, pois $-xy^2 = yf_1 - xf_2$,

Proposição 2.1. Sejam $J \subseteq I$ ideais de $K[x]$. Se $ml(I) = ml(J)$, então $I = J$

Demonstração. Suponha por contradição que $I \neq J$. Como $\geq$ é uma boa ordem, então conjunto $I \setminus J$ tem um elemento f cujo monômio líder é mínimo com relação a $\geq$. Porém como $ml(I) = ml(J)$, temos que $ml(f) \in ml(J)$. Portanto existe $g \in J$ tal que $ml(g) = ml(f)$, implicando que $ml(f) \geq ml(f - g)$. Mas, pela minimidade de f, temos que $f - g \in J$. Como $g \in J$, então $f = (f - g) + g \in J$, que contradiz a hipótese feita sobre J e completa a demonstração. □

Corolário 2.2. Se G é uma base de Gröbner de um ideal I de $K[x]$, então G gera I.

Demonstração. Pela definição de Base de Gröbner temos que $ml(I) = ml(\langle G \rangle)$, então pela proposição anterior temos que $I = \langle G \rangle$. □

Observação 2.1. Um resultado análogo ao anterior para módulos pode ser encontrado em [5].

Um outro resultado importante que segue da proposição 2.1 é o teorema da base de Hilbert.

Teorema 2.3. (Teorema da base de Hilbert) Todo ideal de $K[x]$ admite um numero finito de geradores.

Demonstração. Ver [4] página 145. □

Vamos denotar por $R_G(f)$ o resto da divisão de f por G.

Proposição 2.2. Sejam I um ideal de $K[x]$ e G uma base de Gröbner para I. Então, $f \in I$ se e somente se o resto da divisão de f por G é zero.

Demonstração. Seja $R_G(f)$ o resto da divisão de f por G. Como G gera I, então se $R_G(f) = 0$ temos que $f \in I$. Agora suponhamos que $f \in I$ e $R_G(f) = r$. Aplicando o algoritmo da divisão para f e $G = \langle g_1, ..., g_n \rangle$ existem polinômios $r, q_1, ..., q_s \in K[x]$ tais que

$$f = \sum_{i=1}^{s} q_i g_i + r.$$

Segue então que

$$r = f - \sum_{i=1}^{s} q_i g_i \in I.$$

Se $r \neq 0$, então temos que $ml(r) \in ml(I) \subseteq \langle ml(I) \rangle = \langle ml(G) \rangle$, ou seja, existe $g_j \in G$ tal que $ml(g_j) \mid ml(r)$, contradizendo o fato de r ser o resto da divisão de f por G. Portanto, $r = 0$. □

Corolário 2.4. Sejam $G = \{g_1, ..., g_n\}$ uma base de Gröbner e f um polinômio do anel $K[x]$. Então existe um único polinômio r tal que

$$f = q_1 g_1 + ... + q_s g_s + r,$$

onde $q_1, ..., q_s \in \mathbb{K}[x_1, ..., x_n]$ e nenhum monômio de r pertence ao ideal gerado pelos monômios líderes dos $g_i's$.

Demonstração. Suponha por contradição que também podemos escrever f na forma

$$f = q'_1 g_1 + ... + q'_s g_s + r'$$

em que, como no enunciado do corolário, $q'_1, ..., q'_s \in K[x]$ e nenhum monômio de r' pertence as expressões para f. Obtemos então

$$(q_1 g_1 + ... + q_s g_s + r) - (q'_1 g_1 + ... + q'_s g_s + r') = 0.$$

Assim

$$(q_1 - q'_1)g_1 + ... + (q_s - q'_s)g_s + r - r' = 0$$

donde podemos concluir que $r - r' \in \langle g_1, ..., g_s \rangle$. Logo, pela proposição anterior, o resto da divisão de $r - r'$ por G tem que ser zero. Contudo, pela hipótese, nenhum monômio de r e r' é divisível pelo termo inicial de algum g, mas isso implica que o resto da divisão de $r - r'$ por G é o próprio $r - r'$. Portanto, $r - r' = 0$, como queríamos mostrar. □

Observação 2.2. Um resultado análogo ao anterior para módulos pode ser encontrado em [1] capitulo 3.

Proposição 2.3. Seja G uma base de Gröbner no anel $K[x]$, com respeito a alguma ordem monomial. Suponhamos que g e h são elementos de G e que $ml(g)$ divide $ml(h)$. Então

$$H = G \setminus \{h\}$$

também é uma base de Gröbner de $\langle G \rangle$.

Demonstração. Basta mostrarmos que para todo $f \in \langle G \rangle$ existe $g \in H$ tal que $ml(g)|ml(f)$.

Como G é uma base de Gröbner, então $ml(f)$ é divisível pelo monômio líder de algum polinômio de G. Se este polinômio não for h, então pertence a H e nada a fazer, Por outro lado, se o polinômio for h, então

$$ml(g) \text{ divide } ml(h) \text{ que divide } ml(f).$$

Assim, em qualquer caso $ml(f)$ é divisível pelo monômio líder de um elemento de H como queríamos mostrar. □

O seguinte resultado será importante no último capítulo desse texto e afirma que um submódulo de $\mathbb{F}_q[t]^r$ adimite base de Gröbner do tipo $\{g^{(1)}, \ldots, g^{(r)}\}$ tal que

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

Proposição 2.4. Se M é um submódulo de $\mathbb{F}_q[t]^r$, então M admite uma base de Gröbner tal que: para cada $j = 1, \ldots, r$, existe no máximo um um elemento da base cujo monômio líder é $t^i e_j$.

2.3 ALGORITMO DE BUCHBERGER

Inicialmente podemos não ter ideia de como calcular a base de Gröbner de um ideal, mas em meados de 1960 Bruno Buchberger apresentou um algoritmo simples para a obtenção dessa base. Antes de apresentarmos esse algoritmo precisamos introduzir alguns conceitos.

Definição 2.10. O mínimo múltiplo comum (MMC), de dois monômios $\prod_{i=1}^{n} x_i^{\alpha_i}$ e $\prod_{i=1}^{n} x_i^{\beta_i} \in \mathbb{M}_n$ é o monômio

$$MMC\left(\prod_{i=1}^{n} x_i^{\alpha_i}, \prod_{i=1}^{n} x_i^{\beta_i}\right) = \prod_{i=1}^{n} x_i^{\gamma_i},$$

onde $\gamma_i = max\{\alpha_i, \beta_i\}$ para todo $i = 1, ..., n$.

Exemplo 2.6. Considere $m_1 = x^3y^2z^4$ e $m_2 = x^2y^4z^6$, então o $MMC(m_1, m_2) = x^3y^4z^6$

Definição 2.11. Fixando uma ordem monomial em $\mathbb{M}_n$ e dados elementos $f, g \in K[x]\backslash\{0\}$, o S-polinômio de f e g, que denotamos por $S(f, g)$ é o polinômio

$$S(f, g) = MMC(ml(f), ml(g))\left(\frac{f}{tl(f)} - \frac{g}{tl(g)}\right).$$

Exemplo 2.7. Seja $f = y^2 - x$ e $g = xy - y$, então $MMC(ml(f), ml(g)) = xy^2$ e

$$S(f, g) = xy^2\left(\frac{y^2 - x}{y^2} - \frac{xy - y}{xy}\right) = -x^2 + y^2$$

Proposição 2.5. Fixada uma ordem monomial $\leq$ sobre $\mathbb{M}_n$, temos que um subconjunto G é uma base de Gröbner se, e somente se,

$$R_G(S(g_i, g_j)) = 0,$$

para todo par $(g_i, g_j) \in G \times G$.

Demonstração. Ver [8], proposição 4.15. □

Teorema 2.5. Dada uma ordem monomial e $\{g_1, ..., g_s\} \subset K[x]$, podemos obter uma Base de Gröbner G para o ideal $I = \langle g_1, ..., g_s\rangle$ aplicando o seguinte algoritmo:

Algoritmo de Buchberger

Entrada: $\{g_1, ..., g_s\} \subset K[x]$

Defina $G_0 = \emptyset, G_1 = \{g_1, ..., g_s\}$ e $i = 1$;

Enquanto $G_{i-1} \neq G_i$ Faça

Para todo $f, h \in G_i$

Calcule o resto r da divisão de $S(f, h)$ por G_i

Se $r \neq 0$, **então**

$G_{i+1} = G_i \cup \{r\}$;

Se não ;

$G_{i+1} = G_i$;

$i = i + 1$

Saída: $G = G_i$ Base de Gröber para I.

Demonstração. Primeiramente vamos mostrar que esse algoritmo finaliza depois de um número finito de iterações. Suponha que esse algoritmo nunca pare, então existe uma sequencia infinita de conjuntos

$$G_1 \subsetneq G_2 \subsetneq ... \subsetneq G_i \subsetneq ...,$$

com $G_{i+1} = G_i \cup \{r\}$, tal que $r \neq 0$ e $ml(g)$ não divide $ml(r)$ para todo $g \in G_i$. Então

$$\langle ml(G_1) \rangle \subsetneq \langle ml(G_2) \rangle \subsetneq ... \subsetneq \langle ml(G_i) \rangle \subsetneq ...,$$

mas pelo Teorema da Base de Hilbert temos que todo ideal de $K[x]$ é finitamente gerado, assim podemos concluir que essa cadeia é estacionária. Agora que sabemos que esse algoritmo finaliza depois de um número finito de iterações, então existe $j > 0$ tal que o resto da divisão de $S(f, h)$ por G_j é zero, para todo $f, h \in G_j$, assim pela proposição 2.5 temos que G_j é uma base de Gröbner para I. □

Observação 2.3. Um algoritmo análogo para encontrar uma base de Gröbner para módulos pode ser encontrado em [1] capitulo 3.

Exemplo 2.8. Considere $I = \langle x^2, xy + y^2 \rangle$, como no exemplo 2.5, sabemos que $G = \{x^2, xy + y^2\}$ não é uma base de Gröbner, então vamos aplicar o algoritmo de Buchberger para encontrar uma base.

Passo 1: Consideremos $G_1 = \{f_1, f_2\}$, então $S(f_1, f_2) = -xy^2$, fazendo a divisão de $S(f_1, f_2)$ por G_1, temos resto $f_3 = y^3$.

Passo 2: Agora considere $G_2 = \{f_1, f_2, f_3\}$. Então

$$S(f_1, f_3) = 0 \text{ e } S(f_2, f_3) = y^4.$$

Como $S(f_2, f_3) = 0f_1 + 0f_2 + yf^3$, temos que o resto da divisão de $S(f_2, f_3)$ por G_2 é zero, assim podemos concluir que G_2 é uma base de Gröbner para I.

3 PRIMEIRA APLICAÇÃO DE BASES DE GRÖBNER A CÓDIGOS

3.1 PEGADA

Novamente, consideramos K um corpo e $K[x]$ o anel de polinômios de n variáveis com coeficientes em K.

Definição 3.1. Seja $I \subset K[x]$ um ideal. A pegada de I (com respeito a uma ordem monomial fixada) é o conjunto:

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

Exemplo 3.1. Considere o ideal $I = \langle x, y\rangle \subset K[x, y]$, como o monômio líder de qualquer polinômio não constante de $K[x, y]$ é divisível por x ou por y, podemos concluir que $G = \{x, y\}$ é uma base de Gröbner para I e $\Delta(I) = \{1\}$.

Proposição 3.1. Seja $I \subset K[x]$ um ideal e seja $\{g_1, ..., g_s\}$ uma de base de Gröbner para I. Então, o monômio M pertence a $\Delta(I)$ se, somente se, M não é múltiplo de $ml(g_i)$ para todo $i = 1, ..., s$

Demonstração. Suponha que $M \in \Delta(I)$. Se $ml(g_i)$ dividisse M teríamos $M \in I$, contradizendo a hipótese de que $M \in \Delta(I)$. Portanto, $ml(g_i)$ não divide M para todo $i = 1, ..., s$. Agora suponha que M não é múltiplo de $ml(g_i)$ para todo $i = 1, ..., s$, então, pela definição de base de Gröbner, temos que M não é monômio líder de nenhum polinômio de I. □

Exemplo 3.2. Seja $I = \langle x^2, xy + y^2, y^3\rangle \subset K[x, y]$, e considere $\mathbb{M}_n$ com a ordem lexicográfica, como sabemos pelo exemplo 2.8 que $G = \{x^2, xy + y^2, y^3\}$ é uma base de Gröbner e pela proposição 3.1, temos que $\Delta(I)$ é formado pelos monômios que não são combinação de $ml(I) = \{x^2, xy, y^3\}$, assim temos que $\Delta(I) = \{1, x, y, y^2\}$.

Teorema 3.1. Seja $I \subset K[x]$ um ideal, então

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

é uma base para $K[x]/I$ como um K-espaço vetorial.

Demonstração. Seja $G = \{g_1, ..., g_t\}$ uma base de Gröbner para I com respeito a mesma ordem monomial usada para determinar $\Delta(I)$ e seja $f \in K[x]$. Dividindo f por G obtemos $q_1, ..., q_r$ e r tais que

$$f = q_1g_1 + ... + q_tg_t + r$$

com $r = \sum_{i=1}^{t} a_iM_i$, $a_i \in K[x]$ e $M_i \in \Delta(I)$ para todo $i = 1, ..., t$. Como $f + I = q_1g_1 + ... + q_tg_t + r + I$ e $q_ig_i \in I$, temos $f + I = r + I$. Portanto $\mathscr{B}$ gera $K[x]/I$ como

um k-espaço vetorial. Agora seja $\sum_{i=1}^{l} b_i(M_i + I) = 0 + I$, onde $b_i \in K$ e $M_i \in \Delta(I)$ para todo $i = 1, ..., l$. Então $\sum_{i=1}^{l} b_i M_i \in I$ com $b_i = 0$, pois caso $b_i \neq 0$ e temos que $ml(g_i)$ não divide M_i para todo $j = 1, ..., t$ e $i = 1, ..., l$ teríamos $\sum_{i=1}^{l} b_i M_i \notin I$. Isso mostra que $\mathscr{B}$ é linearmente independente sobre K. Assim concluímos que $\mathscr{B}$ é uma base para $K[x]/I$ □

Exemplo 3.3. Considerando I como no exemplo 3.2, temos que $K[x, y]/I$ é um K-espaço vetorial de dimensão 4 e $\{1 + I, x + I, y + I, y^2 + I\}$ é uma base.

Sejam $I \subset K[x]$ um ideal e $\{f_1, ..., f_t\}$ uma base para I. Vamos denotar por $\Delta(ml(f_1), ..., ml(f_t))$ o conjunto

$$\{M \in \mathbb{M}_n \mid M \text{ não é um múltiplo de } f_i \text{ para todo } i = 1, ..., t\}$$

Observação 3.1. $\Delta(I) \subset \Delta(ml(f_1), ..., ml(f_t))$ e $\Delta(I) = \Delta(ml(f_1), ..., ml(f_t))$ se, e somente se, $\{f_1, ..., f_t\}$ é uma base de Gröbner para I

Demonstração. Seja $f \in \Delta(I)$, temos que f não é monômio líder de nenhum polinômio de I. Isso implica que f não é divisível por f_i para todo $i = 1, ..., n$, pois I é um ideal de $K[x]$, assim concluímos que $\Delta(I) \subset \Delta(ml(f_1), ..., ml(f_t))$. Sejam $\Delta(I) = \Delta(ml(f_1), ..., ml(f_t))$ e $f \in I$. Como $\Delta(I) = \Delta(ml(f_1), ..., ml(f_t))$, temos que f é divisível por algum f_i, logo $\{f_1, ..., f_t\}$ é uma base de Gröbner para I. Agora suponhamos que $\{f_1, ..., f_t\}$ é um base de Gröbner. Se $f \in \Delta(ml(f_1), ..., ml(f_t))$, temos que $f \notin I$, pois $\{f_1, ..., f_t\}$ é uma base de Gröbner, logo $f \in \Delta(I)$. □

3.2 NOÇÕES BÁSICAS SOBRE CÓDIGOS

Nesta seção, iremos introduzir algumas noções básicas da teoria dos códigos. Seja $\mathbb{F}_q$ um corpo finito com $q = p^k$ elementos, com p primo. Consideramos o espaço vetorial $n-$dimensional $\mathbb{F}_q^n$ cujos elementos são as n-uplas $a = (a_1, ..., a_n)$ com $a_i \in \mathbb{F}_q$.

Definição 3.2. Para $a = (a_1, ..., a_n)$ e $b = (b_1, ..., b_n)$ em $\mathbb{F}_q^n$ definimos a distância de Hamming entre a e b como

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

Definimos ainda o peso de $a \in \mathbb{F}_q$ como seu número de entradas não-nulas, isto é

$$w(a) = |\{i : a_i \neq 0\}| = d(a, 0)\,.$$

Podemos provar que a distância de Hamming é uma métrica em $\mathbb{F}_q^n$, em particular, vale a desigualdade triangular:

$$d(a, c) \leq d(a, b) + d(b, c)$$

para todos $a, b, c \in \mathbb{F}_q^n$;

Definição 3.3. Um código C é um subespaço vetorial de $\mathbb{F}_q^n$ cujos elementos são chamados de palavras do código. Chamamos de n o comprimento de C e $\dim C$ é a dimensão de C. Um $[n, k]$-código é um código de comprimento n e dimensão k.

Definição 3.4. A distância mínima $d(C)$ de um código $C \neq \{0\}$ é definida por

$$d(C) = \min\{d(a, b) \,|\, a, b \in C \text{ e } a \neq b\} = \min\{wt(c) \,|\, 0 \neq c \in C\}.$$

Vamos nos referir a um $[n, k]-$código com distância mínima d por $[n, k, d]$-código.

Exemplo 3.4. No jogo de Pac-Man os únicos movimentos que precisamos fazer é direita, esquerda, para cima e para baixo. Ao criar um controle para jogar Pac-Man podemos codificar os quatro comandos como elementos de $\mathbb{F}_2 \times \mathbb{F}_2$ da seguinte maneira

$$\begin{array}{ll} \text{Esquerda} \longrightarrow 00 & \text{Para cima} \longrightarrow 10 \\ \text{Direita} \longrightarrow 01 & \text{Para baixo} \longrightarrow 11 \end{array}$$

Mas se recebermos 00, por exemplo, não é possível saber se foi de fato enviado 00 ou 10 ou 01, devido a proximidade das palavras, então, para termos um um código melhor podemos modificá-lo da seguinte maneira

$$\begin{array}{llll} 00 & \longrightarrow 00000 & 10 & \longrightarrow 10110 \\ 01 & \longrightarrow 01011 & 11 & \longrightarrow 11101 \end{array}$$

Agora caso o controle transmita um digito errado, podemos descobrir o erro, o que não era possível anteriormente. Observe que o conjunto C formado por $\{00000, 01011, 10110, 11101\}$ é um subespaço vetorial de $\mathbb{F}_2^5$. Assim temos que C é um código com $n = 5, k = 2$ e $d = 3$.

Para um $[n, k, d]-$código C, seja $t = [(d-1)/2]$ onde $[x]$ denota a parte inteira do número real x (i.e., $x = [x] + \epsilon$ com $[x] \in \mathbb{Z}$ e $0 \leq \epsilon < 1$). Então, C é dito capaz de corrigir até t erros e detectar até $d-1$ erros. Assim, se $u \in \mathbb{F}_q$ e $d(u, c) \leq t$ para todo $c \in C$ então c é uma palavra-código com $d(u, c) \leq t$

Exemplo 3.5. Considerando o exemplo 3.4 temos $t = [(d-1)/2] = [(3-1)/2] = 1$. Portanto o código C é capaz de corrigir um erro e consegue detectar até 2 erros.

Um modo simples de descrever um código C explicitamente é escrever uma base de C (como espaço vetorial sobre $\mathbb{F}_q^n$).

Definição 3.5. Seja C um $[n, k]$ código sobre $\mathbb{F}_q$. Uma matriz geradora de C é uma matriz $k \times n$ cujas linhas formam uma base de C

As palavras do código são, então, todas as combinações lineares das linhas da matriz geradora M, isto é, o código linear é o espaço gerado pelas linhas de sua matriz geradora. Dessa forma, um processo imediato de codificação é: dado $w \in \mathbb{F}_q^k$, multiplicamos o vetor linha $w = (w_1, ..., w_k)$ por M, obtendo uma palavra codificada $c = wM$.

Exemplo 3.6. Olhando novamente para o exemplo 3.4 temos que $\{01011, 10110\}$ é uma base para C, assim a matriz geradora de C é

$$M = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Vamos agora codificar 11, para isso basta multiplicarmos o vetor (1,1) pela matriz M, assim

$$\begin{bmatrix} 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Logo temos a palavra codificada 11101.

Definição 3.6. O produto interno canônico em $\mathbb{F}_q^n$ é definido por

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

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

Essa é uma forma bilinear não degenerada em $\mathbb{F}_q^n$.

Definição 3.7. Se $C \subseteq \mathbb{F}_q^n$ é um código então

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

é chamado o dual de C. O código C é chamado auto-dual se $C = C^{\perp}$ e auto-ortogonal se $C \subseteq C^{\perp}$.

Observação 3.2. Da Álgebra Linear, temos que o dual de um $[n, k]$-código é um $[n, n-k]$-código e $(C^{\perp})^{\perp} = C$. Em particular, a dimensão de um código auto-dual de comprimento n é $n/2$.

Definição 3.8. Uma matriz geradora H de $C^{\perp}$ é dita matriz de teste de paridade de C.

Claramente uma matriz de teste de paridade H de um $[n, k]$ código C é uma matriz $(n-k) \times n$ de posto $n-k$, e temos que

$$C = \{u \in \mathbb{F}_q^n \mid H.u^t = 0\},$$

onde u^t denota a transposta de u. Assim uma matriz de verificação de paridade identifica se um vetor $u \in \mathbb{F}_q^n$ está no código ou não.

Um dos problemas básicos na teoria de códigos algébricos é o de construir, sobre um alfabeto fixado $\mathbb{F}_q$, códigos cuja dimensão e distância mínima sejam grandes em comparação com o seu comprimento. Entretanto, há algumas restrições: se a dimensão de um código é grande (com relação ao seu comprimento), então sua distância mínima é pequena. A cota mais simples é a chamada Cota de Singleton:

Proposição 3.2. Para um $[n, k, d]$-código C vale

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

Demonstração. Considere o subespaço $E \subseteq \mathbb{F}_q^n$ dado por

$$E := \{(a_1, ...a_n) \leq \mathbb{F}_q^n \mid a_i = 0 \text{ para todo } i \leq d\}$$

Como cada $a \in E$ tem peso menor ou igual a $d-1$, então $E \cap C = \{0\}$. Como $\dim E = d-1$ obtemos

$$k + (d-1) = \dim C + \dim E = \dim(C + E) + \dim(C \cap E) = \dim(C + E) \leq n$$

□

Códigos cujos parâmetros atingem essa cota, isto é, tais que $k + d = n + 1$ são chamados códigos MDS (do inglês, *maximum distance separable*). É possível provar que se $n \leq q + 1$, então existe um código MDS sobre $\mathbb{F}_q$ para toda dimensão $k \leq n$.

3.3 CÓDIGOS CARTESIANOS AFINS

Iniciaremos essa seção apresentando um conceito clássico da geometria algébrica. Para o leitor que desejar saber mais sobre o assunto, sugerimos [6].

Definição 3.9. Seja $I \subset K[x]$ um ideal. A variedade afim associada a I é o conjunto

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

Podemos ver que se $I = (g_1, ..., g_t)$, então $(a_1, ..., a_n) \in V(I)$ se, e somente se, $g_i(a_1, ..., a_n) = 0$ para todo $i = 1, ..., t$. Dado $V = V(I)$ podemos considerar o conjunto de todos os polinômios que possuem todos os elementos de V como raiz. Denotaremos esse conjunto por $I(V)$. Temos que $I \subset I(V)$, mas será que $I(V) \subset I$? A resposta está no seguinte teorema, cuja demonstração pode ser encontrada em [6].

Teorema 3.2 (**Teorema dos zeros de Hilbert**)**.** Sejam K algebricamente fechado e I um ideal de $K[x]$. Então $I(V(I)) = \sqrt{I}$.

Lema 3.1. Seja $I \subset K[x]$ um ideal e seja $P_1, ..., P_r$ elementos distintos de $V(I)$. Então, existem polinômios $p_1, ..., p_r \in K[x]$ tais que $p_i(P_j) = \delta_{ij}$ para todo $i, j \in \{1, ..., r\}$, onde δ_{ij} é o delta de Kronecker ($p_i(P_j)$ é igual a 0 se $i \neq j$ e 1 se $i = j$).

Demonstração. Seja $P_i = (a_{i1}, ..., a_{in}) \in K^n$ onde $i = 1, ..., r$. Vamos mostrar como obter polinômios p_i como no enunciado. Como todos os pontos são distintos, para $i \in \{2, ..., n\}$ existe $j_i \in \{1, ..., n\}$ tal que $a_{1j_i} \neq a_{ij_i}$. Seja $h_i = (x_{j_i} - a_{ij_i})/(a_{1j_i} - a_{ij_i})$, então $h_i(P_1) = 1$ e $h_i(P_i) = 0$ para todo $i = 2, ..., r$. Assim, tomando $p_1 = \prod_{i=2}^{r} h_i$, obtemos $p_1(P_j) = 1$ e $p_1(P_i) = 0$ para todo $i = 2, ..., r$. De forma análoga podemos obter $p_2, ..., p_r$. □

Proposição 3.3. Seja $I \subset K[x]$ um ideal tal que $\Delta(I)$ é um conjunto finito. Então $V(I)$ é também um conjunto finito e $\#(V(I)) \leq \#(\Delta(I))$.

Demonstração. Sejam $P_1, ..., P_r$ elementos distintos de $V(I)$, a partir desses elementos encontraremos um conjunto em $K[x]/I$ que é linearmente independente e possui r elementos. Isso provará a proposição, pois sabemos que $\#(V(I))$ é a dimensão de $K[x]/I$ como $K-$espaço vetorial, pelo teorema 3.1. Pelo lema 3.1, sabemos que existem $p_1, ..., p_r \in K[x]$ tais que $p_i(P_j) = \delta_{ij}$ para todo $i, j \in \{1, ..., r\}$. Assumindo que $\sum_{i=1}^{r} a_i(p_i + I) = 0 + I$, onde $a_1, ..., a_r \in K$, então $\sum_{i=1}^{r} a_i p_i \in I$. Assim $\sum_{i=1}^{r} a_i p_i(P_j) = 0$, o que implica que $j \in \{1, ..., r\}$. Logo $\{p_1 + I, ..., p_r + I\}$ é um conjunto linearmente independente sobre $K[x]/I$, como queríamos. □

A demonstração do resultado a seguir pode ser encontrada em [2], teorema 8.32.

Teorema 3.3. Seja $I \subset K[x]$ um ideal tal que $\Delta(I)$ é um conjunto finito e seja L uma extensão algebricamente fechada de K. Então, o conjunto

$$V_L(I) = \{(a_1, ..., a_n) \in L^n | f(a_1, ..., a_n) = 0 \text{ para todo } f \in I\}$$

é finito e $\#(V(I)) \leq \#(\Delta(I))$. Além disso, se K é um corpo perfeito (isto é, finito ou de característica zero) e I é um ideal radical, então $\#(V_L(I)) = \#(\Delta(I))$.

Em 1988, Fitzgerald e Lax (ver [9]) propuseram uma construção de códigos utilizando variedades afins que apresentaremos a seguir.

Sejam $I = (g_1, ..., g_s) \subset \mathbb{F}_q[x]$ e $I_q = (g_1, ..., g_t, x_1^q - x_1, ..., x_n^q - x_n)$. Temos que

$$\prod_{a \in \mathbb{F}_q} (x - a) = (x^q - x)$$

sempre que $V(I) = V(I_q)$. A partir de agora, vamos considerar a ordem lexicográfica graduada em $M \subset \mathbb{F}_q[x]$. Pela observação 3.1 obtemos que

$$\#(\Delta(I_q)) \leq \#(\Delta(ml(g_1), ..., ml(g_t), x_1^q, ..., x_n^q)) \leq q^n$$

e, pela proposição 3.3, temos que

$$\#(V(I_q)) \leq \#(\Delta(I_q))\,.$$

Consideramos $V(I_q) = \{P_1, ..., P_n\}$ e a aplicação

$$\begin{aligned} \varphi : \mathbb{F}_q[x]/I_q &\longrightarrow \mathbb{F}_q^m \\ f + I_q &\longmapsto (f(P_1), ..., f(P_m)) \end{aligned}$$

Proposição 3.4. A função φ é um isomorfismo de $\mathbb{F}_q$-espaços vetoriais.

Demonstração. Temos que φ é uma transformação linear, então basta mostrarmos que φ é sobrejetora e $\dim(\mathbb{F}_q[x]/I_q) = m$. Como $x_i^q - x_i \in I_q$ para todo $i = 1, ..., n$, obtemos que I_q é um ideal radical, pois contém um polinômio de uma variável sem quadrado em cada variável (veja, por exemplo, [2], proposição 8.14). Além disso, para qualquer extensão algébrica fechada L de $\mathbb{F}_q$, temos $V_L(I_q) = V_{\mathbb{F}_q}(I_q)$. Assim, pelos teoremas 3.1 e 3.3, obtemos que $\dim(\mathbb{F}_q[x]/I_q) = \#(\Delta(I_q)) = m$. Pelo lema 3.1, temos que existem polinômios $p_1, ..., p_m \in \mathbb{F}_q[x]$ tais que $p_i(P_j) = \delta_{ij}$ para todo $i, j \in \{1, ..., m\}$, donde $\varphi(p_i + I_q) = (p_i(P_1), ..., p_i(P_m)) = e_i$, onde e_i é o i-ésimo vetor da base canônica de $\mathbb{F}_q^m$ para todo $i \in \{1, ..., m\}$. Isso prova que φ é sobrejetora. Portanto, φ é um isomorfismo. □

Definição 3.10. Seja $L \subset \mathbb{F}_q[x]/I_q$ um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q[x]/I_q$. A imagem $\varphi(L) = C(L)$ é chamado código de variedade afim associado a L.

Sejam $A_1, ..., A_n$ subconjuntos não vazios de $\mathbb{F}_q$ e $X = A_1 \times ... \times A_n$. Para cada $i \in \{1, ..., n\}$, seja $f_i = \prod_{c \in A_i} (x_i - c)$. Se $I = (f_1, ..., f_n)$, então $V(I) = X$. Ainda, se $I_q = (f_1, ..., f_n, x_1^q - x_1, ..., x_n^q - x_n)$, temos que $I_q = I$, pois f_i é um fator de $x_i^q - x_i$. Consideramos, para todo inteiro $d \geq 0$, o $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q[x]/I$ dado por

$$L_d = \{p + I \,|\, p = 0 \text{ ou } \deg(p) \leq d\}\,,$$

onde $p \in \mathbb{F}_q[x]$.

Definição 3.11. O código cartesiano afim $C(d)$ é a imagem de L_d por φ.

Quando $A_i = \mathbb{F}_q$ para todo $i = 1, ..., n$ temos os codigos de Reed-Muller generalizados, um exemplo muito estudado de códigos lineares.

Agora vamos determinar o comprimento de $C(d)$. Seja $d_i = \#(A_i)$ para todo $i = \{1, ..., n\}$. Então, $V(I) = d_1 \cdot ... \cdot d_n$ é o comprimento de $C(d)$ para todo $d \geq 0$.

Lema 3.2. $\{f_1, ..., f_n\}$ é uma base de Gröbner para I.

Demonstração. Como $f_i = \prod_{c \in A_i} (x_i - c)$ e $\#(A_i) = d_i$, então $ml(f_i) = x_i^{d_i}$ para todo $\{i = 1, ..., n\}$. Assim temos

$$\Delta(I) \subset \{x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n} | 0 \leq \alpha_i < d_i, \text{ para todo } i = \{1, ..., n\}\}$$

Como

$$\#(V(I)) = d_1 \cdot ... \cdot d_n \leq \#(\Delta(I)) \leq d_1 \cdot ... \cdot d_n$$

obtemos em particular que $\#\Delta(I) = d_1, ..., d_n$. Isso mostra que $B = \{f_1, ..., f_n\}$ é uma base de Gröbner para I. De fato, caso contrário, pelo algoritmo de Buchberger (Teorema 2.5), teríamos que adicionar a B um polinômio cujo o monômio líder não é múltiplo de $x_i^{d_i}$ para todo $i = \{1, ..., n\}$, o que implicaria que $\#(\Delta(I)) < d_1 \cdot ... \cdot d_n$. Isso e uma contradição, pois estaríamos retirando um elemento de $\Delta(I)$ e acrescentando em B o que causaria desigualdade. □

Lema 3.3. O ideal de $X = A_1 \times ... \times A_n$ é I.

Demonstração. Da forma que X e I foram definidos, temos que $I \subset I(X)$, com isso $V(I) \supset V(I(X))$, mas como $V(I(X)) \supset X$ e $V(I) = X$, então $\#(V(I)) \geq \#(V(I(X))) \geq \#(X) = \#(V(I))$. Pela proposição 3.3 e o lema 3.2 temos que $d_1 \cdot ... \cdot d_n \leq \#(V(I(X))) \leq \#(\Delta I(X)) \leq \#(\Delta(I)) = d_1 \cdot ... \cdot d_n$. Como $\{f_1, ..., f_n\} \subset I \subset I(X)$, pela demostração do lema anterior temos que $\{f_1, ..., f_n\}$ é uma base de Gröbner para $I(X)$, daí pelo corolário 2.2, segue que $I = I(X)$. □

Agora, queremos calcular a dimensão de $C(d)$. Como φ é um isomorfismo e $C(d) = \varphi(L_d)$ temos que $\dim C(d) = \dim L_d$. Seja

$$\Delta(I)_{\leq d} = \{M \in \Delta(I) | \deg(M) \leq d\}.$$

Proposição 3.5. O conjunto $\{M + I \mid M \in \Delta(I)_{\leq d}\}$ é uma base para L_d.

Demonstração. Pelo teorema 3.1, temos que $\{M + I | M \in \Delta(I)_{\leq d}\}$ é um conjunto linearmente independente que contém L_d. Seja $f \in \mathbb{F}_q[x], f \neq 0$ tal que $\deg(f) \leq d$. Seja r o resto da divisão de f por $\{f_1, ..., f_n\}$, então $f + I = r + I$ e $\deg(r) < d$. Daí temos que $r \in \Delta(I)_{\leq d}$, o que implica que $f + I$ é uma combinação dos elementos de $\{M + I | M \in \Delta(I)_{\leq d}\}$. □

Lema 3.4. A dimensão de $C(d)$ é $\dim C(d) = \#(\Delta(I)_{\leq d})$, em particular $\dim C(d) = d_1 \cdot ... \cdot d_n$ e $d_{\min} C(d) = 1$ para todo $d \geq \sum_{i=1}^{n} (d_i - 1)$

Demonstração. Como $\dim C(d) = \dim L_d$ e $\dim L_d = \#\Delta(I)_{\leq d}$, então $\dim C(d) = \#\Delta(I)_{\leq d}$. Já que $\{f_1, ..., f_n\}$ é uma base de Gröbner para I, temos que

$$\Delta(I) = \{x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n} | 0 \leq \alpha_i \leq d_i - 1, \text{ para todo } i = \{1, ..., n\}\},$$

assim $\Delta(I)_{\leq d} = \Delta(I)$ onde $d \geq \sum_{i=1}^{n}(d_i - 1)$. Logo $\Delta(I)_{\leq d} = \Delta(I) = d_1 \cdot ... \cdot d_n$. Pelo fato que $\varphi(L(d)) = \mathbb{F}_q^{d_1 \cdot ... \cdot d_n}$, temos, pela Cota de Singleton (proposição 3.2), que $d_{\min} C(d) = 1$. $\square$

Teorema 3.4. A dimensão de $C(d)$ para $0 \leq d < \sum_{i=1}^{n}(d_i - 1)$ é dada por

$$\dim(C(d)) = \binom{n+d}{d} - \sum_{i=1}^{n}\binom{n+d-d_i}{d-d_i} + ... + (-1)^j \sum_{1 \leq i_1 < ... < i_j \leq n}\binom{n+d-d_{i_1}-...-d_{i_j}}{d-d_{i_1}-...-d_{i_j}} + ... + (-1)^n \binom{n+d-d_1-...-d_n}{d-d_1-...-d_n}.$$

Demonstração. Pelo lema anterior, sabemos que $\dim C(d) = \#(\Delta(I)_{\leq d})$. Então, $\dim C(d)$ é igual ao número de monômios de $\Delta(I)$ da forma $x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n}$ com $0 \leq \prod_{i=1}^{n} \alpha_i \leq d_i$. Seja

$$h(t) = (1 + t + ... + t^{d_1 - 1}) \cdot ... \cdot (1 + t + ... + t^{d_n - 1}).$$

O coeficiente de t^a em $h(t)$ é igual ao número de monômios em $\Delta(I)$ com grau a para todo $a \in \{0, ..., \sum_{i=1}^{n}(d_i - 1)\}$. Assim para encontrar a $\dim C(d)$, basta calcular os coeficientes de $t^0, t, ..., t^d$ e soma-los. Porém existe uma maneira mais rápida, pois existe uma bijeção entre os conjuntos $\Delta(I)_{\leq d}$ e $\nabla_d = \{x_0^{\alpha_0} \cdot ... \cdot x_n^{\alpha_n}$ com $\sum_{i=0}^{n} \alpha_i = d$ e $0 \leq \alpha_i \leq d_i - 1$, para todo $i = 1, ..., n\}$ dada por $\beta : \Delta(I)_{\leq d} \longrightarrow \nabla_d$ onde $\beta(M) = x_0^d M(x_1/x_0, ..., x_n/x_0)$. Temos que $\beta^{-1} : \nabla_d \longrightarrow \Delta(I)_{\leq d}$ é dada por $\beta^{-1}(N) = N(1, x_1, ..., x_n)$. Como α_0 é um inteiro maior que zero que satisfaz $\sum_{i=0}^{n} \alpha_i = d$ e como α_i varia zero a $d_i - 1$ para todo $i = 1, ..., n$, então α_0 pode variar de zero a d. Agora consideremos

$$H(t) = (1 + t + t^2 + ... + t^d) \cdot (1 + t + ... + t^{d_1 - 1}) \cdot ... \cdot (1 + t + ... + t^{d_n - 1})$$

então o coeficiente de t^d é a cardinalidade de ∇_d, mas se considerarmos

$$H(t) = (1 + t + t^2 + ...) \cdot (1 + t + ... + t^{d_1 - 1}) \cdot ... \cdot (1 + t + ... + t^{d_n - 1})$$

o coeficiente de t^d continua sendo a cardinalidade de ∇_d, pois a parte $t^{d+1} + t^{d+2} + ...$ não altera o valor do coeficiente de t^d. Para calcular o coeficiente de t^d observemos que $H(t)$ é uma função real de uma variável t definida em uma vizinhança de 0, para $|t| < 1$. Daí $1 + t + t^2 + ... = \frac{1}{1-t}$, assim temos

$$H(t) = \frac{1}{1-t} \cdot \frac{1-t^{d_1}}{1-t} \cdot ... \cdot \frac{1-t^{d_n}}{1-t}$$

logo

$$H(t) = \frac{1}{1-t} \cdot \prod_{i=1}^{n}(1 - t^{d_i}).$$

Usando que $\frac{1}{(1-t)^{n+1}} = \sum_{j=0}^{\infty} \binom{n+j}{j} t^j$, obtemos

$$\begin{aligned}
H(t) =& \sum_{j=0}^{\infty} \binom{n+j}{j} t^j \cdot \prod_{i=1}^{n} (1 - t^{d_i}) \\
=& \left(\sum_{j=0}^{\infty} \binom{n+j}{j} t^j \right) (1 - \sum_{i=1}^{n} t^{d_i} + \sum_{1 \le i_1 < i_2 \le n} t^{d_{i_1}+d_{i_2}} + ... + \\
& (-1)^j \sum_{1 \le i_1 < ... < i_j \le n} t^{d_{i_1}+...+d_{i_j}} + ... + (-1)^n t^{d_{i_1}+...+d_{i_n}}) \\
=& \sum_{j=0}^{\infty} \binom{n+j}{j} t^j - \sum_{j=0}^{\infty} \binom{n+j}{j} t^j \cdot \sum_{i=1}^{n} t^{d_i} + \sum_{j=0}^{\infty} \binom{n+j}{j} t^j \cdot \sum_{1 \le i_1 < i_2 \le n} t^{d_{i_1}+d_{i_2}} + ... + \\
& \sum_{j=0}^{\infty} \binom{n+j}{j} t^j \cdot (-1)^j \sum_{1 \le i_1 < ... < i_j \le n} t^{d_{i_1}+...+d_{i_j}} + ... + \sum_{j=0}^{\infty} \binom{n+j}{j} t^j) \cdot (-1)^n t^{d_{i_1}+...+d_{i_n}}
\end{aligned}$$

Como queremos calcular o coeficiente de t^d e já que j varia de zero a infinito, então vamos olhar apenas para os valores de j que nos darão t^d. Assim teremos

$$\binom{n+d}{d} t^d - \sum_{i=1}^{n} \binom{n+d-d_i}{d-d_i} t^d + ... + (-1)^j \sum_{1 \le i_1 < ... < i_j \le n} \binom{n+d-d_{i_1}-...-d_{i_j}}{d-d_{i_1}-...-d_{i_j}} t^d + ... + (-1)^n \binom{n+d-d_{i_1}-...-d_{i_n}}{d-d_{i_1}-...-d_{i_n}} t^d,$$

como queríamos. □

Para encontrar a distância mínima de $C(d)$, para $0 \le d < \sum_{i=1}^{n}(d_i - 1)$, precisaremos do seguinte resultado.

Lema 3.5. Sejam $0 < d_1 \le ... \le d_n$ e $s < \sum_{i=1}^{n}(d_i - 1)$ inteiro. Seja $m(\alpha_1, ..., \alpha_n) = \prod_{i=1}^{n}(d_i - \alpha_i)$, onde $0 \le \alpha_i < d_i$ é um inteiro para todo $i = 1, ..., n$. Então

$$\min\{m(\alpha_1, ..., \alpha_n) | \alpha_1 + ... + \alpha_n \le s\} = (d_{k+1} - l) \prod_{i=k+2}^{n} d_i$$

onde k e l são unicamente definidos por $s = \sum_{i=1}^{k}(d_i - 1) + l$ com $0 \le l < d_{k+1} - 1$. Se $k + 1 = n$ então teremos que $\prod_{i=k+2}^{n} d_i = 1$ e se $s < d_1 - 1$ então $k = 0$ e $l = s$.

Demonstração. Observe que o valor mínimo é alcançado quando temos os valores máximos para α_i, ou seja, para $\sum_{i=1}^{n} \alpha_i = s$, o lema afirma que esse valor máximo é atingido nos seguintes valores de α_i

$$(\alpha_1 = d_1 - 1, ..., \alpha_k = d_k - 1, \alpha_{k+1} = l, \alpha_{k+2} = 0, ..., \alpha_n = 0)$$

Portanto seja $\alpha = (\alpha_1, ..., \alpha_n)$ com $\sum_{i=1}^{n} \alpha_i = s$, vamos provar que $\alpha_i = d_i - 1$ para $i = 1, ..., k$ e $\alpha_i = 0$ para $i = k+2, ..., n$, então suponha que $\alpha_{i_1} < d_{i_1} - 1$ para algum $i_1 \in \{1, ..., k\}$ e seja $i_2 \in \{k+1, ..., n\}$ tal que $\alpha_{i_2} > 0$ e $\alpha_{i_1} + \alpha_{i_2} \leq d_{i_1} - 1$. Denotemos por α' a n-upla obtida de α substituindo α_{i_1} por $\alpha_{i_1} + \alpha_{i_2}$ e α_{i_2} por 0, assim teremos que

$$m(\alpha) - m(\alpha') = (\alpha_{i_1}\alpha_{i_2} + (di_2 - d_{i_1})\alpha_{i_2}) \cdot \prod_{i=1; i\neq i_1, i_2}^{n} (d_i - \alpha_i) \geq 0,$$

isso implica que $m(\alpha) \geq m(\alpha')$. Agora se $i_2 \in \{k+1, ..., n\}$ com $\alpha_{i_2} > 0$ e $\alpha_{i_1} + \alpha_{i_2} > d_{i_1} - 1$, então denotaremos por α'' a n-upla obtida de α substituindo α_{i_1} por $d_{i_1} - 1$ e α_{i_2} por $\alpha_{i_2} - (d_{i_1} - 1 - \alpha_{i_1})$, teremos

$$m(\alpha) - m(\alpha'') = (d_{i_1 - 1 - \alpha_{i_1}})(d_{i_1 - 1 - \alpha_{i_2}}). \prod_{i=1; i\neq i_1, i_2}^{n} (d_i - \alpha_i) \geq 0,$$

implicando que $m(\alpha) \geq m(\alpha'')$. Assim provamos que se m atingir o mínimo de α podemos assumir que $\alpha_i = d_i - 1$ para todo $i = 1, ..., k$ e $\alpha_i = 0$ para $i = k+2, ..., n$. Agora falta provar que $\alpha_{k+1} = l$. Temos que $s = \sum_{i=1}^{n} \alpha_i$, $\sum_{i=1}^{k} \alpha_i = \sum_{i=1}^{k} (d_i - 1)$ e $\sum_{i=k+2}^{n} = 0$, assim

$$l = s - \sum_{i=1}^{k} (d_i - 1) = \sum_{i=1}^{k} \alpha_i + \alpha_{k+1} + \sum_{i=k+2}^{n} \alpha_i - \sum_{i=1}^{k} (d_i - 1) = \alpha_{k+1},$$

como queríamos. □

Teorema 3.5. Seja $0 \leq d < \sum_{i=1}^{n} (d_i - 1)$, a distância mínima de $C(d)$ é $(d_{k+1} - l) \prod_{i=k+2}^{n} (d_i - 1)$, onde k e l são unicamente definidos por $d = \sum_{i=1}^{k} (d_i - 1) + l$ com $0 \leq l < d_{k+1} - 1$. Como no resultado anterior, se $k + 1 = n$ teremos que $\prod_{i=k+2}^{n} d_i = 1$, e se $d < d_1 - 1$ então $k = 0$ e $l = d$.

Demonstração. Seja $F \in L_d$ e seja $J_F = (F, f_1, ..., f_n)$, então o número de zeros da palavra do código $\varphi(F + I) = (F(P_1), ..., F(P_m))$ é igual a $\#\{V(F) \cap \{P_1, ..., P_m\}\} = \#\{V(F) \cap V(f_1, ..., f_n)\} = \#(V(F, f_1, ..., f_n)) = \#(V(J_F))$. Assim temos que $w(\varphi(F + I)) = \prod_{i=1}^{n} d_i - \#(V(J_F))$. Pela proposição 3.3 obtemos que $\#V(J_F) \leq \#(\Delta(J_F))$. Seja $M = x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n}$ o monômio líder de F, pela observação 3.1 temos que $\Delta(J_F) \subset \Delta(M, x_1^{d_1}, ..., x_n^{d_n})$, como $0 \leq \alpha_i \leq d_i$, então temos $\prod_{i=1}^{n} (d_i - 1)$ elementos da forma $x^{\alpha_1} \cdot ... \cdot x^{\alpha_n}$. Os elementos que são múltiplos de $x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n}$, são da forma $x_1^{\lambda_1} \cdot ... \cdot x_n^{\lambda_n}$ com $\alpha_i \leq \lambda_i \leq d_i$, então fazendo a contagem temos $\prod_{i=1}^{n} (d_i - \alpha_i + 1)$ elementos. Assim podemos concluir que $\#\Delta(M, x^{d_1}, ..., x^{d_n}) = \prod_{i=1}^{n} (d_i + 1) - \prod_{i=1}^{n} (d_i - \alpha_i + 1) = \prod_{i=1}^{n} d_i - \prod_{i=1}^{n} (d_i - \alpha_i)$,

daí $\#\Delta(J_F) \leq \prod_{i=1}^{n} d_i - \prod_{i=1}^{n}(d_i - \alpha_i)$. Então, $w(\varphi(F+I)) \geq (d_{k+1} - l) \prod_{i=k+2}^{n} d_i$. Pelo lema anterior como $(d_{k+1} - l) \prod_{i=1}^{n}$ é o mínimo de $m(\alpha_1, ..., \alpha_n)$, então $w(\varphi(F+I)) \geq (d_{k+1} - l) \prod_{i=k+2}^{n} d_i$. Para ver que essa cota é alcançada, tomemos $A_i = \{a_{i1}, ..., a_{id_i}\}$ para $i = 1, ..., n$ e seja $G(x_1, ..., x_n) = \left(\prod_{i=1}^{k} \prod_{j=1}^{d_i - 1} (x_i - a_{ij}) \right) \prod_{j=1}^{l} (x_{k+1} - a_{k+1\,j})$, então $\deg(G) = \deg \left(\prod_{i=1}^{k} \prod_{j=1}^{d_i - 1} (x_i - a_{ij}) \right) + \deg \left(\prod_{j=1}^{l} (x_{k+1} - a_{k+1\,j}) \right) = \sum_{i=1}^{k} (d_i - 1) + l = d$

Temos que $A_1 \times ... \times A_n$ possui $\prod_{i=1}^{n} d_i$ elementos. Vamos calcular o número de elementos pertencente a $A_1 \times ... \times A_n$ que não é raiz de G. Nas k primeiras coordenadas temos uma única opção que é $(a_{id_1}, ..., a_{id_k})$, na $(k+1)$-ésima coordenadas temos $(d_{k+1} - l)$ opções e a partir de $k+1$ temos d_i opções para cada $i > k+1$, então G possui $\prod_{i=1}^{n} d_i - (d_{k+1} - l) \prod_{i=k+2}^{n} d_i$ zeros em $A_1 \times ... \times A_n$, assim $w(\varphi(G+I)) = (d_{k+1} - l) \prod_{i=k+2}^{n} d_i$.

□

4 INTRODUÇÃO A TEORIA DE CORPOS DE FUNÇÕES ALGÉBRICAS

Nesse capítulo, apresentaremos algumas definições e resultados básicos da teroria de corpos de funções algébricas necessários para o estudo de códigos algébrico-geométricos que faremos no capítulo seguinte. Sugerimos como bibliografia para o assunto a referência [11].

4.1 LUGARES

Definição 4.1. Um corpo de funções algébricas F/K de uma variável sobre um corpo K é uma extensão $F \supseteq K$ tal que F é uma extensão algébrica finita de $K(x)$ para algum $x \in F$ transcendente sobre K.

Para simplificar referiremos a F/K como um corpo de funções algébricas. O conjunto $\widetilde{K} = \{z \in F \mid z \text{ é algébrico sobre } K\}$ é um subcorpo de F, pois soma, produto e inverso de elementos algébricos é algébrico. $\widetilde{K}$ é chamado corpo de constante de F/K. Temos que $K \subseteq \widetilde{K} \subsetneq F$ e é claro que que $F/\widetilde{K}$ é um corpo de funções sobre $\widetilde{K}$. Dizemos que K é algebricamente fechado em F se $\widetilde{K} = K$.

Observação 4.1. Um elemento $z \in F$ é transcendente sobre K se, e somente se, a extensão $F/K(z)$ é de grau finito.

Definição 4.2. Um anel de valorização do corpo de funções F/K é um anel $\mathcal{O} \subseteq F$ com as seguintes propriedades:

i) $K \subsetneq \mathcal{O} \subsetneq F$.

ii) Para cada $z \in F$, temos que $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.

Proposição 4.1. Seja $\mathcal{O}$ o anel de valorização de um corpo de funções F/K. Então temos:

a) $\mathcal{O}$ é um anel local, isto é, $\mathcal{O}$ possui um único ideal maximal $P = \mathcal{O} \setminus \mathcal{O}^{\times}$, onde $\mathcal{O}^{\times} = \{z \in \mathcal{O} |$ existe um elemento $w \in \mathcal{O}$ com $zw = 1\}$ é o grupo de unidades de $\mathcal{O}$.

b) Seja $0 \neq x \in F$. Então $x \in P$, se e somente se, $x^{-1} \notin \mathcal{O}$.

c) Para um corpo $\widetilde{K}$ de constantes de F/K temos $\widetilde{K} \subseteq \mathcal{O}$ e $\widetilde{K} \cap P = \{0\}$.

Demonstração. a) Primeiramente provaremos que P é um ideal. Seja $x \in P$ e $z \in \mathcal{O}$, então $xz \notin \mathcal{O}^{\times}$, pois se existisse $y \in \mathcal{O}$ tal que $(xz)y = 1$, isso implicaria que x é

invertível contradizendo o fato de $x \in P$. Agora se $x, y \in P \setminus \{0\}$, então xy^{-1} ou yx^{-1} pertence a $\mathscr{O}$, suponha sem perda de generalidade que $xy^{-1} \in \mathscr{O}$, isso implica que $xy^{-1}+1 \in \mathscr{O}$, assim $x+y = (xy^{-1}+1)y \in P$. P é um ideal maximal único, pois seja um ideal J tal que $P \subset J \subset \mathscr{O}$, e seja $a \in J \setminus P$, logo a é invertível e portanto teremos $J = \mathscr{O}$.

b) Se $x \in P$, segue que $x^{-1} \notin \mathscr{O}$. Por outro lado se $x^{-1} \notin \mathscr{O}$, então $x \in \mathscr{O}$, isso implica que $x \in P$, pela definição de P

c) Seja $z \in \widetilde{K}$ e suponha que $z \notin \mathscr{O}$. Pela definição de $\mathscr{O}$ temos que $z^{-1} \in \mathscr{O}$. Como $\widetilde{K}$ é corpo, então z é algébrico sobre K, o que implica que z^{-1} também é algébrico sobre K, assim existem $a_1, ..., a_m \in K$ tais que

$$a_m(z^{-1})^m + \ldots + a_1(z^{-1}) + 1 = 0.$$

Mas ainda,

$$(z^{-1})(a_m(z^{-1})^{m-1} + \ldots + a_1) = -1$$

implica que

$$z = -(a_m(z^{-1})^{m-1} + \ldots + a_1) \in K[z^{-1}] \subseteq \mathscr{O}$$

que é uma contradição, logo $\widetilde{K} \subseteq \mathscr{O}$. De forma análoga, podemos mostrar que se $z \in \widetilde{K} \setminus \{0\}$, então $z \in \mathscr{O}$, consequentemente $z \in \mathscr{O}^*$ e daí $\widetilde{K} \cap P = \{0\}$

□

Lema 4.1. Sejam $\mathscr{O}$ o anel de valorização do corpo de funções algébricas F/K, seja P seu ideal maximal e $0 \neq x \in P$. Sejam ainda $x_1, ..., x_n \in P$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$ para cada $i = 1, 2, \ldots, n-1$. Então temos que

$$n \leq [F : K(x)] < \infty.$$

Demonstração. Pela proposição 4.1(c), temos que $x \notin \widetilde{K}$, logo x é transcendente sobre K e pela observação 4.1 podemos afirmar que a extensão $[F : K(x)]$ é finita. Assim, é suficiente provar que o conjunto formado por $x_1, x_2, \ldots, x_n$ é linearmente independentes sobre $K(x)$. Suponhamos que existe uma combinação linear não trivial $\sum_{i=1}^{n} \varphi_i(x)x_i = 0 \quad \text{com} \quad \varphi_i(x) \in K(x)$.

Podemos assumir sem perda de generalidade que $\varphi_i(x) \in K[x]$ e x não divide $\varphi_i(x)$ para todo i. Seja $a_i = \varphi_i(0)$ o termo independente de $\varphi_i(x)$ e fixemos $j \in \{1, 2, \ldots, n\}$ tal que $a_j \neq 0$, mas $a_i = 0$ para todo $i > j$. Assim obtemos

$$\sum_{i \neq j} \varphi_i(x)x_i + \varphi_j(x)x_j = 0 \Rightarrow -\varphi_j(x)x_j = \sum_{i \neq j} \varphi_i(x)x_i$$

com $\varphi_i(x) \in \mathscr{O}$, para $i \in \{1, \ldots, n\}$ pois $x = x_1 \in P$, $x_i \in x_j P$ para $i < j$ e $\varphi_i(x) = x g_i(x)$, para $i > j$, onde $g_i(x) \in K[x]$. Portanto,

$$\begin{aligned} -\varphi_j(x) &= \sum_{i<j} \varphi_i(x) \frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} g_i(x) x_i \\ &= \sum_{i<j} \varphi_i(x) \frac{x_j p_i}{x_j} + \sum_{i>j} \frac{x_j p}{x_j} g_i(x) x_i \end{aligned}$$

com $p, p_i \in P$, de modo que a última parcela da igualdade anterior é um elemento de P. Por outro lado, $\varphi_j(x) = a_j + x g_j(x)$, com $g_j(x) \in K[x] \subseteq \mathscr{O}$. Assim, $a_j = \varphi_j(x) - x g_j(x) \in P \cap K \subseteq P \cap \widetilde{K} = \{0\}$ o que é uma contradição, já que $a_j \neq 0$. □

Teorema 4.1. Seja $\mathscr{O}$ um anel de valorização do corpo de funções F/K e seja P o único ideal maximal. Então temos o seguinte:

a) P é um ideal principal.

b) Se $P = t\mathscr{O}$ então cada $0 \neq z \in F$ possui uma única representação da forma $z = t^n u$ para algum $n \in \mathbb{Z}$ e $u \in \mathscr{O}^\times$.

Demonstração. a) Suponhamos que P não seja um ideal principal, tomando $x_1 \in P \backslash \{0\}$, como $P \neq x_1\mathscr{O}$, existe $x_2 \in P \setminus x_1\mathscr{O}$. Assim temos que $x_2 x_1^{-1} \notin \mathscr{O}$ e, pela proposição 4.1, temos que $x_2^{-1} x_1 \in P$. Portanto $x_1 = x_2(x_2^{-1} x_1) \in x_2 P$. Fazendo este mesmo argumento, obtemos uma sequência infinita $x_1, x_2, \ldots$ de elemento de P tais que $x_n \in x_{n+1} P$, para cada $n \geq 1$, que é uma contradição pelo lema anterior.

b) Seja $z \in F \setminus \{0\}$, sem perda de generalidade, suponhamos que $z \in \mathscr{O}$. Se z é invertível então $z = t^0 z$. Agora suponha $z \in P$, temos que $P = t\mathscr{O}$ e, pelo lema anterior, o comprimento da sequência

$$x_1 = z, \quad x_2 = t^{m-1}, \quad x_3 = t^{m-2} \quad \ldots \quad x_m = t$$

é finito. Assim, existe um valor máximo $m \geq 1$ tal que $z \in t^m \mathscr{O}$. Agora $z = t^m u$ com $u \in \mathscr{O}^\times$, pois se $u \notin \mathscr{O}^\times$, então $u \in P = t\mathscr{O}$ e daí $z \in t^{m+1}\mathscr{O}$, que é uma contradição pela maximalidade de m. Para provar a unicidade, suponhamos que $z = u t^n = v t^m$, onde $u, v \in \mathscr{O}^\times$ e $n \geq m$. Logo $u v^{-1} = t^{n-m}$, e portanto $n = m$ e $u v^{-1} = 1$, isto é, $n = m$ e $u = v$.

□

Definição 4.3. a) Um lugar P do corpo de funções F/K é um ideal maximal de algum anel de valorização $\mathscr{O}$ de F/K. Cada elemento $t \in P$ tal que $P = t\mathscr{O}$ é chamado um elemento primo de P.

b) $\mathbb{P}_F := \{P \mid P \text{ é um lugar de F/K}\}$.

Definição 4.4. Uma valorização discreta de F/K é uma função $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:

i) $v(x) = \infty$ se, e somente se, $x = 0$.

ii) $v(xy) = v(x) + v(y)$, para cada $x, y \in F$.

iii) $v(x + y) \geq \min\{v(x), v(y)\}$ para todo $x, y \in F$.

iv) Existe um elemento $z \in F$ tal que $v(z) = 1$.

v) $v(a) = 0$ para todo $a \in K \setminus \{0\}$.

Lema 4.2 (Desigualdade Triangular Estrita)**.** Seja v uma valorização discreta de F/K, então $v(x + y) = \min\{v(x), v(y)\}$ para cada par $x, y \in F$ tal que $v(x) \neq v(y)$.

Demonstração. Seja $a \in K$, então $v(a) = 0$, assim $v(ay) = v(a) + v(y) = v(y) = v(-1) + v(y)v(-y)$, ou seja, $v(y) = v(-y)$. Se $v(x) < v(y)$ e suponha que $v(x+y) \neq \min\{v(x), v(y)\}$, temos $v(x + y) > v(x)$. Então obtemos que $v(x) = v((x + y) - y) \geq \min\{v(x + y), v(y)\} > v(x)$, contradição. □

Definição 4.5. Definimos $v_P : F \to \mathbb{Z} \cup \{\infty\}$ uma função que associada a um lugar $P \in \mathbb{P}_F$ que age da seguinte maneira: dado um elemento primitivo t de P, cada elemento não nulo $z \in F$ tem uma representação única na forma $z = t^n u$, onde $u \in \mathcal{O}_P^*$ e $n \in \mathbb{Z}$. Assim, definimos $v_P(z) = n$ e $v(0) = \infty$.

Teorema 4.2. Seja F/K um corpo de funções algébricas.

a) Seja $P \in \mathbb{F}_P$. v_P define uma valorização discreta, além disso temos

$$\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\}$$

$$\mathcal{O}_P^{\times} = \{z \in F \mid v_P(z) = 0\}$$

$$P = \{z \in F \mid v_P(z) > 0\}.$$

b) Um elemento $z \in F$ é um elemento primo de P se, e somente se, $v_P(z) = 1$.

c) Reciprocamente, suponha que v é uma valorização discreta de F/K. Então, o conjunto

$$P = \{z \in F \mid v(z) > 0\}$$

é um lugar de F/K e

$$\mathcal{O}_P = \{z \in F \mid v(z) \geq 0\}$$

é o anel de valorização correspondente.

Demonstração. a) Primeiramente vamos provar que v_p e uma valorização discreta.

i) Pela definição temos que $v_P(x) = 0$, se e somente se, $x = 0$.

ii) Para $x = 0$ ou $y = 0$ é imediato. Seja x e y elementos não nulos de de F, como $x = t^n u$ e $y = t^m w$, então $x \cdot y = t^n u \cdot t^m w = t^{n+m} uw$, isto é, $v_P(x \cdot y) = v_P(x) + v_P(y)$.

iii) Sejam $x = t^n u$ e $y = t^m w$ e suponhamos que $n < m$, então $x + y = t^n u + t^m w = t^n(u + t^{m-n} w)$, isso implica que $v_P(x + y) = n$, se $u + t^{m-n} w$ é invertível ou $v(x + y) > n$, se $u + t^{m-n} w$ não é invertível.

iv) $v_P(t) = 1$.

v) Para todo $0 \neq a \in K$, temos que a é invertível, donde $a = t^0 a$, logo $v_P(a) = 0$.

Seja $z \in F$ tal que $v_P(z) \geq 0$, assim $z = t^n u$ com $u \in \mathscr{O}_P^{\times}$, então $z \in \mathscr{O}_P$. Consequentemente

$$\mathscr{O}_P = \{z \in F \mid v_P(z) \geq 0\}$$

Analogamente podemos provar que

$$\mathscr{O}_P^* = \{z \in F \mid v_P(z) = 0\}$$

e como $P = \mathscr{O} \setminus \mathscr{O}_P^*$, temos que

$$P = \{z \in F \mid v_P(z) > 0\}.$$

b) $\Rightarrow$) Seja t um elemento primo de P, então $t = t1$, logo $v_P(t) = 1$.

$\Leftarrow$) Seja $z \in F$ tal que $v_P(z) = 1$. Fixando um elemento primo t de P temos que $z = tu$ onde $u \in \mathscr{O}_P^*$. Assim, $P = t\mathscr{O}_P = z\mathscr{O}_P$, portanto z é um elemento primo de P.

c) Primeiramente mostremos que $\mathscr{O}_P = \{z \in F \mid v(z) \geq 0\}$ é um subanel de F. De fato, $0 \in \mathscr{O}_P$, pois $v(0) = \infty > 0$. Sejam $x, y \in \mathscr{O}_P$, então $v(x) \geq 0$ e $v(y) \geq 0$. Logo,

$$v(x - y) \geq \min\{v(x), v(y)\} \geq 0$$

$$v(xy) = v(x) + v(y) \geq 0.$$

Assim, temos que $x - y$ e xy são elementos de $\mathscr{O}_P$, portanto $\mathscr{O}_P$ é um subanel de F. Como existe $z \in F$ tal que $v(z) = -1$, então $\mathscr{O}_P \subsetneq F$. Já que $v(a) = 0$ para todo $a \in K \setminus \{0\}$, então $K \subseteq \mathscr{O}_P$. Sabemos que existe um $z \in \mathscr{O}_P$ tal que $v(z) = 1$, e daí $K \subsetneq \mathscr{O}_P$. Agora, seja $z \in F \setminus \{0\}$, temos que

$$0 = v(1) = v(zz^{-1}) = v(z) + v(z^{-1}) \Longrightarrow v(z) \geq 0 \quad \text{ou} \quad v(z^{-1}) \geq 0$$

consequentemente, $z \in \mathcal{O}_P$ ou $z^{-1} \in \mathcal{O}_P$. Assim podemos concluir que $\mathcal{O}_P$ é um anel de valorização.

Seja $z \in \mathcal{O}_P^{\times}$, temos que

$$0 = v(1) = v(zz^{-1}) = v(z) + v(z^{-1}),$$

com $z^{-1} \in \mathcal{O}_P$. Mas $v(z) \geq 0$ e $v(z^{-1}) \geq 0$, que implica que $v(z) = v(z^{-1}) = 0$. Reciprocamente, seja $z \in \mathcal{O}_P$ tal que $v(z) = 0$ devemos mostrar que $z^{-1} \in \mathcal{O}_P$. Temos que

$$0 = v(1) = v(zz^{-1}) = v(z) + v(z^{-1}) = v(z^{-1})$$

, isto é, $v(z^{-1}) = 0$ e daí $z^{-1} \in \mathcal{O}_P$. Portanto, um elemento z é invertível em $\mathcal{O}_P$ se, e somente se, $v(z) = 0$. Logo, $P = \mathcal{O}_P^{\times} \setminus \mathcal{O}_P = \{z \in F \mid v(z) > 0\}$.

□

Definição 4.6. Seja $P \in \mathbb{P}_F$.

a) $F_P = \mathcal{O}_P/P$ é o corpo de classes residuais de P. A aplicação $x \longmapsto x(P) = x + P$ é chamada aplicação das classes residuais com respeito a P.

b) O grau de P é $\deg(P) = [F_P : K]$. Um lugar de grau 1 é dito lugar racional de F/K.

Proposição 4.2. Seja $P \in \mathbb{P}_F$ e $0 \neq x \in P$, então $\deg(P) \leq [F : K(x)] < \infty$.

Demonstração. Pela proposição 4.1 e a observação 4.1 temos que $[F : K(x)] < \infty$.

Precisamos mostrar que se $z_1(P), \ldots, z_n(P)$ são linearmente independentes sobre K, então $z_1, \ldots, z_n \in \mathcal{O}_P$ são linearmente independentes sobre $K(x)$ e assim teríamos que $\deg(P) \leq [F : K(x)]$.

Suponhamos que existe uma combinação linear não trivial,

$$\sum_{i=1}^{n} \varphi_i(x) z_i = 0,$$

com $\varphi_i(x) \in K(x)$ e $\varphi_i(x) \neq 0$ para algum $i \in \{1, ..., n\}$. Sem perda de generalidade, suponhamos que $\varphi_i(x) \in K[x]$ e que nem todos os $\varphi_i(x)$ são divisíveis por x, então $\varphi_i(x) = a_i + xg_i(x)$, com $a_i \in K \setminus \{0\}$, $g_i(x) \in K[x]$ para algum $i \in \{1, ..., n\}$. Notemos que se $x \in P$ e $g_i(x) \in K[x] \subseteq \mathcal{O}_P$, então $\varphi_i(x)(P) = a_i(P) = a_i$. Assim,

$$0 = 0(P) = \sum_{i=1}^{n} f_i(x)(P) z_i(P) = \sum_{i=1}^{n} a_i z_i(P)$$

o que é uma contradição pois $z_1(P), \ldots, z_n(P)$ são linearmente independentes sobre K. □

Definição 4.7. Sejam $P \in \mathbb{P}_F$ um lugar de F/K e $z \in F$. Dizemos que P é um zero de z se $v_P(z) > 0$ e P é dito polo de z se $v_P(z) < 0$. Se $v_P(z) = m > 0$, então P é dito um zero de ordem m. Agora, se $v_P(z) = -m < 0$, então P é um polo de z de ordem m.

Teorema 4.3. Sejam F/K um corpo de funções algébricas e R um subanel de F com $K \subseteq R \subseteq F$. Suponha que $\{0\} \neq I \subsetneq R$. Então, existe um lugar $P \in \mathbb{F}_P$ tal que $I \subseteq P$ e $R \subseteq \mathscr{O}_P$.

Demonstração. Consideremos o conjunto

$$\mathscr{F} = \{S \mid S \text{ é um subanel de } F \text{ com } R \subseteq S \text{ e } IS \neq S\}.$$

Pela definição os elementos de IS são da forma $\sum a_i s_i$ com $a_i \in I$ e $s_i \in S$, ou seja, IS é um ideal de S. Pela relação de inclusão, temos que $\mathscr{F}$ é parcialmente ordenado e como $R \subset \mathscr{F}$, então $\mathscr{F} \neq \emptyset$.
Seja $\mathscr{H} \subseteq \mathscr{F}$ uma cadeia em $\mathscr{F}$, então defina

$$T = \bigcup \{S; S \in \mathscr{H}\}$$

é um subanel de F com $R \subseteq T$. Verifiquemos agora que $IT \neq T$. Suponhamos que $IT = T$, então $1 \in$, isso implica que $1 = \sum_{i=1}^{n} a_i s_i$, onde $a_i \in I$ e $s_i \in T$. Como $\mathscr{H}$ é totalmente ordenado, existe $S_0 \in \mathscr{H}$ tal que $s_i \in S_0$ para cada $i = 1, \ldots, n$, isso implica que $1 \in IS_0$, com isso $S_0 \subset IS_0$, então $S_0 = IS_0$ o que é uma contradição, pois $S_0 \in \mathscr{H} \subseteq \mathscr{F}$. Portanto, $T \in \mathscr{F}$, o que implica que toda cadeia em $\mathscr{F}$ é limitada superiormente em $\mathscr{F}$, assim pelo lema de Zorn $\mathscr{F}$ tem um elemento maximal, isto é, existe $\mathscr{O} \subset F$ tal que $\mathscr{O} \subseteq F$, $R \subseteq \mathscr{O} \subseteq F$, $I\mathscr{O} \neq \mathscr{O}$ e $\mathscr{O}$ é maximal. Vamos mostrar que $\mathscr{O}$ é um anel de valorização de F/K. Se $\mathscr{O} = K$, como por hipótese, $K \subseteq R$, então $R = K$, assim R é um corpo, com isso seus únicos ideais seriam os triviais, o que é uma contradição. Portanto, $K \subsetneq \mathscr{O}$. Como $I \neq \{0\}$ e $I\mathscr{O} \neq \mathscr{O}$, então $\mathscr{O} \subseteq F$ e $I \subset \mathscr{O} \setminus \mathscr{O}^{\times}$, pois se $\mathscr{O} = F$, teríamos que $IF = F$ o que é uma contradição, e daí $\mathscr{O} \subsetneq F$. Agora suponhamos que I não esta contido em $\mathscr{O} \setminus \mathscr{O}^{\times}$. Então, existe um elemento $z \in F$ tal que $z \notin \mathscr{O}$ e $z^{-1} \notin \mathscr{O}$. Como $\mathscr{O}$ é maximal, temos que $\mathscr{O}[z]$ e $\mathscr{O}[z^{-1}]$ não são elementos de $\mathscr{F}$, já que $R \subseteq \mathscr{O}[z] \subseteq F$ e $R \subseteq \mathscr{O}[z^{-1}] \subseteq F$, obtemos que $I\mathscr{O}[z] = \mathscr{O}[z]$ e $I\mathscr{O}[z^{-1}] = \mathscr{O}[z^{-1}]$. Assim, existem $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m \in I\mathscr{O}$ tais que

$$a_0 + a_1 z + \ldots + a_n z^n = 1 = b_0 + b_1 z^{-1} + \ldots + b_m z^{-m}.$$

Como $I\mathscr{O} \neq \mathscr{O}$, então $n \geq 1$ e $m \geq 1$. Suponhamos que n e m são os valores mínimos que satisfazendo as equações acima e consideremos $m \leq n$. Multiplicando o lado esquerdo por $(1 - b_0)$ e o direito por $a_n z^n$ teremos

$$(1 - b_0)a_0 + (1 - b_0)a_1 z + \ldots + (1 - b_0)a_n z^n = (1 - b_0)$$

e

$$(b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \ldots + b_m a_n z^{n-m} = 0.$$

Somando essas duas expressões temos

$$\begin{aligned} 1 =& a_0(1 - b_0) + a_1(1 - b_0)z + \ldots + a_{n-m-1}(1 - b_0)z^{n-m-1} + \\ & [a_{n-m}(1 - b_0) + a_n b_m]z^{n-1} + \cdots + [a_{n-1}(1 - b_0) + a_n b_1]z^{n-1} + b_0 \end{aligned}$$

que contradiz a minimalidade de n. Assim, temos que $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$ para todo elemento de F. Portanto, $\mathcal{O}$ é um anel de valorização de F/K e $I \subset P = \mathcal{O} \setminus \mathcal{O}^{\times}$. □

Corolário 4.4. Sejam F/K um corpo de funções e $z \in F$ transcendente sobre K. Então z possui pelo menos um zero e um polo. Em particular $\mathbb{P}_F \neq \emptyset$.

Demonstração. Tome $R = K[z]$ e $I = zK[z]$. Então existe um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$ (teorema 4.3). Como $z \in I \subseteq P$, então $v_P(z) > 0$, ou seja, P é um zero de z. Analogamente, existe um zero Q para z^{-1}, isto é, um polo de z. □

4.2 APROXIMAÇÃO FRACA

Teorema 4.5 (Teorema da Aproximação Fraca ou Teorema da independência)**.** Sejam $P_1, \ldots, P_n \in \mathbb{P}_F$ lugares dois a dois distintos de F/K, $x_1, \ldots, x_n \in F$ e $r_1, \ldots, r_n \in \mathbb{Z}$. Então, existe $x \in F$ tal que

$$v_{P_i}(x - x_i) = r_i \text{ para todo } i = 1, \ldots, n.$$

Demonstração. Chamaremos cada v_{P_i} de v_i por simplicidade.
Afirmação 1: Existe $u \in F$ tal que $v_1(u) > 0$ e $v_i(u) < 0$, para cada $i = 2, \ldots, n$. Provaremos aplicando indução sobre n. Para $n = 2$, devido a maximalidade dos anéis $\mathcal{O}_{P_i}$, temos que os anéis são dois a dois distintos. Assim, existem $y_1 \in \mathcal{O}_{P_1} \setminus \mathcal{O}_{P_2}$ e $y_2 \in \mathcal{O}_{P_2} \setminus \mathcal{O}_{P_1}$. Então $v_1(y_1) \geq 0$, $v_2(y_1) < 0$, $v_1(y_2) < 0$ e $v_2(y_2) \geq 0$. Agora, tomemos $u = y_1/y_2$, assim teremos $v_1(u) > 0$ e $v_2(u) > 0$.

Para $n > 2$, pela hipótese de indução existe um elemento y com $v_1(y) > 0$ e $v_i(y) < 0$ para todo $i \in \{2, \ldots, n-1\}$. Se $v_n(y) > 0$, basta tomarmos $u = y$. Mas se $v_n(y) \geq 0$, tomemos $z \in F$ tal que $v_1(z) > 0$ e $v_n(z) < 0$ e considere $u = y + z^r$, com $r \geq 1$ tal que $rv_i(z) \neq v_i(y)$ para $i = 1, \ldots, n-1$. Assim

$$v_1(u) \geq \min\{v_1(y), rv_1(z)\} > 0$$

e

$$v_i(u) = \min\{v_i(y), rv_i(z)\} < 0 \text{ para todo } i \in \{2, \ldots, n\}.$$

Afirmação 2: Existe $w \in F$ tal que $v_1(w-1) > r_1$ e $v_i(w) > r_i$ para $i = \{2, \ldots, n\}$.

Seja u como na afirmação 1. Defina $w = (1+u^s)^{-1}$. Assim para $s \in \mathbb{N}$ suficientemente grande, como $v_1(1) = 0$, temos

$$\begin{aligned} v_1(w-1) = v_1\left(\frac{-u^s}{1+u^s}\right) &= v_1(-u^s) + v_1((1+u^s)^{-1}) \\ &= sv_1(u) - v_1(1+u^s) \\ &= sv_1(u) + \min\{v_1(1), v_1(u^s)\} = sv_1(u) > r_1 \end{aligned}$$

O mesmo resultado vale para v_i para cada $i = \{2, \ldots, n\}$. Logo,

$$v_i(w) = -v_i(w^{-1}) = v_i(1 + u^s) = -sv_i(u) > r_i \text{ para todo } i = \{2, \ldots, n\}.$$

Afirmação 3: Dados $y_1, \ldots, y_n \in F$, existe $z \in F$ com $v_i(z - y_i) > r_i$ para todo $i \in \{1, 2, \ldots, n\}$.
Escolha $s \in \mathbb{Z}$ tal que $v_i(y_j) \geq s$ para todos $i, j \in \{1, \ldots, n\}$. Assim, pela afirmação 2, existem $w_1, \ldots, w_n \in F$ tais que $v_i(w_i - 1) > r_i - s$ e $v_i(w_j) > r_i - s$ para $i \neq j$. Tomemos $z = \sum_{j=1}^{n} y_j w_j$, então

$$\begin{aligned} v_i(z - y_i) &= v_i\Big(\sum_{j=1/j\neq i}^{n} y_j w_j + y_i(w_i - 1)\Big) \\ &= \min\{v_i(y_i(w_i - 1)), v_i(y_1 w_1), \ldots, v_i(y_{i-1} w_{i-1}), v_i(y_{i+1} w_{i+1}), \ldots v_i(y_n w_n)\} > r_i \end{aligned}$$

Prova final do teorema
Pela afirmação 3 existe $z \in F$ tal que $v_i(z - x_i) > r_i$ para todo $i \in \{1, 2, \ldots, n\}$. Agora tomemos z_i tal que $v_i(z_i) = r_i$. Novamente pela afirmação 3, existe z' tal que $v_i(z' - z_i) > r_i$ para todo $i \in \{1, 2, \ldots, n\}$, assim $v_i(z') = v_i((z' - z_i) + z_i) = \min\{v_i(z' - z_i), v_i(z_i)\} = r_i$. Deste modo, para $x = z + z'$, temos:

$$v_i(x - x_i) = v_i((z - x_i) + z') = \min\{v_i(z - x_i), v_i(z')\} = r_i,$$

como queríamos. □

Corolário 4.6. Todo corpo de funções possui infinitos lugares.

Demonstração. Suponha que existe somente um quantidade finita de lugares, $P_1, \ldots, P_n$. Pelo Teorema da Aproximação Fraca, existe um elemento $x \in F \setminus \{0\}$ tal que $v_{P_i}(x) > 0$ para todo$i \in \{1, 2, \ldots, n\}$. Então x é um elemento transcendente de K que não possui polos, contradizendo o corolário 4.4. □

Proposição 4.3. Sejam F/K um corpo de funções algébricas e $P_1, \ldots, P_r$ zeros do elemento $x \in F$. Então

$$\sum_{i-1}^{r} v_{P_i}(x) \deg(P_i) \leq [F : K(x)].$$

Demonstração. Considere $v_i = v_{P_i}$, $f_i = \deg(P_i)$ e $e_i = v_i(x)$.

Pelo Teorema da Aproximação Fraca 4.5, existe t_i tal que $v_i(t_i) = 1$ para todo $i \in \{1, ..., n\}$ e $v_k(t_i) = 0$, para todo $k \neq i$. Agora sejam $s_{i1}, \ldots, s_{if_i} \in \mathcal{O}_{P_i}$ tais que $s_{i1}(P_i), \ldots, s_{if_i}(P_i)$ formam uma base de F_{P_i} sobre K.

Em particular, com uma aplicação mais fraca do Teorema da Aproximação Fraca, existem $z_{ij} \in F$ tais que para todos i, j

$$v_i(s_{ij} - z_{ij}) > 0 \text{ e } v_k(z_{ij}) \geq e_n \text{ para } k \neq i.$$

O conjunto $\{t^a z_{ij}; 1 \leq i \leq r,\ 1 \leq j \leq f_i \text{ e } 0 \leq a \leq e_i - 1\}$ é linearmente independente sobre $K(x)$. De fato se existir uma combinação linear não trivial

$$\sum_{i=1}^{r} \sum_{j=1}^{j_i} \sum_{a=0}^{e_i-1} \varphi_{ija}(x) t_i^a z_{ij} = 0 \tag{4.1}$$

sobre $K(x)$, suponhamos sem perda de generalidade que $\varphi_{ija}(x) \in K[x]$ e que nem todos os $\varphi_{ija}(x)$ são divisíveis por x. Então, existem índices $k \in \{1, \ldots, r\}$ e $c \in \{0, \ldots, e_k - 1\}$ tais que $x \mid \varphi_{kja}(x)$ para todo $a < c$ e $j \in \{1, \ldots, f_k\}$, e $x \nmid \varphi_{kjc}(x)$ para algum $j \in \{1, \ldots, f_k\}$. Agora, multiplicando (4.1) por t_k^{-c}, obtemos

$$\sum_{i=1}^{r} \sum_{j=1}^{j_i} \sum_{a=0}^{e_i-1} \varphi_{ija}(x) t_i^a t_k^{-c} z_{ij} = 0. \tag{4.2}$$

Para $i \neq k$ todas as parcelas de (4.2) estão em P_k, já que

$$v_k(\varphi_{ija}(x) t_i^a t_k^{-c} z_{ij}) = v_k(\varphi_{ija}(x)) + v_k(t_i^a) + v_k(t_k^{-c}) + v_k(z_{ij}) \geq 0 - c + e_k > 0.$$

Para $i = k$ e $a < c$ temos que

$$v_k(\varphi_{kja}(x) t_k^{a-c} z_{kj}) = v_k(\varphi_{kja}(x)) + v_k(t_k^{a-c}) + v_k(z_{kj}) \geq e_k + a - c > e_k - c > 0.$$

Para $i = k$ e $a > c$ temos que

$$v_k(\varphi_{kja}(x) t_k^{a-c} z_{kj}) \geq e_k + a - c \geq a - c > 0$$

Combinando com (4.2), obtemos

$$\sum_{j=1}^{f_k} \varphi_{kjc}(x) z_{kj} \in P_k.$$

Como múltiplos de x pertencem a P_k, então $\varphi_{kjc}(x)(P_k) \in K$ e nem todos $\varphi_{kjc}(x)(P_k)$ são nulos, pois x não divide todos os $\varphi_{kjc}(x)$. Assim temos uma combinação linear não trivial

$$\sum_{j=1}^{f_k} \varphi_{kjc}(x)(P_k) z_{kj}(P_k) = 0$$

sobre K, o que é uma contradição, pois como $v_i(s_{ij} - z_{ij}) > 0$, então $s_{ij} - z_{ij} \in P_i$ isso implica que $s_{ij}(P_i) = z_{ij}(P_i)$ e, como $\{s_{i1}(P_i), \ldots, s_{if_i}(P_i)\}$ é uma base de F_{P_i} sobre K, então $\{z_{k1}(P_k), \ldots, z_{kf_k}(P_k)\}$ é uma base de F_{P_i} sobre K. Assim concluímos que o conjunto $\{t^a z_{ij}; 1 \leq i \leq r,\ 1 \leq j \leq f_i \text{ e } o \leq a \leq e_i - 1\}$ é linearmente independente sobre $K(x)$, e como o número de elementos dessa forma é igual a

$$\sum_{i+1}^{r} f_i e_i = \sum_{i=1}^{r} v_{P_i} \deg(P_i),$$

concluímos a proposição $\square$

Corolário 4.7. Em um corpo de funções algébricas F/K, cada elemento $0 \neq x \in F$ possui somente um número finito de zeros e polos.

Demonstração. Se x é constante e como $\widetilde{K} \cap P = \{0\}$, então x não possui zeros nem polos. Se x é um elemento transcendente sobre K, então o número de zeros de x é menor ou igual a $[F : K(x)]$ pela proposição 4.3. De forma análoga, mostramos que x^{-1} tem um número finito de zeros, e portanto, x possui um número finito de polos. □

4.3 DIVISORES

Definição 4.8. O grupo dos divisores de F/K é definido como o grupo abeliano livre gerado pelos lugares de F/K e é denotado como $Div(F)$. Um divisor é uma soma formal

$$D = \sum_{P \in \mathbb{P}_F} n_p P, \text{ com } n_p \in \mathbb{Z} \text{ e quase todo } n_P = 0.$$

Definição 4.9. O suporte de D é definido como

$$supp(D) = \{P \in \mathbb{P}_F \mid n_P \neq 0\}.$$

Um divisor da forma $D = P$ com $P \in \mathbb{P}_F$ é chamado divisor primo e dados dois divisores $D = \sum n_P P$ e $D' = \sum n'_P P$ definimos a soma como

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P.$$

O elemento neutro do grupo $Div(F)$ é o divisor

$$0 = \sum_{P \in \mathbb{P}_F} n_P P, \text{ onde } n_p = 0 \text{ para todo } P \in \mathbb{P}_F.$$

Seja $D = \sum_{P \in \mathbb{P}_F} n_P P$ um divisor de F/K e Q um lugar de F/K. Definimos a valorização em D como $v_Q(D) := n_Q$ e uma ordem parcial em $Div(F)$ é definida por

$$D_1 \leq D_2 \text{ se, e somente se, } v_P(D_1) \leq v_P(D_2) \text{ para todo } P \in \mathbb{P}_F.$$

O grau de um divisor D é definido como

$$\deg(D) = \sum_{P \in \mathbb{P}_F} v_P(D) \deg(P).$$

Logo, a aplicação $\deg : Div(F) \longrightarrow \mathbb{Z}$ é um homomorfismo de grupos. Assim faz sentido a definição a seguir.

Definição 4.10. Seja $0 \neq x \in F$ e denotemos Z e N o conjunto de zeros e polos de x respectivamente. Então definimos

i) $(x)_0 = \sum_{P \in Z} v_P(x)P$, o divisor de zeros de x.

ii) $(x)_\infty = \sum_{P \in N} (-v_P(x))P$, o divisor de polos de x.

iii) $(x) = (x)_0 - (x)_\infty$, o divisor principal de x.

Definição 4.11. O conjunto de divisores $Princ(F) = \{(x) \mid 0 \neq x \in F\}$ é dito o grupo dos divisores principais de F/K. Esse grupo é um subgrupo de $Div(F)$.

Definição 4.12. O grupo quociente

$$Cl(F) = Div(F)/Princ(F)$$

é chamado grupo das classes de divisores de F/K. Para $D \in Div(F)$, o elemento correspondente em $Cl(F)$ é denotado por $[D]$. Dois divisores D e D' serão chamados de equivalentes se $[D] = [D']$, isto é, se existir algum $0 \neq x \in F$ tal que $D = D' + (x)$. Nesse caso, escreveremos $D \sim D'$.

Definição 4.13. Para um divisor $A \in Div(F)$, definimos o espaço de Riemman-Roch associado a A por

$$\mathscr{L}(A) = \{x \in F \mid (x) \geq -A\} \cup \{0\}.$$

Note que, para $0 \neq x \in F$, $(x) \geq -A$ se e somente se $v_P(x) \geq v_P(-A) = -v_P(A)$ para todo $P \in \mathbb{P}_F$, para $x = 0$, $v_P(x) = \infty \geq -v_P(A)$ para todo $P \in \mathbb{P}_F$. Então, $\mathscr{L}(A) = \{x \in F \mid v_P(x) \geq -v_P(A)\ \forall P \in \mathbb{P}_F\}$. Assim, se

$$A = \sum_{P \in \mathbb{P}_F} n_P P = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j, \text{ onde } n_i > 0 \text{ e } m_j > 0,$$

temos que $0 \neq x \in \mathscr{L}(A)$ se e somente se $v_P(x) \geq -v_P(\sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j)$ para todo $P \in \mathbb{P}_F$, isto é, $v_{P_i}(x) \geq -n_i$ para $i = 1, ..., r$ e $v_{Q_j}(x) \geq m_j$ para $j = 1, ..., s$. Portanto, $\mathscr{L}(A)$ é o conjunto de todas as funções $x \in F$ tais que x possui zeros de ordem pelo menos m_j em Q_j ($j = 1, ..., s$) e possui polos apenas em P_i com ordem no máximo n_i $(i = 1, ..., r)$.

Lema 4.3. Seja $A \in Div(F)$. Então temos:

a) $\mathscr{L}(A) \neq \{0\}$ se e somente se existe um divisor A' tal que $A' \backsim A$ e $A' \geq 0$.

b) $\mathscr{L}(A)$ é um espaço vetorial sobre K.

c) Se A' é um divisor equivalente a A, então $\mathscr{L}(A') \cong \mathscr{L}(A)$.

e) $\mathscr{L}(0) = K$.

f) Se $A < 0$, então $\mathscr{L}(A) = \{0\}$.

Demonstração. a)

$$\begin{aligned}\mathscr{L}(A) \neq \{0\} &\Leftrightarrow \exists\, x \in F \setminus \{0\} \text{ tal que } (x) \geq -A \\ &\Leftrightarrow A' = A + (x) \text{ tal que } A' \sim A \text{ e } A' \geq 0 \\ &\Leftrightarrow \exists\, A' \in Div(F) \text{ tal que } A' \sim A \text{ e } A' \geq 0.\end{aligned}$$

b) É claro que $0 \in \mathscr{L}(A)$, assim $\mathscr{L}(A) \neq \emptyset$. Sejam $x, y \in \mathscr{L}(A)$ e $\lambda \in K$. Então,

$$v_P(x+y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(A) \quad \text{e}$$

$$v_P(\lambda x) = v_P(\lambda) + v_P(x) = v_P(x) \geq -v_P(A)$$

para todo $P \in \mathbb{P}_F$. Assim temos que $x+y$ e λx pertence a $\mathscr{L}(A)$. Isto é, $\mathscr{L}(A)$ é um espaço vetorial sobre K.

c) Temos que se $A \sim A'$, então existe $z \in F \setminus \{0\}$ tal que $A = A' + (z)$. Considere a aplicação

$$\begin{aligned}\varphi : \mathscr{L}(A) &\longrightarrow F \\ x &\longmapsto xz\end{aligned}$$

Temos que φ é uma aplicação linear. Agora seja $x \in \mathscr{L}(A) \setminus \{0\}$, então $(x) \geq -A$. Como $\varphi(x) = xz \neq 0$, então $(xz) \geq -A'$. Portanto, $\varphi(x) = xz \in \mathscr{L}(A')$. Se $x = 0$, temos que $\varphi(x) = \varphi(0) = 0 \in \mathscr{L}(A')$. De forma análoga, temos que $\psi : \mathscr{L}(A') \longrightarrow F$ definida como $x \longmapsto xz^{-1}$ é uma transformação linear cuja imagem está contida em $\mathscr{L}(A)$. E como ψ é a inversa de φ, podemos concluir que $\mathscr{L}(A') \simeq \mathscr{L}(A)$.

d) Note que se $x \in K \setminus \{0\}$, então $(x) \geq -0 = 0$ e $K \subset \mathscr{L}(0)$. Reciprocamente, se $x \in \mathscr{L}(0) \setminus \{0\}$, então $(x) \geq 0$. Isto implica que $v_P(x) \geq 0$, logo x não possui polos. Então, pelo corolário 4.4, temos que $x \in K$.

f) Suponha por absurdo que existe um elemento $x \in \mathscr{L}(A) \setminus \{0\}$. Então, $(x) \geq -A$, o que implica que x não possui polos, mas possui pelo menos um zero, contradizendo o corolário 4.4.

□

Lema 4.4. Sejam $A, B \in Div(F)$ com $A \leq B$. Então, $\mathscr{L}(A) \subseteq \mathscr{L}(B)$ e

$$\dim(\mathscr{L}(B)/\mathscr{L}(A)) \leq \deg(B) - \deg(A).$$

Demonstração. Seja $x \in \mathscr{L}(A) \setminus \{0\}$, então $v_P(x) \geq -v_P(A)$ para todo $P \in \mathbb{P}_F$. Como $A \leq B$, então $-v_P(A) \geq -v_P(B)$, daí $v_P(x) \geq -v_P(B)$, isso implica que $x \in \mathscr{L}(B)$, portanto $\mathscr{L}(A) \subseteq \mathscr{L}(B)$.

Mostremos agora para $B = A + P$ onde $P \in \mathbb{P}_F$. O caso geral segue por indução. Tome $t \in F$ tal que $v_P(t) = v_P(B) = v_P(A) + v_P(P) = v_P(A) + 1$. Seja $x \in \mathscr{L}(A)$, então

$$v_P(x) \geq -v_P(B) = -v_P(t) \Rightarrow v_P(xt) = v_P(x) + v_P(t) \geq 0 \Rightarrow xt \in \mathscr{O}_P.$$

Agora defina

$$\begin{aligned} \varphi : \mathscr{L}(B) &\longrightarrow F_P \\ x &\longmapsto (xt)P \end{aligned}$$

Observemos que

$$\begin{aligned} x \in Ker(\varphi) &\Leftrightarrow xt \in P \Leftrightarrow v_P(xt) > 0 \\ &\Leftrightarrow v_P(x) + v_P(t) > 0 \Leftrightarrow v_P(x) > -v_P(t) \\ &\Leftrightarrow v_P(x) \geq 1 - v_P(t) \Leftrightarrow v_P(x) \geq 1 - v_P(B) = -v_P(A) \\ &\Leftrightarrow x \in \mathscr{L}(A). \end{aligned}$$

Portanto, $Ker(\varphi) = \mathscr{L}(A)$. Consequentemente, φ induz uma transformação linear injetiva e daí

$$\dim(\mathscr{L}(B)/\mathscr{L}(A)) \leq \dim(F_P) = \deg(P) = \deg(B) - \deg(A).$$

□

Proposição 4.4. Para cada divisor $A \in Div(F)$, o espaço $\mathscr{L}(A)$ é um espaço de dimensão finita sobre K. Mais precisamente, se $A = A_+ - A_-$, onde A_+ e A_- são divisores positivos, então $\dim(\mathscr{L}(A)) \leq \deg(A_+) + 1$.

Demonstração. Temos que $\mathscr{L}(0) = K$ pelo lema 4.3. Então,

$$\dim(\mathscr{L}(A_+)/\mathscr{L}(0)) = \dim(\mathscr{L}(A_+)) - \dim(\mathscr{L}(0)) = \dim(\mathscr{L}(A_+)) - 1,$$

assim

$$\dim(\mathscr{L}(A_+)) = \dim(\mathscr{L}(A_+)/\mathscr{L}(0)) + 1.$$

Mostremos agora que $\dim \mathscr{L}(A) \leq \deg A_+ + 1$. Temos que $0 \leq A_+$, então pelo Lema 4.4, temos que

$$\dim(\mathscr{L}(A_+)) \leq \deg(A_+) - \deg(0) + 1 = \deg(A_+) + 1,$$

o que conclui a prova, pois

$$A = A_+ - A_- \leq A_+ + 0 \Rightarrow A \leq A_+ \Rightarrow \mathscr{L}(A) \subseteq \mathscr{L}(A_+).$$

□

Definição 4.14. Para $A \in Div(F)$, o inteiro $\ell(A) = \dim(\mathscr{L}(A))$ é dito dimensão do divisor A.

Teorema 4.8. Se $x \in F \setminus K$, então

$$\deg((x)_0) = \deg((x)_\infty) = [F : K(x)].$$

Demonstração. Sejam $n = [F : K(x)]$ e $B = (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x)P_i$, onde os P_i com $i = 1, \ldots, r$ são os polos de x. Então temos, pela proposição 4.3:

$$\deg(B) = \sum_{i=1}^{r} v_{P_i}(x^{-1}) \deg(P_i) \leq [F : K(x)] = n.$$

Mostremos agora que $n \leq \deg B$. Seja $\{u_1, \ldots, u_n\}$ uma base de $F/K(x)$ e $0 \neq C \in Div(F)$ tais que $(u_j) \geq -C$ para todo $j = 1, \ldots, n$. Mostremos que os elementos $x^i u_j$ com $0 \leq i \leq k$ e $1 \leq j \leq n$ pertencem a $\mathscr{L}(kB + C)$ e são linearmente independentes sobre K. Como $i \leq k$ e $(u_j) \geq -C$ para cada $i = 1, \ldots, n$, então

$$(x^i u_j) = (x^i) + (u_j) = i(x) + (u_j) = i(x)_0 - i(x)_\infty + (u_j) \geq -i(x)_\infty - kB - C,$$

logo $x^i u_j \in \mathscr{L}(kB + C)$. Além disso, se tivermos

$$\sum_{j=1}^{n} \sum_{i=1}^{k} a_{ij} x^i u_j = 0, \text{ então } \sum_{j=1}^{n} \left(\sum_{i=1}^{k} a_{ij} x^i \right) u_j = 0,$$

com $a_{ij}x^j \in K(x)$, então $\sum_{k}^{i=1} a_{ij} x^i = 0$ para todo j=1,. . . ,n, pois $\{u_1, ..., u_n\}$ é uma base de F. Mas, como x é um elemento transcendente sobre K, isso implica que $a_{ij} = 0$ para cada $1 = 1, \ldots, k$ e $j = 1, \ldots, n$. Assim, o conjunto $\{x^i u_j; 0 \leq i \leq k \text{ e } 1 \leq j \leq n\}$ é linearmente independente sobre K. Como esse conjunto possui $n(k + 1)$ elementos, então, pela proposição anterior, temos que

$$\begin{aligned} &n(k + 1) \leq \dim(kB + C) = \deg((KB + C)_+) + 1 = k \deg(B) + \deg(C) + 1 \\ &\Rightarrow k(\deg(B) - n) \geq n - \deg(C) - 1 \end{aligned}$$

para todo $k \geq 0$. Como o lado direito desta última desigualdade não depende de k, podemos concluir que $\deg(B) \geq n$. Como $(x)_0 = (x^{-1})_\infty$, temos $\deg(x)_0 = (x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$ e, assim, $\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$ □

Corolário 4.9. Seja A um divisor de F/K.

a) Se A' é um divisor de F/K tal que $A' \sim A$, então $\ell(A) = \ell(A')$ e $\deg(A) = \deg(A')$.

b) Se $\deg(A) < 0$, então $\ell(A) = 0$.

c) Se $\deg(A) = 0$, então são equivalentes:

   i) A é um divisor principal.

ii) $\ell(A) \geq 1$.

iii) $\ell(A) = 1$.

Proposição 4.5. Existe uma constante $\gamma \in \mathbb{Z}$ tal que para todos os divisores $A \in Div(F)$ temos que:

$$\deg(A) - \ell(A) \leq \gamma.$$

Demonstração. Inicialmente observemos que se $A_1 \leq A_2$ então, $\dim(\mathscr{L}(A_2)/\mathscr{L}(A_1)) \leq \deg(A_2) - \deg(A_1)$, assim pelo lema 4.4, temos que

$$\dim \mathscr{L}(A_2) - \dim \mathscr{L}(A_1) \leq \deg(A_2) - \deg(A_1),$$

então

$$\deg(A_1) - \ell(A_1) \leq \deg(A_2) - \ell(A_2). \tag{4.3}$$

Seja $x \in F \setminus K$ e $B = (x)_\infty$. Analogamente à demonstração do Teorema 4.8, existe $C \geq 0$ um divisor dependendo de x tal que $\ell(kB + C) \geq (k+1)\deg(B)$ para todo $k \geq 0$. Novamente pelo Lema 4.4, temos que

$$\ell(kB + C) - \ell(kB) = \dim(\mathscr{L}(kB + C)/\mathscr{L}(kB)) \leq \deg(kB + C) - \deg(kB) = \deg(C),$$

assim

$$\ell(kB + C) \leq \ell(kB) + \deg(C).$$

Usando o fato que $\deg(B) = n = [F : K(x)]$ (pela demonstração do Teorema 4.8), temos que

$$\ell(kB) + \deg(C) \geq (k+1)\deg(B)$$

isso implica que

$$\begin{aligned} \ell(kB) &\geq (k+1)\deg(B) - \deg(C) \\ &= k\deg(B) + \deg(B) - \deg(C) \\ &= k\deg(B) + (\deg(B) - \deg(C)), \end{aligned}$$

daí

$$\ell(kB) \geq k\deg(B) + ([F : K(x)] - \deg(C)), \text{ para todo } k \geq 0,$$

assim

$$\deg(kB) - \ell(kB) \leq \gamma$$

para todo $k \geq 0$ e para algum $\gamma \in \mathbb{Z}$, onde $\gamma = [F : K(x)] - \deg(C)$.

Agora devemos mostrar que podemos substituir kB por γ. Mas para isso precisaremos provar a seguinte afirmação:

Afirmação. Dado $A \in DivF$, existem divisores A_1, D e um inteiro $k \geq 0$ tais que $A \leq A_1$,

$A_1 \sim D$ e $D \leq kB$.
Prova da afirmação
Tomemos $A_1 \geq A$ tal que $A_1 \geq 0$. Assim, temos que

$$\begin{aligned}\ell(kB) - \ell(kB - A_1) &= \dim(\mathscr{L}(kB)/\mathscr{L}(kB - A_1)) \\ &\leq \deg(kB) - (\deg(kB - A_1)),\end{aligned}$$

logo

$$\ell(kB - A_1) \geq \ell(kB) - \deg(A_1) \geq \deg(kB) - \gamma - \deg(A_1) > 0$$

para um k suficientemente grande. Logo, existe um elemento $0 \neq z \in \mathscr{L}(kB - A_1)$. Definindo $D = A_1 - (z)$, teremos que $A_1 \sim D$ e $D \leq A_1 - (A_1 - kB) = kB$, como queríamos.
Agora pela Afirmação, podemos concluir o resultado pois

$$\begin{aligned}\deg(A) - \ell(A) &\leq \deg(A_1) - \ell(A_1) \\ &= \deg(D) - \ell(D) \quad \text{pelo Corolário 4.9} \\ &\leq \deg(kB) - \ell(kB) \\ &\leq \gamma.\end{aligned}$$

□

Definição 4.15. O gênero g de F/K é definido por

$$g = \max\{\deg(A) - \ell(A) + 1 \mid A \in Div(F)\}.$$

Teorema 4.10 (Riemann)**.** Seja F/K um corpo de funções de gênero g. Então:

a) Para todo $A \in Div(F)$, temos $\ell(A) \geq \deg(A) + 1 - g$.

b) Existe um inteiro c, dependendo somente do corpo de funções algébricas F/K, tal que $\ell(A) = \deg(A) + 1 - g$ sempre que $\deg(A) \geq c$.

Demonstração. a) Segue direto da definição de gênero g.

b) Tomemos $A_0 \in DivF$ tal que $g = \deg(A_0) - \ell(A_0) + 1$ e definamos $c = \deg(A_0) + g$. Se $\deg(A) \geq c$, então

$$\begin{aligned}\ell(A - A_0) &\geq \deg(A - A_0) + 1 - g \\ &= \deg(A) - \deg(A_0) + 1 - g \\ &\geq c - \deg(A_0) + 1 - g \\ &= 1\end{aligned}$$

Tomemos $z \in \mathscr{L}(A - A_0) \setminus 0$ e definamos o divisor $A' = A + (z) \geq A_0$. Então, temos que

$$\begin{aligned} \deg(A) - \ell(A) &= \deg(A') - \ell(A') \qquad \text{Pelo Corolário 4.9} \\ &\geq \deg(A_0) - \ell(A_0) \qquad \text{Pelo Lema 4.4} \\ &= g - 1. \end{aligned}$$

Logo, $\ell(A) \leq \deg(A) - g + 1$ e por (a) obtemos a igualdade.

□

As definições a seguir são importantes para a compreensão do enunciado do Teorema de Riemann-Roch.

Definição 4.16. Um diferencial de Weil de F/K é uma transformação K-linear

$$w : \mathscr{A}_F \to K$$

que se anula em $\mathscr{A}_F(A) + F$ para algum divisor $A \in Div(F)$. Chamamos

$$\Omega_F = \{w \mid w \text{ é um diferecial de Weil de } F/K\}.$$

O módulo do diferencial de Weill de F/K, para cada $A \in Div(F)$, definimos

$$\Omega_F(A) = \{w \in \Omega_F \mid w \text{ se anula em } \mathscr{A}_F(A) + F\}.$$

Podemos considerar Ω_F como um espaço vetorial sobre K e $\Omega_F(A)$ um subespaço vetorial de Ω_F, que é unidimensional sobre F.

Definição 4.17. a) O divisor (w) do diferencial de Weil $w \neq 0$ é o único divisor de F/K satisfazendo:

i) w se anula em $\mathscr{A}_F((w)) + F$.

ii) Se w se anula em $\mathscr{A}_F(A) + F$, então $A \leq (w)$.

b) Para $0 \neq w \in \Omega_F$ e $P \in \mathbb{P}_F$, definimos $v_P(w) = v_P((w))$.

c) Um divisor W é chamado divisor canônico de F/K se $W = (w)$, para algum $w \in \Omega_F$.

Observação 4.2. Segue diretamente das definições que

$$\Omega_F(A) = \{w \in \Omega_F \mid w = 0 \text{ ou } (w) \geq A\}.$$

Proposição 4.6. a) Para $0 \neq x \in F$ e $0 \neq w \in \Omega_F(A)$, temos que $(xw) = (x) + (w)$.

b) Dois divisores canônicos de F/K são equivalentes.

Os divisores canônicos têm um importante papel na teoria de corpos de funções, já que, nesse caso, é possível obter o seguinte resultado, cuja demonstração pode ser encontrada em [11]

Teorema 4.11 (Riemann-Roch)**.** Seja W um divisor canônico de F/K. Então, para cada divisor $A \in Div(F)$,

$$\ell(A) = \deg(A) + 1 - g + \ell(W - A).$$

Corolário 4.12. Para um divisor canônico W, temos $\deg(W) = 2g - 2$ e $\ell(W) = g$.

Teorema 4.13. Se A é um divisor de F/K de grau $\deg(A) \geq 2g - 1$, então

$$\ell(A) = \deg(A) + 1 - g.$$

5 CÓDIGOS ALGÉBRICO-GEOMÉTRICOS DE GOPPA

Neste capítulo, descrevemos a construção de códigos corretores de erros proposta por Goppa usando corpos de funções algébricas. Definiremos os códigos algébrico-geométricos de Goppa, desenvolvendo suas propriedades básicas. Na seção 5.2, apresentaremos como um exemplo os códigos construídos por meio de corpos de funções de gênero zero.

5.1 CÓDIGOS ALGÉBRICO-GEOMÉTRICOS

Seja $n = q - 1$ e seja $\beta \in \mathbb{F}_q$ um elemento primitivo do grupo multiplicativo $\mathbb{F}_q^\times$, isto é, tal que $\mathbb{F}_q^\times = \{\beta, \beta^2, ..., \beta^n = 1\}$. Para um inteiro k com $1 \leq k \leq n$, consideraremos o espaço vetorial $k-$dimensional

$$\mathscr{L}_k = \{f \in \mathbb{F}_q[X] \mid \deg f \leq k - 1\} \tag{5.1}$$

e a função valorização $ev(f) : \mathscr{L}_k \longrightarrow \mathbb{F}_q^n$ dada por

$$ev(f) := (f(\beta), f(\beta^2), ..., f(\beta^n)) \in \mathbb{F}_q^n$$

Essa função é $\mathbb{F}_q$-linear e injetiva, pois os polinômios $f \in \mathbb{F}_q[X]$ de grau menor que n tem menos que n zeros. Portanto

$$C_k = \{f(\beta), f(\beta^2), ..., f(\beta^n) \mid f \in \mathscr{L}_k\}$$

é um $[n, k]$ código sobre $\mathbb{F}^q$, chamado de código de Reed-Solomon. O peso de uma palavra do código $0 \neq c = ev(f) \in C_k$ é dado por

$$wt(c) = n - |\{i \in \{1, ..., n\}; f(\beta^i) = 0\}| \geq n - \deg f \geq n - (k - 1).$$

Agora, vamos introduzir a noção de código algébrico geométrico. Vamos fixar algumas notações válidas para esta seção.

- $F/\mathbb{F}_q$ é um corpo de funções algébricas de gênero g.
- $P_1, ..., P_n$ são lugares dois a dois distintos de $F/\mathbb{F}_q$.
- $D = P_1 + ... + P_n$.
- G é um divisor de $F/\mathbb{F}_q$ tal que $suppG \cap suppD = \emptyset$.

Definição 5.1. O código algébrico geométrico $C_{\mathscr{L}}(D, G)$ associado aos divisores D e G é definido por

$$C_{\mathscr{L}}(D, G) = \{(x(P_1), ..., x(P_n)) \mid x \in \mathscr{L}(G)\} \subseteq \mathbb{F}_q^n$$

Note que essa definição faz sentido, pois se $x \in \mathscr{L}(G)$ temos que $v_{P_i}(x) \geq 0$ $(i = 1, ..., n)$, pois $suppG \cap supp(D) = \emptyset$. A classe residual $x(P_i)$ de x modulo P_i é um elemento do corpo das classes resíduos de P_i (ver definição 4.6). Como $\deg P_i = 1$, esse corpo de classes de resíduos é $\mathbb{F}_q$.

De forma análoga a (5.1) vamos considerar a aplicação valorização $ev_D : \mathscr{L}(G) \longrightarrow \mathbb{F}_q^n$ dada por

$$ev_D(x) = (x(P_1), ..., x(P_n)) \in \mathbb{F}_q^n. \tag{5.2}$$

A aplicação de avaliação é $\mathbb{F}_q$-Linear, e $C_{\mathscr{L}}(D, G)$ é a imagem de $\mathscr{L}(G)$ por ev_D.

Teorema 5.1. $C_{\mathscr{L}}(D, G)$ é um $[n, k, d]$ código com parâmetros

$$k = \ell(G) - \ell(G - D) \text{ e } d \geq n - \deg G.$$

Prova. A aplicação de valorização em (5.2) é uma aplicação sobrejetiva linear de $\mathscr{L}(G)$ para $C_{\mathscr{L}}(D, G)$. Provemos agora que $Ker(ev_D) = \mathscr{L}(G - D)$. De fato,

$$\begin{aligned}
Ker(ev_D) &= \{x \in \mathscr{L}(G) \mid x(P_i) = 0 \text{ para todo } i = 1, ..., n\} \\
&= \{x \in \mathscr{L}(G) \mid v_{P_i} \geq 1 \text{ para todo } i = 1, ..., n\} \\
&= \mathscr{L}(G) \cap \{x \in F \mid v_p(x) \geq 1 \, \forall P \in \{P_1, ..., P_n\}\} \\
&= \mathscr{L}(G) \cap \{x \in F \mid v_p(x) \geq -v_p(D) \, \forall P \in \{P_1, ..., P_n\}\} \\
&= \{x \in F \mid v_p(x) \geq -v_p(G) \, \forall P \in \{\mathbb{P}_F \setminus \{P_1, ..., P_n\}\} \cap \\
&\quad \{x \in F \mid v_p(x) \geq -v_p(D) \, \forall P \in \{P_1, ..., P_n\}\} \\
&= \{x \in F \mid v_P(x) \geq -v_P(G - D) \text{ para todo } P \in \mathbb{P}_F\} \\
&= \mathscr{L}(G - D).
\end{aligned} \tag{5.3}$$

Assim segue que $k = \dim C_{\mathscr{L}}(D, G) = \dim \mathscr{L}(G) - \dim \mathscr{L}(G - D) = \ell(G) - \ell(G - D)$. Agora assumindo que $C_{\mathscr{L}}(D, G) \neq 0$, seja $x \in \mathscr{L}(G)$ com $wt(ev_D(x)) = d$. Então existem $n - d$ índices $j_1, ..., j_{n-d} \in \{j, ..., n\}$ tais que $x(P_{j_i}) = 0$; isso implica que $x \in \mathscr{L}(G - (P_{j_1} + ... + P_{j_{n-d}})) \setminus \{0\}$, i.e., $\ell(G - (P_{j_1} + ... + P_{j_{n-d}})) \geq 1$, então pelo corolário 4.9 segue que $\deg(G - (P_{j_1} + ... + P_{j_{n-d}})) \geq 0$. Portanto: $\deg G - (n - d) \geq 0$ e assim concluímos que $d \geq n - \deg G$. □

Corolário 5.2. Suponha que o grau de G é estritamente menor que n. Então, a aplicação valorização $ev_D : \mathscr{L}(G) \longrightarrow C_{\mathscr{L}}(D, G)$ é injetiva e temos:

(a) $C_{\mathscr{L}}(D, G)$ é um $[n, k, d]$ código com

$$d \geq n - \deg G \text{ e } k = \ell(G) \geq \deg G + 1 - g$$

consequentemente,

$$k + d \geq n + 1 - g. \tag{5.4}$$

(b) Se, além disso, $2g-2 < \deg G < n$, então $k = \deg G + 1 - g$.

(c) Se $\{x_1, ..., x_k\}$ é uma base de $\mathscr{L}(G)$, então a matriz

$$M = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \dots & x_1(P_n) \\ \vdots & \vdots & & \vdots \\ x_k(P_1) & x_k(P_2) & \dots & x_k(P_n) \end{pmatrix}_{k\times n}$$

é a matriz geradora de $C_{\mathscr{L}}(D, G)$.

Demonstração. Como $\deg G < n$ e $\deg(G - D) = \deg G - \deg D < n - n = 0$, então $\dim(G - D) = 0$ isso implica que $\mathscr{L}(G - D) = Ker(ev_D) = \{0\}$, e portanto, ev_D é uma aplicação injetiva.

(a) Como $k = \ell(G), d \geq n - \deg G$ e $\ell(G) \geq \deg G + 1 - g$, então

$$k + d \geq \ell(G) + n - \deg G \geq n + 1 - g.$$

(b) Se $2g - 2 < \deg G$, então pelo teorema 4.13 temos: $k = \ell(G) = \deg G + 1 - g$.

(c) Como $\{x_1, ..., x_n\}$ é base de $\mathscr{L}(G)$ e ev_D é injetiva, temos que $\{x(P_1), ..., x(P_n)\}$ é base de $C_{\mathscr{L}}(D, G)$ e M é uma matriz geradora.

□

Observe que a cota inferior (5.4) para a distância mínima é muito parecida com a cota superior de Singleton. Confrontando ambas cotas e com $\deg G < n$, temos

$$n + 1 - g \leq k + d \leq n + 1 \tag{5.5}$$

Note que $k + d = n + 1$ se F é um corpo de funções com gênero $g = 0$, assim os códigos geométricos de Goppa construídos por meio de corpos de funções racionais $\mathbb{F}_q(z)$ são também código MDS. A fim de obter uma distância mínima significativa, geralmente considera-se $\deg G < n$.

Definição 5.2. O inteiro $d^* := n - \deg(G)$ é chamado de distância projetada do código $C_{\mathscr{L}}(D, G)$.

Observação 5.1. Suponha que $\ell(G) > 0$ e $d^* = n - \deg(G) > 0$. Então $d^* = d$ se e somente se existe um divisor D' com $0 \leq D' \leq D$, $\deg(D') = \deg(G)$ e $\ell(G - D') > 0$.

Demonstração. Suponha que $d^* = d = n - \deg G$ e seja $x \in \mathscr{L}(G)$ tal que $wt(ev_D(x)) = d$. Então, $ev_D = (x(P_1), ..., x(P_n))$ possui $\deg G = n - d$ coordenadas nulas, sejam elas

$x(P_{i_1}), ...x(P_{i_{\deg G}})$. Seja $D' = \sum_{j=1}^{\deg G} P_{i_j}$, então $\deg D' = \deg G, 0 \leq D' \leq D$ e $\ell(G - D') > 0$, pois $x \in \mathscr{L}(G - D')$.

Agora suponha que e exista um divisor D' com $0 \leq D' \leq D, \deg G$ e $\ell(G - D) > 0$, então existe $x \in \mathscr{L}(G - D')$, se tomarmos $P \in suppD$, teremos

$$v_p(x) \geq -v_p(G - D') \geq -v_p(G) + v_p(D')$$

isso implica que $x(P) = 0$ para pelo menos $\deg D'$ lugares, logo $wt(ev_P(x)) \leq n - \deg D'$. Daí $d \leq n - \deg G = d^*$ e pelo teorema 5.1 $d \geq n - \deg G$. Portanto $d = d^*$. □

Definição 5.3. Dois códigos $C_1, C_2 \subseteq \mathbb{F}_q^n$ são ditos equivalentes se existe um vetor $a = (a_1, ..., a_n) \in \mathbb{F}_q^n$ tal que $C_2 = aC_1$, isto é:

$$C_2 = \{(a_1c_1, ..., a_nc_n) \mid (c_1, ..., c_n) \in C_1\}$$

Proposição 5.1. (a) Suponha G_1 e G_2 divisores com $G_1 \sim G_2$ (i.é. $G_1 = G_2 + (y)$ para algum $y \in F$) e $suppG_1 \cap suppD = suppG_2 \cap suppD = \emptyset$. Então os códigos $C_{\mathscr{L}}(D, G_1)$ e $C_{\mathscr{L}}(D, G_2)$ são equivalentes.

(b) Inversamente, se um código $C \subseteq \mathbb{F}_n^q$ é equivalente a $C_{\mathscr{L}}(D, G)$ então existe um divisor $G' \sim G$ tal que $suppG' \cap suppD = \emptyset$ e $C = C_{\mathscr{L}}(D, G')$.

Demonstração. **(a)** Temos $G_1 \sim G_2$, então $G_2 = G_1 - (y)$. Como $suppG_1 \cap suppD = \emptyset$ e $suppG_2 \cap suppD = \emptyset$ e $(y) = G_1 - G_2$ então $v_{P_i(y)=0}$, para todo $i = 1, ..., n$, assim $a = (y(P_1), ..., y(P_n)) \in \mathbb{F}_q^n$. Pelo lema 4.3 temos que a aplicação

$$\begin{aligned} \varphi : \mathscr{L}(G_1) &\longrightarrow \mathscr{L}(G_2), \\ x &\longmapsto xy \end{aligned}$$

é bijetiva. Então, dado $c \in \mathscr{L}(G_2)$, podemos escrever $c = xy$ para algum $x \in F$. Assim

$$\begin{aligned} C_{\mathscr{L}}(D, G) &= \{((c(P_1), ..., c(P_n)) \mid c \in \mathscr{L}(G_2)\} \\ &= \{(xy(P_1), ..., xy(P_n)) \mid x \in \mathscr{L}(G_1)\} \\ &= \{(y(P_1), ..., y(P_n)(x(P_1), ..., x_(P_n) \mid x \in \mathscr{L}(G_1)\} \\ &= aC_{\mathscr{L}}(D, G_1) \end{aligned}$$

(b) Seja $C = a \cdot C_{\mathscr{L}}(D, G)$ com $a = (a_1, ..., a_n) \in \mathbb{F}_q^n$. Pelo teorema da aproximação fraca, podemos escolher z tal que $v_{P_i}(z - a_i) = 1 > 0$, assim $z(P_i) = a_i$. Tomemos $G' = G - (z)$, então $C = C_{\mathscr{L}}(D, G')$.

□

5.2 CÓDIGOS RACIONAIS

Nesta seção, como um exemplo do que vimos na anterior, vamos investigar os códigos geométricos de Goppa associados a divisores de um corpo de funções racionais, mas para isso vamos primeiramente estudar um pouco sobre esses corpos de funções racionais. Ao longo da seção, K representa um corpo e $K[x]$ o anel de polinômios sobre uma variável x com coeficientes em K.

Definição 5.4. Um corpo de funções racionais é um corpo de funções algébricas F/K, com $F = K(x)$, onde x é transcendente sobre K e

$$K(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], g(x) \neq 0 \right\}.$$

Dado um polinômio mônico e irredutível $p(x) \in K[x]$ consideraremos o anel de valorização

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \nmid g(x) \right\},$$

de $K(x)/K$ com ideal maximal

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \mid f(x), p(x) \nmid g(x) \right\}.$$

Analogamente, teremos

$$\mathcal{O}_{\infty} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f(x) \leq \deg(g(x)) \right\}$$

é outro anel de valorização do corpo de funções racionais $K(x)/K$, que define o lugar

$$P_{\infty} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f(x) < \deg(g(x)) \right\}$$

que tem como elemento primo $t = 1/x$. Chamaremos P_{∞} de lugar infinito de $K(x)$.

Vamos agora provar alguns resultados de dos corpos de funções racionais

Proposição 5.2. Seja $K(x)/K$ o corpo de funções racionais.

a) Se $P = P_{p(x)} \in \mathbb{P}_{K(x)}$, onde $p(x) \in K[x]$ é um polinômio mônico irredutível. Então, $p(x)$ é um elemento primo de P, e a valorização correspondente v_P pode ser descrito, da seguinte maneira: se $z \in K(x) \setminus \{0\}$ é escrito na forma $z = p(x)^n(f(x)/g(x))$ com $n \in \mathbb{Z}$, $f(x), g(x) \in K[x]$, $p(x) \nmid f(x)$ e $p(x) \nmid g(x)$, então $v_P(z) = n$. O corpo das classes residuais $K(x)_P = \mathcal{O}_P/P$ é isomorfo a $K[x]/\langle p(x) \rangle$. Consequentemente, $\deg P = \deg(p(x))$

b) No caso que $p(x) = x - \alpha$ com $\alpha \in K$, o grau de $P = P_{x-\alpha}$ é 1, e as aplicações das classes residuais é dado por

$$z(P) = z(\alpha) \text{ para } z \in K(x),$$

onde $z(\alpha)$ é definido da seguinte forma: escreva $z = f(x)/g(x)$ com polinômios primos relativos em $K[x]$, então

$$z(\alpha) : \begin{cases} f(\alpha)/g(\alpha), & \text{se } g(\alpha) \neq 0 \\ \infty, & \text{se } g(\alpha) = 0 \end{cases}$$

c) Seja $P = P_\infty$ é o lugar infinito de $K(x)/K$, então $\deg P_\infty = 1$. O elemento primo para P_∞ é $t = 1/x$. A correspondente valorização discreta v_∞ é dada por

$$v_\infty \left(\frac{f(x)}{g(x)} \right) = \deg(f(x)) - \deg(g(x)),$$

onde $f(x), g(x) \in K[x]$. A aplicação das classes residuais correspondente a P_∞ é determinada por $z(P_\infty) = z(\infty)$ para $z \in K(x)$, onde $z(\infty)$ é definido da forma usual, se

$$z = \frac{a_n x^n + \ldots + a_0}{b_m x^m + \ldots + b_0} \text{ com } a_n, b_m \neq 0,$$

então

$$z(\infty) : \begin{cases} a_n/b_m, & \text{se } n = m, \\ 0, & \text{se } n < m, \\ \infty, & \text{se } n > m. \end{cases}$$

Demonstração. a) Consideremos $P = P_{p(x)} \in \mathbb{P}_F$, $p(x) \in K[x]$ irredutível. O ideal $P_{p(x)} \subset \mathcal{O}_{p(x)}$ é gerado por $p(x)$, pois se $\frac{f(x)}{g(x)} \in P_{p(x)}$, então $p(x)|f(x)$ e $p(x)$ não divide $g(x)$, daí $\frac{f(x)}{g(x)} = \frac{h(x)}{g(x)} p(x) \in \mathcal{O}_{p(x)} p(x)$. Portanto $P_{p(x)} \subset p(x)\mathcal{O}_{p(x)}$. Ja que $p(x) \in P_{p(x)}$, então $p(x)\mathcal{O}_{p(x)}$. Agora vamos definir

$$\begin{aligned} \varphi : K[x] &\longrightarrow K(x)_P \\ f(x) &\longmapsto f(x)(P) \end{aligned}$$

φ está bem definida,pois $\varphi(x) = \varphi(x)/1$, implicando que $\varphi(x) \in \mathcal{O}_{p(x)}$. Além disso φ é um homomorfismo e $\varphi(x) \in Ker\varphi \Leftrightarrow \varphi(x)(P) = (P) \Leftrightarrow p(x|\varphi(x)) \Leftrightarrow \varphi(x) \in (p(x))$.

Provemos agora que φ é sobrejetivo. De fato, seja $z \in \mathcal{O}_{p(x)}$, então existem $u(x), v(x) \in K[x]$ tais que $z = f(x)/g(x)$ e $p(x) \nmid v(x)$. Mas ainda, como $p(x)$ é irredutível, $m.d.c.(p(x), v(x)) = 1$, então existem $a(x), b(x) \in K[x]$ tal que $a(x)p(x) + b(x)v(x) = 1$. Por isso

$$z = 1.z = a(x)p(x) + b(x)v(x)\frac{u(x)}{v(x)} = \frac{a(x)}{v(x)}p(x) + b(x)u(x).$$

$$\Longrightarrow z(P) = (b(x)u(x))(P)$$

$$\Longrightarrow \varphi(b(x))u(x) = z(P)$$

Consequentemente, temos que $\varphi(b(x)u(x)) = (b(x)u(x))P = z(P)$. Deste modo, pelo teorema dos isomorfismos, $K(x)_P$ é isomorfo a $K[x]/\langle p(x)\rangle$. Como $[K[x]/(p(x)) : K] = [K(x)_p : K] \Rightarrow \deg P = \deg(p(x))$.

b) Seja $P = P_\alpha$ com $\alpha \in K$. Se $f(x) \in K[x]$ então $(x-\alpha) \mid (f(x) - f(\alpha))$. Assim

$$f(x)P = (p(x)q(x))\,(P) + f(\alpha)(P) = f(\alpha).$$

Seja $z \in \mathcal{O}_P$, então existem $f(x), g(x) \in K[x]$ tais que $z = f(x)/g(x)$ e $(x-\alpha) \nmid g(x)$, onde $g(x)P = g(\alpha) \neq 0$. Assim obtemos

$$z(P) = \frac{f(x)(P)}{g(x)(P)} = \frac{f(\alpha)}{g(\alpha)} = z(\alpha).$$

Agora se $z \notin \mathcal{O}_P$, então $z = f(x)/g(x)$ com $f(x), g(x) \in K[x]$ e $m.d.c\,(f(x), g(x)) = 1$, temos que $z(P) = \infty = z(\alpha)$

iii) Provemos que $1/x$ é um elemento primo de $P_\infty = P$. Considere $z = f(x)/g(x) \in P$, isto implica que $\deg f < \deg g$. Como $x \neq 0$, então $z = \frac{1}{x}\frac{xf(x)}{g(x)}$ pois $\deg(xf(x)) \leq \deg g(x)$, assim $(xf(x))/g(x) \in \mathcal{O}_\infty$. Logo $P = (1/x)\mathcal{O}_\infty$ o que implica que $\frac{1}{x}$ é primo de P_∞. Ja que P_∞ com respeito a x é P_0 em relação a $\frac{1}{x}$, então $\frac{K(x)}{P_\infty} \simeq \frac{K(1/x)}{P_0} \simeq \frac{K[1/x]}{(1/x)} \Rightarrow \deg P_0 = 1 \Rightarrow \deg P_\infty = 1$.

□

Teorema 5.3. Não existe lugares do corpo de funções racionais $K(x)/K$, além dos lugares $P_{p(x)}$ e P_∞ definidos no inicio dessa seção.

Demonstração. Seja P um lugar de $K(x)/K$, $\mathcal{O}_P$ o anel de valorização correspondente a P. Então:
Caso I: Suponha $x \in \mathcal{O}_P$, então $K[x] \subset \mathcal{O}_P$, isso implica que $I = K[x] \cap P$ é um ideal de $K[x]$, como P é maximal, então I é maximal em $K[x]$, assim $K[x]/I$ é corpo. Á vista disso temos um mergulho $K[x]/I \hookrightarrow K(x)_P$. Como K é corpo, então $K[x]$ é um domínio de ideais principais, logo um polinômio mônico irredutível $p(x) \in K[x]$ tal que $I = (p(x))$, então $I = K[x] \cap P = p(x)K[x]$.

Notemos que cada $g(x) \in K[x]$ com $p(x) \nmid g(x) \Rightarrow g(x) \notin I \Rightarrow g(x) \notin P$, então $g(x)^{-1} = \frac{1}{g(x)} \in \mathbb{O}_P$. Portanto

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \nmid g(x) \right\}.$$

Seja $f(x)/g(x) \in \mathcal{O}_{p(x)}$, ja que $p(x) \nmid g(x)$, teremos que $g(x)^{-1} \in \mathcal{O}_P$, logo $f(x)/g(x) \in \mathcal{O}_P$.

Portanto, $\mathcal{O}_{p(x)} \subseteq \mathcal{O}_P$, visto que $\mathcal{O}_{p(x)}$ é um anel de valorização e a partir disso $\mathcal{O}_{p(x)}$ é maximal, assim temos $\mathcal{O}_{p(x)} = \mathcal{O}_P$, daí $P_p(x) = P$.

Caso II: Agora, suponha $x \notin \mathcal{O}_{\mathscr{P}}$, então $x^{-1} \in \mathcal{O}_P$ e $x^{-1} \in P$, assim $K[x^{-1}] \subseteq \mathcal{O}_P \Rightarrow x^{-1} \in P \cap K[x^{-1}] \Rightarrow x^{-1}K[x^{-1}] \subset P \cap K[x^{-1}]$ ideais de $K[x^{-1}]$. Como x^{-1} é irredutível temos analogamente ao caso I que $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$ e

$$\begin{aligned}
\mathcal{O}_P &\supseteq \left\{ \frac{f(x^{-1})}{g(x^{-1})} \mid f(x^{-1}), g((x^{-1})) \in K[x^{-1}], x^{-1} \nmid g(x^{-1}) \right\} \\
&= \left\{ \frac{a_0 + a_1x^{-1} + \ldots + a_nx^{-n}}{b_0 + b_1x^{-1} + \ldots + b_mx^{-m}}, \ b_0 \neq 0 \right\} \\
&= \left\{ \frac{(a_0x^n + a_1x^{n-1} + \ldots + a_n)/x^n}{(b_0^m + b_1x^{m-1} + \ldots + b_m)/x^m}, \ b_0 \neq 0 \right\} \\
&= \left\{ \frac{a_0x^{m+n} + \ldots + a_nx^m}{b_0x^{m+n} + \ldots + b_mx^n}, \ b_0 \neq 0 \right\} \\
&= \left\{ \frac{u(x)}{v(x)} \mid u(x), v(x) \in K[x] \text{ e } \deg u(x) \leq \deg v(x) \right\} = \mathcal{O}_\infty
\end{aligned}$$

Portanto, como $\mathcal{O}_\infty$ é maximal, então $\mathcal{O}_\infty = \mathcal{O}_P$, logo $P = P_\infty$ □

Proposição 5.3. Todo corpo de funções racionais $K(x)/k$, possui gênero $g = 0$.

Demonstração. Seja P_∞ o polo divisor de x. Considere para $r \geq 0$ o espaço vetorial $\mathscr{L}(rP_\infty)$, temos que $1, x, ..., x^r$ estão em $\mathscr{L}(rP_\infty)$, assim pelo teorema de Riemann

$$r + 1 \leq \ell(rP_\infty) = \deg(rP_\infty) + 1 - g = r + 1 - g$$

para r suficientemente grande, como $g \geq 0$, então podemos concluir que $g = 0$. □

Agora vamos descrever os códigos de Goppa de forma bem explícita por meio de matrizes geradora e de paridade. Na teoria de códigos, essa classe de códigos é conhecida pelo nome de Códigos Generalizados de Reed-Solomon.

Definição 5.5. Um código algébrico geométrico $C_{\mathscr{L}}(D, G)$ associado a divisores G e D de um corpo de funções racionais $\mathbb{F}_q^n$ é código racional.

Observe que o comprimento de um código geométrico racional de Goppa é limitado por $q + 1$ pois $\mathbb{F}_q$ tem somente $q + 1$ lugares de grau um: o polo P_∞ de z e para cada $\alpha \in \mathbb{F}_q$, o zero P_α de $z - \alpha$.

Proposição 5.4. Seja $C = C_{\mathscr{L}}(D, G)$ um código geométrico racional de Goppa sobre $\mathbb{F}_q$ e sejam n, k, d os parâmetros de C. Então, temos:

(a) $n \leq q + 1$.

(b) $k = 0$ se e somente se $\deg G < 0$ e $k = n$ se e somente $\deg G > n - 2$.

(c) Para $0 \leq \deg G \leq n-2$,

$$k = 1 + \deg G \text{ e } d = n - \deg G.$$

Em particular, C é um código MDS.

(d) $C^{\perp}$ é também um código geométrico racional de Goppa.

Demonstração. **(a)** Temos que $D = P_1 + ... + P_n$ com os $P_{i's}$ lugares dois a dois distintos de grau um em $\mathbb{F}_q$. Como $\mathbb{F}_q$ possui apenas $q+1$ lugares de grau um, então $n = \deg D \leq q+1$.

(b) Tomemos $k = 0$ e suponhamos que $\deg G \geq 0$. Então, podemos ter $\deg G < n$ ou $\deg G \geq n$.
Se $\deg G < n$, como $g = 0$, então pelo corolário 3.2 teremos $k = \ell(G) = \deg G + 1 \geq 1$, uma contradição. Agora, se $\deg G \geq n$, então $G - D$ satisfaz a igualdade de Riemann, donde $\ell(G-D) = \deg(G-D) + 1$. Segue que

$$k = \ell(G) + 1 - \ell(G-D) - 1 = \deg G + 1 - \deg G + n - 1 = n \geq 1,$$

uma contradição. Portanto, podemos concluir que $\deg G < 0$. Agora suponhamos que $\deg G < 0$ então $\mathscr{L}(G) = 0$. Logo, $Im\ ev_D = 0$ e $k = 0$. Portanto, $k = 0$ se e somente se $\deg G < 0$.
Seja $k = n$, então, pela cota de Singleton, $k + d \leq n + 1$, donde $d \leq 1$, isto é, $1 \geq \deg G - n \Rightarrow \deg G > n - 2$. Reciprocamente, suponha que $\deg G > n - 2$. Como $g = 0$ e $n \geq 1$, então $n - 2 \geq -1 = 2g - 1$, donde $\ell(G) = \deg G + 1$ e $\deg(G - D) = \deg G - n \geq n - 1 + n = -1$. Assim, $\ell(G - d) = \deg G - n + 1$. Portanto:

$$k = \ell(G) - \ell(G-D) = \deg G + 1 - (\deg G - n + 1) = n$$

Em particular, pela cota de Singleton e pelo corolário 5.2, temos $n+1-g \leq k+d \leq n+1$. Mas como $g = 0$, temos $k + d = n + 1$, o que implica que C é um código MDS.

(c) Se $0 \leq \deg(G) \leq n-2$, então $\deg(G) \geq 0$ isso implica que $\ell(G) = \deg(G) + 1$ e como $\deg(G) \leq n - 2$, então $\deg(G - D) < 0$, assim $\ell(G - D) = 0$. Logo $k = \ell(G) - l(G - D) = 1 + \deg(G)$. Pela cota de Singleton temos que $d \leq n+1-k = n - \deg(G)$. Mas pelo corolário 5.2, temos que $d \geq n - \deg(G)$. Portanto, $d = n - \deg(G)$.

(d) $C^{\perp} = C_{\mathscr{L}}(D,G)^{\perp} = C_{\Omega}(D,G) = C_{\mathscr{L}}(D,H), H = D - G + (\eta)$.

□

A seguir, determinaremos matrizes geradoras para um código racional de Goppa.

Proposição 5.5. Seja $C = C_{\mathscr{L}}(D, G)$ um código racional de Goppa sobre $\mathbb{F}_q$ com parâmetros n, k e d.

(a) Se $n \leq q$ então existem elementos $\alpha_1, ..., \alpha_n \in \mathbb{F}_q$ dois a dois distintos e $v_1, ..., v_n \in \mathbb{F}_q^n$ (não necessariamente distintos) tais que

$$C = \{(v_1 f(\alpha_1), ..., v_n f(\alpha_n)) \mid f \in \mathbb{F}_q[z] \text{ e } \deg f \leq k-1\}$$

A matriz

$$M = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \dots & \alpha_n v_n \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \dots & \alpha_n^2 v_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \dots & \alpha_n^{k-1} v_n \end{pmatrix}$$

é uma matriz geradora para C.

(b) Se $n = q + 1$, C tem uma matriz geradora

$$M = \begin{pmatrix} v_1 & v_2 & \dots & v_n & 0 \\ \alpha_1 v_1 & \alpha_2 v_2 & \dots & \alpha_n v_n & 0 \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \dots & \alpha_n^2 v_n & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \dots & \alpha_n^{k-1} v_n & 1 \end{pmatrix}$$

onde $\mathbb{F}_q = \{\alpha_1, ..., \alpha_{n-1}\}$ e $v_1, ..., v_{n-1} \in \mathbb{F}_q^{\times}$.

Demonstração. **(a)** Inicialmente vamos construir uma base para $C_{\mathscr{L}}(D, G)$. Seja $D = P_1 + ... + P_n$ com $n \leq q$. Como há $q + 1$ lugares de grau um em $F/\mathbb{F}_q$, então existe P de grau um não pertencente ao suporte de D. Seja $Q = P_1$, então $Q \neq P$. Assim, $\deg(G - P) = 0 \geq 2g - 1$ (pelo teorema 4.13) e $\ell(Q - P) = \deg(Q - P) + 1 - g = 1$. Pelo corolário 4.9 $Q - P$ é principal, então existe $z \in F$ com $(z) = Q - P$. Logo $(z)_0 = Q$ e $(z)_\infty = P$, porém $[F : \mathbb{F}_q(z)] = \deg(z)_\infty = 1$, donde $F = \mathbb{F}_q(z)$ e $P = P_\infty$. Suponhamos que $\deg G > n - 2$, pelo corolário 5.4 $k = n$, o que implica que $C_{\mathscr{L}}(D, G) = \mathbb{F}_q^n$. Agora, suponha que $\deg G \leq n - 2$. Pelo corolário 5.4 $\deg G = k - 1$. O divisor $B = (k-1)P_\infty - G$ tem grau zero e $\ell(B) = 1$, o que implica que B é principal. Então, existe $u \in F$ tal que $B = (u)$. Observemos que $\{u, zu, ..., z^{k-1}u\} \subset \mathscr{L}(G)$, pois para $0 \leq i \leq k - 1$ temos:

$$(z^i u) = i(z) + (u) = i(Q - P_\infty) + (k-1)P_\infty - G = iQ + ((k-1) - i)P_\infty - G,$$

assim $(z^i u) \geq -G$.
Como $F = \mathbb{F}_q(z)$ e $\ell(G) = k$, então $\{u, zu, ..., z^{k-1}u\}$ é linearmente independente sobre $\mathbb{F}_q$. De fato, se

$$\sum_{i=0}^{k-1} a_i(z^i u) = 0,$$

então

$$\sum_{i=0}^{k-1} a_i(z^i u) = u\sum_{i=0}^{k-1} a_i(z^i) \Rightarrow \sum_{i=0}^{k-1} a_i(z^i) = 0 \Rightarrow a_i = 0$$

pois z é transcendente sobre $\mathbb{F}_q$. Portanto $\{u, zu, ..., z^{k-1}u\}$ é base para $\mathscr{L}(G)$, ou seja,

$$\mathscr{L}(G) = \{uf(z) | f \in \mathbb{F}_q[z],\ \deg f \leq k-1\}$$

Tomando $\alpha_i = z(P_i)$ e $v_i = u(P_i)$, teremos

$$(uf(z))(P_i) = u(P_i)f(z(P_i)) = v_i f(\alpha_i), \text{ para } i = 1, ..., n\,.$$

Portanto:

$$C = C_{\mathscr{L}}(D, G) = \{(v_1.f(\alpha_1), ..., v_n.f(\alpha_n)) \mid \deg(f(x)) \leq k-1\}$$

e, como $k = \deg G + 1$, teremos que

$$\beta = \{(v_1, ..., v_n), (\alpha_1 v_1, ..., \alpha_n v_n), ..., (\alpha_1^{k-1} v_1, ..., \alpha_n^{k-1} v_n)\},$$

gera C. Então β é uma base de C e, assim, M é uma matriz geradora.

(b) A prova é essencialmente a mesma de $n \leq q$. Agora, temos $n = q+1$ e podemos escolher z de forma que $P_n = P_\infty$ é o polo de z. Como anteriormente, $(k-1)P_\infty - G = (u)$ com $0 \neq u \in F$ e $\{u, zu, ..., z^{k-1}u\}$ é uma base de $\mathscr{L}(G)$. Observemos que $P_n = P_\infty = (z)_\infty$. Temos que, para todo $j = 1, ..., k-2$, $uz^j(P_n) = 0$, pois $v_{p_n}(uz^j) = k-1-j \geq 1$. Mas para $j = k-1$, $v_{P_n} = 0$, ou seja, $\gamma = uz^{k-1}(P_k - 1) \in \mathbb{F}_q$ temos:

$$((uz^{k-1})(P_1), ..., (uz^{k-1})(P_n)) = (\alpha_1^{k-1} v_1, ..., \alpha_{n-1}^{k-1} v_{n-1}, \gamma).$$

Substituindo u por $\gamma^{-1}u$ obtemos que

$$\beta = \{(v_1, ..., v_n, 0), (\alpha_1 v_1, ..., \alpha_n v_n, 0), ..., (\alpha_1^{k-1} v_1, ..., \alpha_n^{k-1} v_n, 1)\},$$

é uma base de $C = C_{\mathscr{L}}(D, G)$ e M é a matriz geradora.

□

6 SEGUNDA APLICAÇÃO DE BASES DE GRÖBNER A CÓDIGOS

6.1 AUTOMORFISMOS DE CÓDIGOS ALGÉBRICO-GEOMÉTRICOS

Sejam $(c_1, ..., c_n) \in \mathbb{F}_q^n$ e S_n o grupo simétrico, cujos elementos são permutações do conjunto $\{1, 2, ..., n\}$ para $\pi \in S_n$. Considerando $\pi(c_1, ..., c_n) = (c_{\pi(1)}, ..., c_{\pi(n)})$, o grupo de automorfismo de C é dado por

$$Aut(C) = \{\pi \in S_n;\ \pi(C) = C\} = \{\pi \in S_n;\ \pi(c) \in C \text{ para todo } c \in C\}.$$

Vamos estudar os automorfismos de um código algébrico-geométrico induzidos pelos automorfismos do corpo de funções correspondente.

Fixado um corpo de funções $F/\mathbb{F}_q$, consideramos $Aut(F/\mathbb{F}_q)$ o grupo de automorfismos de F sobre $\mathbb{F}_q$, isto é, $\sigma(a) = a$ para todo $\sigma \in Aut(F/\mathbb{F}_q)$ e $a \in \mathbb{F}_q$. Esse grupo age em $\mathbb{P}_F$ definindo $\sigma(P) := \{\sigma(x);\ x \in P\}$, induzindo, dessa forma, uma relação entre v_P e $v_{\sigma(P)}$ dada por $v_{\sigma(P)}(y) = v_P(\sigma^{-1}(y))$ para todo $y \in F$. Além disso, $\deg(\sigma(P)) = \deg P$ e obtemos uma ação no grupo dos divisores dada por

$$\sigma(\sum n_P P) := \sum n_P \sigma(P)$$

Consideremos agora $P_1, ..., P_n$ lugares de grau um de $F/\mathbb{F}_q$ distintos, o divisor $D = P_1 + ... + P_n$ e G um divisor tal que $supp(G) \cap supp(D) = \emptyset$. Seja $C = C_{\mathscr{L}}(D, G)$ um código de Goppa. Definimos $Aut_{D,G}(F/\mathbb{F}_q)$ o subgrupo dos automorfismo de $Aut(F/\mathbb{F}_q)$ formado pelos automorfismos que fixam D e G, isto é

$$Aut_{D,G}(F/\mathbb{F}_q) = \{\sigma \in Aut(F/\mathbb{F}_q);\ \sigma(D) = D \text{ e } \sigma(G) = G\}$$

Lema 6.1. Todo $\sigma \in Aut_{D,G}(F/\mathbb{F}_q)$ induz um automorfismo não-trivial:

$$\sigma(f(P_1), ..., f(P_n)) = ((f \circ \sigma^{-1})(P_1), ..., (f \circ \sigma^{-1})f(P_n))$$

Demonstração. Ver [10] lema II.A.1 □

Corolário 6.1. Seja $\sigma \in Aut_{D,G}(F/\mathbb{F}_q)$ e $Supp(D) = O_1 \cup ... \cup O_r$ a decomposição do $supp(D)$ em órbitas disjuntas sobre a ação σ. Então as entradas das palavras códigos correspondem aos lugares em cada O_i que são permutados ciclicamente por σ.

Vamos ver agora como dar uma estrutura de módulos para códigos geométricos de Goppa $C_{\mathscr{L}}(D, G)$ associando a um submódulo de $\mathbb{F}_q[t]^r$. Se considerarmos um automorfismo $\sigma \in Aut_{D,G}(F/\mathbb{F}_q)$, então os lugares $c \in supp(D)$, com $c = (c_1, ..., c_n)$ são divididos em $r-$ciclos cíclicos pela ação de σ, que chamaremos de orbitas e denotaremos por $O_1, ..., O_r$. Cada orbita O_i possui r_i elementos onde $\sum_{i=1}^{r} r_i = n$. Denotaremos os elementos de

$O_i = (P_{i,0}, ..., P_{i,r_i-1})$ para $i = 1, ..., r$, onde $P_{i,0}$ é um elemento escolhido aleatoriamente de O_i. Definimos $P_{i,j} = \sigma^j(P_{i,0})$. Assim,vemos que $P_{i,r_i} = P_{i,0}$, e por convenção, escreveremos $P_{i,-1} = \sigma^{-1}(P_{i,0}) = P_{i,r_i-1}$.

Temos que se $c \in C$, então $c = (f(P_1), ..., f(P_n))$, com $f \in \mathscr{L}(G)$. Reorganizando as coordenadas de O_i, se necessário, podemos representar as palavras de C como $r-$uplas de polinômios de uma variável

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

com

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

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

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

Assim temos, $C_{\mathscr{L}}(D, G)$ associado ao submódulo $E \leq \mathbb{F}_q[t]^r$ que é a imagem inversa de $\pi^{-1}(C)$ da sobrejeção

$$\pi : \mathbb{F}_q[t]^r \longrightarrow \bigoplus_{i=1}^{r} \frac{\mathbb{F}_q[t]}{\langle t^{r_i} - 1 \rangle}$$

6.2 CODIFICAÇÃO DE CÓDIGOS GEOMÉTRICOS DE GOPPA

Um código $C \subset \mathbb{F}_q^n$ pode ser interpretado como a imagem de aplicação injetiva $\alpha : \mathbb{F}_q^k \longrightarrow C$. Como vimos na seção 3.2, usando a matriz geradora M do código C temos um algortimo de codificação imediato dado pelo produto de um vetor linha $w = (w_1, ..., w_k)$ por M. Nessa seção, vamos apresentar o algoritmo de codificação de Little, Saints e Heegard, que utiliza a base de Gröbner e possui uma maior eficiência para a codificação de códigos geométricos de Goppa. Na seção 6.3, veremos um exemplo de codificação utilizando esse algoritmo.

Definição 6.1. Dada uma base de Gröbner $\mathscr{G}$ para E, as posições de informação são os coeficientes dos k primeiros monômios líderes da forma $t^l e_j$ com $l \leq r_i - 1$, que aparecem nas r-uplas construídas das palavras $(h_1(t), ..., h_r(t))$ do código, ordenando de forma decrescente com a ordem POT. Denotaremos esses monômios por $m_l = t^{i_l} e_{j_l}$, para $l = 1, 2, ..., k$.

Para $h = (h_1(t), ..., h_r(t))$, definiremos o vetor $VC(h) \in \mathbb{F}_q^n$ como sendo o vetor formado pelos coeficientes dos termos de h na ordem POT.

Para a codificação utilizaremos o seguinte algoritmo

O Algoritmo de Codificação (Little, Saints e Heegard)

Entrada: Base de Gröbner $\mathscr{G}$, $w = (w_1, ..., w_k) \in \mathbb{F}_q^k$ e $\{m_1, ..., m_k\}$

Saída: $E(w) \in C_{\mathscr{L}}(D, G)$

Início: Seja $f = \sum_{i=1}^{k} w_i m_i$

Defina $E(w) = VC(f - R)$

Com $f = a_1 g_1 + ... + a_s g_s + R$, onde $a_1, ..., a_s \in \mathbb{F}_q[t]$, $g_1, ..., g_s$ são os elementos de $\mathscr{G}$ e R é o resto.

Assim $f - R$ esta associado a uma palavra código de C e pela construção da f, temos uma bijeção entre $f - R$ e uma palavra de C. Para maiores detalhes ver [10].

Para encontrar $a_1, ..., a_s$ e R utilizaremos um algoritmo semelhante ao algoritmo da divisão.

ALGORITMO (6.1)

Inicio $d = f; R = 0; j = 1$

Para $i = 1$ até r, faça

Se $tl(g_j)$ contém e_i, **então**

$a_i = Quoc(d_i, g_{j_i})$

$R_i = Res(d_i, g_{j_i})$

$d = d - a_i g_j - R_i e_i$

$R = R + R_i e_{i+1}$

$j = j + 1$

Caso contrário

$a_i = 0$

$R = R + d_i e_i$

$d = d - d_i e_i$

Onde $Quoc(d_i, g_{j_i})$ é o quociente da divisão de d_i por g_{j_i} e $Res(d_i, g_{j_i})$ é o resto.

6.3 CODIFICAÇÃO DE CÓDIGOS HERMITIANOS

Nesta seção, vamos apresentar um exemplo de utilização dos algortimos vistos na seção anterior utilizando o corpo de funções Hermitiano. Para isso, enunciamos a seguir as principais propriedades de tal corpo de funções. Mais sobre o assunto pode ser encontrado nos exemplos 6.3.6 e 6.4.3 e no Lema 6.4.4 da referência [11].

Definição 6.2. O corpo de funções $H = \mathbb{F}_{q^2}(x, y)$ definido como

$$H = \mathbb{F}_{q^2}(x, y), \text{ onde } x^{q+1} = y^q + y$$

é chamado corpo de funções Hermitiano $H/\mathbb{F}_{q^2}$ sobre $\mathbb{F}_{q^2}$.

Lema 6.2. O corpo de funções Hermitiano possui as seguintes propriedades:

a) O gênero de $H/\mathbb{F}_{q^2}$ é $g = \frac{q(q-1)}{2}$.

b) H possui $q^3 + 1$ lugares de grau um sobre $\mathbb{F}_{q^2}$, a saber:

   a) P_∞ o polo comum de x e y;

   b) outros q^3 lugares de grau um: para cada par $(\alpha, \beta) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ tal que $\beta^q + \beta = \alpha^{q+1}$ existe único lugar $P_{\alpha,\beta}$ de grau um tal que $x(P_{\alpha,\beta}) = \alpha$ e $y(P_{\alpha,\beta}) = \beta$.

Exemplo 6.1. Vamos estudar o corpo de funções Hermitiano, onde $x^4 = y^3 + y$ em $\mathbb{F}_9 \setminus \{0\} = \{1, \alpha, \alpha^2, ..., \alpha^7\}$.

Pelo lema 6.2 esse corpo de funções possui gênero $g = 3$ e pelo teorema 5.1 e de Riemann Roch temos $k = \deg(19P_\infty) - g + 1 = 19 - 3 + 1 = 17$

Temos que α é um gerador de $\mathbb{F}_9^*$, isto é, uma raiz não trivial de $x^9 - x$. Note que

$$x^9 - x = x(x^8 - 1) = x(x^2 - 1)(x^2 + 1)(x^4 + 1) = x(x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$$

O corpo $\mathbb{F}_9$ possui quatro elementos com ordem igual a 8, isto é, quatro elementos primitivos sendo eles as raízes de $x^4 + 1$. Considerando α uma dessas raízes, temos que $\alpha^3, \alpha^5, \alpha^7$ são os demais elementos primitivos do corpo. É útil ver ainda que

$$x^4 + 1 = (x^2 + x - 1)(x^2 - x - 1) \text{ sobre } \mathbb{F}_3$$

Isso é interessante no caso Hermitiano, pois temos uma função do tipo $N(x) = Tr(y)$, onde $N(x) = x^4$ é a norma de $\mathbb{F}_9$ em $\mathbb{F}_3$ e $Tr(y) = y^3 + y$ é o traço de $\mathbb{F}_9$ sobre $\mathbb{F}_3$. Os lugares de grau um do corpo Hermitiano são correspondentes aos pares $(x, y) \in \mathbb{F}_9^2$ que satisfaz a equação $x^4 = y^3 + y$, isto é, os lugares de $(x, y) \in \mathbb{F}_9$ tais que $N(x) = Tr(y)$. Pelo lema 6.2 temos $3^3 + 1 = 28$ lugares de grau um, sendo que um deles é o P_∞. Assim, vamos calcular a norma e o traço dos elementos de $\mathbb{F}_9$. Claro que $Tr(0) = N(0) = 0$. Ainda, $Tr(1) = 1$ e $N(1) = -1$. Os demais estão na tabela a seguir:

i	α^i	$N(\alpha^i) = \alpha^{4i}$	α^{3i}	$Tr(\alpha^i) = \alpha^{3i} + \alpha^i$
1	α	$\alpha^4 = -1$	α^3	$\alpha^3 + \alpha$
2	α_2	$\alpha^8 = 1$	$\alpha^6 = -\alpha^2$	$-\alpha^2 + \alpha^2 = 0$
3	α^3	$\alpha^{12} = -1$	$\alpha^9 = \alpha$	$\alpha^3 + \alpha$
4	α^4	$\alpha^{16} = 1$	$\alpha^{12} = -1$	$\alpha^4 - 1 = -2 = 1$
5	$\alpha^5 = -\alpha$	$\alpha^{20} = -1$	$\alpha^{15} = -\alpha^3$	$-\alpha^3 - \alpha = -(\alpha^3 + \alpha)$
6	$\alpha^6 = -\alpha^2$	$\alpha^{24} = 1$	$\alpha^{18} = \alpha^2$	$\alpha^2 - \alpha^2 = 0$
7	$\alpha^7 = -\alpha^3$	$\alpha^{28} = -1$	$\alpha^{21} = -\alpha$	$-\alpha^3 - \alpha = -(\alpha^3 + \alpha)$

Assim, para ter certeza dos lugares de grau um diferentes de P_∞, falta saber $\alpha^3 + \alpha$. Como $\alpha^2 + \alpha - 1 = 0$, temos que $\alpha^3 = -\alpha^2 + \alpha$, assim $\alpha^3 + \alpha = -\alpha^2 - \alpha = -1$. Logo,

$$Tr(\alpha) = Tr(\alpha^3) = -1 = Tr(1)$$

$$Tr(\alpha^4) = Tr(\alpha^5) = Tr(\alpha^7) = 1.$$

Juntando isso, obtemos os 27 lugares de grau um diferentes de P_∞ do corpo de funções Hermitiano sobre $\mathbb{F}_9$:

$$(1,\alpha^4),(1,\alpha^5),(1,\alpha^7),(\alpha,1),(\alpha,\alpha),(\alpha,\alpha^3),(\alpha^2,\alpha^4),(\alpha^2,\alpha^5),(\alpha^2,\alpha^7),(\alpha^3,1),(\alpha^3,\alpha),$$

$$(\alpha^3,\alpha^3),(\alpha^4,\alpha^4),(\alpha^4,\alpha^5),(\alpha^4,\alpha^7),(\alpha^5,1),(\alpha^5,\alpha),(\alpha^5,\alpha^3),(\alpha^6,\alpha^4),(\alpha^6,\alpha^5),(\alpha^6,\alpha^7),$$

$$(\alpha^7,1),(\alpha^7,\alpha),(\alpha^7,\alpha^3),(0,0),(0,\alpha^2),(0,\alpha^6)$$

onde cada par (α,β) representa o lugar $P_{\alpha,\beta}$.

Definição 6.3. Seja $r \in \mathbb{Z}$, $C_r = C_{\mathscr{L}}(D, rP_\infty)$, onde $D = \sum_{i=1}^{q^3} P_i$ a soma de todos os lugares de $H/\mathbb{F}_{q^2}$ com grau um, exceto P_∞, C_r é chamado de código Hermitiano.

Observemos que os códigos Hermitianos tem comprimento q^3 sobre $\mathbb{F}_{q^2}$ e que se $r < 0$, então $\mathscr{L}(rQ_\infty) = 0$ e, então $C_r = 0$. Para o caso $r > q^3 + q^2 - q - 2 = q^3 + 2g - 2$, temos pelo teorema 5.1 e pelo teorema de Riemann-Roch que

$$\begin{aligned}\dim C_r &= \ell(rQ_\infty) - \ell(rQ_\infty - D)\\ &= (r + 1 - g) - (r - q^3 + 1 - g)\\ &= q^3\\ &= n\end{aligned}$$

Consequentemente $C_r = \mathbb{F}_{q^2}^n$. Os casos em que $0 \leq r \leq q^3 + 2q - 2$ também são conhecidos (ver [11] seção 8.3).

Exemplo 6.2. Seja $C_{19} = C_{\mathscr{L}}(D, 19P_\infty)$ um código sobre o corpo de funções Hermitiano, onde $x^4 = y^3 + y$ em $\mathbb{F}_9 \setminus \{0\} = \{1, \alpha, \alpha^2, ..., \alpha^7\}$ com automorfismo σ dado por $\sigma(x) = \alpha x$ e $\sigma(y) = \alpha^4 y$. No exemplo 6.1, calculamos os 27 lugares racionais diferentes de P_∞ de tal corpo de funções, assim, usando o Lema 6.1 temos:

$\sigma((1, \alpha^4)) = (\alpha, \alpha^8) = (\alpha, 1)$,
$\sigma((1, \alpha^5)) = (\alpha, \alpha^9) = (\alpha, \alpha)$,
$\sigma((1, \alpha^7)) = (\alpha, \alpha^{11}) = (\alpha, \alpha^3)$,
$\sigma((\alpha, 1)) = (\alpha^2, \alpha^4)$,
$\sigma((\alpha, \alpha)) = (\alpha^2, \alpha^5)$,
$\sigma((\alpha, \alpha^3)) = (\alpha^2, \alpha^7)$,
$\sigma((\alpha^2, \alpha^4)) = (\alpha^3, \alpha^8) = (\alpha^3, 1)$,
$\sigma((\alpha^2, \alpha^5)) = (\alpha^3, \alpha)$,
$\sigma((\alpha^2, \alpha^7)) = (\alpha^2, \alpha^{11}) = (\alpha^3, \alpha^3)$,
$\sigma((\alpha^3, 1)) = (\alpha^4, \alpha^4)$,
$\sigma((\alpha^3, \alpha)) = (\alpha^4, \alpha^5)$,
$\sigma((\alpha^3, \alpha^3)) = (\alpha^4, \alpha^7)$,
$\sigma((\alpha^4, \alpha^4)) = (\alpha^5, \alpha^8) = (\alpha^5, 1)$,
$\sigma((\alpha^4, \alpha^5)) = (\alpha^5, \alpha^9) = (\alpha^5, \alpha)$,
$\sigma((\alpha^4, \alpha^7)) = (\alpha^5, \alpha^{11}) = (\alpha^5, \alpha^3)$,
$\sigma((\alpha^5, 1)) = (\alpha^6, \alpha^4)$,
$\sigma((\alpha^5, \alpha)) = (\alpha^6, \alpha^5)$,
$\sigma((\alpha^5, \alpha^3)) = (\alpha^6, \alpha^7)$,
$\sigma((\alpha^6, \alpha^4)) = (\alpha^7, \alpha^8) = (\alpha^7, 1)$,
$\sigma((\alpha^6, \alpha^5)) = (\alpha^7, \alpha^9) = (\alpha^7, \alpha)$,
$\sigma((\alpha^6, \alpha^7)) = (\alpha^7, \alpha^{11}) = (\alpha^7, \alpha^3)$,
$\sigma((\alpha^7, 1)) = (\alpha^8, \alpha^4) = (1, \alpha^4)$,
$\sigma((\alpha^7, \alpha)) = (\alpha^8, \alpha^5) = (1, \alpha^5)$,
$\sigma((\alpha^7, \alpha^3)) = (\alpha^8, \alpha^7) = (1, \alpha^7)$,
$\sigma((0, 0)) = (0, 0)$,
$\sigma((0, \alpha^2)) = (0, \alpha^6)$,
$\sigma((0, \alpha^6)) = (0, \alpha^{10}) = (0, \alpha^2)$.

Assim temos as seguintes 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
$O_5 = ((0, 0))$

A partir dessas decomposições podemos representar as palavras de C como quíntuplas de polinômios em uma variável da forma

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

Como 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 $\mathscr{L}(19P_\infty)$. Utilizando a ordem POT e o algoritmo de Buchberger (teorema 2.5) conseguimos a base de Gröbner $\mathscr{G} = \{g_1, g_2, g_3, g_4, g_5\}$, garantida pela proposição 2.4,

para o submódulo E de $\mathbb{F}_9[t]^5$, onde

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

Assim obtemos as seguintes posições de informação:
$m_1 = t^7 e_1, ..., m_7 = te_1, m_8 = e_1$
$m_9 = t^7 e_2, ..., m_{15} = te_2$
$m_{16} = t^7 e_3, m_{17} = t^6 e_3.$
Agora vamos codificar

$$w = (0, 0, 0, 0, 0, 0, \alpha^3, 0, 0, 0, 0, 0, 0, 0, \alpha^2, \alpha, 0) \in \mathbb{F}_9^{17}$$

Definindo

$$\begin{aligned}
f &= \sum_{i=1}^{17} w_i m_i\\
&= \alpha^3 te_1 + \alpha^2 te_2 + \alpha t^7 e_3\\
&= (\alpha^3 t, \alpha^2 t, \alpha t^7, 0, 0) \in \mathbb{F}_9[t]^5.
\end{aligned}$$

A partir do algoritmo 6.1 vamos calcular o resto da divisão de f por $\mathscr{G}$. Pelo algoritmo temos $d_1 = f_1$ e

$$d_i = f_i - \sum_{k=1}^{i-1} a_k g_{k_i} - R_k \text{ para } i \geq 2$$

Já que

$$f - \alpha^3 t g_1 = (0, \alpha^2 t - \alpha^9 t, \alpha t^7 - \alpha^4 t^6 - \alpha^4 t^5 - \alpha^9 t^4 - \alpha^5 t^3 - \alpha^4 t^2 - \alpha^5 t, -\alpha^5 t^2 - \alpha^4 t, 0)$$

e $\alpha^9 = \alpha$ e $\alpha^2 - \alpha = 1$, então

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

Assim, dividindo $d_1 = \alpha^3 t$ por $g_{1_1} = 1$, temos o quociente $\alpha^3 t$ e resto

$$R_1 = 0.$$

Dividindo $d_2 = t$ por g_{2_2}, temos o quociente 1 e resto

$$R_2 = -\alpha^5.$$

Dividindo $d_3 = \alpha t^7 - \alpha^4 t^6 - (\alpha^4+1)t^5 - (\alpha^5+\alpha)t^4 - (\alpha^7+\alpha^5)t^3 - \alpha^4 t^2 - (\alpha^7+\alpha^5)t - \alpha^7 + \alpha^5 = \alpha t^7 - \alpha^4 t^6 + \alpha^4 t^3 - \alpha^4 t^2 + \alpha^4 t - \alpha^2$ por g_{3_3} temos quociente $\alpha t - \alpha$

$$R_3 = -2\alpha^3 t^5 + \alpha^2 t^4 + \alpha t^3 - \alpha t^2 + \alpha^2$$

Dividindo $d_4 = 2\alpha^3 t^5 - \alpha^2 t^4 + \alpha t^3 + \alpha t^2 - \alpha^2$ por g_{4_4} temos quociente $2\alpha^3 t^3 - 2\alpha^2 t^2 + \alpha^2 t - 3\alpha^2$ e

$$R_4 = -\alpha$$

E finalmente dividindo $d_5 = 2\alpha^3 t^5 - \alpha^2 t^4 + \alpha t^3 + \alpha t^2 - t - \alpha^2$ por g_{5_5}, temos quociente $2\alpha^3 t^4 + \alpha^5 t^3 + \alpha t^2 + 2\alpha t + \alpha^3$ e resto

$$R_5 = \alpha^4$$

Assim,

$$R = (R_1, R_2, R_3, R_4, R_5) = (0, -\alpha^5, -2\alpha^3 t^5 + \alpha^2 t^4 + \alpha t^3 - \alpha t^2 + \alpha^2, -\alpha, \alpha^4)$$

Portanto,

$$f - R = (\alpha^3 t, \alpha^2 t + \alpha^5, \alpha t^7 + 2\alpha^3 t^5 - \alpha^2 t^4 - \alpha t^3 + \alpha t^2 - \alpha^2, \alpha, -\alpha^4) \in E$$

logo,
$VC(f-R) = (0,0,0,0,0,0,\alpha^3,0,0,0,0,0,0,0,\alpha^2,\alpha^5,\alpha,0,2\alpha^3,-\alpha^2,-\alpha,\alpha,0,-\alpha^2,0,\alpha,-\alpha^4)$.

REFERÊNCIAS

[1] Adans, W. e Loustaunau, P., *An introduction to Gröbner Bases*, American Mathematical Society, 1939.

[2] Becker, T. e Weispfenning, V., Gröbner Bases - *A computational approach to commutative algebra, Berlin, Germany:* Springer Verlag, 1998, 2nd. pr.

[3] Carvalho, C., Gröbner bases methods in coding theory, Publications of CIMPA, Mexico 2012.

[4] Coutinho, S. C., *Polinômios e Computação Algébrica.* Rio de janeiro, IMPA, 2012.

[5] Cox, D., Little, J. e O'Shea, D. *Ideals, varieties and algorithms.* Springer, New York, 1992.

[6] Fulton, W., *Algebraic curves - An Introducton to Algebraic Geometry.* Mathematics Lecture Note Series. Benjamin/Cummings Publishing Company, 1969.

[7] Hefez A. e Vilela M. L. T., *Códigos Corretores de Erros.* 2ª Edição, Rio de janeiro, IMPA, 2008.

[8] Hernandes, M. E., *Um primeiro contato com base de Gröbner.* Publicações matemáticas, IMPA, 2011.

[9] Fitzgerald, J., e Lax, R.F.,*Decoding Affine Variety Codes Using Gröbner Bases.* Des. Codes and Cryptogr., vol. 13, pp. 157-158, 1998

[10] Little, J. Heergard, C. e Saints, K., *Systematic encoding via Gröbner bases for class of algebraic geometric Goppa codes,* IEEE Trans. Infor. Theory 41(6) (1995), 1752-1761.

[11] Stichtenoth, H., *Algebraic Function Fields and Codes. 2 ed.* New York: Springer-Verlag, 2009.

[12] 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.