Universidade Federal de Pernambuco
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Programa de Pós-Graduação em Matemática

Federico Fornasiero

O diagrama de raízes de certos códigos AG

Recife
2018

Federico Fornasiero

O diagrama de raízes de certos códigos AG

Este trabalho foi apresentado á Pós-Graduação em Matemática do Centro de Ciências Exatas e da Natureza da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Doutor em Matemática.

ORIENTADOR: **Miguel Fidencio Loayza Lozano**
COORIENTADOR: **Fernando Eduardo Torres Orihuela**

Recife

2018

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

F727d Fornasiero, Federico
O diagrama de raízes de certos códigos AG / Federico Fornasiero. – 2018.
79 f.

Orientador: Miguel Fidencio Loyaza Lozano.
Tese (Doutorado) – Universidade Federal de Pernambuco. CCEN, Matemática, Recife, 2018.
Inclui referências e apêndice.

1. Matemática. 2. Diagrama de raízes. I. Lozano, Miguel Fidencio Loyaza (orientador). II. Título.

510 CDD (23. ed.) UFPE- MEI 2018-098

FEDERICO FORNASIERO

O DIAGRAMA DE RAÍZES DE CERTOS CÓDIGOS AG

Tese apresentada ao Programa de Pós-graduação do Departamento de Matemática da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Doutorado em Matemática.

Aprovado em: 09/05/2018

BANCA EXAMINADORA

Prof. Dr. Eduardo Shirlippe Góes Leandro (Examinador Interno)
Universidade Federal de Pernambuco

Prof. Dr. Fernado Antônio Nóbrega Santos (Examinador Interno)
Universidade Federal de Pernambuco

Prof. Dr. Fernando Eduardo Torres Orihuela (Examinador Externo)
Universidade Estadual de Campinas

Prof.Dr. Guilherme Chaud Tizziotti (Examinador Externo)
Universidade Federal de Uberlândia

Prof. Dr. Jorge Nicolas Caro Montoya (Examinador Externo)
Universidade Federal de Pernambuco

RESUMO

Os códigos algébricos geométricos (abreviando, códigos AG) foram estudados pela primeira vez por Goppa, em [9] e em [10]. A importância dos códigos AG surgiu posteriormente. De fato, Tsfasman, Vladuts e Zink, em [21], encontraram uma família de códigos AG cujos parâmetros limites ultrapassavam o limite de Gilbert-Varshamov, que era alcançado com códigos casuais. Alguns anos depois, Garcia e Stichtenoth melhoraram as construções envolvidas, em [7]. Heegard, Little e Saints introduziram, em [13], um algoritmo de codificação para uma classe de códigos AG por meio de bases de Gröbner. Tal algoritmo é mais compacto comparado ao algoritmo de codificação usual via matriz geradora. Sabendo da complexidade de se encontrar uma base de Gröbner, Heegard, Little e Saints, em [14], introduziram o conceito de diagrama de raízes, o qual permite a construção de um algoritmo que constrói uma base de Gröbner para códigos pontuais sobre a curva Hermitiana, com uma complexidade menor do que o algoritmo de Buchberger. Portanto, esta tese tem o objetivo de construir o diagrama de raízes sobre os códigos algébricos geométricos pontuais, definidos sobre os modelos planos da curva de Kondo e de alguns quocientes da curva Hermitiana.

Palavras-chave: Códigos AG. Diagrama de raízes. Codificação. Bases de Gröbner.

ABSTRACT

Algebraic geometric codes (for short, AG-codes) were studied for the first time for Goppa, in [9] and in [10]. The importance of such codes arose later. In fact, Tsfasman, Vladuts and Zink, in [21], have found a family of AG-codes whose limit parameters beat the Gilbert-Varshamov bound, that was reached with casual codes. Several years later, Garcia and Stichtenoth improved the main constructions, in [7]. Heegard, Little and Saints itroduced, in [13], an encode algorithm for a class of AG-codes using the tools of Gröbner basis. This algorithm is more compact compared with the usual algorithm via generator matrix. Due to the complexity to find a Gröbner basis, Heegard, Little e Saints, in [14], introduced the concept of root diagram, that permit the construction of an algorithm that find a Gröbner basis for one-point codes over the Hermitian curve, with a lower complexity that the Buchberger's algorithm. So, the main purpose of this thesis is to construct the root diagram of one-point AG codes arising from the Kondo curve and from certain quotients of the Hermitian curve.

Keywords: AG codes. Root diagram. Encoding. Gröbner bases.

SUMÁRIO

1 INTRODUÇÃO

Os códigos algébricos geométricos (abreviando, códigos AG) foram estudados pela primeira vez por Goppa, em [9] e em [10]. A importância dos códigos AG surgiu posteriormente. De fato, Tsfasman, Vladuts e Zink, em [21], encontraram uma família de códigos AG cujos parâmetros limites ultrapassavam o limite de Gilbert-Varshamov, que era alcançado com códigos casuais. Alguns anos depois, Garcia e Stichtenoth melhoraram as construções envolvidas, em [7].

Heegard, Little e Saints introduziram, em [13], um algoritmo de codificação para uma classe de códigos AG por meio de bases de Gröbner. Tal algoritmo é mais compacto comparado ao algoritmo de codificação usual via matriz geradora.

Buchberger, em [1], introduziu pela primeira vez o conceito de base de Gröbner e um algoritmo para achá-la, que pode ser considerado como uma generalização do algoritmo de Euclides para a computação do máximo divisor comum e da eliminação de Gauss para sistemas de equações lineares. A complexidade do algoritmo de Buchberger é difícil de estimar, devido ao número de escolhas que podem mudar o tempo de computação. Mesmo assim, Dubé, em [4], mostrou que o grau máximo dos elementos de uma base de Gröbner reduzida é:

$$K = 2\left(\frac{d^2}{2} + d\right)^{2^{n-1}},$$

onde n é o número de indeterminadas e d é o grau máximo dos polinômios geradores do ideal. Isso permite a utilização das técnicas da álgebra linear, sobre o espaço vetorial dos polinômios de grau máximo K, para obter um algoritmo de complexidade $d^{2^{n+o(1)}}$. Sabendo da complexidade de se encontrar uma base de Gröbner, Heegard, Little e Saints,

em [14], introduziram o conceito de diagrama de raízes, o qual permite a construção de um algoritmo que constrói uma base de Gröbner para códigos pontuais sobre a curva Hermitiana, com uma complexidade menor do que o algoritmo de Buchberger. Esse algoritmo utiliza somente ferramentas de problemas de interpolação e de evaluação de funções, ou seja, não utiliza divisões nem reduções de polinômios como no algoritmo de Buchberger que, de fato, são as operações que aumentam a complexidade do algoritmo.
Em [5], Farran, Munuera, Tizziotti e Torres estenderam os resultados do artigo [14] para códigos sobre a curva norma-traço.

Seja $A = \{a_1, \ldots, a_q\}$ o *alfabeto*, ou seja, um conjunto finito de símbolos. Uma *palavra* é uma sequência finita de símbolos do alfabeto A, e um *código q-ário* é um conjunto finito de palavras sobre um alfabeto de q elementos.
Seja $\mathbb{F}_q$ o corpo finito de q elementos. Um *código linear* q-ário de *comprimento* n é um subespaço vetorial de $\mathbb{F}_q^n$.
Seja C um código linear. A *dimensão* de C, denotada por $k(C)$ ou simplesmente por k, é a dimensão de C como subespaço vetorial.
Se $x, y \in A^n$, a *distância de Hamming* é o número de coordenadas em que as duas palavras diferem, ou seja:

$$d(x, y) := \#\{i \mid x_i \neq y_i\}.$$

Seja C um código com pelo menos duas palavras. Define-se a *distância mínima* de C por:

$$d(C) := min\{d(x, y) \mid x, y, \in C, \;\; x \neq y\}.$$

Seja γ uma curva algébrica não singular, projetiva, geometricamente irredutível, de gênero $g \geq 1$ sobre o corpo finito $\mathbb{F}_q$ com q elementos, $\mathbb{F}_q(\gamma)$ o corpo das funções racionais em γ e $\mathbb{F}_q(\gamma)^*$. Dado um divisor G em γ, considere o espaço vetorial

$$L(G) = \{f \in \mathbb{F}(\gamma)^* \mid (f) + G \geq 0\} \cup \{0\}.$$

Para distintos pontos racionais $P_1, \cdots, P_n$ em γ com $P_i \in supp(G)$ para todo i, considere a aplicação:

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

Sejam $D = \sum_{i=1}^{n} P_i$ e $G = \sum_{i=1}^{l} a_i Q_i$ divisores em γ tais que $supp(G) \cap supp(D) = \emptyset$. Definimos o código de Goppa algébrico geométrico $C_L(D, G)$ por

$$C_L(D, G) := ev_L(L(G)).$$

Tal código também é chamado de código AG. Se $G = aQ$ para algum ponto racional $Q \in \gamma$, o código $C_L(D, G)$ é chamado de código AG pontual.

O algoritmo de codificação, assim como o algoritmo de decodificação, são ferramentas muito importantes na teoria de códigos, pois permitem transformar as palavras em palavras cifradas, ou vice-versa. O objetivo desta tese é, portanto, construir o diagrama de raízes sobre códigos pontuais construídos sobre a curva estudada por Kondo et al., em [11], e sobre alguns quocientes da curva Hermitiana estudados por Matthews, em [17], para que se possa achar uma base de Gröbner associada ao módulo C', com uma complexidade computacional inferior àquela do algoritmo de Buchberger e, como consequência, se possam codificar de uma forma algorítmica as palavras do código.
As curvas escolhidas para este trabalho são importantes já que são *maximais*, ou seja, atingem o limite de Hasse-Weil ([23], p.502). Em outras palavras, as curvas algébricas atingem o limite máximo de pontos racionais e, portanto, os códigos construídos a partir destas curvas tem dimensão maior.

A estrutura da tese é a seguinte.
O Capítulo 1 introduz o estudo de curvas algébricas (não necessariamente sobre um corpo finito) de uma forma moderna, mais detalhadamente depois de algumas Seções introdutórias sobre as curvas algébricas e o corpo de funções de uma curva, definem-se os conceitos de divisores e de valorizações e conclui-se com o Teorema de Riemann-Roch (2.3.4).
Nas Seções 1.4, 1.5, 1.6, 1.7 e 1.8 apresenta-se, de uma forma detalhada, as motivações deste trabalho, analizando em detalhes o artigo [13].
A Seção 1.9 define o objeto de estudo deste trabalho e analiza a Seção 6, p.311, do artigo [14].
Os últimos dois Capítulos da tese apresentam o meu trabalho. Todos os resultados apresentados são originais e, em particular, no Capítulo 3 se constrói o diagrama de

raízes para códigos pontuais construídos sobre o modelo plano $y^q + y = x^{q^r+1}$, com r ímpar, da curva de Kondo sobre o corpo $\mathbb{F}_{q^{2r}}$, e os resultados principais são os Teoremas de construção do diagrama de raízes, ou seja (3.0.5) e (3.0.6). Como conclusão do Capítulo, o Teorema (3.0.8) permite construir o algoritmo que permite achar a base de Gröbner do módulo C' associada ao código.

Analogamente, o Capítulo 4 mostra como se pode construir um diagrama de raízes sobre os códigos pontuais construídos sobre alguns quocientes da curva Hermitiana, com modelo plano definido pela equação $y^q + y = x^m$ com $m|q-1$ sobre o corpo $\mathbb{F}_{q^2}$. Os teoremas que permitem a construção do diagrama de raízes são os Teoremas (4.0.2) e (4.0.3) e, como antes, o Capítulo conclui-se com o Teorema (4.0.5), cuja consequência é o algoritmo que permite encontrar a base de Gröbner do módulo C' associada ao código.

As duas curvas podem ser consideradas uma extensão da curva Hermitiana $y^q + y = y^{q+1}$ sobre o corpo $\mathbb{F}_{q^2}$ pois, respectivamente, para $r = 1$ e $m = q + 1$ as equações coincidem.

Finalmente, nas conclusões, são explicados com mais detalhes os resultados obtidos e a importância de tais resultados, assim como alguns possíveis desenvolvimentos da pesquisa desta tese.

2 PRELIMINARES

As curvas algébricas formam um conjunto de objetos muito estudado na matemática. Nesta breve introdução mostra-se um modo moderno de trabalhar sobre elas, além de ver algumas propriedades que são utilizadas ao longo do trabalho.

Notação: quando escrevemos K entendemos um corpo algebricamente fechado, e, especificamente, o fecho algébrico de um corpo finito $\mathbb{F}_q$ com q elementos. De forma semelhante, quando falamos de curva algébrica definida sobre K, estamos falando de uma classe de proporcionalidade de polinômios homogêneos em 3 indeterminadas (ou 2 indeterminadas, se estamos trabalhando no caso projetivo ou no caso afim, respectivamente, e no segundo caso não é necessário que o polinômio seja homogêneo) com coeficientes em K, e para indicar que a curva γ é representada com um polinômio $F(X_0, X_1, X_2)$ escrevemos simplesmente:

$$\gamma : F(X_0, X_1, X_2) = 0.$$

A ideia intuitiva de considerar uma curva algébrica como conjunto (finito, no nosso caso) de pontos é evidente quando definimos formalmente o suporte de uma curva.

Definição 2.0.1. Seja γ uma curva algébrica definida sobre K.
O suporte de γ se define como o conjunto dos pontos do plano projetivo $\mathbb{P}^2(K)$ cujas coordenadas homogêneas $(X_0 : X_1 : X_2)$ satisfazem a seguinte equação:

$$F(X_0, X_1, X_2) = 0.$$

Vale ressaltar que duas curvas algébricas distintas podem ter o mesmo suporte, como no caso das seguintes curvas:

$$\gamma_1 : X_0 = 0, \quad \gamma_2 : X_0^2 = 0.$$

É fácil mostrar que estamos pedindo que o polinômio seja homogêneo, porque as coordenadas são definidas a menos de proporcionalidade, ou seja, para garantir que:

$$F(X_0, X_1, X_2) = 0 \Leftrightarrow F(aX_0, aX_1, aX_2) = 0.$$

Quando isso não gera confusão, consideramos equivalente a defínção de suporte e de curva.

Exemplo 2.0.2. Consideremos a curva $\gamma : X_0^2 + 2X_1^2 = 0$ sobre o corpo $\mathbb{F}_5$. Se considerássemos somente os pontos de $\mathbb{F}_5$ a curva γ teria apenas o ponto $(0 : 1 : 0)$. Entretanto, no fecho algébrico de $\mathbb{F}_5$ existe também um elemento tal que $a^2 = -2$, e então neste corpo temos também, por exemplo, o ponto $(a : 1 : 0)$.

Definição 2.0.3. Seja $\gamma : F(X_0, X_1, X_2) = 0$ uma curva algébrica.

- O grau d do polinômio F chama-se *ordem* da curva γ;
- γ é *irredutível* se F é irredutível sobre $K[X_0, X_1, X_2]$.

Suponhamos que γ não seja irredutível. Já que $K[X_0, X_1, X_2]$ é um domínio fatorial, podemos escrever F como produto de fatores irredutíveis (cada um com um exponente inteiro positivo):

$$F = F_1^{r_1} \cdots F_k^{r_k}.$$

Falamos que as curvas $\gamma_i : F_i(X_0, X_1, X_2) = 0$ são as componentes irredutíveis de γ e que r_i é a multiplicidade de γ_i como componente de γ.

É claro que o conjunto dos pontos de γ coincide com a união dos conjuntos dos pontos das curvas γ_i.

Seja l_∞ a reta de $\mathbb{P}^2(K)$ de equação $X_0 = 0$. Os pontos do tipo $(0, X_1, X_2)$ são ditos *pontos no infinito*.

Para cada ponto $P \in \mathbb{P}^2(K)$ que não está na reta l_∞ com coordenadas homogêneas (X_0, X_1, X_2) substituímos:

$$x = \frac{X_1}{X_0} \quad y = \frac{X_2}{X_0}.$$

O par (x, y) é dito *par das coordenadas afins* de P.

Escrever $P = (x, y)$ significa que P é o ponto de coordenadas homogêneas $(1 : x : y)$ e os

pontos $P \in \mathbb{P}^2(K)$, que não estão na reta l_∞, são ditos *pontos afins* da curva.
O polinômio $f(x, y) := F(1, x, y)$ se chama *polinômio desomogeneizado de* F e a equação $f(x, y) = 0$ se chama *equação afim* de γ.
Pode-se também trabalhar em uma curva afim γ e depois passar ao caso projetivo.
Neste caso, se $f(x, y)$ é um polinômio não homogêneo de grau positivo d, o polinômio homogeneizado se define como:

$$F(X_0, X_1, X_2) := X_0^d \cdot f\left(\frac{X_1}{X_0}, \frac{X_2}{X_0}\right),$$

e pode-se demonstrar que:

Teorema 2.0.4. *([6], Seção 2.6, Proposição 5, p.24)*
A aplicação de homogeneização estabelece uma bijeção entre os polinômios de $K[x, y]$, de grau d, e os polinômios homogêneos de $K[X_0, X_1, X_2]$, de grau d, que não são divididos por uma potência de X_0.

Concluímos a Seção com uma última definição:

Definição 2.0.5. Seja F uma curva algébrica projetiva e P um ponto da curva. O ponto P é dito *singular* se as derivadas parciais $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$, $\frac{\partial F}{\partial Z}$ se anulam simultaneamente.

2.1 O corpo das funções racionais

Desde agora vamos supor que a curva γ seja não singular, ou seja, que não tenha pontos singulares, ou seja, os pontos com multiplicidade maior que 1.
Esta hipótese permite introduzir os objetos do estudo de uma forma mais simples.
Seja então $\gamma : f(x, y) = 0$ uma curva afim com f irredutível e coeficientes em K. Denotamos com (f) o ideal principal de $K[x, y]$ gerado pelo f.
Um ponto P *K-racional* de uma curva $\gamma : f(x, y) = 0$(ou simplesmente racional, se não há necessidade de enfatizar qual seja o corpo K) é um ponto (X, Y) que satisfaz $f(X, Y) = 0$ com $X, Y \in K$.

Definição 2.1.1. O *anel das coordenadas afins* de γ é definido como o anel quociente:

$$K[\gamma]_= K[x, y]/(f).$$

Nota-se que, sendo (f) um ideal primo, $K[\gamma]$ é um domínio, e então podemos construir o corpo das frações dele.

Definição 2.1.2. O *corpo das funções racionais* $K(\gamma)$ é o corpo das frações de $K[\gamma]$.

Uma descrição explicita de $K(\gamma)$ é:

$$K(\gamma) = \left\{ \frac{g+(f)}{h+(f)} \mid g, h \in K[x,y],\ h \notin (f) \right\},$$

onde $\frac{g_1+(f)}{h_1+(f)} = \frac{g_2+(f)}{h_2+(f)}$ se $f | g_1h_2 - g_2h_1$.

Uma função racional não será definida em determinado ponto de uma curva γ, se o seu denominador for nulo naquele ponto específico. Portanto, se dado $P = (p_1, p_2) \in \gamma$ existem $g, h \in K[x,y]$ com $h(P) \neq 0$ tais que uma função racional $\alpha = \frac{g+(f)}{h+(f)}$ a função α se diz *regular ou definida* em P e resulta bem definido $\alpha(P) = g(P)/h(P)$.

Exemplo 2.1.3. Notamos que na definição de função regular é suficiente que exista uma escolha de g, h que representem a função α que cumpra a propriedade, não precisa ser verdade para cada escolha de g, h.
Seja $f(x,y) = x + x^2 + y^2 + y^3$ e seja $P = (0,0)$.
Seja:

$$\alpha = \frac{x + x^2 + (f)}{y + (f)}.$$

A princípio, parece que a função não é regular em P, mas já que $x+x^2+(f) = -y^2-y^3+(f)$ podemos concluir que:

$$\alpha = \frac{-y^2 - y^3 + (f)}{y + (f)} = \frac{-y^2 - y + (f)}{1 + (f)},$$

ou seja, α é regular em P e $\alpha(P) = 0$.

Podemos fazer o mesmo no caso projetivo, ou seja, se $\Gamma : F(X_0, X_1, X_2) = 0$ é uma curva algébrica (irredutível, por hipótese) o corpo das frações $K(\Gamma)$ é o corpo obtido homogeneizando os elementos de $K(\gamma)$, onde γ é a curva desomogeneizada de Γ. Enfim, podemos utilizar as duas representações, afim e homogênea, dependendo de quando for mais conveniente, mas notamos que:

- Na representação homogênea precisamos que os dois polinômios tenham os mesmos graus no numerador e no denominador, e por este motivo, às vezes pode ser difícil trabalhar com esta representação;

- Na representação homogênea, o conceito de função racional se extende também para os pontos ao infinito. Então, se precisamos trabalhar com aqueles pontos, temos que utilizar esta representação.

Terminamos a Seção definindo um objeto matemático que será utilizado nos Capítulos 2 e 3 da tese.

Definição 2.1.4. Para um ponto racional $P \in \gamma$ o *semigrupo de Weierstrass* de γ em P é:

$$H(P) := \{n \in \mathbb{N}_0 \mid \exists f \in \mathbb{F}_q(\gamma) \text{ com } div_\infty(f) = nP\}.$$

2.2 Valorizações

Seja $\gamma_f(x, y) = 0$ uma curva algébrica e $P(a_1, a_2)$ um ponto afim da curva.

Definição 2.2.1. O anel local $K[\gamma]_P$ de γ é o subanel de $K(\gamma)$ cujos elementos são as funções definidas em P.

Pode-se demonstrar que $K[\gamma]_P$ é um domínio, local e noetheriano, e que tem como ideal maximal o ideal M_P que é constituído das funções racionais que se anulam em P. Além disso, se P é um ponto simples temos que o ideal M_P é principal.

Definição 2.2.2. Seja P um ponto simples. Um *parâmetro local* de γ em P é um gerador de M_P.

Proposição 2.2.3. *([8], Proposição 1.33, p.14)*
Seja γ uma curva algébrica e t um parâmetro local de γ em P. Então, para cada $\alpha \in K[\gamma]_P$ não nula, existe um único $m \in \mathbb{Z}$, $m \geq 0$ e um único $u \in K[\gamma]_P$ inversível, tal que $\alpha = ut^m$.

No caso de um ponto simples vale o seguinte Corolário:

Corolário 2.2.4. *([8], Corolário 1.34, p.14)*
Seja γ uma curva algébrica e t um parâmetro local de γ em um ponto simples P. Então, para cada $\alpha \in K(\gamma)$ não nula, existe um único $m \in \mathbb{Z}$ e um único $u \in K[\gamma]_P$ inversível, tal que $\alpha = ut^m$.

Pode-se mostrar que o número m não depende da escolha do parâmetro local.

Definição 2.2.5. Seja P um ponto de uma curva algébrica γ não singular e $\alpha \in K(\gamma)$ não nula. Definimos a *ordem* de $\mathrm{ord}_P(\alpha)$ como o inteiro m do (2.2.4), e para $\alpha = 0$ definimos a $\mathrm{ord}_P(0) = \infty$

Observamos que:

$$K[\gamma]_P = \{\alpha \in K(\gamma) \mid \mathrm{ord}_P(\alpha) \geq 0\},$$

e que:

$$M_P = \{\alpha \in K(\gamma) \mid \mathrm{ord}_P(\alpha) > 0\}.$$

A ord_P das funções racionais tem as seguintes propriedades:

Proposição 2.2.6. *([19], Teorema 1.1.13, p.5) Seja γ uma curva algébrica não singular e P um ponto de γ. Então, $\forall \alpha, \beta \in K(\gamma)$ vale:*

- $\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_P(\alpha) + \mathrm{ord}_P(\beta)$;
- $\mathrm{ord}_P(\alpha^k) = k \cdot \mathrm{ord}_P(\alpha)$;
- $\mathrm{ord}_P(\alpha + \beta) \geq min\{\mathrm{ord}_P(\alpha), \mathrm{ord}_P(\beta)\}$;
- $\mathrm{ord}_P(a) = 0$ *para cada* $a \in K$.

Definição 2.2.7. Um ponto P de uma curva algébrica γ é dito *zero* de multiplicidade m para $\alpha \in K(\gamma)$ se $\mathrm{ord}_P(\alpha) = m > 0$, e é dito *polo* de multiplicidade $-m$ se $\mathrm{ord}_P(\alpha) = m < 0$.

Pode-se demonstrar o seguinte Teorema, que vou apresentar somente na versão afim. (Para mais detalhes, veja o Teorema 1 do Capítulo 3.2, do [6].)

Teorema 2.2.8. *Seja γ uma curva algébrica definida para um polinômio F, $P \in \gamma$ um ponto simples. Seja $l : ax + by + c = 0$ uma reta que passa por P que não seja a reta tangente a curva em P. Então:*

$$t = ax + by + c + (F)$$

é um parâmetro local de γ em P.

Exemplo 2.2.9. Seja $K = \mathbb{C}$ e seja $\gamma : x^2 + y^2 - 1 = 0$. Seja agora:

$$\alpha = \frac{x(x-1)^2 + (\gamma)}{(y-1)^2 + (\gamma)}.$$

O objetivo é calcular as ordens de α nos pontos $P_1 = (1, 0), \quad P_2 = (0, 1)$.

Para fazer as contas escrevemos $\alpha = xu^2$, onde:

$$u = \frac{x - 1 + (\gamma)}{y - 1 + (\gamma)}.$$

Nota-se que x é definida em P_1 e que é inversível, então a $ord_{P_1}(x) = 0$. Nota-se também que:

$$\frac{(x-1)(x+1) + (\gamma)}{(y+1)^2 + (\gamma)} = \frac{y^2 + (\gamma)}{(y-1)^2 + (\gamma)},$$

ou seja, podemos escrever $u = h_1 h_2$ onde:

$$h_1 = \frac{y + (\gamma)}{(y-1) + (\gamma)} \quad h_2 = \frac{y + (\gamma)}{x + 1 + (\gamma)}.$$

Para o Teorema (2.2.8) temos que h_1, h_2 são parâmetros locais (já que o ponto P_1 passa pela reta $y = 0$ e os denominadores são inversíveis).

Concluindo:

$$\mathrm{ord}_{P_1}(\alpha) = \mathrm{ord}_{P_1}(x) + 2\mathrm{ord}_{P_1}(h_1 h_2) = 0 + 2 + 2 = 4,$$

ou seja, P_1 é um zero de α com multiplicidade 4.

Com cálculos parecidos, podemos ver que $x + (\gamma)$ é um parâmetro local de α em P_2 e que $\mathrm{ord}_{P_2}(\alpha) = -3$, ou seja, P_2 é um polo de α de multiplicidade 3.

2.3 Divisores e o Teorema de Riemann-Roch

Seja γ uma curva algébrica não singular. O grupo abeliano gerado pelos pontos de γ é chamado *grupo dos divisores* de γ, e os elementos são ditos *divisores*, ou seja, um

divisor D é uma soma formal finita de pontos de γ, ou seja, $D = \sum_{P\in\gamma} n_P P$ onde $n_P \in \mathbb{Z}$ e $n_P \neq 0$ somente para um número finito de pontos P.

O *grau* de um divisor D é a soma dos inteiros n_P ou seja, $deg(D) = \sum_{P\in\gamma} n_P$.

Define-se a soma em modo natural:

$$D + D' = \sum_{P\in\gamma} n_P P + \sum_{P\in\gamma} n'_P P := \sum_{P\in\gamma} (n_P + n'_P) P,$$

e o elemento neutro é o divisor onde $n_P = 0$ para cada $P \in \gamma$.

Se $n_P \geq 0$ para cada $P \in \gamma$ o divisor é chamado *positivo ou efetivo*.

Podemos associar de uma forma natural um divisor a cada função racional, chamado de *divisor principal*:

$$(f) := \sum_{P\in\gamma} \mathrm{ord}_P(f) P,$$

onde $\mathrm{ord}_P(f)$ foi definido na Seção 1.2. Esse divisor é não nulo se, e somente se, a função não é constante. Nesse caso, podemos escrever este divisor como diferença de dois divisores efetivos, ou seja:

$$(f) = (f)_0 - (f)_\infty,$$

onde:

$$(f)_0 := \sum_{\mathrm{ord}_P(f)>0} \mathrm{ord}_P(f) P, \;\; (f)_\infty := \sum_{\mathrm{ord}_P(f)<0} -\mathrm{ord}_P(f) P$$

são ditos, respectivamente, *divisor dos zeros e divisor dos polos* de f. Dizemos então que dois divisores são *equivalentes* se $D - D' = (f)$ para alguma função racional f.

De fato, uma função racional tem o mesmo número finito de zeros e de polos ([19], Corolário 1.3.4, p.15), portanto, o grau de um divisor principal é zero.

Definição 2.3.1. O *espaço de Riemann-Roch* associado a um divisor D é definido como:

$$L(D) := \{0\} \cup \{f \in K(\gamma) \mid f \neq 0, \; (f) + D \geq 0\}.$$

Pode-se ver que $L(D)$ é um espaço vetorial, e denotamos com $l(D)$ a sua dimensão.

Lema 2.3.2. *([6], Seção 8.2, Proposição 3, p.99)*
Sejam D e D' dois divisores.

- *Se D é equivalente a D', então $L(D)$ e $L(D')$ são isomorfos como espaços vetoriais;*

- *se* $deg(D) < 0$, *então* $L(D) = \{0\}$;
- $L(0) = K$, *onde* K *é o corpo base.*

Definição 2.3.3. O *gênero* de uma curva algébrica γ é:

$$\max\{deg(D) - l(D) + 1 \mid D \text{ divisor de } \gamma\}.$$

Seja $\gamma : F(X_0, X_1, X_2) = 0$ e seja $d = deg(F)$. Em caso de uma curva não singular o gênero vale $g = (d-1)(d-2)/2$. Dizemos que um divisor W é *canônico* se $deg(W) = 2g-2$ e $l(W) = g$.
O seguinte Teorema é um dos Teoremas mais famosos da geometria algébrica, e aqui estamos considerando a versão das curvas algébricas.

Teorema 2.3.4. *(Riemann-Roch)([19], Teorema 1.5.15, p.30)*
Seja D *um divisor de uma curva* γ. *Então:*

$$l(D) = deg(D) + 1 - g + l(W - D),$$

onde W *é o divisor canônico.*

Em geral não é fácil calcular $l(W - D)$, mas se o grau de D é grande o suficiente, vale o seguinte:

Corolário 2.3.5. *([19], Teorema 1.5.17, p.31) Para cada* D *tal que* $deg(D) \geq 2g - 1$ *vale:*

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

No Capítulo 3, particularmente no exemplo (4.0.6), é possível ver uma aplicação prática deste Teorema.

2.4 Códigos algébricos geométricos e Bases de Gröbner

Seja γ uma curva algébrica projetiva, lisa e irredutível sobre um corpo finito $\mathbb{F}_q$. Denotamos os pontos racionais de γ sobre $\mathbb{F}_q$ com P_i.

Teorema 2.4.1. *(limite de Hasse-Weil)([23], p.502) Seja γ uma curva algébrica com coeficientes em $\mathbb{F}_q$ de gênero g.*
Se m é o número de pontos racionais da curva γ, então:

$$m \geq 1 + q + 2g\sqrt{q}.$$

Se a curva atinge o limite, se diz que a curva é maximal.

Seja agora $D = \sum_{i=1}^{n} P_i$ e G dois divisores da curva γ, tais que os P_i sejam distintos e $\text{supp}(D) \cap \text{supp}(G) = \emptyset$.
Consideremos enfim o espaço vetorial $L(G)$ das funções racionais sobre γ que têm polos e zeros limitados da G, ou seja:

$$L(G) = \{f \in \mathbb{F}_q(\gamma)^* \mid (f) + G \geq 0\} \cup \{0\}.$$

O *código algébrico geométrico* associado a curva γ e aos divisores G, D denota-se com $C_L(\gamma, D, G)$, ou simplesmente $C_L(D, G)$ ou $C(D, G)$, e é definido como:

$$C(D, G) := \{(f(P_1), \ldots, f(P_n)) \mid f \in L(G)\}.$$

Em geral, prefere-se trabalhar com curvas maximais, já que o número de pontos racionais da curva atinge o limite de Hasse-Weil e, portanto, o código AG associado tem dimensão maior.
O objetivo desta Seção é construir um método de codificação para um código AG, que permita codificar as palavras com um número finito de passos.
O exemplo que motivou este tipo de trabalho é o exemplo dos códigos cíclicos (uma referência é [22], Capítulo 6), ou seja:
Um *código cíclico* é um código linear onde se $(c_1, \ldots, c_n)$ é uma palavra do código então $(c_n, c_1, \ldots, c_{n-1})$ é uma palavra do código também.
Consideremos C um ideal no anel $\frac{\mathbb{F}_q[x]}{<x^n-1>}$. Cada código cíclico pode ser associado com um ideal deste tipo (veja, por exemplo [22], Teorema 6.1.3, p.76).
C pode ser gerado de um único polinômio mônico $g(x)|x^n - 1$ (módulo $x^n - 1$).
Podemos codificar sistematicamente utilizando somente a informação contida em $g(x)$ e o algoritmo de divisão de polinômios, ou seja, se $g(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_0$ e

$k = \dim(C) = n - r$, pegamos como informação os coeficientes de $x^{n-1}, \ldots, x^r$. Tomando então uma combinação linear:

$$p(x) = c_{n-1}x^{n-1} + \cdots + c_r x^r,$$

podemos calcular o resto $r(x)$ de $p(x)$ dividido por $g(x)$. Nota-se que $p(x) - r(x)$ é um múltiplo de $g(x)$, ou seja, é uma palavra do código.
Nota-se também que como $r(x)$ é um polinômio de grau $r-1$, o polinômio $p(x) - r(x)$ contém os mesmos elementos de grau $x^{n-1}, \ldots, x^r$, que eram as nossas informações, ou seja, encontramos um método algorítmico para codificar o código cíclico.
Consideremos agora um código $C(D, G)$. Para obter um método de codificação precisamos que a curva tenha um grupo de automorfismos que não seja trivial.

Definição 2.4.2. Seja γ uma curva algébrica e $K(\gamma)$ o corpo das funções racionais da curva γ. Um *K-automorfismo da curva γ* é um automorfismo de corpos de $K(\gamma)$ que fixa os elementos de K

Definição 2.4.3. Seja C um código linear. Um mapa $f : \mathbb{F}_q^m \to \mathbb{F}_q^n$ é chamado de *isometria* se respeita a distância de Hamming.
Um mapa $g : \mathbb{F}_q^m \to \mathbb{F}_q^n$ é dito *semilinear* se existe um automorfismo de corpos α de $\mathbb{F}_q$, tal que para cada $u, v \in \mathbb{F}_q^n$ e para cada $k \in \mathbb{F}_q$, tem-se que $g(u+v) = g(u) + g(v)$ e que $g(ku) = \alpha(k)g(u)$.
Um *automorfismo* de um código linear C é uma isometria semilinear $h : \mathbb{F}_q^m \to \mathbb{F}_q^n$ tal que $h(C) = C$.

Os automorfismos de uma curva algébrica formam um grupo, denotado com $\mathrm{Aut}(\gamma)$.
Em [19] (Proposição 8.23, p.291) mostra-se que se existe um automorfismo $\sigma \in \mathrm{Aut}(\gamma)$ que fixa D e G, ou seja, tal que $\sigma(D) = D$ e $\sigma(G) = G$, o mapa:

$$f \mapsto f \circ \sigma^{-1},$$

leva o subespaço vetorial $L(G) \subset \mathbb{F}_q(\gamma)$ dentro do próprio $L(G)$ e então induz um automorfismo do código $C(D, G)$.

Considerando a decomposição induzida pelas órbitas nas palavras do código pela ação do subgrupo cíclico H gerado pelo automorfismo σ do código definido acima, notamos que as palavras do código podem ser classificadas em blocos, um para cada órbita, e cada bloco é permutado ciclicamente. Então a ideia é utilizar um método parecido ao dos códigos cíclicos.

Exemplo 2.4.4. Consideremos o modelo plano da curva Hermitiana γ sobre o corpo finito $\mathbb{F}_{q^2}$ definido pela equação afim:

$$x^{q+1} = y^q + y.$$

Esta curva tem um único ponto no infinito $(0 : 1 : 0)$ que denotamos com Q e outros q^3 pontos racionais que denotamos com P_i para cada $i = 1, \ldots, q^3$.
A teoria geral da teoria de corpos finitos mostra que o grupo multiplicativo de um corpo finito é cíclico, então consideramos α um gerador de $\mathbb{F}_{q^2}^*$. Consideremos o automorfismo:

$$\sigma : \begin{cases} x & \to & \alpha x \\ y & \to & \alpha^{q+1} y \end{cases}.$$

O automorfismo σ fixa Q e permuta os outros q^3 pontos racionais.
A escolha deste automorfismo é interessante pois é o automorfismo que tem ordem máximo $m^2 - 1$ e, portanto, permite ter menos órbitas que têm comprimento máximo do que se utilizássemos qualquer outro automorfismo. Além disso, este automorfismo pode ser utilizado para qualquer modelo plano de curvas hermitianas.
Considerando então os divisores:

$$D = \sum_{i=1}^{q^3} P_i, \qquad G = aQ,$$

temos que o automorfismo σ induz um automorfismo em cada código $C(D, aQ)$.
Uma ótima referência para os resultados básicos sobre os corpos finitos está em [12], por enquanto alguns resultados sobre a curva Hermitiana e o grupo de automorfismos dela podem ser encontrados em [25] e em [20].

2.5 A estrutura de módulo sobre os códigos AG

Seja γ uma curva algébrica projetiva sobre um corpo finito $\mathbb{F}_q$ e seja σ um $\mathbb{F}_q$-*automorfismo racional* da curva, ou seja, um automorfismo de γ que preserva $\mathbb{F}_q$. O automorfismo permuta os pontos racionais de γ, e então pode-se estender aos divisores de γ formados pelos pontos racionais. Supondo que exista um automorfismo σ tal que fixa dois divisores D e G da curva e que induz uma permutação não trivial dos pontos do divisor D.

Lema 2.5.1. *([19] Proposição 8.23, p.291) O automorfismo σ induz um automorfismo não trivial:*

$$\begin{aligned} \sigma(f(P_1),\ldots,f(P_n)) &= ((f\circ\sigma^{-1})(P_1),\ldots,(f\circ\sigma^{-1})(P_n)) \\ &= (f(\sigma^{-1}(P_1)),\ldots,f(\sigma^{-1}(P_n))) \end{aligned}$$

.

Um Corolário imediato tem a ver com as palavras do código.

Corolário 2.5.2. *([13], II.A.2, p.1754) Seja H o subgrupo cíclico do grupo de automorfismos da curva gerado pelo elemento σ, e considerando a decomposição dos pontos do suporte de D em órbitas distintas pela ação dos elementos de H que denotamos com:*

$$\mathrm{supp}(D) = \bigcup_{i=1}^{r} O_i,$$

então as entradas do código que correspondem aos pontos de cada órbita O_i são permutadas ciclicamente pela ação de σ.

Exemplo 2.5.3. Considerando a curva Hermitiana:

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

sobre o corpo $\mathbb{F}_9$ e, como no exemplo 2.4.4, seja σ o automorfismo:

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

com α gerador de $\mathbb{F}_9^*$. Este automorfismo fixa o ponto no infinito e também o divisor D que é a soma dos 27 pontos racionais da curva, ou seja:

$$D = \sum_{i=1}^{27} P_i.$$

Representamos o corpo $\mathbb{F}_9$ como:

$$\frac{\mathbb{F}_3}{< \alpha^2 + \alpha - 1 >}.$$

$H = \langle \sigma \rangle$ decompõe o suporte do divisor D em 5 órbitas distintas, 3 com oito elementos, 1 com dois elementos, e 1 com um único elemento.

$$\begin{aligned}
O_1 &= \{(1, \alpha^7), (\alpha, \alpha^3), (\alpha^2, \alpha^7), (\alpha^3, \alpha^3), (\alpha^4, \alpha^7), (\alpha^5, \alpha^3), (\alpha^6, \alpha^7), (\alpha^7, \alpha^3)\};\\
O_2 &= \{(1, \alpha^5), (\alpha, \alpha), (\alpha^2, \alpha^5), (\alpha^3, \alpha), (\alpha^4, \alpha^5), (\alpha^5, \alpha), (\alpha^6, \alpha^5), (\alpha^7, \alpha)\};\\
O_3 &= \{(1, \alpha^4), (\alpha, 1), (\alpha^2, \alpha^4), (\alpha^3, 1), (\alpha^4, \alpha^4), (\alpha^5, 1), (\alpha^6, \alpha^4), (\alpha^7, 1)\};\\
O_4 &= \{(0, \alpha^2), (0, \alpha^6)\};\\
O_5 &= \{(0, 0)\}.
\end{aligned}$$

Nota-se que neste caso tem uma escolha de um automorfismo de um código com um número menor de órbitas e ordem maior que $q^2 - 1$. Consideremos:

$$\tau : \begin{cases} x \rightarrow \alpha^2 x \\ y \rightarrow \alpha^2 + y \end{cases}.$$

Pode-se demonstrar que τ é um automorfismo da curva que fixa os divisores D e G e que decompõe os pontos racionais em 3 órbitas, duas de ordem 12 e uma de ordem 3. Mas em geral, para este tipo de trabalho, escolhem-se automorfismos que tenham produtos de α com a x e a y, para poder utilizar a ciclicidade do grupo multiplicativo do corpo.

Agora consideramos a estrutura do código como $\mathbb{F}_q[t]$-módulo induzida pelo automorfismo. A ideia é que multiplicar por t no módulo significa aplicar o automorfismo σ.

Rotulamos os pontos racionais da curva de uma forma diferente, em particular denotamos os pontos racionais de D como $P_{i,j}$, onde a letra i indica que o ponto esta na órbita i-ésima

e j varia entre $0, \ldots, |O_i| - 1$.

Especificamente, fixando um elemento $P_{i,0}$ na órbita i-ésima, enumeramos os pontos $P_{i,j} = \sigma^j(P_{i,0})$. Como consequências imediatas temos que $P_{i,|O_i|} = P_{i,0}$ e podemos escrever que $P_{i,-1} = \sigma^{-1}(P_i, 0)$.

Podemos então representar as palavras do código como r-uplas (onde lembramos que r é o número das órbitas) de polinômios em uma indeterminada, ou seja, da forma:

$$(h_1(t), \ldots, h_n(t)),$$

onde:

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

e $f \in L(G)$.

Agora, para poder utilizar as permutações cíclicas das entradas das r-uplas, podemos vê-las como elementos do módulo:

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

Desta forma, multiplicar cada polinômio $h_i(t)$ por t tem o seguinte resultado:

$$\begin{aligned} t \cdot h_i(t) &= t \cdot \sum_{j=0}^{|O_i|-1} f(P_{i,j})t^j \\ &= \sum_{j=0}^{|O_i|-1} f(P_{i,j})t^{j+1} \\ &= \sum_{j=0}^{|O_i|-1} f(P_{i,j-1})t^j \mod < t^{|O_i|} - 1 > \\ &= \sum_{j=0}^{|O_i|-1} f(\sigma^{-1}(P_{i,j}))t^j \end{aligned}$$

ou seja, multiplicar um elemento do código por t é a mesma coisa que aplicar o automorfismo do código induzido por σ.

Vamos ver uma descrição alternativa deste módulo, para poder utilizar as bases de Gröbner de módulos sobre um anel de polinômios. Considere-se o $\mathbb{F}_q[t]$-submódulo C' do módulo livre $\mathbb{F}_q[t]^r$ gerado pelas palavras do código $C(D, G)$ ou seja, C' é a imagem

inversa $\pi^{-1}(C)$ onde:

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

Neste sentido podemos associar ao código um submódulo de um módulo livre sobre $\mathbb{F}_q[t]$, e então podemos aplicar a teoria de bases de Gröbner de módulos sobre um anel de polinômios.

2.6 Bases de Gröbner

A teoria das bases de Gröbner sobre aneis de polinômios é clássica, enquanto a teoria de bases de Gröbner de um módulo sobre um anel de polinômios é menos conhecida. O leitor pode considerar como referências os livros [3], [15] e [16].
Neste caso estamos considerando módulos sobre polinômios em uma indeterminada, então a estrutura algébrica vai simplificar-se muito.

Definição 2.6.1. Considere o $\mathbb{F}_q[t]$-módulo livre $F := \mathbb{F}_q[t]^r$.

- Um *monômio* $m \in F$ é um elemento da forma $m = t^i \mathbf{e}_j$, com $1 \leq i \leq r$, e $\mathbf{e}_j$ é o j-ésimo elemento da base canônica de F;
- Uma *ordem monomial* em F é uma ordem total $>$ que satisfaz $t^i \mathbf{e}_j > \mathbf{e}_j$ para cada j e para cada $i > 0$ (ou, escrito em outras palavras, $1 < t^i$ para cada $i > 0$), e que respeite a estrutura de módulo, ou seja:

$$m_1 > m_2 \Leftrightarrow t^i m_1 > t^i m_2.$$

Já que estamos trabalhando em polinômios em uma indeterminada, temos apenas dois tipos de ordem que podemos definir, ou seja, a ordem que dá mais importância ao grau dos polinômios ou a ordem que dá mais importância aos índices da base canônica. Seja primeiro uma ordem definida sobre os $\mathbf{e}_j$. Em geral considera-se:

$$\mathbf{e}_1 > \mathbf{e}_2 > \cdots > \mathbf{e}_r.$$

Podemos então definir duas ordens, ou seja:

Definição 2.6.2.

- A *ordem* POT (Position Over Term) sobre F é definida como:

$$t^i\mathbf{e}_j >_{\text{POT}} t^k\mathbf{e}_l,$$

se, e somente se, $j < l$ ou $j = l$ e $i > k$. Neste caso estamos dando mais importância aos índices da base canônica;

- A *ordem* TOP (Term Over Position) sobre F é definida como:

$$t^i\mathbf{e}_j >_{\text{TOP}} t^k\mathbf{e}_l,$$

se, e somente se, $i > k$ ou $i = k$ e $j < l$. Neste caso estamos dando mais importância aos exponentes de t.

Em geral é possível separar os índices da base canônica em subconjunto e definir uma ordem TOP ou POT em cada subconjunto para depois definir uma ordem nos subconjuntos, etc. Mas neste caso estamos trabalhando com uma única indeterminada e a única ordem possível sobre os monômios de $\mathbb{F}_q[t]$ é o grau, então as únicas escolhas de uma ordem monomial são aquelas mostradas acima.

Definição 2.6.3. Seja fixada uma ordem monomial $>$.

- O *termo inicial* de $f \in F$, ou termo líder, é o (único) maior termo de f com a ordem monomial $>$ e será denotado por $LT(f)$;

- Seja E um submódulo de F. O conjunto de todos os termos iniciais de E será denotado por $LT(E)$ e forma um submódulo de F;

- Uma *base de Gröbner* de um submódulo E de F é um conjunto $G = \{g_1, \ldots, g_s\}$ de geradores de E tal que $LT(E) =< LT(g_1), \ldots, LT(g_s) >$;

- Os monômios de $LT(E)$ são ditos monômios *"não padrão"* e os monômios no complementar de $LT(E)$ são ditos *monômios "padrão"*;

- Uma base de Gröbner *reduzida* é uma base de Gröbner onde os coeficientes de todos os elementos são 1 e o monômio inicial de cada g_i não aparece em nenhum g_j se $i \neq j$.

Como no caso de ideais, uma base de Gröbner de um submódulo E sempre existe e pode-se utilizar uma variação do algoritmo de Buchberger para poder achá-la (por exemplo, ver o livro [3], Capítulo 2, Teorema 2, p.90). O algoritmo de Buchberger foi melhorado várias vezes, utilizando, entre as outras, a teoria das sizigias.
Uma base de Gröbner não é única, mas pode-se mostrar que uma base de Gröbner reduzida é sim única, e que é minimal (ou seja, os elementos são tais que geram minimalmente o submódulo $LT(E) =< LT(g_1), \ldots, LT(g_s) >$).

Proposição 2.6.4. *([13], II.B.4, p.1756) Seja E um submódulo do módulo livre $F = \mathbb{F}_q[t]^r$. Então E tem uma base de Gröbner G com a propriedade que para cada j, tal que $j = 1, \ldots, r$, existe no máximo um elemento de G que tem termo inicial da forma $t^i\mathbf{e}_j$, e em particular G contém no máximo r elementos.*

Demonstração. Considere-se uma base de Gröbner $G = \{g_1, \ldots, g_s\}$ e assumimos que tem dois elementos g_i e g_k com a propriedade enunciada, ou seja, $LT(g_i) = t^i\mathbf{e}_j$ e $LT(g_k) = t^k\mathbf{e}_j$ com o mesmo j.
Sem perda de generalidade podemos considerar $i < k$. Então o termo inicial de g_k é múltiplo do termo inicial de g_i. Podemos então retirar o elemento g_k da base G obtendo uma nova base de Gröbner G' uma vez que isso gera o mesmo submódulo $LT(E)$. Repetindo este argumento para cada par de elementos que tem termos iniciais com o mesmo vetor da base canônica, obtemos uma base de Gröbner, que tem elementos da base distintos $\mathbf{e}_j$ com j que varia entre 1 e r, ou seja, a base de Gröbner tem no máximo r elementos. □

Notamos que na aplicação que estamos considerando, incluindo os elementos $q_i = (t^{|O_i|} - 1)\mathbf{e}_i$ como geradores para poder simular as permutações cíclicas das órbitas do automorfismo, a base de Gröbner tem exatamente r elementos.
Como no caso dos ideais, fixando uma ordem monomial e uma base de Gröbner G podemos utilizar o algoritmo de divisão e obter um resto que é chamado de *forma normal* de f e se denota com f^G, ou seja:

$$f = a_1g_1 + \cdots + a_sg_s + f^G.$$

A forma normal é univocamente determinada pela f e pela escolha da ordem, e encontra-se subtraindo múltiplos dos g_i para cancelar o termo inicial do dividendo intermediário, e quando isso não é possível, os termos que sobram são colocados no resto. (O algoritmo é bem parecido com aquele dos ideais que pode ser encontrado em [3], Capítulo 2, Teorema 3, p.64).

Se utilizarmos a ordem POT, o algoritmo de divisão permite fazer divisões de polinômios em uma indeterminada. Veremos isso mais detalhadamente.

Seja $E \subset F$ um submódulo, $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner de E obtida a partir da ordem POT, tal que os g_i tenham termos iniciais com vetores distintos da base. Sem perda de generalidade podemos ordenar os g_i de forma tal que os termos iniciais são listados de forma decrescente.

Dado:

$$f = \sum f_i \mathbf{e}_i,$$

queremos computar a forma normal f^G.

Se $LT(g_1)$ contém $\mathbf{e}_1$ e

$$g_1 = \sum g_{1i} \mathbf{e}_i,$$

então começamos dividindo g_{11} em f_1 em $\mathbb{F}_q[t]$ ou seja:

$$f_= a_1 g_{11} + R_1,$$

com $R_1 = 0$ ou R_1 de grau menor de g_{11}. Subtraindo agora $a_1 g_1 + R_1 \mathbf{e}_1$ em f obtemos o dividendo intermediário p e o resto intermediário R da forma:

$$\begin{aligned} p &= \sum_{i=2}^{r} (f_1 - a_1 g_{1i}) \mathbf{e}_i \\ R &= R_1 \mathbf{e}_i \end{aligned}$$

Desse modo, p não tem nenhum elemento com $\mathbf{e}_1$ e então podemos continuar dividindo até ter todos os elemento no dividendo intermediário tendo vetores da base canônica que não aparecem em nenhum $LT(g_j)$. Em particular, podemos utilizar o seguinte algoritmo para achar a forma normal com a ordem POT.

Como antes, denotamos:

$$f = \sum f_i \mathbf{e}_i,$$

e

$$g_j = \sum g_{ji}\mathbf{e}_i.$$

O algoritmo para achar a forma normal de f é:

Algoritmo 1: O algoritmo para achar a forma normal de f

Entrada: f, a base de Gröbner G ordenada com POT

Saída: $a_1, \ldots, a_s$, a forma normal $R = f^G$

início

$p := f$; $R := 0$ $j := 1$;

para $i = 1$ *até* r **faça**

se $LT(g_j)$ *contém* $\mathbf{e}_i$ **então**

$a_i := \text{Quot}(p_i, g_{ji})$;

$R_i := \text{Res}(p_i, g_{ij})$;

$p := p - a_i g_j - R_i \mathbf{e}_i$;

$R := R + R_1 \mathbf{e}_i$;

$j := j + 1$;

fim

senão

$a_i := 0$;

$R := R + p_o \mathbf{e}_i$;

$p := p - p_i \mathbf{e}_i$;

fim

fim

fim

Onde Quot indica a função que calcula o quociente entre p_i e g_{ij} e Res indica a função que calcula o resto.

2.7 O algoritmo de codificação

Consideremos um código $C(D, G)$ e σ um automorfismo sobre a curva γ.

Para a construção anterior, podemos considerar a estrutura de $\mathbb{F}_q$-módulo sobre o código

e fazer os cálculos sobre o submódulo C' de $\mathbb{F}_q[t]^r$ gerado pelas r-tuplas $(h_1(t), \ldots, h_r(t))$ e os elementos $q_i = (t^{|O_i|} - 1)\mathbf{e}_i$, onde r é o número das órbitas do suporte de D sobre a ação do grupo dos automorfismos gerados pelo σ.
Inicialmente, fixamos uma ordem e calculamos uma base de Gröbner reduzida para C'.

Proposição 2.7.1. *Dada uma base de Gröbner para o módulo, determinamos (e definimos) as posições de informação e as verificações de paridade da seguinte forma:*

- *As posições de informação são os coeficientes dos monômios "não padrão" que aparecem nas r-uplas construídas das palavras $(h_1(t), ..., h_r(t))$ do código, ou seja, são os coeficientes dos monômios "não padrão" da forma $t^l\mathbf{e}_i$ onde $l \leq |O_i| - 1$. Ignoramos as potências maiores de t;*
- *As verificações de paridade são os monômios "padrão".*

Fixamos agora a ordem POT. Para calcular a forma normal dos elementos utilizamos várias vezes a divisão polinomial em uma indeterminada, como visto antes.
Seja $VC(h)$ o vetor dos coeficientes dos termos de h e sejam $t^{i_l}\mathbf{e}_{j_l} =: m_l$ ordenados com a ordem POT, agora podemos construir o algoritmo de codificação.

Algoritmo 2: O algoritmo de codificação

Entrada: $w \in \mathbb{F}_q^k$, a base de Gröbner G ordenada com POT, $\{m_l\}$

Saída: $E(w) \in C(D, G)$

início

$f := \sum_{i=1}^{k} w_i m_i$;
$f' := f^G$;
$E(w) := VC(f - f')$;

fim

Fazemos agora algumas considerações sobre este algoritmo.
Primeiramente, vale ressaltar que este algoritmo utiliza o algoritmo precedente para poder calcular a forma normal de F.
Nota-se também que utilizando uma base de Gröbner reduzida, cada elemento da base de Gröbner tem um monômio inicial "não padrão" e no máximo $n - k$ monômios "padrão", então temos no máximo $r \cdot (n - k)$ coeficientes.

Enfim, notamos que a escolha da ordem POT, que permite utilizar o algoritmo de divisão em uma indeterminada, calcula uma base de Gröbner diagonal para C' (ou seja, se a base é $\{g_1, \ldots, g_k\}$ então g_2 tem 0 na primeira componente, g_3 tem 0 nas primeiras duas componentes, etc.).

2.8 Um exemplo completo

Vou aplicar todo o estudo feito até agora seguindo o exemplo em [13], p.1758.
Seja $C(D, 19Q)$ o código construído sobre a curva Hermitiana:

$$\gamma : x^4 = y^3 + y,$$

onde Q é o único ponto no infinito da curva γ e D é a soma dos outros pontos racionais.
Representamos $\mathbb{F}_9$ como $\frac{\mathbb{F}_9[\alpha]}{<\alpha^2+\alpha-1>}$.
Seja σ o automorfismo:

$$\tau : \begin{cases} x & \rightarrow & \alpha^2 x \\ y & \rightarrow & \alpha^2 + y \end{cases}$$

Fazendo agir o subgrupo gerado pelo τ os pontos afins da curva se dividem em 3 órbitas, duas de comprimento 12 e uma de comprimento 3.
Pode-se demonstrar que x tem um polo de ordem 3 em Q e que y tem um polo de ordem 4 em Q e que uma base de $L(19Q)$ é dada pelas funções monomiais:

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

Utilizando a ordem POT sobre $\mathbb{F}_9[t]^3$ podemos construir uma base de Gröbner reduzida do submódulo C'. Como geradores do submódulo, consideramos as 17 palavras do código que correspondem às linhas de uma matriz geradora de $C(D, 19Q)$ e $(t^{12} - 1)\mathbf{e}_i$ com $i = 1, 2$ e $(t^3 - 1)\mathbf{e}_3$.

A base de Gröbner tem então 3 elementos:

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

Por definição, as posições de informação são os coeficientes dos monômios "não padrão", ou seja, são os coeficientes de:

- $t^{11}\mathbf{e}_1, \ldots, t\mathbf{e}_1, \mathbf{e}_1$;
- $t^{11}\mathbf{e}_2, \ldots, t^7\mathbf{e}_2$.

Para ver como funciona a codificação, aplicamos o algoritmo de codificação à palavra:

$$w = (t, \alpha t^8 + t^7, 0),$$

onde ja convertemos os vetores de $\mathbb{F}_9^{17}$ em 3-tuplas de polinômios, utilizando a estrutura de módulo.
Começamos subtraindo tg_1 de w:

$$w - tg_1 = (0, \alpha t^8 + \alpha^6 t^7 + \alpha^3 t^5 + \alpha^3 t^4 - t^3 + \alpha^2 t^2 + \alpha^5 t, \alpha t^3 - t^2 + \alpha^5 t).$$

(Observando que $-\alpha = \alpha^5$, $-\alpha^7 = \alpha^3$, $-\alpha^6 = \alpha^2$ e $1 - \alpha^3 = \alpha^6$).

Agora dividimos a segunda componente com o monômio inicial de g_2, obtendo um quociente de $\alpha t + \alpha$ e um resto:

$$R_2\mathbf{e}_2 = (0, \alpha^3 t^6 + \alpha^5 t^5 + \alpha^6 t^4 + \alpha^7 t^- t^2 + \alpha^3 t + \alpha^5, 0),$$

e então:

$$w - tg_1 - (\alpha t + \alpha)g_2 - R_2\mathbf{e}_2 = (0, 0, \alpha t^3 + \alpha t^2 + \alpha^5 t + \alpha^3).$$

Dividindo por g_3 temos:

$$R_3\mathbf{e}_3 = (0, 0, \alpha t^2 + \alpha^5 t - 1).$$

A forma normal é $w' = (0, R_2, R_3)$ e então a palavra do código é:

$$w - w' = (t, \alpha t^8 + t^7 + \alpha^7 t^6 + \alpha t^5 + \alpha^2 t^4 + \alpha^3 t^3 + t^2 + \alpha^5 t^5 \alpha^7 t + \alpha, \alpha^5 t^2 + \alpha t + 1).$$

2.9 O diagrama de raízes

Agora vou definir o objeto de estudo desta tese.

Definição 2.9.1. Seja γ o modelo plano de uma curva com coeficientes em $\mathbb{F}_q$, sejam D e G dois divisores da curva e σ um automorfismo da curva que fixa os dois divisores.
Para cada $i = 1, \ldots, r$ seja O_i a i-ésima órbita de σ. Seja $\mathcal{R}_i \subseteq \mathbb{F}_q^*$ o conjunto das raízes de $t^{|O_i|} - 1$.
O *diagrama de raízes* de um código C sobre $\mathbb{F}_q$ com um automorfismo σ é uma tabela formada por r linhas, onde, para cada i, a i-ésima linha é formada por caixas sobre os elementos de R_i com uma marca X sobre as raízes de $g_i^{(i)}(t)$, ou seja, a i-ésima componente do elemento $g^{(i)}$ da base de Gröbner do submódulo C' (ver o algoritmo 2)

Exemplo 2.9.2. ([14], p.311) Seja $C = C(D, 19P_\infty)$ o código construído sobre o modelo plano da curva Hermitiana $\gamma : x^4 = y^3 + y$ sobre $\mathbb{F}_9$, α um gerador de $\mathbb{F}_9^*$ e σ o automorfismo:

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

O automorfismo σ tem ordem 8 e permuta os 27 pontos $\mathbb{F}_9$ racionais em 5 órbitas: 3 de comprimento 8, 1 de comprimento 2 e 1 de comprimento 1.
Com o algoritmo 2 consegue-se uma base de Gröbner diagonal $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_5\}$, com

- $g_1^{(1)} = 1$;
- $g_2^{(2)} = t + \alpha^5$;
- $g_3^{(3)} = t^6 + \alpha t^5 + \alpha^2 t^2 + \alpha^7 t^3 + \alpha t^2 + \alpha^4 t + \alpha^5$;
- $g_4^{(4)} = t^2 - 1$;
- $g_5^{(5)} = t - 1$.

Vamos analizar como se constrói o diagrama de raízes

- Como as 3 primeiras órbitas têm comprimento 8 e as raízes de $t^8 - 1$ são todos os elementos de $\mathbb{F}_9^*$, colocamos caixas embaixo de todos os α^i com $i = 0, \ldots, 7$;
  - $g_1^{(1)} = 1$ logo não possui raiz e portanto não marcamos nenhum X na linha 1;
  - $g_2^{(2)} = t + \alpha^5$ possui $\alpha = -\alpha^5$ como raiz, e portanto marcamos um X embaixo de α;

– $g_3^{(3)}$ tem raiz α^i com $i = 1, \ldots, 6$ e portanto as marcamos no diagrama.

- A linha 4 tem duas caixas embaixo de 1 e α^4 que são as raízes de $t^{|O_4|} - 1 = t^2 - 1$ e as marcamos com X já que $t^2 - 1 = g_4^{(4)}$;

- A linha 5 tem apenas uma caixa embaixo do 1, que é raiz de $t^{|O_5|} - 1 = t - 1$ e será marcada com um X já que $t - 1 = g_5^{(5)}$.

O diagrama portanto será:

	0	1	2	3	4	5	6	7
1								
2		X						
3		X	X	X	X	X	X	
4	X				X			
5	X							

onde os números colocados na primeira linha representam as potências de α e os números da primeira coluna representam respectivamente os números das órbitas.

Proposição 2.9.3. ([13], Proposition 2.3) *A dimensão do código C é igual ao número de caixas vazias do diagrama $\mathcal{R}_C$.*

3 O DIAGRAMA DE RAÍZES DA CURVA DE KONDO

Este Capítulo e o seguinte são os Capítulos principais do trabalho. Todos os resultados apresentados, assim como os exemplos, são originais e aparecem pela primeira vez nesta tese.

Seja $K := \mathbb{F}_{q^{2r}}$ e seja:

$$\delta : y^q + y = x^{q^r+1},$$

com r ímpar, o modelo plano de uma curva algébrica definida sobre o corpo K. Notamos que para $r = 1$ o modelo define a curva Hermitiana. Denotamos o corpo de funções dela com $F := K(\delta)$.

Kondo e al. em [11], mostram que esta curva é maximal e portanto tem q^{2r+1} pontos racionais, mais um ponto no infinito que será denotado com P_∞.

No mesmo artigo mostra-se que dado $\alpha \in K^*$ tal que $\alpha^{(q^r+1)(q-1)} = 1$ a função:

$$\sigma : \begin{cases} x & \to & \alpha x \\ y & \to & \alpha^{q^r+1} y \end{cases} .$$

define um automorfismo da curva que fixa o ponto no infinito P_∞.

De forma semelhante ao que foi feito no exemplo (2.9.2), precisa-se que a ordem do automorfismo divida a ordem de $\mathbb{F}^*_{q^{2r}}$.

Neste caso a ordem do automorfismo é $(q^r + 1)(q - 1)$ e a ordem do grupo multiplicativo é:

$$|\mathbb{F}^*_{q^{2r}}| = q^{2r} - 1 = (q^r + 1)(q^r - 1) = (q^r + 1)(q - 1)(q^{r-1} + \cdots + q + 1),$$

portanto podemos construir o diagrama de raízes.

Proposição 3.0.1. *O automorfismo σ divide os pontos racionais da curva δ em $q(q^{r-1}+\cdots+q)+2$ órbitas da seguinte maneira:*

- *$q(q^{r-1}+\cdots+q)$ órbitas de comprimento $(q^r+1)(q-1)$;*
- *uma órbita de comprimento $q-1$;*
- *uma órbita de comprimento 1.*

Demonstração.

- O ponto $(0,0)$ é o único elemento da órbita dele. Esse é o único caso onde $y=0$;
- Fixamos $x=0$ e $y\neq 0$. O polinômio y^q+y tem q raízes distintas (pois a derivada dele é $qy+1=1\neq 0$), e então tem $q-1$ raízes distintas de 0. Já que a órbita de um ponto do tipo $(0,y)$ tem ordem $q-1$ por construção, então temos uma única órbita de ordem $q-1$;
- Seja (x,y) com $x\neq 0$ e $y\neq 0$ os demais $q^{2r+1}-q=q(q^{2r}-1)$ pontos. Para cada $a\in\mathbb{F}^*_{q^{2r}}$ o polinômio $y^q+y=a^{q^r+1}$ tem q raízes distintas.
  Temos então $q(q^{2r}-1)$ pontos, e já que as órbitas tem ordem $(q^r+1)(q-1)$ temos um número de órbitas igual a:

$$\frac{q(q^{2r}-1)}{(q^r+1)(q-1)}=q(q^{r-1}+\cdots+q+1).$$

□

Seja então a um gerador de $\mathbb{F}^*_{q^{2r}}$ (a teoria garante que o grupo multiplicativo de um corpo finito é cíclico). Então existe k tal que $\alpha=a^k$ e o automorfismo σ pode ser escrito da seguinte maneira:

$$\sigma:\begin{array}{rcl} x & \to & a^k x \\ y & \to & a^{k(q^r+1)}y \end{array}, \tag{3.1}$$

onde a condição $\alpha^{(q^r+1)(q-1)}=1$ nos leva a concluir que $k=\frac{q^{2r-1}}{(q^r+1)(q-1)}=(q^{r-1}+\cdots+q+1)$. Para cada $i=1,\ldots,q(q^{r-1}+\cdots+q)$, O_i será uma órbita de comprimento $(q^r+1)(q-1)$, $O_{q(q^{r-1}+\cdots+q)+1}$ será a órbita de comprimento $q-1$ e $O_{q(q^{r-1}+\cdots+q)+2}$ será a órbita de

comprimento 1.

Para $i = 1, \ldots, q(q^{r-1} + \cdots + q)$, dado um ponto $P_{i,0} = (a^{t_i}, a^{l_i})$ para a definição de σ temos que os pontos $P_{i,j} = \sigma^j(P_{i,0}) = (a^{ti+jk}, a^{li+jk(q^r+1)})$, com
$j \in \{1, \ldots, (q^r+1)(q-1)-1\}$ e no caso da órbita de comprimento $q-1$, tomando o ponto $P_{q(q^{r-1}+\cdots+q),0} = (0, a^{l_i})$ temos que os demais pontos tem a forma $P_{i,j} = (0, a^{l_i+jk(q^r+1)})$ com $j \in \{1, \ldots, q-2\}$. Portanto, segue que:

Proposição 3.0.2. *Para $1 \leq i \leq q(q^{r-1} + \cdots + q)$, seja $P_{i,0} = (a^{t_i}, a^{l_i}) \in O_i$, e para $i = q(q^{r-1} + \cdots + q) + 1$ seja $P_{i,0} = (0, a^{l_i}) \in O_i$. Para cada $1 \leq i \leq q(q^{r-1} + \cdots + q) + 1$, seja:*

$$M_i := \prod_{j=0}^{q-2}(y - a^{l_i+jk(q^r+1)}) = y^{q-1} - a^{l_i(q-1)}.$$

Então, para cada $1 \leq i \leq q(q^{r-1} + \cdots + q) + 1$, a órbita O_i é a interseção da curva δ com $M_i(y)$. Além disso, $M_i(y)$ é uma constante não nula quando restrita à órbita O_ℓ, se $\ell \neq i$.

Demonstração. Seja $1 \leq i \leq q(q^{r-1} + \cdots + q)$ e seja $P_{i,0} = (a^{t_i}, a^{l_i}) \in O_i$. Daí,

$$O_i = \{(a^{t_i}, a^{l_i}), \ldots, (a^{t_i+k((q^r+1)(q-1)-1)}, a^{l_i+k((q^r+1)(q-1)-1)(q^r+1)})\}.$$

Como a é um gerador de $\mathbb{F}^*_{q^{2r}}$ e $k = \frac{q^{2r}-1}{(q^r+1)(q-1)} = (q^{r-1} + \cdots + q + 1)$, vemos que todos os pontos de O_i satisfazem $M_i(y)$. Além disso, dado $P_{\ell,j} = (a^{t_\ell+jk}, a^{l_\ell+jk(q^r+1)}) \in O_\ell$, com $\ell \neq i$, como $a^{l_\ell} \neq a^{l_i}$, com $1 \leq l_\ell, l_i \leq q^{2r} - 1$, e a é um gerador de $\mathbb{F}^*_{q^{2r}}$, segue que $a^{l_\ell(q-1)} \neq a^{l_i(q-1)}$ e que $M_i(y)$ é constante quando restrita à órbita O_ℓ, se $\ell \neq i$. De forma semelhante se trata o caso em que $i = q(q^{r-1} + \cdots + q) + 1$. □

Proposição 3.0.3. *Para $1 \leq i \leq q(q^{r-1} + \cdots + q)$ e $0 \leq j \leq (q^r+1)(q-1)-1$, a função:*

$$B_{i,j}(x, y); = \prod_{s=1}^{q-2}(y - a^{l_i+k(q^r+1)(j+s)}) \prod_{s=1}^{(q^r+1)-1}(x - a^{t_i+k(j+s)}),$$

se anula em todos os pontos das órbitas O_i tais que $a_i^t \neq 0$, com exceção do ponto $P_{i,j}$. De forma semelhante, as funções:

$$B_{i,j}(x, y); = \prod_{s=1}^{q-2}(y - a^{l_i+k(q^r+1)(j+s)}),$$

se anulam em todos os pontos da órbita O_i tal que $a^{t_i} = 0$ com exceção do ponto $P_{i,j}$.

Demonstração. A demonstração deste assunto é consequência da construção de cada uma das órbitas O_i. □

Consideremos agora o código $C := C(\delta, D, mP_\infty)$ onde $D := \sum P_{i,j}$ é o divisor gerado pela soma formal dos pontos racionais da curva, fora do ponto no infinito. O objetivo agora é construir o diagrama de raízes do código C associado a esta curva.

Observação 3.0.4. Como $(x)_\infty = qP_\infty$ e $(y)_\infty = (q^r+1)P_\infty$, concluímos que:

• Para cada $i \in \{1, \ldots, q(q^{r-1} + \cdots + q) + 1\}$ vale $(M_i(y))_\infty = (q-1)(q^r+1)P_\infty$, ou seja, $M_i(y) \in L((q-1)(q^r+1)P_\infty)$;

• Para cada $1 \leq i \leq q(q^{r-1}+\cdots+q)$ e $0 \leq j \leq (q^r+1)(q-1)-1$ vale $(B_{i,j}(x,y))_\infty = ((q-2)(q^r+1)+q((q^r+1)-1))P_\infty$, ou seja, $B_{i,j} \in L(((q-2)(q^r+1)+q((q^r+1)-1))P_\infty)$;

• Para $i = q(q^{r-1}+\cdots+q)+1$ e $0 \leq j \leq q-2$ vale $(B_{i,j}(x,y))_\infty = (q-2)(q^r+1)P_\infty$, ou seja, $B_{i,j}(x,y)) \in L((q-2)(q^r+1)P_\infty)$.

Os resultados a seguir nos dão uma descrição completa do diagrama de raízes de um código pontual sobre a curva δ.

Teorema 3.0.5. *(Construção do diagrama de raízes: primeira parte.)*
Seja $\mathcal{R}_C$ o diagrama de raízes do código pontual $C = C(D, mP_\infty)$. Fixamos uma órbita i com $i = 1, \ldots, q(q^{r-1} + \cdots + q) + 1$. Se:

$$m \geq (i-1)(q-1)(q^r+1),$$

a i-ésima linha do diagrama não é completamente preenchida, ou seja, não tem marca X em cada caixa da linha.
Se:

$$m \geq (i-1)(q-1)(q^r+1) + (q-2)(q^r+1) + q((q^r+1)-1),$$

a i-ésima linha do diagrama é completamente vazia.

Demonstração. Seja $C = C(D, mP_\infty)$ um código pontual construído sobre a curva δ e seja $\mathcal{G} = \{g_1(t), \ldots, g_{q(q^{r-1}+\cdots+q)+2}(t)\}$ uma base de Gröbner para $\overline{C}$. Para $i \in \{1, \ldots, q(q^{r-1} + \cdots + q) + 1\}$, considere $F_i(y) := M_1(y) \cdots M_{i-1}(y)$. Pela Observação 3.0.4, segue que $F_i(y) \in L((i-1)(q-1)(q^r+1)P_\infty)$. Logo, se $m \geq (i-1)(q-1)(q^r+1)$ temos que $F_i \in L(mP_\infty)$ e, portanto, $ev(F_i) := (F_i(P_{1,0}), \ldots, F_i(P_{\theta,|O_\theta|-1})) \in C$.

Nos pontos racionais das primeiras $i-1$ órbitas a função F_i se anula, então C' contém um elemento da forma $(0, \ldots, 0, h_i(t), \ldots, h_\theta(t))$ onde θ e o número das órbitas e $h_i(t) = \sum_{j=0}^{|O_i|-1} F_i(P_{i,j})t^j$.

Sendo cada $M_k(P_{i,j})$ constante para cada $0 < k < i$, então $F_i(P_{i,j}) = c \neq 0$ constante, portanto $h_i(t) = c \cdot \sum_{j=0}^{|O_i|-1} t^j$ e então $h(1) \neq 0$ pois a cardinalidade da órbita não é múltipla da caraterística do corpo.

Por definição de base de Gröbner, e já que temos uma base diagonal, o elemento $g_i^i(t)$ divide $h_i(t)$ mas $g_i^i(1) \neq 0$ então a raiz 1 de $t^{|O_i|} - 1$ não está em $g_i^i(t)$ e então a linha não está completamente preenchida.

Agora, suponhamos que $m \geq (i-1)(q-1)(q^r+1) + (q-2)(q^r+1) + q((q^r+1)-1)$ e se considere a função $F_i'(x,y) = B_{i,0}(x,y)F_i(y)$. Novamente, pela Observação 3.0.4, segue que $F_i'(x,y) \in L(mP_\infty)$ e, portanto, $ev(F_i) \in C$.

Nota-se que $F_i'(P) = 0$ nas primeiras $i-1$ órbitas e também na i-ésima órbita, fora do ponto $P_{i,0}$ que é constante (digamos $F_i'(P_{i,0}) = c$). Então C' contém o elemento $(0, \ldots, 0, c, h_{i+1}(t), \ldots, h_\theta(t))$. Exatamente como antes, o elemento da base de Gröbner $g_i^i(t)|c$, ou seja, é constante, e então não contém nenhuma das raízes de $t^{|O_i|} - 1$, e então a linha é completamente vazia. □

Para completar o diagrama precisamos do resultado (2.9.3)

Teorema 3.0.6. *(Construção do diagrama de raízes, segunda parte)*
Seja $\mathcal{R}_C$ o diagrama de raízes do código $C = C(D, mP_\infty)$ sobre a curva δ. Se existe $i \in \{1, \ldots, q(q^{r-1} + \cdots + q)\}$, tal que:

$$(i-1)(q-1)(q^r+1) \leq m < (i-1)(q-1)(q^r+1) + (q-2)(q^r+1) + q((q^r+1)-1),$$

então a i-ésima linha de $\mathcal{R}_C$ não é totalmente preenchida nem vazia e os lugares que não serão marcados na linha i correspondem às raízes no conjunto

$$E_i = \{\alpha^{-k_i(\beta+\delta(q^r+1))} \in \mathbb{F}_{q^{2r}}^* \mid 0 \leq \beta \leq (q^r+1)(q-1)-1,$$
$$0 \leq \delta \leq q-2,\ (i-1)(q-1)(q^r+1)+\beta q+\delta(q^r+1) \leq m\},$$

onde $k_i = \frac{q^{2r}-1}{|O_i|}$

Demonstração. Seja D_i o conjunto de raízes que não estão marcadas na linha i de $\mathcal{R}_C$. Vejamos que $D_i = E_i$.

Considere a função $f_i(x,y) = F_i(y)x^\beta y^\gamma$, onde $F_i(y)$ é a mesma de antes. Temos que $f_i(x,y) \in L(mQ)$ dada as condições de β e de δ. Associada a $f_i(x,y)$ conseguimos um elemento $h = (h_1(t), \ldots, h_{q(q^{r-1}+\cdots+q)+2}(t)) \in \overline{C}$. Como $F_i(y)$ se anula em todos os pontos pertencentes a $O_1 \cup \ldots \cup O_{i-1}$, temos que $h_1(t) = \cdots = h_{i-1}(t) = 0$. Seja $P_{i,j} = \sigma(P_{i,0}) = (\alpha^{t_i+j}, \alpha^{l_i+j(q^r+1)}) \in O_i$.
Então, $f_i(P_{i,j}) = F_i(\alpha^{l_i+j(q^r+1)})\alpha^{\beta(t_i+k_i)}\alpha^{\gamma(l_i+j(q^r+1))}$. Agora, sabemos que $F_i(\alpha^{l_i+jk_i(q^r+1)})$ é uma constante não nula independente de j. Daí, tomando $b_i = (F_i(\alpha^{l_i+j(q^r+1)})\alpha^{\beta t_i+\gamma l_i})^{k_i}$, que é não nulo, temos que $f_i(P_{i,j})^{k_i} = b_i\alpha^{jk_i(\beta+\gamma(q^r+1))}$.

Logo, $h_i(t) = \sum_{j=0}^{(q^r+1)(q-1)-1} f_i(P_{i,j})t^j = [(q^r+1)(q-1)-1]b_i \sum_{j=0}^{(q^r+1)(q-1)-1} (\alpha^{j(\beta+\gamma(q^r+1))}t)^j$ cujas raízes são todas diferentes de $\alpha^{-jk_i(\beta+\gamma(q^r+1))}$. Consequentemente, $\alpha^{-jk_i(\beta+\gamma(q^r+1))}$ também não serão raízes de $g_i^{(i)}(t)$ implicando que as mesmas não serão marcadas na linha i de $\mathcal{R}_C$. Logo, $E_i \subset D_i$.

Agora, pela Proposição 2.9.3, sabemos que $\dim(C) = \sum \sharp D_i$. Em [18] foi calculado que o semigrupo de Weierstrass da curva δ em P_∞ é $H(P_\infty) = \langle q, q^r+1\rangle$ e então $\dim(C) = \sharp\{(\beta,\gamma) \in \mathbb{N}^2 \ ; \ 0 \leq \beta \leq (q^r+1)-1 \text{ and } \beta q+\gamma(q^r+1) \leq m\}$.

Seja $\widehat{E}_i = \{(\beta,\gamma) \in \mathbb{N}^2 \mid 0 \leq \beta \leq (q^r+1)-1, 0 \leq \gamma \leq q-2,\ (i-1)(q-1)(q^r+1)+\beta q+\gamma(q^r+1) \leq m\}$. Assim, $\sharp\{(\beta,\gamma) \in \mathbb{N}^2 \ ; \ 0 \leq \beta \leq (q^r+1)-1 \text{ and } \beta q+\gamma(q^r+1) \leq m\} = \sum \sharp\widehat{E}_i$ e, como $\sum \sharp\widehat{E}_i = \sharp \sum E_i$, segue que $\sum \sharp D_i = \sum \sharp E_i$. Portanto, $E_i = D_i$

□

Para $1 \leq i \leq q(q^{r-1}+\cdots+q)$ considere o ideal $I(O_i) = \{f(x,y) \in \mathbb{F}_{q^{2r}}[x,y] \ :$

$f(P_{i,j}) = 0$ for all $P_{i,j} \in O_i\}$ e o anel $\mathbb{F}_{q^{2r}}[x,y]/I(O_i)$ (para as duas outras órbitas será análogo).

Lema 3.0.7. *Seja i tal que $1 \leq i \leq q(q^{r-1} + \cdots + q)$ e seja V_i o $\mathbb{F}_{q^{2r}}$-espaço gerado por $\left\{\prod_{j=1}^{i-1} M_j(y)x^\beta y^\gamma : 0 \leq \beta \leq (q^r+1)-1 \text{ e } 0 \leq \gamma \leq q-2\right\}$. Então:*
(1) *A projeção natural $V_i \to \mathbb{F}_{q^r}[x,y]/I(O_i)$ é um isomorfismo de $\mathbb{F}_{q^{2r}}$-espaços vetoriais;*
(2) *Para quaisquer $a_0, \ldots, a_{(q^r+1)(q-1)-1} \in \mathbb{F}_{q^r}$, existe um único $\widehat{f}(x,y) \in V_i$ satisfazendo $\widehat{f}(P_{i,j}) = a_j$, para todo j e $f(R) = 0$ para todo $R \in O_1 \cup \ldots \cup O_{i-1}$.*

Demonstração. Para $1 \leq i \leq q(q^{r-1} + \cdots + q)$, a órbita O_i possui $(q^r+1)(q-1)$ distintos valores na coordenada x. Além disso, na órbita O_i tem-se a relação $y = a^{l_i - t_i(q^r+1)}x^{q^r+1}$. Considere o homomorfismo $\varphi_i : \mathbb{F}_{q^{2r}}[x,y] \to \mathbb{F}_{q^{2r}}[x]/\langle x^{(q^r+1)(q-1)} - 1\rangle$ dado por $\varphi_i(f(x,y)) = \overline{f(x, a^{l_i - t_i(q^r+1)}x^{q^r+1})}$, para cada $f(x,y) \in \mathbb{F}_{q^{2r}}[x,y]$. Então, pelo Teorema de isomorfismo $\mathbb{F}_{q^{2r}}[x,y]/I(O_i) \simeq \mathbb{F}_{q^{2r}}[x]/\langle x^{(q^r+1)(q-1)} - 1\rangle$. Logo, $\mathbb{F}_{q^{2r}}[x,y]/I(O_i)$ é um espaço de dimensão $(q^r+1)(q-1)$.

Agora, considere a aplicação $\phi_i : V_i \to \mathbb{F}_{q^{2r}}[x,y]/I(O_i)$ dada por $\phi_i(f(x,y)) = f(x, a^{l_i - t_i(q^r+1)}x^{q^r+1})$, para cada $f(x,y) \in V_i$. Como foi visto antes, temos que, para $1 \leq j \leq i-1$, cada $M_j(y)$ é uma constante não nula quando for calculada nos pontos de O_i. Daí, temos que:

$$\phi_i\left(\prod_{j=1}^{i-1} M_j(y)x^\beta y^\gamma\right) = c \cdot x^{\beta + \gamma(q^r+1)}, \text{ para algum } c \in \mathbb{F}_{q^{2r}}^*.$$

Como $0 \leq \beta \leq (q^r+1)-1$ e $0 \leq \gamma \leq q-2$, obtemos múltiplos não nulos de x^λ, para cada $\lambda = 0, 1, \ldots, (q^r+1)(q-1)-2$. Logo, ϕ_i é sobrejetiva e, como V_i e $\mathbb{F}_{q^{2r}}[x,y]/I(O_i)$ tem a mesma dimensão, segue que ϕ_i é um isomorfismo, mostrando **(1)**.

Para mostrar **(2)**, usando interpolação de Lagrange, conseguimos $F(x) \in \mathbb{F}_{q^{2r}}[x]/\langle x^{(q^r+1)(q-1)} - 1\rangle \simeq \mathbb{F}_{q^{2r}}[x,y]/I(O_i)$ que resolve o problema de interpolação sobre os pontos de O_i. Portanto como ϕ_i é um isomorfismo, tomando $f(x,y) = \phi_i^{-1}(F(x)) \in V_i$ o resultado segue, já que $f(x,y)$ se anula nas órbitas $O_1, \ldots, O_{i-1}$.

□

Agora mostramos uma aplicação importante do diagrama de raízes, em particular

mostraremos um Teorema que permite a construção de uma base de Gröbner para o módulo $\overline{C}$.

Teorema 3.0.8. *Com as notações precedentes, consideremos o código $C(D, mP_\infty)$. Fixando um índice i com $1 \leq i \leq q(q^{r-1} + \cdots + q)$, sejam $a^{s_1}, \ldots, a^{s_l}$ as raízes marcadas na i-ésima linha do diagrama $\mathcal{R}_C$. Consideremos o polinômio:*

$$p(t) := \prod_{k=1}^{l}(t - a^{s_k}) = \sum_{j=0}^{|O_i|-1} a_j t^j,$$

e as funções

$$f_i(x, y) := F_i(y) \left(\sum_{j=0}^{|O_i|} a_j \frac{B_{i,j}(x, y)}{B_{i,j}(P_{i,j})} \right),$$

então $f_i \in L(mP_\infty)$ e o elemento $\mathbf{g}$ do módulo associado tem $i-1$ componente nulas e a i-ésima componente é $g_i(t) = p(t)$.

Demonstração. Para a observação 3.0.4 e o Teorema 3.0.5 temos que $f_i(x, y) \in L(mP_\infty)$. Agora, sendo que $f_i(P_{i,j}) = a_j$ se $j = 0, 1, \ldots, |O_i| - 1$ e $f_i(R) = 0$ se $R \in O_k$ com $k = 1, \ldots, i-1$ isso resolve o problema de interpolação de Lagrange, e em particular esta solução é única. Então o elemento $\mathbf{g} = (g_1(t), \ldots, g_r(t)) \in \overline{C}$ onde:

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

verifica o Teorema já que por construção temos que $g_1(t) = \cdots = g_{i-1}(t) = 0$ e $g_i(t) = p_t$. □

Agora podemos construir a base de Gröbner, com um algoritmo análogo ao de Little et al. em[13].

No algoritmo considere-se:

- *Rootdiagram*$[i]$ o procedimento que fornece uma lista de raízes em correspondência às caixas marcadas na i-ésima linha do diagrama $\mathcal{R}_C$;

- *Boxes*$[i]$ o procedimento que fornece o número de caixas da i-ésima linha, ou seja, o comprimento da órbita O_i;

- $Evaluate[i, point]$ o procedimento que pega como entrada os coeficientes $\{a_k\}$ do único polinômio mônico sobre $\mathbb{F}_{q^{2r}}$ como no Teorema 3.0.8 e fornece o valor da função $f_i(x, y)$ do mesmo Teorema no ponto $P_{i,j}$.

Algoritmo 3: O algoritmo para achar a base de Gröbner do módulo $\overline{C}$ associado ao código C construído sobre a curva de Kondo

Entrada: $\mathcal{R}_C$, os pontos racionais $P_{i,j}$ do supp(D)

Saída: a base de Gröbner G

início

$G := \{\}$;

para $i = 1$ *até* $q(q^{r-1} + \cdots + q) + 2$ **faça**

se $|Rootdiagram[i]| < Boxes[i]$ **então**

para $k = 1$ *até* $q(q^{r-1} + \cdots + q) + 2$ **faça**

$g_k^{(i)} := 0$;

se $k \geq 1$ **então**

para $j = 0$ *até* $Boxes[k] - 1$ **faça**

$g_k^{(i)} := g_k^{(i)} + Evaluate[i, P_{k,j}]t^j \mathbf{e}_k$

fim

fim

fim

fim

senão

$\mathbf{g^i} := (t^{Boxes[i]} - 1)\mathbf{e}_i$

fim

$G := G \cup \{\mathbf{g}^{(i)}\}$

fim

retorna G

fim

O algoritmo tem uma complexidade menor que o algoritmo para de Buchberger para o cálculo de uma base de Gröbner. De fato, este algoritmo utiliza somente ferramentas de problemas de interpolação e de evaluação de funções. Em particular, não utiliza divisões nem reduções de polinômios que, de fato, são as operações que aumentam

a complexidade do algoritmo (por mais detalhes: [14], pp.305-307).

Exemplo 3.0.9. Vamos agora fazer um exemplo para construir o diagrama de raízes associado a um código.

O exemplo de diagrama de raízes da curva de Kondo com parâmetros menores tem $q = r = 3$ já que por hipótese r tem que ser ímpar, mas por $r = 1$ trata-se dos diagramas de raízes da curva Hermitiana já estudados em [14].

Além disso, no caso $q = 2$ o automorfismo seria, na segunda coordenada $y \to a^{k(2^r+1)}$ com $a^{(2^r+1)(2-1)} = 1 = a^{k(2^r+1)}$ ou seja, o automorfismo seria o automorfismo identidade na indeterminada y e portanto o estudo das funções $M_i(y)$ não seria interessante.

Fixados estes parâmetros, consideremos o código $C(\delta, D, 2250P_\infty)$, em $\mathbb{F}_{729}$ sobre a curva $\delta : x^{28} = y^3 + y$. Escolheu-se o número 2250 para mostrar um diagrama de raízes que tivesse todos os casos distintos do Teorema (3.0.6).

Consideremos o automorfismo:

$$\sigma : \begin{array}{rcl} x & \to & a^{13}x \\ y & \to & a^{364}y \end{array} .$$

Este automorfismo divide os $3^7 = 2187$ pontos racionais em 41 órbitas, em particular:

Uma órbita de comprimento 1 $(0, 0)$;

Uma órbita de comprimento 2 $(0, A^{182}), (0, A^{546})$;

39 órbitas de comprimento 56, conforme a Apêndice.

Além disso, notamos que as raízes de $t^2 - 1$ são $1 = a^0$ e a^{364}, enquanto as raízes de $t^{56} - 1$ são as potências de a^{13}, conforme o diagrama que segue.

Sendo que $109 + 56(i - 1) < 2150$ para cada $i \leq 37$ as primeiras 37 linhas estão vazias.

Analogamente, sendo que $2150 < 56(i - 1)$ é verificado para cada $i \geq 39$ as únicas linhas completamente preenchidas são aquelas das órbitas com primeira coordenada nula.

- Na linha 39 as raízes que NÃO SÃO marcadas são aquelas que respeitam as

condições $0 \geq \delta \geq 1$, $0 \geq \beta \geq 55$ e enfim $2128 + 3\beta + 28\delta \leq 2250$:

- se $\delta = 0$ então $3\beta \leq 122 \Rightarrow \beta \leq 40$;
- se $\delta = 1$ então $3\beta \leq 94 \Rightarrow \beta \leq 31$.

Então as raízes marcadas são aquelas nos diagramas seguintes:

(δ, β)	$(0, 41)$	$(0, 42)$	$\cdots$	$(0, 55)$
raiz marcada (teorema)	a^{-533}	a^{-546}	$\cdots$	a^{-715}
raiz inversa	$a^{195} = a^{13 \cdot 15}$	$a^{182} = a^{13 \cdot 14}$	$\cdots$	a^{13}

(δ, β)	$(1, 32)$	$(1, 33)$	$\cdots$	$(1, 55)$
raiz marcada (teorema)	a^{-780}	a^{-793}	$\cdots$	a^{-1079}
raiz inversa	$a^{676} = a^{13 \cdot 52}$	$a^{663} = a^{13 \cdot 51}$	$\cdots$	$a^{13 \cdot 29}$

- Na linha 38, analogamente, as raízes que não são marcadas são aquelas que respeitam as condições de β e δ de antes, mais a condição $2072 + 3\beta + 28\delta \leq 2250$;
  - se $\delta = 0$ então $3\beta \leq 178$ que é sempre verificado no intervalo de β;
  - se $\delta = 1$ então $3\beta \leq 150 \Rightarrow \beta \leq 50$.

  Então as raízes que estão marcadas são aquelas no diagrama seguinte:

(δ, β)	$(1, 51)$	$(1, 52)$	$(1, 53)$	$(1, 54)$	$(1, 55)$
raiz marcada (teorema)	a^{-1027}	a^{-1040}	a^{-1053}	a^{-1066}	a^{-1079}
raiz inversa	$a^{429} = a^{13 \cdot 33}$	$a^{13 \cdot 32}$	$a^{13 \cdot 31}$	$a^{13 \cdot 30}$	$a^{13 \cdot 29}$

Então isso fornece o seguinte diagrama de raízes. Na primeira coluna do diagrama o número k significa $a^{13 \cdot k}$.

Por motivos de espaço as órbitas desde 1 até 37 são colocadas como uma única órbita, já que estão vazias.

De forma análoga, as caixas da órbita 38 estão vazias em correspondência de $k = 16, \ldots, 28$ assim como as caixas da órbita 39 estão marcadas em correspondência dos mesmos valores de k.

Tabela 3.1: Diagrama de raízes da curva δ

	órbitas 1-37	órbita 38	órbita 39	órbita de ordem 2	órbita de ordem 1
0				X	X
1			X		
2			X		
3			X		
4			X		
5			X		
6			X		
7			X		
8			X		
9			X		
10			X		
11			X		
12			X		
13			X		
14			X		
15			X		
...					
28				X	
29		X	X		
30		X	X		
31		X	X		
32		X	X		
33		X	X		
34			X		
35			X		
36			X		
37			X		
38			X		
39			X		
40			X		
41			X		
42			X		
43			X		
44			X		
45			X		
46			X		
47			X		
48			X		
49			X		
50			X		
51			X		
52			X		
53					
54					
55					

4 O DIAGRAMA DE RAÍZES DE ALGUNS QUOCIENTES DA CURVA HERMITIANA

Consideremos $\mathbb{F}_{q^2}$ o corpo finito com q^2 elementos, para q uma potência de um primo ímpar. Os quocientes afins ϵ da curva Hermitiana estão definidos em [17] pelo modelo plano:

$$y^q + y = x^m, \tag{4.1}$$

onde m é um inteiro positivo tal que $m > 2, \quad m|(q+1)$. O artigo mostra também que, fixado m, a curva ϵ é maximal e portanto tem $q(m(q-1)+1)+1$ pontos racionais.

Seja α um gerador do conjunto de unidades de $\mathbb{F}_{q^2}$ e seja k tal que $mk = q+1$. A função:

$$\sigma : \begin{array}{rcl} x & \to & \alpha^k x \\ y & \to & \alpha^{q+1} y \end{array},$$

define um automorfismo sobre a curva ϵ de ordem $m(q-1)$ que gera uma partição sobre o conjunto dos pontos racionais em órbitas da forma seguinte:

Proposição 4.0.1. *O automorfismo σ decompõe os pontos racionais afins da curva ϵ em $q+2$ órbitas disjuntas $O_1, \ldots, O_q, O_{q+1}, O_{q+2}$, tal que*

- $O_{q+2} = \{P_{q+2,0} := (0,0)\}$;
- *A órbita* $O_{q+1} = \{(0,y) \mid y^q + y = 0,\ y \neq 0\}$ *tem comprimento* $q-1$;

- *Para $1 \leq i \leq q$ a órbita O_i tem comprimento $(q-1)m$.*

Demonstração. Dado que o polinômio $y^q + y = 0$ tem derivada igual a zero, logo tem q raízes distintas. Se $\beta_{q+1} \neq 0$ é uma raiz, seja $\beta_{l,q+1} = \alpha^{l(q+1)}\beta_{q+1}$, então se $r \neq l, \quad \beta_{l,q+1} \neq \beta_{r,q+1}$, e também :

$$\begin{aligned}\beta_{l,q+1}^q + \beta_{l,q+1} &= (\alpha^{l(q+1)}\beta_{q+1})^q + \beta^{l(q+1)}\beta_{q+1} = (\alpha^q)^{l(q+1)}\beta_{q+1}^q + \alpha^{l(q+1)}\beta_{q+1} \\ &= \alpha^{l(q+1)}(\beta_{q+1}^q + \beta_{q+1}) = 0.\end{aligned}$$

Portanto, a órbita de $(0, \beta_{q+1})$ pelo automorfismo σ consta dos pontos:

$$O_{q+1} = \{P_{i,q+1} = (0, \beta_{l,q+1}) \mid l = 0, \ldots, q-2\},$$

e é claro que $|O_{q+1}| = q - 1$.

Para encontrar as órbitas restantes, fixamos $x = 1$, e estudamos as raízes do polinômio $y^q + y = 1$.

Se α, como antes, é um elemento gerador das unidades de $\mathbb{F}_{q^2}$, então o elemento:

$$\beta := \tfrac{1}{2}(1 + \alpha - \alpha^q),$$

satisfaz:

$$\beta - \beta^q = \alpha - \alpha^q, \qquad \beta + \beta^q = 1.$$

Portanto $(1, \beta) \in \epsilon$, e a primeira identidade conclui que $\beta \notin \mathbb{F}_q$ (pois de outro modo $\alpha^q = \alpha$ o que contradiz que α é gerador).

Observa-se também que o único elemento em $\mathbb{F}_q \subset \mathbb{F}_{q^2}$ que é raiz do polinômio $y^q + y = 1$ é $y = \frac{1}{2}$; portanto para $i = 1, \ldots, q$ tomando $\beta_i = i\beta - (i-1)\frac{1}{2}$, segue-se que $(1, \beta_i) \in \epsilon$. Logo,

$$\begin{aligned}\beta_i^q + \beta_i &= \big(i\beta - (i-1)\tfrac{1}{2}\big)^q + \big(i\beta - (i-1)\tfrac{1}{2}\big) = \big(i^q\beta^q - (i-1)^q\tfrac{1}{2}^q\big) + \big(i\beta - (i-1)\tfrac{1}{2}\big) \\ &= i(\beta^q + \beta) - (i-1) = i - (i-1) = 1.\end{aligned}$$

Além disso, $\beta_i \neq \beta_j$ se $j \neq j$, pois $\beta \notin \mathbb{F}_q$. Seja O_i a órbita de $(1, \beta_i)$ sobre σ. Examinando a componente x, cada órbita tem comprimento $m(q-1)$, e as órbitas

$O_1, \ldots, O_q$ são disjuntas dois a dois, mais concretamente:

$$O_i = \{P_{i,j} = (\alpha^{jk}, \alpha^{j(q+1)}\beta_i) \mid j = 0, \ldots, m(q-1) - 1\}.$$

□

Nota-se que se $(a, b), (\tilde{a}, b) \in \epsilon$, então $(a, b), (\tilde{a}, b)$ estão na mesma órbita. Logo, se $b = 0$, então $a = \tilde{a} = 0$.

Se $b \neq 0$ é fixado, seja $c = b^q + b$. Em [17] mostra-se que o polinômio $x^m - c = 0$ tem m raízes (possivelmente repetidas).

Seja x_0 uma raiz, o elemento $x_j = \alpha^{jk(q-1)}x_0$, satisfaz $x_j^m - c = 0$, e para $i \neq j$, com $i, j = 0, \ldots, m-1$, tem-se que $x_i \neq x_j$.

Portanto $x_0, x_1, \ldots, x_{m-1}$ são todas as raízes de $x^m - c = 0$, logo:

$$\sigma^{j(q-1)}(x_0, y) = (\alpha^{jk(q-1)}x_0, \alpha^{j(q-1)(q+1)}y) = (x_j, y).$$

Conservando a notação da prova do Teorema 4.0.1, definimos as funções:

$$M_i(y) := \prod_{\substack{y_i \in \mathbb{F}_{q^2} \\ (x, y_i) \in O_i}} (y - y_i) = \begin{cases} \prod_{r=0}^{q-2}(y - \alpha^{r(q+1)}\beta_i), & \text{Para } i = 1, \ldots, q+1 \\ y^{q-1} & \text{Para } i = q+2. \end{cases}$$

A função M_i é constante em cada órbita, pois para l os pontos de O_l tem a forma:

$$P_{l,j} = (p_{l,q+1}\ \alpha^{jk}, p_{l,q+2}\ \alpha^{j(q+1)}\beta_l),$$

onde $p_{l,r} = 0$ se $i \geq r$; e $p_{i,r} = 1$ se $i < r$ então

$$\begin{aligned} M_i(\alpha^{j(q+1)}\beta_l) &= \prod_{r=0}^{q-2}(\alpha^{l(q+1)}\beta_l - \alpha^{r(q+1)}\beta_i) = \left(\alpha^{j(q+1)}\right)^{(q-1)} \prod_{r=0}^{q-2}(\beta_l - \alpha^{(r-j)(q+1)}\beta_i) \\ &= \alpha^{j(q+1)(q-1)}M_i(\beta_l) = M_i(\beta_l). \end{aligned}$$

Além disso, se $i = l$ $M_i(\alpha^{j(q+1)}\beta_l) = 0$, pois um dos fatores torna-se zero.

A função

$$B_{i,j}(x,y) = \prod_{\substack{\delta \neq \alpha^{j(q+1)}\beta_i \\ (\alpha^{jk}, y_i) \in O_i}} (y - y_i) \prod_{\substack{x_j \neq p_{i,q+1}\alpha^{jk} \\ (x_j, \alpha^{j(q+1)}\beta_i) \in O_i}} (x - x_j)$$

$$= \begin{cases} \prod_{\substack{r=0 \\ r\neq j}}^{q-2} (y - \alpha^{r(q+1)}\beta_i) \prod_{\substack{r=0 \\ r\neq j}}^{m-1} (x - \alpha^{r(q-1)k}), & \text{Para } i=1,\ldots,q, \\ & j=0,\ldots,m-2 \\ \prod_{\substack{r=0 \\ r\neq j}}^{q-2} (y - \alpha^{r(q+1)}\beta_{q+1}) & \text{Para } i=q+1, \\ & j=0,\ldots,q-2 \end{cases}.$$

Satisfaz que $B_{i,j}(P_{i,r}) \neq 0$, se, e somente se,$j = r$, isto é, B se anula em todos os pontos da órbita i, menos no ponto $P_{i,j}$.

Considerando o ponto no infinito Q, em [17] prova-se que $(x)_Q = q,\ (y)_Q = m$.

Portanto $(M_i)_Q = (q-1)m$, para todo $i = 0 \ldots, q+1$, e também $(B_{i,j})_Q = (q-2)m + (m-1)q$ se $i \neq q+1$, enquanto $(B_{q+1,j})_Q = (q-2)m$.

Teorema 4.0.2. *(Construção do diagrama de raízes, primeira parte)*
Seja $\mathcal{R}_\mathcal{C}$ o diagrama de raízes correspondente ao código $C = C(\epsilon, D, NQ)$. Para $1 \leq i \leq q+1$ fixado, a linha i-ésima de $\mathcal{R}_\mathcal{C}$ satisfaz as seguintes condições:

- *Se $(i-1)(q-1)m \leq N$, a i-ésima linha não está totalmente preenchida.*
- *Se $i < q+1$, e, $(i-1)(q-1)m + (q-2)m + (m-1)q \leq N$, então a i-ésima linha é vazia.*
- *Se $i = q+1$, e, $q(q-1)m + (q-2)m \leq N$, então a i-ésima linha é vazia.*

Demonstração. Seja $F_i(x,y) = M_1(y)M_2(y)\cdots M_{i-1}(y)$, pela análise anterior:

$$(F_i)_Q = (i-1)(M_i)_Q = (i-1)(q-1)m,$$

de modo que se $(i-1)(q-1)m \leq N$, $(F_i)_Q \leq (NQ)_Q$, de modo que $F_i \in \mathcal{L}(NQ)$. e portanto o elemento:

$$ev(F_i) = (F_i(P_{1,0}), \ldots, F_i(P_{1,m(q-1)-1}), F_i(P_{2,0}), \ldots F_i(P_{q+1,q-2}), F_i(P_{q+2,0}))) \in C(\epsilon, D, NQ),$$

e $ev(F_i)$ tem uma projeção natural $h^{(i)} = (h_1^{(i)}(t), \ldots, h_{q+2}^{(i)}(t))$ sobre o módulo $\bar{C}$ onde cada polinômio está definido por:

$$h_s^{(i)}(t) = \sum_{j=0}^{|O_s|-1} F_i(P_{s,j})t^j.$$

Observa-se que a restrição de F_i à qualquer órbita é uma função constante, $F_i(P_{r,j}) = F_i(P_{r,0})$, de modo que:

$$h_s^{(i)}(t) = F_i(P_{s,0}) \sum_{j=0}^{|O_s|-1} t^j.$$

Além disso, se $s < i,\ F_i(P_{s,0}) = 0$, logo $h_s^{(i)}(t) = 0$ e no caso $s = i$, dado que $F_i(P_{i,0}) \neq 0$ temos que $h_i^{(i)}(1) \neq 0$.

Portanto, $h^{(i)} = (0, \ldots, 0, h_i^{(i)}(t), \ldots, h_{q+2}^{(i)}(t))$ com $h_i^{(i)}(t) \neq 0$.

Tomando uma base de Gröbner triangular, que existe por quanto foi feito nas Seções 1.6 e 1.9 (utilizando a ordem POT), temos $\{\mathbf{g}^{(1)}, \ldots, \mathbf{g}^{(q+2)}\}$ para $\bar{C}$, e então:

$$\mathbf{g}_i^{(i)} | h_i^{(i)},$$

e, portanto, segue que $g_i^{(i)}(1) \neq 0$ e consequentemente a linha do diagrama de raízes não está completamente preenchida.

Agora, seja N tal que $(i-1)(q-1)m + (q-2)m + (m-1)q \leq N$, então $(F_i B_{i0})_Q = (i-1)(q-1)m + (q-2)m + (m-1)q$, logo $F_i B_{i0} \in L(NQ)$.

Seja:

$$f_s^{(i)}(t) := \sum_{j=0}^{|O_s|-1} F_i B_{i0}(P_{s,j}) t^j = \sum_{j=0}^{|O_s|-1} F_i(P_{s,j}) B_{i0}(P_{s,j}) t^j = F_i(P_{s,0}) \sum_{j=0}^{|O_s|-1} B_{i0}(P_{s,j}) t^j,$$

como antes.

Temos que $F_i(P_{s,0}) = 0$ e portanto $f_s^{(i)}(t) = 0$ se $s < i$; além disso,

$$f_i^{(i)}(t) = F_i(P_{i,0}) \sum_{r=0}^{|O_i|-1} B_{i0}(P_{i,j}) t^j,$$

e $B_{i0}(P_{i,j}) \neq 0$ se, e somente se,$j = 0$, então:

$$f_i^{(i)}(t) = F_i(P_{i,0}) B_{i0}(P_{i,0}) t^0 = F_i(P_{i,0}) \neq 0,$$

e enfim:

$$f^{(i)} = (0, \ldots, 0, F_i(P_{i,0}), f_{i+1}^{(i)}(t), \ldots, f_{q+2}^{(i)}(t)) \in \bar{C},$$

e $\mathbf{g}_i^{(i)} | f_i^{(i)} = F_i(P_{i,0})$ que é uma constante não nula, o qual implica que $\mathbf{g}_i^{(i)}$ é constante não nula, ou seja, não possui raízes. Portanto concluímos que a i-ésima linha é completamente vazia.

Os casos $i = q+1$ e $q(q-1)m + (q-2)m \leq N$, seguem por analogia. □

Teorema 4.0.3. *(Construção do diagrama de raízes, segunda parte)*
Seja $\mathcal{R}_\mathcal{C}$ o diagrama de raízes correspondente ao código $C = C(\epsilon, D, NQ)$.
Se existe $1 \leq i \leq q$ tal que:

$$(i-1)(q-1)m \leq N < (i-1)(q-1)m + (q-2)m + (m-1)q,$$

a i-ésima linha não é totalmente preenchida nem vazia e os lugares não marcados correspondem às raízes no conjunto:

$$E_i := \{\alpha^{-k:i(b+mc)} \mid 0 \leq b < m, \quad 0 \leq c < q-1, \quad (i-1)(q-1)m + cm + bq \leq N\},$$

onde $k_i = \frac{q^2-1}{|O_i|}$. No caso $i = q+1$, se $q(q-1)m \leq N < q(q-1)m+(q-2)m$, a $q+1$-ésima não é totalmente preenchida nem vazia e os lugares não marcados correspondem às raízes no conjunto:

$$E_{q+1} := \{\alpha^{-k_i mc} \mid 0 \leq c < q-1, \quad q(q-1)m + cm \leq N\},$$

onde $k_i = \frac{q^2-1}{|O_{q+1}|}$.

Demonstração. Seja D_i o conjunto de raízes que não estão marcadas no diagrama. Vamos mostrar que $D_i = E_i$.
Para $i < q+1$, dado que $(i-1)(q-1)m \leq N < (i-1)(q-1)m+(q-2)m+(m-1)q$ então a i-ésima linha não é totalmente preenchida nem é vazia. Tomando b, c que satisfazem as condições como no conjunto E_i, considerando-se a função:

$$\Gamma_i^{b,c}(x, y) := F_i(y)x^b y^c,$$

segue-se então que:

$$(\Gamma_i^{b,c})_Q = (i-1)(q-1)m + cm + bq,$$

de modo que $ev(\Gamma_i^{b,c}) \in C(\epsilon, D, NQ)$.
Observa-se que para $s < q+1$:

$$\Gamma_i^{b,c}(P_{s,j}) = F_i(P_{s,j}) = F_i(\alpha^{jk_i}, \alpha^{j(q+1)}\beta_s)\alpha^{bjk_i}\alpha^{cj(q+1)}\beta_s^c = F_i(1, \beta_s)\beta_s^c\alpha^{j(b+cm)k_i}.$$

Portanto, o elemento associado a $\Gamma_i^{b,c}$ em $\bar{C}$ é um vetor $(\tau_i^{b,c})$ de $q+2$ componentes, cuja s-ésima componente é o polinômio

$$(\tau_i^{b,c})_s(t) = \sum_{j=0}^{|O_s|-1} \Gamma_{q+1}^{b,c}(P_{s,j})t^j = \begin{cases} F_i(1,\beta_s)\beta_s^c \sum_{j=0}^{|O_s|-1} (\alpha^{k_i(b+cm)}t)^j, & \text{se } s < q+1 \\ F_i(0,\beta_{q+1})\beta_{q+1}^c \sum_{j=0}^{|O_{q+1}|-1} (\alpha^{k_i cm}t)^j, & \text{se } s = q+1,\ b=0 \\ F_i(0,0), & \text{se } s = q+2, b=0, c=0. \end{cases}$$

$$= \begin{cases} 0, & \text{se } s < i \\ F_i(1,\beta_{q+1})\beta_i^c|O_{q+1}| & \text{se } s = i < q+1. \\ F_{q+1}(0,\beta_{q+1})\beta_{q+1}^c|O_{q+1}| & \text{se } s = i = q+1,\ b=0 \end{cases} .$$

Podemos portanto ver que se $s < i$ temos $F_i(1,\beta_s) = 0$ e desta forma $(\tau_i^{b,c})_s(t) = 0$; o qual conclui que $\mathbf{g}_i^{(i)} | (\tau_i^{b,c})_i$.
Logo, as raízes de $\mathbf{g}_i^{(i)}$ são raízes também dos polinômios $(\tau_i^{b,c})_i$ para cada b, c e dado que:

$$(\tau_i^{b,c})_i(\alpha^{-k_i(b+mc)}) = F_i(1,\beta_s)\beta_s^c|O_s| \neq 0,$$

temos que $\alpha^{-k_i(b+mc)}$ não é raiz de $\mathbf{g}_i^{(i)}$, isto é, $\alpha^{-k(b+mc)}$ não está marcada.
Logo $E_i \subset D_i$.

Agora pela Proposição (2.9.3) sabemos que $\dim(C) = \sum \sharp D_i$ e sabemos também para quanto demonstrado em [17] que o semigrupo de Weierstrass da curva ϵ em P_∞ é gerado polos m e q, ou seja:

$$\dim(C) = \sharp\{(b,c) \in \mathbb{N}^2 \mid 0 \leq b \leq m-1 \ e \ bm + cq \leq N\}.$$

Portanto seja $E_i' = \{(b,c) \in \mathbb{N}^2 \mid 0 \leq b \leq m-1\ 0 \leq c \leq q-2,\ (i-1)(q-1)m + cm + bq \leq N\}$. Fica evidente que $\sharp\{(b,c) \in \mathbb{N}^2 \mid 0 \leq b \leq m-1 ebm + cq \leq N\} = \sum \sharp E_i'$. Mas como $\sharp \sum E'i = \sum \sharp E_i$ (por como definimos os E_i) e $\sharp \sum E_i' = \sum \sharp D_i$ (por quanto feito agora) temos que $\sum \sharp D_i = \sum \sharp E_i$, ou seja, $E_i = D_i$

Analogamente, se $i = q+1$, α^{-kmc} não é raiz de $(\tau_i^{0,c})_i$, logo também não será de $\mathbf{g}_{q+1}^{(q+1)}$ e portanto $\alpha^{-k(b+mc)}$ não está marcada.
Finalmente, se $s = q+2$, tomamos $(\tau_{q+2}^{0,0})_s(t) = F_{q+2}(0,0)$ que, como foi visto, é uma

constante não nula, logo $\mathbf{g}_{q+2}^{(q+2)}$ é uma constante nção nula, e portanto $\alpha^0 = 1$ não é raiz de $\mathbf{g}_{q+2}^{(q+2)}$ sempre que $(q+1)(q-1)m \leq N$ isto é, $\alpha^0 = 1$ não está marcada.
Logo $E_i \subset D_i$, e a outra inclusão é análoga à feita anteriormente.

□

Para $1 \leq i \leq q$ considere o ideal:

$$I(O_i) = \{f(x,y) \in \mathbb{F}_{q^2}[x,y] : f(P_{i,j}) = 0 \text{ para cada } P_{i,j} \in O_i\},$$

e o anel $\mathbb{F}_{q^2}[x,y]/I(O_i)$. (para as duas outras órbitas é análogo)

Lema 4.0.4. *Seja i tal que $1 \leq i \leq q$ e seja V_i o $\mathbb{F}_{q^2}$-espaço gerado por* $\left\{\prod_{j=1}^{i-1} M_j(y)x^\beta y^\gamma : 0 \leq b \leq m-1 \text{ e } 0 \leq c \leq q-2\right\}$.
Então:

(1) *A projeção natural $V_i \to \mathbb{F}_{q^2}[x,y]/I(O_i)$ é um isomorfismo de $\mathbb{F}_{q^2}$-espaços vetoriais;*
(2) *Para quaisquer $a_0, \ldots, a_{m(q-1)-1} \in \mathbb{F}_{q^2}$, existe um único $\widehat{f}(x,y) \in V_i$ satisfazendo $\widehat{f}(P_{i,j}) = a_j$, para todo j e $f(R) = 0$ para todo $R \in O_1 \cup \ldots \cup O_{i-1}$.*

Demonstração. Para as q órbitas de comprimento maior O_i temos $m(q-1)$ distintos valores na coordenada x. Além disso, na órbita O_i tem-se a relação $y = a^{l_i - t_i m}x^m$. Considere o homomorfismo $\varphi_i : \mathbb{F}_{q^2}[x,y] \to \mathbb{F}_{q^2}[x]/\langle x^{(m(q-1)} - 1\rangle$ dado por $\varphi_i(f(x,y)) = \overline{f(x, a^{l_i - t_i m}x^m)}$, para cada $f(x,y) \in \mathbb{F}_{q^2}[x,y]$. Então, pelo primeiro teorema do isomorfismo, segue que $\mathbb{F}_{q^2}[x,y]/I(O_i) \simeq \mathbb{F}_{q^2}[x]/\langle x^{m(q-1)} - 1\rangle$. Logo, $\mathbb{F}_{q^2}[x,y]/I(O_i)$ é um espaço de dimensção $(q+1)(q-1)$.

Agora, considere a aplicação $\phi_i : V_i \to \mathbb{F}_{q^{2r}}[x,y]/I(O_i)$ dada por $\phi_i(f(x,y)) = f(x, a^{l_i - t_i m}x^m)$, para cada $f(x,y) \in V_i$. Como visto antes sobre as funções $M_i(y)$ temos que, para $1 \leq j \leq i-1$, cada $M_j(y)$ é uma constante não nula quando for calculada nos pontos da órbita O_i. Daí, temos que

$$\phi_i\left(\prod_{j=1}^{i-1} M_j(y)x^b y^c\right) = c \cdot x^{b+cm}, \text{ para algum } c \in \mathbb{F}_{q^2}^*.$$

Como $0 \leq b \leq m-1$ e $0 \leq \gamma \leq q-2$, obtemos múltiplos não nulos de x^λ, para

cada $\lambda = 0, 1, \ldots, m(q-1)-2$. Logo, ϕ_i é sobrejetor e, como V_i e $\mathbb{F}_{q^2}[x,y]/I(O_i)$ tem a mesma dimensão, segue que ϕ_i é um isomorfismo, mostrando **(1)**.

Para mostrar **(2)**, usando interpolação de Lagrange, conseguimos um polinômio $F(x) \in \mathbb{F}_{q^{2r}}[x]/\langle x^{(q^r+1)(q-1)} - 1\rangle \simeq \mathbb{F}_{q^{2r}}[x,y]/I(O_i)$ interpola os pontos de O_i. Tomando portanto $f(x,y) = \phi_i^{-1}(F(x)) \in V_i$ o resultado segue, já que $f(x,y)$ se anula nas órbitas $O_1, \ldots, O_{i-1}$. □

Os últimos resultados desta parte tem o objetivo de achar uma base de Gröbner para o módulo C', com uma complexidade computacional menor que aquela do algoritmo de Buchberger.

Teorema 4.0.5. *Com as notações precedentes, consideramos o código $C(D, mP_\infty)$. Agora fixamos um índice i com $1 \leq i \leq q$, sejam $a^{s_1}, \ldots, a^{s_l}$ as raízes marcadas na i-ésima linha do diagrama $\mathcal{R}_C$. Consideremos o polinômio:*

$$p(t) := \prod_{k=1}^{l}(t - a^{s_k}) = \sum_{j=0}^{|O_i|-1} a_j t^j,$$

e as funções:

$$f_i(x,y) := F : i(y) \left(\sum_{j=0}^{|O_i|} a_j \frac{B_{i,j}(x,y)}{B_{i,j}(P_{i,j})} \right),$$

então $f_i \in L(mP_\infty)$ e o elemento $\mathbf{g}$ do módulo associado tem $i-1$ componente nulas e a i-ésima componente é $g_i(t) = p(t)$.

Demonstração. Para os cálculos feitos no Teorema 4.0.2 e no Teorema 4.0.3 temos que $f_i(x,y) \in L(mP_\infty)$. Agora a demonstração procede com o mesmo rumo daquela do Teorema 3.0.8, já que as escolhas feitas resolvem o problema de Lagrange $f_i(P_{i,j}) = a_j$ se $j = 0, 1, \ldots, |O_i| - 1$ e $f_i(R) = 0$ se $R \in O_k$ com $k = 1, \ldots, i-1$ e em particular esta solução é única. Então o elemento $\mathbf{g} = (g_1(t), \ldots, g_r(t)) \in \overline{C}$ onde:

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

verifica o Teorema já que por construção temos que $g_1(t) = \cdots = g_{i-1}(t) = 0$ e $g_i(t) = p_t$. □

O algoritmo para achar a base de Gröbner é o análogo ao algoritmo do Capítulo precedente.

No algoritmo consideramos

- $Rootdiagram[i]$: dá a lista de raízes em correspondência das caixas marcadas na i-ésima linha do diagrama $\mathcal{R}_C$;
- $Boxes[i]$: dá o comprimento da órbita O_i;
- $Evaluate[i, point]$: toma como entrada os coeficientes $\{a_k\}$ do único polinômio mónico sobre $\mathbb{F}_{q^2}$ dados no Teorema 4.0.5 e fornece a o valor da função $f_i(x, y)$ do mesmo teorema no ponto $P_{i,j}$.

Algoritmo 4: O algoritmo para achar a base de Gröbner do módulo $\overline{C}$ associado ao código C construído sobre os quocientes da curva Hermitiana

Entrada: $\mathcal{R}_C$, os pontos racionais $P_{i,j}$ do supp(D)

Saída: a base de Gröbner G

início

$G := \{\}$;

para $i = 1$ *até* q **faça**

se $|Rootdiagram[i]| < Boxes[i]$ **então**

para $k = 1$ *até* q **faça**

$g_k^{(i)} := 0$;

se $k \geq 1$ **então**

para $j = 0$ *até* $Boxes[k] - 1$ **faça**

$g_k^{(i)} := g_k^{(i)} + Evaluate[i, P_{k,j}]t^j\mathbf{e}_k$

fim

fim

fim

fim

senão

$\mathbf{g^i} := (t^{Boxes[i]} - 1)\mathbf{e}_i$

fim

$G := G \cup \{\mathbf{g}^{(i)}\}$

fim

retorna G

fim

Sobre a complexidade deste algoritmo, valem as mesmas considerações feitas para o algoritmo (3).

Exemplo 4.0.6. $(k = (5^2 - 1)/12 = 2, m = 3, q = 5)$ Em $\mathbb{F}_{25}$, a curva $y^5 + y = x^3$ tem um automorfismo:

$$\sigma(x.y) = (\alpha^2 x, \alpha^6 y)$$

que decompõe os pontos racionais em 5 órbitas de comprimento 12, uma órbita de

comprimento 4, e a órbita consistente do único elemento $(0, 0)$.

O diagrama de raízes está composta por 5 linhas de 12 caixas cada uma, seguida de uma linha de 4 caixas e uma linha com uma caixa.

Os polinômios que correspondem a cada órbita, entre os quais temos que encontrar as raízes, são $t^{12} - 1$, $t^4 - 1$, $t - 1$.

As raízes de $t^{12} - 1$, são todos os elementos da forma $\alpha^{2j},\ j = 0, \ldots, 11$, as raízes de $t^4 - 1$, são todos os elementos da forma $\alpha^{2j},\ j = 0, \ldots, 3$, e a raiz de $t - 1$ é $\alpha^0 = 1$.

Consideremos os espaços $C(\epsilon, D, NQ)$, para $60 \leq N \leq 67$.

Pelo Teorema 4.0.3, os diagramas de raízes são:

$$
\begin{aligned}
O_1 &:= \{(1,\alpha),(\alpha^2,\alpha^7),(\alpha^4,\alpha^{13}),(\alpha^6,\alpha^{19}),(\alpha^8,\alpha),(\alpha^{10},\alpha^7),(\alpha^{12},\alpha^{13}),(\alpha^{14},\alpha^{19}),\\
&\qquad (\alpha^{16},\alpha),(\alpha^{18},\alpha^7),(\alpha^{20},\alpha^{13}),(\alpha^{22},\alpha^{19})\},\\
O_2 &:= \{(1,\alpha^4),(\alpha^2,\alpha^{10}),(\alpha^4,\alpha^{16}),(\alpha^6,\alpha^{22}),(\alpha^8,\alpha^4),(\alpha^{10},\alpha^{10}),(\alpha^{12},\alpha^{16}),(\alpha^{14},\alpha^{22}),\\
&\qquad (\alpha^{16},\alpha^4),(\alpha^{18},\alpha^{10}),(\alpha^{20},\alpha^{16}),(\alpha^{22},\alpha^{22})\}\\
O_3 &:= \{(1,\alpha^{20}),(\alpha^2,\alpha^2),(\alpha^4,\alpha^8),(\alpha^6,\alpha^{14}),(\alpha^8,\alpha^{20}),(\alpha^{10},\alpha^2),(\alpha^{12},\alpha^8),(\alpha^{14},\alpha^{14}),\\
&\qquad (\alpha^{16},\alpha^{20}),(\alpha^{18},\alpha^2),(\alpha^{20},\alpha^8),(\alpha^{22},\alpha^{14})\}\\
O_4 &:= \{(1,\alpha^5),(\alpha^2,\alpha^{11}),(\alpha^4,\alpha^{17}),(\alpha^6,\alpha^{23}),(\alpha^8,\alpha^5),(\alpha^{10},\alpha^{11}),(\alpha^{12},\alpha^{17}),(\alpha^{14},\alpha^{23}),\\
&\qquad (\alpha^{16},\alpha^5),(\alpha^{18},\alpha^{11}),(\alpha^{20},\alpha^{17}),(\alpha^{22},\alpha^{23})\}\\
O_5 &:= \{(1,\alpha^{18}),(\alpha^2,1),(\alpha^4,\alpha^6),(\alpha^6,\alpha^{12}),(\alpha^8,\alpha^{18}),(\alpha^{10},1),(\alpha^{12},\alpha^6),(\alpha^{14},\alpha^{12}),\\
&\qquad (\alpha^{16},\alpha^{18}),(\alpha^{18},1),(\alpha^{20},\alpha^6),(\alpha^{22},\alpha^{12})\}\\
O_6 &:= \{(0,\alpha^3),(0,\alpha^9),(0,\alpha^{15}),(0,\alpha^{21})\}\\
O_7 &:= \{(0,0)\}
\end{aligned}
$$

60	0	2	4	6	8	10	12	14	16	18	20	22
1												
2												
3												
4												
5		X	X		X			X				
6				X			X			X		
7	X											

61	0	2	4	6	8	10	12	14	16	18	20	22
1												
2												
3												
4												
5		X	X		X							
6				X			X			x		
7	X											

62	0	2	4	6	8	10	12	14	16	18	20	22
1												
2												
3												
4												
5		X			X							
6				X			X			X		
7	X											

63	0	2	4	6	8	10	12	14	16	18	20	22
1												
2												
3												
4												
5		X			X							
6				X			X					
7	X											

64	0	2	4	6	8	10	12	14	16	18	20	22
1												
2												
3												
4												
5		X										
6				X			X					
7	X											

65	0	2	4	6	8	10	12	14	16	18	20	22
1												
2												
3												
4												
5		X										
6				X			X					
7	X											

66	0	2	4	6	8	10	12	14	16	18	20	22
1												
2												
3												
4												
5		X										
6				X								
7	X											

67	0	2	4	6	8	10	12	14	16	18	20	22
1												
2												
3												
4												
5												
6				X								
7	X											

Observa-se que pelo Teorema de Riemann-Roch, a $\dim(C) = \dim(L(NQ)) = N + 1 - g$, onde g é o gênero da curva ϵ; tem-se que $g = \frac{(m-1)(q-1)}{2}$ (ver por exemplo [17]), o qual coincide totalmente para todo N tomado em nosso exemplo.

5 CONCLUSÕES

Este trabalho foi feito depois de escolher as curvas de Kondo e alguns quocientes da curva Hermitiana e foi motivado pelos trabalhos [14] e [2].

A técnica de construir códigos sobre curvas algébricas é recente e sempre tenta-se construir códigos com parâmetros melhores.

Com as notações utilizadas sobre as curvas algébricas e sobre os códigos algébricos geométricos, sejam $D = P_1 + \cdots + P_n$ e $G = \sum m_i Q_i$ (e então o $deg(G) = \sum m_i$). Agora, se d é a distância do código e k a relativa dimensão, temos que $d \geq n - deg(G)$ e, pelo Teorema (2.3.4), $k \geq deg(G) + 1 - g$. Segue portanto que:

$$\frac{d}{n} + \frac{k}{n} \geq \frac{n+1-g}{n} = 1 + \frac{1}{n} - \frac{g}{n}.$$

A curva utilizada no trabalho [11] gera, pelo menos de um ponto de vista teórico, um código bom sendo $\frac{\text{genêro da curva}}{\text{número de pontos racionais}} = \frac{q^r(q-1)/2}{q^{2r+1}+1} \simeq 1/2q^r$ que é menor que o do código sobre a curva Hermitiana, que vale $\frac{q(q-1)/2}{q^3+1} \simeq 1/2q$.

Analogamente, no caso da curva estudada no artigo [17] temos que

$\frac{\text{gênero da curva}}{\text{número de pontos racionais}} = \frac{(m-1)(q-1)/2}{(q(m(q-1)+1)+1)} \simeq 1/2q$ que coincide com aquele do código sobre a curva Hermitiana.

Então de um ponto de vista teórico os dois códigos têm bons parâmetros, portanto faz sentido estudar estes códigos e em particular construir o diagrama de raízes deles.

Uma diferença substancial deste trabalho à respeito dos artigos [5] e [14] está na forma de fazer as contas. O Capítulo 2 mostra uma complexidade maior à respeito das demonstrações dos outros autores, já que no automorfismo em vez de considerar um α gerador do grupo multiplicativo do corpo finito, tivemos que escolher α de uma forma mais especifica, para ser garantida a existência do grupo de automorfismos.

Por outro lado, no Capítulo 3 achei uma forma de fazer as contas mais compacta que aquela presente nos trabalhos antecedentes, além de mostrar uma aplicação prática do Teorema de Riemann-Roch aos diagramas de raízes, no Exemplo 3.0.6.

O objetivo deste trabalho foi encontrar os diagramas de raízes de dois códigos e os motivos para os quais faz sentido estudar esses diagramas são principalmente três e de natureza prática.

O primeiro é notar que com a construção de um diagrama de raízes pode-se achar uma base de Gröbner com uma complexidade computacional menor que utilizando o algoritmo de Buchberger.

Vale a pena ressaltar que, para construir o diagrama de raízes, tivemos que supor a existência de uma base de Gröbner diagonal, garantida pelo artigo [13]. Porém, uma vez que temos o diagrama de raízes completamente construído, podemos encontrar computacionalmente uma base de Gröbner, com um tempo de cálculo inferior ao algoritmo de Buchberger, de forma análoga a que foi feito nos artigos [5] e [14].

O segundo motivo para o qual é interessante este trabalho é que, uma vez construída a base de Gröbner para o módulo associado ao código, podemos utilizar o algoritmo e toda a teoria do Capítulo 1 para poder codificar as palavras do código de forma algorítmica.

E terceiro, somente olhando os diagramas é possível dizer se dois códigos não são isomorfos.

Resumindo, o diagrama de raízes associado a um código é uma ferramenta muito útil quando se trabalha com códigos, enquanto permite achar uma base de Gröbner associada ao módulo do código e com essa se podem codificar as palavras do código.

Este trabalho abre também outras perspectivas de trabalho para quem quisesse estudar mais sobre este assunto, em particular na minha opinião, seria interessante se alguém tivesse interesse em tentar trabalhar (talvez juntos) sobre estas questões:

- Tentar construir códigos r-pontuais sobre a curva de Kondo;
- Se os códigos r-pontuais sobre a curva de Kondo tivessem bons parâmetros, seria possível tentar achar o diagrama de raízes associado a estes códigos;
- Tentar generalizar este trabalho para os códigos r-pontuais construídos no artigo [17] sobre alguns quocientes da curva Hermitiana;

- Implementar os algoritmos (3) e (4) para comparar o tempo de cálculo com o do algoritmo de Buchberger;

- Uma vez construída a base de Gröbner do módulo associado aos códigos, podem-se construir outros módulos utilizando as técnicas do livro [15], Seções 3.2, 3.3 e 3.5. Portanto, pode ser interessante construir estes módulos, estudar os parâmetros dos códigos associados, estudar a existência de uma curva associada a tais códigos, apenas para fazer alguns exemplos.

REFERÊNCIAS

[1] BUCHBERGER B., *Theoretical Basis for the Reduction of Polynomials to Canonical Forms*, ACM SIGSAM Bulletin, ACM. 10 (3): 19-29, 1976

[2] CARVALHO C., TORRES F., *On Goppa codes and Weierstrass gaps at several points*, Des. Codes Cryptogr. 35(2), 211-225, 2005

[3] COX D., LITTLE J., O'SHEA D., *Ideals, Varieties, and. Algorithms. An Introduction to Computational Algebraic. Geometry and Commutative Algebra*, Springer, 1992

[4] DUBÉ T. W., *The Structure of Polynomial Ideals and Gröbner Bases.* SIAM Journal on Computing. 19 (4): 750, 1990

[5] FARRAN J.I., MUNUERA C., TIZZIOTTI G., TORRES F., *Gröbner Basis for Norm-Trace codes*, J. Symbolic Comput. **48** 54-63. MR 2980466, 2013

[6] FULTON W., *Algebraic Curves: An Introduction to Algebraic Geometry*, Addison Wesley Publishing Company, 2008

[7] GARCIA A., STICHTENOTH H., *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound.* Inventiones Mathematicae, 121, 211-222, 1995.

[8] GIULIETTI M., *Appunti del Corso di Geometria Superiore, Elementi di Teoria delle Curve Algebriche*, 2010

[9] GOPPA V.D., *Algebraic-geometric codes*, Math.USSR-Izv.21, pp. 75-91, 1983

[10] GOPPA V.D., *Geometry and Codes*, Kluwer, 1988

[11] KONDO S., KATAGIRI T., OGIHARA T., *Automorphism Groups of One-Point codes from partitions the curve* $y^q + y = x^{q^r+1}$, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 47, NO. 6 (semptember 2001), pp. 2573-2579

[12] LIDL R., NIEDERREITER H., *Finite Fields*, Cambridge University Press, second edition, 1996

[13] LITTLE J., HEEGARD C., SAINTS K., *Systematic encoding via Gröbner bases for class of algebraic geometric Goppa codes,* IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 41, NO. 6 (1995), pp. 1752-1761

[14] LITTLE J., HEEGARD C., SAINTS K., *On the structure of Hermitian codes* Journal of Pure and Applied Algebra, 121, (1997), pp. 293-314

[15] KREUZER M., ROBBIANO L., *Computational commutative algebra vol.*1, Springer, 2000

[16] KREUZER M., ROBBIANO L., *Computational commutative algebra vol.*2, Springer, 2005

[17] MATTHEWS G. L., *Weierstrass Semigroups and Codes from a Quotient of the Hermitian Curve* Designs, Codes and Cryptography, Volume 37, Issue 3, pp 473-492

[18] SEPULVEDA A., TIZZIOTTI G., *Weierstrass Semigroup and Codes over the curve* $y^q + y = x^{q*r+1}$, AIMS Journals, submitted

[19] STICHTENOTH H., *Algebraic Function Fields and Codes*, Springer, second edition 2008

[20] TIERSMA H., *Remarks on codes from the Hermitian curve*, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-33, pp. 605-609, 1987

[21] TSFASMAN M.A., VLADUT S.G., ZINK T., *Modular curves, Shumura Curves and Goppa codes better than the Varshamov-Gilbert bound*, Math.Nachr., 109, p.21-28, 1982

[22] VAN LINT J.H., *Introduction to Coding Theory*, Springer, 1982

[23] WEIL A., *Numbers of solutions of equations in finite fields*, Bulletin of the American Mathematical Society, 55 (5): 497-508, 1949

[24] XING C.P., CHEN H., *Improvements on parameters of one-point AG codes from Hermitian codes*, IEEE Trans.Inform.Theory 48 no.2, 535-537, 2002

[25] ——, *A note on Hermitian codes over*$GF(q^2)$, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 34, pp. 1345-1348, 1988

APÊNDICE A–Cálculos

Aqui estão escritas completamente as órbitas da curva de Kondo do exemplo 2.0.10. O ponto (c, d) representa o ponto (a^c, a^d) onde a é um gerador do grupo cíclico das unidades.

Os cálculos foram feito com o calculador de MAGMA[1]. O código:

```
A<u,v> := AffineSpace(FiniteField(729),2);
f := u^28 - v^3-v;
C := Curve(A,f);
C;
```

é o código que define a curva on MAGMA:

```
Curve over GF(3^6) defined by
u^28 + 2*v^3 + 2*v
```

Utilizando a função

```
Points(C);
```

o calculador de MAGMA encontra todos os pontos racionais da curva.

O leitor interessado a repetir os cálculos seguintes para achar as órbitas da curva de Kondo do exemplo, pode implementar em um programa de cálculo algébrico o seguinte algoritmo:

[1] http://magma.maths.usyd.edu.au/calc/

Algoritmo 5: O algoritmo para achar as órbitas da curva de Kondo

Entrada: os pontos racionais $P_1, \ldots, P_n$ do supp(D), o automorfismo σ

Saída: As órbitas $O_1, \ldots, O_k$

início

  para $i = 1$ *até* n **faça**

    $O_i = \{\}$; **se** $P_i \notin O_1, \ldots, O_{i-1}$ **então**

      $O_i = \{P_i\}$; **para** $j = i$ *até* $P_{j+1} = P_i$ **faça**

        $P_{j+1} = \sigma(P_j)$;

        $O_i = O_i \cup P_{j+1}$;

      fim

    fim

    retorna $O_1, \ldots, O_k$

  fim

fim

O elenco completo das órbitas do exemplo 2.0.10 foi calculado com a ajuda do Prof. Oscar Márquez, que implementou um algoritmo análogo ao algoritmo (5) no computador: Órbita((0, 91), (26, 91), (52, 91), (78, 91), (104, 91), (130, 91), (156, 91), (182, 91), (208, 91), (234, 91), (260, 91), (286, 91), (312, 91), (338, 91), (364, 91), (390, 91), (416, 91), (442, 91), (468, 91), (494, 91), (520, 91), (546, 91), (572, 91), (598, 91), (624, 91), (650, 91), (676, 91), (702, 91), (13, 455), (39, 455), (65, 455), (91, 455), (117, 455), (143, 455), (169, 455), (195, 455), (221, 455), (247, 455), (273, 455), (299, 455), (325, 455), (351, 455), (377, 455), (403, 455), (429, 455), (455, 455), (481, 455), (507, 455), (533, 455), (559, 455), (585, 455), (611, 455), (637, 455), (663, 455), (689, 455), (715, 455)),

Órbita((0, 273), (26, 273), (52, 273), (78, 273), (104, 273), (130, 273), (156, 273), (182, 273), (208, 273), (234, 273), (260, 273), (286, 273), (312, 273), (338, 273), (364, 273), (390, 273), (416, 273), (442, 273), (468, 273), (494, 273), (520, 273), (546, 273), (572, 273), (598, 273), (624, 273), (650, 273), (676, 273), (702, 273), (13, 637), (39, 637), (65, 637), (91, 637), (117, 637), (143, 637), (169, 637), (195, 637), (221, 637), (247, 637), (273, 637), (299, 637), (325, 637), (351, 637), (377, 637), (403, 637), (429, 637), (455, 637), (481, 637), (507, 637), (533, 637), (559, 637), (585, 637), (611, 637), (637, 637), (663,

637), (689, 637), (715, 637)),

Órbita((13, 0), (39, 0), (65, 0), (91, 0), (117, 0), (143, 0), (169, 0), (195, 0), (221, 0), (247, 0), (273, 0), (299, 0), (325, 0), (351, 0), (377, 0), (403, 0), (429, 0), (455, 0), (481, 0), (507, 0), (533, 0), (559, 0), (585, 0), (611, 0), (637, 0), (663, 0), (689, 0), (715, 0), (0, 364), (26, 364), (52, 364), (78, 364), (104, 364), (130, 364), (156, 364), (182, 364), (208, 364), (234, 364), (260, 364), (286, 364), (312, 364), (338, 364), (364, 364), (390, 364), (416, 364), (442, 364), (468, 364), (494, 364), (520, 364), (546, 364), (572, 364), (598, 364), (624, 364), (650, 364), (676, 364), (702, 364)),

Órbita((14, 11), (40, 11), (66, 11), (92, 11), (118, 11), (144, 11), (170, 11), (196, 11), (222, 11), (248, 11), (274, 11), (300, 11), (326, 11), (352, 11), (378, 11), (404, 11), (430, 11), (456, 11), (482, 11), (508, 11), (534, 11), (560, 11), (586, 11), (612, 11), (638, 11), (664, 11), (690, 11), (716, 11), (1, 375), (27, 375), (53, 375), (79, 375), (105, 375), (131, 375), (157, 375), (183, 375), (209, 375), (235, 375), (261, 375), (287, 375), (313, 375), (339, 375), (365, 375), (391, 375), (417, 375), (443, 375), (469, 375), (495, 375), (521, 375), (547, 375), (573, 375), (599, 375), (625, 375), (651, 375), (677, 375), (703, 375)),

Órbita((14, 84), (40, 84), (66, 84), (92, 84), (118, 84), (144, 84), (170, 84), (196, 84), (222, 84), (248, 84), (274, 84), (300, 84), (326, 84), (352, 84), (378, 84), (404, 84), (430, 84), (456, 84), (482, 84), (508, 84), (534, 84), (560, 84), (586, 84), (612, 84), (638, 84), (664, 84), (690, 84), (716, 84), (1, 448), (27, 448), (53, 448), (79, 448), (105, 448), (131, 448), (157, 448), (183, 448), (209, 448), (235, 448), (261, 448), (287, 448), (313, 448), (339, 448), (365, 448), (391, 448), (417, 448), (443, 448), (469, 448), (495, 448), (521, 448), (547, 448), (573, 448), (599, 448), (625, 448), (651, 448), (677, 448), (703, 448)),

Órbita((14, 297), (40, 297), (66, 297), (92, 297), (118, 297), (144, 297), (170, 297), (196, 297), (222, 297), (248, 297), (274, 297), (300, 297), (326, 297), (352, 297), (378, 297), (404, 297), (430, 297), (456, 297), (482, 297), (508, 297), (534, 297), (560, 297), (586, 297), (612, 297), (638, 297), (664, 297), (690, 297), (716, 297), (1, 661), (27, 661), (53, 661), (79, 661), (105, 661), (131, 661), (157, 661), (183, 661), (209, 661), (235, 661), (261, 661), (287, 661), (313, 661), (339, 661), (365, 661), (391, 661), (417, 661), (443, 661), (469, 661), (495, 661), (521, 661), (547, 661), (573, 661), (599, 661), (625, 661), (651,

661), (677, 661), (703, 661)),

Órbita((2, 31), (28, 31), (54, 31), (80, 31), (106, 31), (132, 31), (158, 31), (184, 31), (210, 31), (236, 31), (262, 31), (288, 31), (314, 31), (340, 31), (366, 31), (392, 31), (418, 31), (444, 31), (470, 31), (496, 31), (522, 31), (548, 31), (574, 31), (600, 31), (626, 31), (652, 31), (678, 31), (704, 31), (15, 395), (41, 395), (67, 395), (93, 395), (119, 395), (145, 395), (171, 395), (197, 395), (223, 395), (249, 395), (275, 395), (301, 395), (327, 395), (353, 395), (379, 395), (405, 395), (431, 395), (457, 395), (483, 395), (509, 395), (535, 395), (561, 395), (587, 395), (613, 395), (639, 395), (665, 395), (691, 395), (717, 395)),

Órbita((2, 109), (28, 109), (54, 109), (80, 109), (106, 109), (132, 109), (158, 109), (184, 109), (210, 109), (236, 109), (262, 109), (288, 109), (314, 109), (340, 109), (366, 109), (392, 109), (418, 109), (444, 109), (470, 109), (496, 109), (522, 109), (548, 109), (574, 109), (600, 109), (626, 109), (652, 109), (678, 109), (704, 109), (15, 473), (41, 473), (67, 473), (93, 473), (119, 473), (145, 473), (171, 473), (197, 473), (223, 473), (249, 473), (275, 473), (301, 473), (327, 473), (353, 473), (379, 473), (405, 473), (431, 473), (457, 473), (483, 473), (509, 473), (535, 473), (561, 473), (587, 473), (613, 473), (639, 473), (665, 473), (691, 473), (717, 473)),

Órbita((15, 280), (41, 280), (67, 280), (93, 280), (119, 280), (145, 280), (171, 280), (197, 280), (223, 280), (249, 280), (275, 280), (301, 280), (327, 280), (353, 280), (379, 280), (405, 280), (431, 280), (457, 280), (483, 280), (509, 280), (535, 280), (561, 280), (587, 280), (613, 280), (639, 280), (665, 280), (691, 280), (717, 280), (2, 644), (28, 644), (54, 644), (80, 644), (106, 644), (132, 644), (158, 644), (184, 644), (210, 644), (236, 644), (262, 644), (288, 644), (314, 644), (340, 644), (366, 644), (392, 644), (418, 644), (444, 644), (470, 644), (496, 644), (522, 644), (548, 644), (574, 644), (600, 644), (626, 644), (652, 644), (678, 644), (704, 644)),

Órbita((16, 33), (42, 33), (68, 33), (94, 33), (120, 33), (146, 33), (172, 33), (198, 33), (224, 33), (250, 33), (276, 33), (302, 33), (328, 33), (354, 33), (380, 33), (406, 33), (432, 33), (458, 33), (484, 33), (510, 33), (536, 33), (562, 33), (588, 33), (614, 33), (640, 33), (666, 33), (692, 33), (718, 33), (3, 397), (29, 397), (55, 397), (81, 397), (107, 397), (133, 397), (159, 397), (185, 397), (211, 397), (237, 397), (263, 397), (289, 397), (315, 397), (341,

397), (367, 397), (393, 397), (419, 397), (445, 397), (471, 397), (497, 397), (523, 397), (549, 397), (575, 397), (601, 397), (627, 397), (653, 397), (679, 397), (705, 397)),

Órbita((16, 163), (42, 163), (68, 163), (94, 163), (120, 163), (146, 163), (172, 163), (198, 163), (224, 163), (250, 163), (276, 163), (302, 163), (328, 163), (354, 163), (380, 163), (406, 163), (432, 163), (458, 163), (484, 163), (510, 163), (536, 163), (562, 163), (588, 163), (614, 163), (640, 163), (666, 163), (692, 163), (718, 163), (3, 527), (29, 527), (55, 527), (81, 527), (107, 527), (133, 527), (159, 527), (185, 527), (211, 527), (237, 527), (263, 527), (289, 527), (315, 527), (341, 527), (367, 527), (393, 527), (419, 527), (445, 527), (471, 527), (497, 527), (523, 527), (549, 527), (575, 527), (601, 527), (627, 527), (653, 527), (679, 527), (705, 527)),

Órbita((16, 252), (42, 252), (68, 252), (94, 252), (120, 252), (146, 252), (172, 252), (198, 252), (224, 252), (250, 252), (276, 252), (302, 252), (328, 252), (354, 252), (380, 252), (406, 252), (432, 252), (458, 252), (484, 252), (510, 252), (536, 252), (562, 252), (588, 252), (614, 252), (640, 252), (666, 252), (692, 252), (718, 252), (3, 616), (29, 616), (55, 616), (81, 616), (107, 616), (133, 616), (159, 616), (185, 616), (211, 616), (237, 616), (263, 616), (289, 616), (315, 616), (341, 616), (367, 616), (393, 616), (419, 616), (445, 616), (471, 616), (497, 616), (523, 616), (549, 616), (575, 616), (601, 616), (627, 616), (653, 616), (679, 616), (705, 616)),

Órbita((4, 178), (30, 178), (56, 178), (82, 178), (108, 178), (134, 178), (160, 178), (186, 178), (212, 178), (238, 178), (264, 178), (290, 178), (316, 178), (342, 178), (368, 178), (394, 178), (420, 178), (446, 178), (472, 178), (498, 178), (524, 178), (550, 178), (576, 178), (602, 178), (628, 178), (654, 178), (680, 178), (706, 178), (17, 542), (43, 542), (69, 542), (95, 542), (121, 542), (147, 542), (173, 542), (199, 542), (225, 542), (251, 542), (277, 542), (303, 542), (329, 542), (355, 542), (381, 542), (407, 542), (433, 542), (459, 542), (485, 542), (511, 542), (537, 542), (563, 542), (589, 542), (615, 542), (641, 542), (667, 542), (693, 542), (719, 542)),

Órbita((4, 224), (30, 224), (56, 224), (82, 224), (108, 224), (134, 224), (160, 224), (186, 224), (212, 224), (238, 224), (264, 224), (290, 224), (316, 224), (342, 224), (368, 224), (394, 224), (420, 224), (446, 224), (472, 224), (498, 224), (524, 224), (550, 224), (576,

224), (602, 224), (628, 224), (654, 224), (680, 224), (706, 224), (17, 588), (43, 588), (69, 588), (95, 588), (121, 588), (147, 588), (173, 588), (199, 588), (225, 588), (251, 588), (277, 588), (303, 588), (329, 588), (355, 588), (381, 588), (407, 588), (433, 588), (459, 588), (485, 588), (511, 588), (537, 588), (563, 588), (589, 588), (615, 588), (641, 588), (667, 588), (693, 588), (719, 588)),

Órbita((17, 74), (43, 74), (69, 74), (95, 74), (121, 74), (147, 74), (173, 74), (199, 74), (225, 74), (251, 74), (277, 74), (303, 74), (329, 74), (355, 74), (381, 74), (407, 74), (433, 74), (459, 74), (485, 74), (511, 74), (537, 74), (563, 74), (589, 74), (615, 74), (641, 74), (667, 74), (693, 74), (719, 74), (4, 438), (30, 438), (56, 438), (82, 438), (108, 438), (134, 438), (160, 438), (186, 438), (212, 438), (238, 438), (264, 438), (290, 438), (316, 438), (342, 438), (368, 438), (394, 438), (420, 438), (446, 438), (472, 438), (498, 438), (524, 438), (550, 438), (576, 438), (602, 438), (628, 438), (654, 438), (680, 438), (706, 438)),

Órbita((5, 336), (31, 336), (57, 336), (83, 336), (109, 336), (135, 336), (161, 336), (187, 336), (213, 336), (239, 336), (265, 336), (291, 336), (317, 336), (343, 336), (369, 336), (395, 336), (421, 336), (447, 336), (473, 336), (499, 336), (525, 336), (551, 336), (577, 336), (603, 336), (629, 336), (655, 336), (681, 336), (707, 336), (18, 700), (44, 700), (70, 700), (96, 700), (122, 700), (148, 700), (174, 700), (200, 700), (226, 700), (252, 700), (278, 700), (304, 700), (330, 700), (356, 700), (382, 700), (408, 700), (434, 700), (460, 700), (486, 700), (512, 700), (538, 700), (564, 700), (590, 700), (616, 700), (642, 700), (668, 700), (694, 700), (720, 700)),

Órbita((18, 253), (44, 253), (70, 253), (96, 253), (122, 253), (148, 253), (174, 253), (200, 253), (226, 253), (252, 253), (278, 253), (304, 253), (330, 253), (356, 253), (382, 253), (408, 253), (434, 253), (460, 253), (486, 253), (512, 253), (538, 253), (564, 253), (590, 253), (616, 253), (642, 253), (668, 253), (694, 253), (720, 253), (5, 617), (31, 617), (57, 617), (83, 617), (109, 617), (135, 617), (161, 617), (187, 617), (213, 617), (239, 617), (265, 617), (291, 617), (317, 617), (343, 617), (369, 617), (395, 617), (421, 617), (447, 617), (473, 617), (499, 617), (525, 617), (551, 617), (577, 617), (603, 617), (629, 617), (655, 617), (681, 617), (707, 617)),

Órbita((18, 279), (44, 279), (70, 279), (96, 279), (122, 279), (148, 279), (174, 279), (200,

279), (226, 279), (252, 279), (278, 279), (304, 279), (330, 279), (356, 279), (382, 279), (408, 279), (434, 279), (460, 279), (486, 279), (512, 279), (538, 279), (564, 279), (590, 279), (616, 279), (642, 279), (668, 279), (694, 279), (720, 279), (5, 643), (31, 643), (57, 643), (83, 643), (109, 643), (135, 643), (161, 643), (187, 643), (213, 643), (239, 643), (265, 643), (291, 643), (317, 643), (343, 643), (369, 643), (395, 643), (421, 643), (447, 643), (473, 643), (499, 643), (525, 643), (551, 643), (577, 643), (603, 643), (629, 643), (655, 643), (681, 643), (707, 643)),

Órbita((6, 93), (32, 93), (58, 93), (84, 93), (110, 93), (136, 93), (162, 93), (188, 93), (214, 93), (240, 93), (266, 93), (292, 93), (318, 93), (344, 93), (370, 93), (396, 93), (422, 93), (448, 93), (474, 93), (500, 93), (526, 93), (552, 93), (578, 93), (604, 93), (630, 93), (656, 93), (682, 93), (708, 93), (19, 457), (45, 457), (71, 457), (97, 457), (123, 457), (149, 457), (175, 457), (201, 457), (227, 457), (253, 457), (279, 457), (305, 457), (331, 457), (357, 457), (383, 457), (409, 457), (435, 457), (461, 457), (487, 457), (513, 457), (539, 457), (565, 457), (591, 457), (617, 457), (643, 457), (669, 457), (695, 457), (721, 457)),

Órbita((6, 327), (32, 327), (58, 327), (84, 327), (110, 327), (136, 327), (162, 327), (188, 327), (214, 327), (240, 327), (266, 327), (292, 327), (318, 327), (344, 327), (370, 327), (396, 327), (422, 327), (448, 327), (474, 327), (500, 327), (526, 327), (552, 327), (578, 327), (604, 327), (630, 327), (656, 327), (682, 327), (708, 327), (19, 691), (45, 691), (71, 691), (97, 691), (123, 691), (149, 691), (175, 691), (201, 691), (227, 691), (253, 691), (279, 691), (305, 691), (331, 691), (357, 691), (383, 691), (409, 691), (435, 691), (461, 691), (487, 691), (513, 691), (539, 691), (565, 691), (591, 691), (617, 691), (643, 691), (669, 691), (695, 691), (721, 691)),

Órbita((19, 112), (45, 112), (71, 112), (97, 112), (123, 112), (149, 112), (175, 112), (201, 112), (227, 112), (253, 112), (279, 112), (305, 112), (331, 112), (357, 112), (383, 112), (409, 112), (435, 112), (461, 112), (487, 112), (513, 112), (539, 112), (565, 112), (591, 112), (617, 112), (643, 112), (669, 112), (695, 112), (721, 112), (6, 476), (32, 476), (58, 476), (84, 476), (110, 476), (136, 476), (162, 476), (188, 476), (214, 476), (240, 476), (266, 476), (292, 476), (318, 476), (344, 476), (370, 476), (396, 476), (422, 476), (448, 476), (474, 476), (500, 476), (526, 476), (552, 476), (578, 476), (604, 476), (630, 476), (656,

476), (682, 476), (708, 476)),

Órbita((7, 96), (33, 96), (59, 96), (85, 96), (111, 96), (137, 96), (163, 96), (189, 96), (215, 96), (241, 96), (267, 96), (293, 96), (319, 96), (345, 96), (371, 96), (397, 96), (423, 96), (449, 96), (475, 96), (501, 96), (527, 96), (553, 96), (579, 96), (605, 96), (631, 96), (657, 96), (683, 96), (709, 96), (20, 460), (46, 460), (72, 460), (98, 460), (124, 460), (150, 460), (176, 460), (202, 460), (228, 460), (254, 460), (280, 460), (306, 460), (332, 460), (358, 460), (384, 460), (410, 460), (436, 460), (462, 460), (488, 460), (514, 460), (540, 460), (566, 460), (592, 460), (618, 460), (644, 460), (670, 460), (696, 460), (722, 460)),

Órbita((20, 44), (46, 44), (72, 44), (98, 44), (124, 44), (150, 44), (176, 44), (202, 44), (228, 44), (254, 44), (280, 44), (306, 44), (332, 44), (358, 44), (384, 44), (410, 44), (436, 44), (462, 44), (488, 44), (514, 44), (540, 44), (566, 44), (592, 44), (618, 44), (644, 44), (670, 44), (696, 44), (722, 44), (7, 408), (33, 408), (59, 408), (85, 408), (111, 408), (137, 408), (163, 408), (189, 408), (215, 408), (241, 408), (267, 408), (293, 408), (319, 408), (345, 408), (371, 408), (397, 408), (423, 408), (449, 408), (475, 408), (501, 408), (527, 408), (553, 408), (579, 408), (605, 408), (631, 408), (657, 408), (683, 408), (709, 408)),

Órbita((20, 56), (46, 56), (72, 56), (98, 56), (124, 56), (150, 56), (176, 56), (202, 56), (228, 56), (254, 56), (280, 56), (306, 56), (332, 56), (358, 56), (384, 56), (410, 56), (436, 56), (462, 56), (488, 56), (514, 56), (540, 56), (566, 56), (592, 56), (618, 56), (644, 56), (670, 56), (696, 56), (722, 56), (7, 420), (33, 420), (59, 420), (85, 420), (111, 420), (137, 420), (163, 420), (189, 420), (215, 420), (241, 420), (267, 420), (293, 420), (319, 420), (345, 420), (371, 420), (397, 420), (423, 420), (449, 420), (475, 420), (501, 420), (527, 420), (553, 420), (579, 420), (605, 420), (631, 420), (657, 420), (683, 420), (709, 420)),

Órbita((8, 132), (34, 132), (60, 132), (86, 132), (112, 132), (138, 132), (164, 132), (190, 132), (216, 132), (242, 132), (268, 132), (294, 132), (320, 132), (346, 132), (372, 132), (398, 132), (424, 132), (450, 132), (476, 132), (502, 132), (528, 132), (554, 132), (580, 132), (606, 132), (632, 132), (658, 132), (684, 132), (710, 132), (21, 496), (47, 496), (73, 496), (99, 496), (125, 496), (151, 496), (177, 496), (203, 496), (229, 496), (255, 496), (281, 496), (307, 496), (333, 496), (359, 496), (385, 496), (411, 496), (437, 496), (463, 496), (489, 496), (515, 496), (541, 496), (567, 496), (593, 496), (619, 496), (645, 496), (671,

496), (697, 496), (723, 496)),

Órbita((8, 168), (34, 168), (60, 168), (86, 168), (112, 168), (138, 168), (164, 168), (190, 168), (216, 168), (242, 168), (268, 168), (294, 168), (320, 168), (346, 168), (372, 168), (398, 168), (424, 168), (450, 168), (476, 168), (502, 168), (528, 168), (554, 168), (580, 168), (606, 168), (632, 168), (658, 168), (684, 168), (710, 168), (21, 532), (47, 532), (73, 532), (99, 532), (125, 532), (151, 532), (177, 532), (203, 532), (229, 532), (255, 532), (281, 532), (307, 532), (333, 532), (359, 532), (385, 532), (411, 532), (437, 532), (463, 532), (489, 532), (515, 532), (541, 532), (567, 532), (593, 532), (619, 532), (645, 532), (671, 532), (697, 532), (723, 532)),

Órbita((21, 288), (47, 288), (73, 288), (99, 288), (125, 288), (151, 288), (177, 288), (203, 288), (229, 288), (255, 288), (281, 288), (307, 288), (333, 288), (359, 288), (385, 288), (411, 288), (437, 288), (463, 288), (489, 288), (515, 288), (541, 288), (567, 288), (593, 288), (619, 288), (645, 288), (671, 288), (697, 288), (723, 288), (8, 652), (34, 652), (60, 652), (86, 652), (112, 652), (138, 652), (164, 652), (190, 652), (216, 652), (242, 652), (268, 652), (294, 652), (320, 652), (346, 652), (372, 652), (398, 652), (424, 652), (450, 652), (476, 652), (502, 652), (528, 652), (554, 652), (580, 652), (606, 652), (632, 652), (658, 652), (684, 652), (710, 652)),

Órbita((9, 125), (35, 125), (61, 125), (87, 125), (113, 125), (139, 125), (165, 125), (191, 125), (217, 125), (243, 125), (269, 125), (295, 125), (321, 125), (347, 125), (373, 125), (399, 125), (425, 125), (451, 125), (477, 125), (503, 125), (529, 125), (555, 125), (581, 125), (607, 125), (633, 125), (659, 125), (685, 125), (711, 125), (22, 489), (48, 489), (74, 489), (100, 489), (126, 489), (152, 489), (178, 489), (204, 489), (230, 489), (256, 489), (282, 489), (308, 489), (334, 489), (360, 489), (386, 489), (412, 489), (438, 489), (464, 489), (490, 489), (516, 489), (542, 489), (568, 489), (594, 489), (620, 489), (646, 489), (672, 489), (698, 489), (724, 489)),

Órbita((22, 28), (48, 28), (74, 28), (100, 28), (126, 28), (152, 28), (178, 28), (204, 28), (230, 28), (256, 28), (282, 28), (308, 28), (334, 28), (360, 28), (386, 28), (412, 28), (438, 28), (464, 28), (490, 28), (516, 28), (542, 28), (568, 28), (594, 28), (620, 28), (646, 28), (672, 28), (698, 28), (724, 28), (9, 392), (35, 392), (61, 392), (87, 392), (113, 392), (139,

392), (165, 392), (191, 392), (217, 392), (243, 392), (269, 392), (295, 392), (321, 392), (347, 392), (373, 392), (399, 392), (425, 392), (451, 392), (477, 392), (503, 392), (529, 392), (555, 392), (581, 392), (607, 392), (633, 392), (659, 392), (685, 392), (711, 392)),

Órbita((22, 99), (48, 99), (74, 99), (100, 99), (126, 99), (152, 99), (178, 99), (204, 99), (230, 99), (256, 99), (282, 99), (308, 99), (334, 99), (360, 99), (386, 99), (412, 99), (438, 99), (464, 99), (490, 99), (516, 99), (542, 99), (568, 99), (594, 99), (620, 99), (646, 99), (672, 99), (698, 99), (724, 99), (9, 463), (35, 463), (61, 463), (87, 463), (113, 463), (139, 463), (165, 463), (191, 463), (217, 463), (243, 463), (269, 463), (295, 463), (321, 463), (347, 463), (373, 463), (399, 463), (425, 463), (451, 463), (477, 463), (503, 463), (529, 463), (555, 463), (581, 463), (607, 463), (633, 463), (659, 463), (685, 463), (711, 463)),

Órbita((10, 146), (36, 146), (62, 146), (88, 146), (114, 146), (140, 146), (166, 146), (192, 146), (218, 146), (244, 146), (270, 146), (296, 146), (322, 146), (348, 146), (374, 146), (400, 146), (426, 146), (452, 146), (478, 146), (504, 146), (530, 146), (556, 146), (582, 146), (608, 146), (634, 146), (660, 146), (686, 146), (712, 146), (23, 510), (49, 510), (75, 510), (101, 510), (127, 510), (153, 510), (179, 510), (205, 510), (231, 510), (257, 510), (283, 510), (309, 510), (335, 510), (361, 510), (387, 510), (413, 510), (439, 510), (465, 510), (491, 510), (517, 510), (543, 510), (569, 510), (595, 510), (621, 510), (647, 510), (673, 510), (699, 510), (725, 510)),

Órbita((10, 302), (36, 302), (62, 302), (88, 302), (114, 302), (140, 302), (166, 302), (192, 302), (218, 302), (244, 302), (270, 302), (296, 302), (322, 302), (348, 302), (374, 302), (400, 302), (426, 302), (452, 302), (478, 302), (504, 302), (530, 302), (556, 302), (582, 302), (608, 302), (634, 302), (660, 302), (686, 302), (712, 302), (23, 666), (49, 666), (75, 666), (101, 666), (127, 666), (153, 666), (179, 666), (205, 666), (231, 666), (257, 666), (283, 666), (309, 666), (335, 666), (361, 666), (387, 666), (413, 666), (439, 666), (465, 666), (491, 666), (517, 666), (543, 666), (569, 666), (595, 666), (621, 666), (647, 666), (673, 666), (699, 666), (725, 666)),

Órbita((23, 196), (49, 196), (75, 196), (101, 196), (127, 196), (153, 196), (179, 196), (205, 196), (231, 196), (257, 196), (283, 196), (309, 196), (335, 196), (361, 196), (387, 196), (413, 196), (439, 196), (465, 196), (491, 196), (517, 196), (543, 196), (569, 196), (595,

196), (621, 196), (647, 196), (673, 196), (699, 196), (725, 196), (10, 560), (36, 560), (62, 560), (88, 560), (114, 560), (140, 560), (166, 560), (192, 560), (218, 560), (244, 560), (270, 560), (296, 560), (322, 560), (348, 560), (374, 560), (400, 560), (426, 560), (452, 560), (478, 560), (504, 560), (530, 560), (556, 560), (582, 560), (608, 560), (634, 560), (660, 560), (686, 560), (712, 560)),

Órbita((11, 32), (37, 32), (63, 32), (89, 32), (115, 32), (141, 32), (167, 32), (193, 32), (219, 32), (245, 32), (271, 32), (297, 32), (323, 32), (349, 32), (375, 32), (401, 32), (427, 32), (453, 32), (479, 32), (505, 32), (531, 32), (557, 32), (583, 32), (609, 32), (635, 32), (661, 32), (687, 32), (713, 32), (24, 396), (50, 396), (76, 396), (102, 396), (128, 396), (154, 396), (180, 396), (206, 396), (232, 396), (258, 396), (284, 396), (310, 396), (336, 396), (362, 396), (388, 396), (414, 396), (440, 396), (466, 396), (492, 396), (518, 396), (544, 396), (570, 396), (596, 396), (622, 396), (648, 396), (674, 396), (700, 396), (726, 396)),

Órbita((11, 136), (37, 136), (63, 136), (89, 136), (115, 136), (141, 136), (167, 136), (193, 136), (219, 136), (245, 136), (271, 136), (297, 136), (323, 136), (349, 136), (375, 136), (401, 136), (427, 136), (453, 136), (479, 136), (505, 136), (531, 136), (557, 136), (583, 136), (609, 136), (635, 136), (661, 136), (687, 136), (713, 136), (24, 500), (50, 500), (76, 500), (102, 500), (128, 500), (154, 500), (180, 500), (206, 500), (232, 500), (258, 500), (284, 500), (310, 500), (336, 500), (362, 500), (388, 500), (414, 500), (440, 500), (466, 500), (492, 500), (518, 500), (544, 500), (570, 500), (596, 500), (622, 500), (648, 500), (674, 500), (700, 500), (726, 500)),

Órbita((11, 140), (37, 140), (63, 140), (89, 140), (115, 140), (141, 140), (167, 140), (193, 140), (219, 140), (245, 140), (271, 140), (297, 140), (323, 140), (349, 140), (375, 140), (401, 140), (427, 140), (453, 140), (479, 140), (505, 140), (531, 140), (557, 140), (583, 140), (609, 140), (635, 140), (661, 140), (687, 140), (713, 140), (24, 504), (50, 504), (76, 504), (102, 504), (128, 504), (154, 504), (180, 504), (206, 504), (232, 504), (258, 504), (284, 504), (310, 504), (336, 504), (362, 504), (388, 504), (414, 504), (440, 504), (466, 504), (492, 504), (518, 504), (544, 504), (570, 504), (596, 504), (622, 504), (648, 504), (674, 504), (700, 504), (726, 504)),

Órbita((25, 170), (51, 170), (77, 170), (103, 170), (129, 170), (155, 170), (181, 170), (207,

170), (233, 170), (259, 170), (285, 170), (311, 170), (337, 170), (363, 170), (389, 170), (415, 170), (441, 170), (467, 170), (493, 170), (519, 170), (545, 170), (571, 170), (597, 170), (623, 170), (649, 170), (675, 170), (701, 170), (727, 170), (12, 534), (38, 534), (64, 534), (90, 534), (116, 534), (142, 534), (168, 534), (194, 534), (220, 534), (246, 534), (272, 534), (298, 534), (324, 534), (350, 534), (376, 534), (402, 534), (428, 534), (454, 534), (480, 534), (506, 534), (532, 534), (558, 534), (584, 534), (610, 534), (636, 534), (662, 534), (688, 534), (714, 534)),

Órbita((25, 222), (51, 222), (77, 222), (103, 222), (129, 222), (155, 222), (181, 222), (207, 222), (233, 222), (259, 222), (285, 222), (311, 222), (337, 222), (363, 222), (389, 222), (415, 222), (441, 222), (467, 222), (493, 222), (519, 222), (545, 222), (571, 222), (597, 222), (623, 222), (649, 222), (675, 222), (701, 222), (727, 222), (12, 586), (38, 586), (64, 586), (90, 586), (116, 586), (142, 586), (168, 586), (194, 586), (220, 586), (246, 586), (272, 586), (298, 586), (324, 586), (350, 586), (376, 586), (402, 586), (428, 586), (454, 586), (480, 586), (506, 586), (532, 586), (558, 586), (584, 586), (610, 586), (636, 586), (662, 586), (688, 586), (714, 586)),

Órbita((25, 308), (51, 308), (77, 308), (103, 308), (129, 308), (155, 308), (181, 308), (207, 308), (233, 308), (259, 308), (285, 308), (311, 308), (337, 308), (363, 308), (389, 308), (415, 308), (441, 308), (467, 308), (493, 308), (519, 308), (545, 308), (571, 308), (597, 308), (623, 308), (649, 308), (675, 308), (701, 308), (727, 308), (12, 672), (38, 672), (64, 672), (90, 672), (116, 672), (142, 672), (168, 672), (194, 672), (220, 672), (246, 672), (272, 672), (298, 672), (324, 672), (350, 672), (376, 672), (402, 672), (428, 672), (454, 672), (480, 672), (506, 672), (532, 672), (558, 672), (584, 672), (610, 672), (636, 672), (662, 672), (688, 672), (714, 672))