Códigos associados a curvas elipticas maximais

Jéfferson Luiz Rocha Bastos

***Resumo*— Em [4] é proposta uma integração entre modulação e codificação de canal baseada no gênero da superfície na qual o canal de trasmissão pode ser mergulhado. Esta integração é feita usando códigos de Goppa, sendo assim necessário saber os parâmetros destes códigos. Além disto, como o canal de transmissão pode variar com o tempo, e assim o gênero da superfície, é interessante tentar estabelecer relações entre códigos associados a curvas de gêneros distintos. Este artigo apresenta um resultado onde são calculados os parâmetros de todos os códigos de Goppa associados a curvas elípticas maximais. Além disso, apresenta uma maneira de se fazer puncionamento no códigos associado a curva Hermitiana de gênero $g = 1$ obtendo um código racional.**

***Palavras-Chave*— Curvas Algébricas, Códigos de Goppa, Curvas Elipticas.**

***Abstract*— In [4] an integration of modulation and channel codification is proposed based on the surface genus in which the channel can be embedded. This integration is achieved through Goppa codes, the parameters of which must be known. Besides, since the channel may vary in time, and also the surface genus, it is interesting to try and establish relations among codes associated to curves of distinct genera. This article shows a result in which all code parameters related to maximal elliptic curves are calculated. It also shows a way of punctoring the code related to the Hermitian curve of genus $g = 1$ in order to obtain a rational code.**

***Keywords*— Algebraic Curves, Goppa codes, Elliptic curves.**

I. Introdução

Sejam k um corpo e $\overline{k}$ seu fecho algébrico. Nesta seção veremos as definições do espaço projetivo, o espaço onde as curvas algébricas são definidas, de curvas algébricas e outros conceitos fundamentais à teoria dos códigos de Goppa.

O **plano projetivo** $\mathbb{P}^2(k)$ é definido como o conjunto quociente de $k^3 \setminus (0,0,0)$ por uma relação de equivalência $\sim$, ou seja,

$$\mathbb{P}^2(k) = \frac{k^3 \setminus (0,0,0)}{\sim},$$

onde

$$\begin{gathered}(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \\ \Updownarrow \\ \exists\ a \in k^*;\ x_1 = ax_2,\ y_1 = ay_2,\ z_1 = az_2.\end{gathered}$$

Como os pontos de $\mathbb{P}^2(k)$ são classes de equivalência, vamos usar a notação $(x : y : z)$ para representar estes elementos.

Seja $F(X,Y,Z) \in k[X,Y,Z]$ um polinômio homogêneo de grau d, e tal que $f(X,Y) = F(X,Y,1)$ seja absolutamente irredutível. Definimos a **curva plana projetiva** de grau d associada ao polinômio F, denotada por $\mathcal{X}$ ou por $\mathcal{X}_F$, como sendo o conjunto

$$\mathcal{X} = \{(x : y : z) \in \mathbb{P}^2(k) |\ F(x,y,z) = 0\},$$

Jéfferson Luiz Rocha Bastos¸ Departamento de Matemática, IBILCE, Universidade Estadual Paulista - UNESP, São José do Rio Preto, Brasil, E-mail: jeferson@ibilce.unesp.br

ou simplesmente

$$\mathcal{X} : F(X,Y,Z) = 0.$$

Dada uma curva podemos associar o seu **gênero**, denotado por $g(\mathcal{X})$, que satisfaz a seguinte desigualdade

$$g(\mathcal{X}) \leq \frac{(d-1)(d-2)}{2}.$$

Esta desigualdade passa a ser uma igualdade quando a curva for **não singular**, isto é, quando vale a condição

$$\begin{gathered}F(x,y,z) = F_X(x,y,z) = F_Y(x,y,z) = F_Z(x,y,z) = 0 \\ \Downarrow \\ (x,y,z) = (0,0,0),\end{gathered}$$

onde $F_X,\ F_Y,\ F_Z$ denotam as derivadas parciais de F com relação às variáveis $X,\ Y,\ Z$, respectivamente. Seja $\mathcal{X}$ uma curva plana projetiva definida por um polinômio homogêneo F e seja K um corpo qualquer contendo k. Um $K-$**ponto racional** em $\mathcal{X}$ é um ponto $(x : y : z) \in \mathbb{P}^2(K)$ tal que $F(x,y,z) = 0$. Denotamos o conjunto dos $K-$pontos racionais da curva $\mathcal{X}$ como

$$\mathcal{X}(K) = \{(x : y : z) \in \mathbb{P}^2(K) |\ F(x,y,z) = 0\}.$$

Seja $\mathcal{X}$ uma curva definida em $\mathbb{F}_q$. Um **divisor** D em $\mathcal{X}$ é uma soma formal de pontos da curva com coeficientes inteiros, isto é, um divisor é um elemento da forma

$$D = \sum n_Q Q,$$

onde $n_Q \in \mathbb{Z}$ e Q são pontos (de grau arbitrário) em $\mathcal{X}$.

Se $n_Q \geq 0\ \forall Q$, dizemos que o divisor D é **efetivo** e denotamos por $D \geq 0$. Definimos o **grau** de um divisor como sendo

$$gr(D) = \sum n_Q gr(Q),$$

e o **suporte** de um divisor D, denotado por $Supp(D)$, como sendo o conjunto dos pontos Q da curva que aparecem com coeficientes não nulos no divisor D, isto é,

$$Supp(D) = \{Q |\ n_Q \neq 0\}.$$

Seja $F(X,Y,Z)$ um polinômio que define uma curva plana projetiva $\mathcal{X}$ sobre $\mathbb{F}_q$ e seja

$$E = \left\{ \frac{G(X,Y,Z)}{H(X,Y,Z)} | G,\ H \text{ homogêneos de mesmo grau} \right\} \cup \{0\}.$$

O **corpo das funções racionais** em $\mathcal{X}$, denotado por $\mathbb{F}_q(\mathcal{X})$ é o conjunto quociente de E por uma relação de equivalência $\sim$, isto é,

$$\mathbb{F}_q(\mathcal{X}) = \frac{E}{\sim},$$

onde

$$\frac{G}{H} \sim \frac{G'}{H'} \Longleftrightarrow GH' - G'H \in \langle F \rangle, \qquad (1)$$

com $\langle F\rangle$ representando o ideal gerado pelo polinômio F em $k[X,Y,Z]$.

Seja $\mathcal{X}$ uma curva definida pelo polinômio F, e $f=\dfrac{G}{H}\in \mathbb{F}_q(\mathcal{X})$. O **divisor de** f é definido como

$$div(f)=\sum_{P\in\mathcal{X}_F\cap\mathcal{X}_G} I(P,F,G)P-\sum_{Q\in\mathcal{X}_F\cap\mathcal{X}_H} I(Q,F,H)Q. \quad (2)$$

Seja D um divisor sobre uma curva não singular. O **espaço das funções racionais associadas a** D é o conjunto

$$\mathcal{L}(D)=\{f\in\mathbb{F}_q(\mathcal{X})|\ div(f)+D\geq 0\}\cup\{0\}.$$

Agora podemos definir os códigos algébricos-geométricos da seguinte forma. Considere $\mathcal{X}$ como uma curva plana projetiva definida sobre $\mathbb{F}_q$, D um divisor em $\mathcal{X}$ e $\mathcal{P}=\{P_1,...,P_n\}$ um conjunto de n pontos $\mathbb{F}_q$-racionais distintos em $\mathcal{X}$. Suponha que $\mathcal{P}\cap Supp(D)=\emptyset$.

O **código algébrico-geométrico** associado à curva $\mathcal{X}$, ao conjunto $\mathcal{P}$ e ao divisor D é o conjunto

$$\mathcal{C}(\mathcal{X},\mathcal{P},D)=\{(f(P_1),...,f(P_n))|\ f\in\mathcal{L}(D)\}\in\mathbb{F}_q^n. \quad (3)$$

Os parâmetros do código definido em (3) são dados pelo seguinte resultado.

Teorema 1 ([1],[3]): Seja $\mathcal{X}$ uma curva plana, projetiva, de gênero g, definida sobre $\mathbb{F}_q$. Seja $\mathcal{P}\subset\mathcal{X}(\mathbb{F}_q)$ um conjunto de n pontos $\mathbb{F}_q-$racionais distintos, e seja D um divisor tal que $2g-2<gr(D)<n$. Então o código algébrico-geométrico $\mathcal{C}(\mathcal{X},\mathcal{P},D)$ é linear de comprimento n, dimensão $k=gr(D)+1-g$ e distância mínima $d\geq n-gr(D)$.

II. Curvas Elipticas

Nesta seção serão obtidos os parâmetros de todos os códigos associados às curvas elípticas maximais, isto é, curvas de gênero $g=1$ e que sejam maximais. Isto será feito por meio da seguinte proposição.

Teorema 2 ([4]): Seja $\mathcal{X}$ uma curva elíptica maximal sobre o corpo finito $K=\mathbb{F}_{p^{2t}}$, seja $P_\infty=(0:1:0)$ o ponto no infinito de $\mathbb{P}^2(K)$, $D=rP_\infty$ um divisor sobre $\mathcal{X}$ e $\mathcal{P}=\{\text{pontos racionais}\}\backslash\{P_\infty\}$. Então vale:

- $car(K)=2$
  O código $\mathcal{C}(\mathcal{X},\mathcal{P},D)$ possui parâmetros $n=2^{2t}+2^{t+1}$, $k=r$, $d=n-r$ se r for um número par. Se r for ímpar então $d=n-r$ ou $d=n-r+1$, o que não altera a quantidade de erros corrigidos pelo código.
- $car(K)=p\neq 2$
  O código $\mathcal{C}(\mathcal{X},\mathcal{P},D)$ possui parâmetros $n=p^{2t}+2p^t$, $k=r$, $d=n-r$.
  Demonstração:
- $car(K)=2$

De acordo com [2] a curva $\mathcal{X}$ pode ser escrita como

$$ZY^2+a_1XYZ+a_3YZ^2=X^3+a_2ZX^2+a_4XZ^2+a_6Z^3. \quad (4)$$

Como, por hipótese, a curva é maximal, então deverá conter $1+2^{2t}+2^{t+1}$ pontos racionais. Substituindo $Z=0$ em (4) temos $X^3=0$. Assim, $P_\infty=(0:1:0)\in\mathcal{X}$ e $div(\mathcal{X}\cap Z)=3P_\infty$.

Os restantes $2^{2t}+2^{t+1}$ pontos racionais possuem coordenada $Z=1$. Dado $\alpha\in\mathbb{F}_{2^{2t}}$, substituindo $X=\alpha$ em (4) obtemos

$$Y^2+(a_1\alpha+a_3)Y=\alpha^3+a_2\alpha^2+a_4\alpha+a_6. \quad (5)$$

Se $a_1\neq 0$, tomando-se $\alpha=\frac{a_3}{a_1}$ a equação (5) transforma-se em

$$Y^2=\alpha^3+a_2\alpha^2+a_4\alpha+a_6,$$

possuindo solução única. Mais ainda, dado $\beta\neq\alpha$ a equação

$$Y^2+(a_1\beta+a_3)Y=\beta^3+a_2\beta^2+a_4\beta+a_6$$

possui duas ou nenhuma solução. Assim, caso $a_1\neq 0$ conseguiremos um número ímpar de pontos racionais com coordenada $Z=1$. Como precisamos de $2^{2t}+2^{t+1}$ pontos concluímos que, se a curva é maximal, devemos ter $a_1=0$. Além disso, existem $\frac{2^{2t}+2^{t+1}}{2}=2^{2t-1}+2^t$ elementos em $\mathbb{F}_{2^{2t}}$ para os quais a equação

$$Y^2+a_3Y=\alpha^3+a_2\alpha^2+a_4\alpha+a_6, \quad (6)$$

possui duas soluções. Sejam $\alpha_i,\ i=1,2,...,2^{2t-1}+2^t$, os elementos em $\mathbb{F}_{2^{2t}}$ para os quais a equação (6) possui 2 soluções. Desta forma, os pontos racionais são $(\alpha_i:\beta_1^i:1)$, $(\alpha_i:\beta_2^i:1)$, $i=1,...,2^{2t-1}+2^t$.

Os outros divisores de intersecção são dados por

$$div(\mathcal{X}\cap X)=P_\infty+Q_1+Q_2;$$
$$div(\mathcal{X}\cap Y)=R_1+R_2+R_3,\ R_i\neq P_\infty.$$

Desta forma, temos

$$div(\frac{X^iY^j}{Z^{i+j}})=i(Q_1+Q_2)+j(R_1+R_2+R_3)-(2i+3j)P_\infty.$$

Como os divisores são da forma $D=rP_\infty$, segue que

$$\frac{X^iY^j}{Z^{i+j}}\in\mathcal{L}(D)\Leftrightarrow 2i+3j\leq r.$$

- $0<r=2u<2^{2t}+2^{t+1}$
  Neste caso, temos
  $$1,\frac{X}{Z},...,\frac{X^u}{Z^u}\in\mathcal{L}(D).$$
  O elemento
  $$\frac{X^u}{Z^u}+S_1(\underline{\alpha})\frac{X^{u-1}}{Z^{u-1}}+S_2(\underline{\alpha})\frac{X^{u-2}}{Z^{u-2}}+...+S_u(\underline{\alpha}),$$
  onde os S_i's são os polinômios simétricos elementares e $\underline{\alpha}=(\alpha_1,...,\alpha_u)$, se anula em $2u=r$ pontos racionais, isto é, temos uma palavra-código com peso $n-r$. Portanto, $d=n-r$.
- $0<r=2u+1<2^{2t}+2^{t+1}$
  Neste caso, sabemos que $d=n-r$ ou $d=n-r+1$. Porém, temos também que
  $$\left[\tfrac{n-r-1}{2}\right]=\left[\tfrac{2^{2t}+2^{t+1}-2u-2}{2}\right]=2^{2t-1}+2^t-u-1;$$
  $$\left[\tfrac{n-r+1-1}{2}\right]=\left[\tfrac{2^{2t}+2^{t+1}-2u-1}{2}\right]=2^{2t-1}+2^t-u-1.$$
  Portanto, sendo $d=n-r$ ou $d=n-r+1$, não teremos alteração na quantidade de erros corrigidos pelo código.

• $car(K) = p \neq 2$
Neste caso, usando a forma canônica de Legendre [2], a curva tem equação da forma

$$Y^2 = X(X-1)(X-\lambda),\ \lambda \in K,\ \lambda \neq 0, 1.$$

Os divisores de intersecção são dados por

$$div(\mathcal{X} \cap Z) = 3P_\infty;$$
$$div(\mathcal{X} \cap X) = P_\infty + 2(0:0:1) = P_\infty + 2P_1;$$
$$div(\mathcal{X} \cap Y) = Q_1 + Q_2 + Q_3,\ Q_i \neq P_\infty.$$

Desta forma,

$$div(\frac{X^iY^j}{Z^{i+j}}) = 2iP_1 + j(Q_1 + Q_2 + Q_3) - (2i + 3j)P_\infty.$$

Portanto,

$$\frac{X^iY^j}{Z^{i+j}} \in \mathcal{L}(D) \Leftrightarrow 2i + 3j \leq r.$$

Como a curva é maximal ela deve possuir $1+p^{2t}+2p^t$ pontos racionais. O ponto $P_\infty = (0:1:0)$ é, novamente, o único ponto no infinito e, pela equação da curva, podemos encontrar também os pontos $P_1 = (0:0:1),\ P_2 = (1:0:1),\ P_3 = (\lambda:0:1)$. Os demais $p^{2t} + 2p^t - 3$ pontos racionais são da forma $(\alpha_i : \beta_1^i : 1),\ (\alpha_i : \beta_2^i : 1)$, com $i = 1, ..., \frac{p^{2t}+2p^t-3}{2}$.

- $r = p^{2t} + 2p^t - 1$(par)
  Neste caso, temos que $d = 1$ ou $d = 2$ e este código denotará a modulação ou o rótulo dos pontos da constelação de sinais.
- $0 < r = 2u < p^{2t} + 2p^t - 3$
  Neste caso, temos

  $$1, \frac{X}{Z}, ..., \frac{X^u}{Z^u} \in \mathcal{L}(D),$$

  e o elemento

  $$\frac{X^u}{Z^u} + S_1(\underline{\alpha})\frac{X^{u-1}}{Z^{u-1}} + S_2(\underline{\alpha})\frac{X^{u-2}}{Z^{u-2}} + ... + S_u(\underline{\alpha})$$

  se anula em $2u = r$ pontos racionais, gerando uma palavra-código com peso $n - r$. Portanto, $d = n - r$.
- $r = 3$
  Neste caso, $\frac{Y}{Z} \in \mathcal{L}(3P_\infty)$ e este se anula em $P_1,\ P_2$ e P_3, gerando uma palavra-código com peso $n - 3$.
- $3 < r = 2u + 1 < p^{2t} + 2^p t$
  Seja $r - 3 = 2v$. Temos que

  $$1, \frac{XY}{Z^2}, ..., \frac{X^vY}{Z^{v+1}} \in \mathcal{L}(D).$$

  O elemento

  $$\frac{X^vY}{Z^{v+1}} + S_1(\underline{\alpha})\frac{X^{v-1}Y}{Z^v} + S_2(\underline{\alpha})\frac{X^{v-2}Y}{Z^{v-1}} + ... + S_v(\underline{\alpha})\frac{Y}{Z},$$

  com $\underline{\alpha} = (\alpha_1, ..., \alpha_v)$, se anula em $2v + 3 = r$ pontos racionais, gerando uma palavra-código com peso $n - r$.

Além de encontrarmos os parâmetros dos códigos associados aos espaços $\mathcal{L}(rP_\infty)$, podemos também encontrar geradores para estes espaços. Para isso, vamos considerar os seguintes casos:

- $r = 3q$
  Os elementos

  $$1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}, ..., \frac{Y^{q-1}}{Z^{q-1}}, \frac{XY^{q-1}}{Z^q}, \frac{Y^q}{Z^q}$$

  estão em $\mathcal{L}(D)$ e são todos linearmente independentes. Como temos $3(q-2)+6 = 3q$ elementos, eles formam uma base do espaço.
- $r = 3q + 1$
  Os elementos

  $$1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{Y^q}{Z^q}, \frac{X^iY^j}{Z^{i+j}}, i = 0, 1, 2,\ j = 1, 2, ..., q-1$$

  estão em $\mathcal{L}(D)$ e são todos linearmente independentes. Como temos $3(q-1)+4 = 3q+1$ elementos, eles formam uma base do espaço.
- $r = 3q + 2$
  Os elementos

  $$1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{Y^q}{Z^q}, \frac{XY^q}{Z^{q+1}}, \frac{X^iY^j}{Z^{i+j}}$$

  com $i = 0, 1, 2,\ j = 1, 2, ..., q-1$ estão em $\mathcal{L}(D)$ e são todos linearmente independentes. Como temos $3(q-1)+5 = 3q+2$ elementos, eles formam uma base do espaço.

Podemos observar que se $r_1 < r_2$ então $\mathcal{L}(r_1P_\infty)$ é um subespaço de $\mathcal{L}(r_2P_\infty)$ e o código $\mathcal{C}(\mathcal{X}, \mathcal{P}, r_1P_\infty)$ é um subcódigo de $\mathcal{C}(\mathcal{X}, \mathcal{P}, r_2P_\infty)$. ■

III. EXEMPLO

Vamos considerar a curva Hermitiana $\mathcal{C}$, sobre o corpo $\mathbb{F}_4$, definida pela equação

$$\mathcal{C} : ZY^2 + Z^2Y = X^3. \quad (7)$$

Esta curva possui nove pontos racionais listado na Tabela I. Considerando $\mathcal{P} = \{P_1, ..., P_8\}$ e $D = rP_\infty$, temos que

TABELA I
PONTOS $\mathbb{F}_4$-RACIONAIS DA CURVA HERMITIANA.

$P_\infty = (0:1:0)$	$P_1 = (0:0:1)$	$P_2 = (0:1:1)$
$P_3 = (1:\alpha:1)$	$P_4 = (1:\alpha^2:1)$	$P_5 = (\alpha:\alpha:1)$
$P_6 = (\alpha^2:\alpha^2:1)$	$P_7 = (\alpha^2:\alpha:1)$	$P_8 = (\alpha:\alpha^2:1)$

se $0 < gr(D) < 8$, o código resultante terá parâmetros $(n, k, d) = (8, gr(D), d)$, com $8 - gr(D) \leq d \leq 8 - gr(D) + 1$.

Para calcularmos a matriz geradora dos códigos de Goppa, precisamos conhecer uma base do espaço

$$\mathcal{L}(D) = \{\varphi \in \mathbb{F}_q(\mathcal{C}) |\ div(\varphi) + rP_\infty \geq 0\}$$

com elementos da forma $\frac{X^iY^J}{Z^{i+j}}$. Usando a equação da curva, é possível mostrar que

$$\frac{X^iY^j}{Z^{i+j}} \in \mathcal{L}(rP_\infty) \Longleftrightarrow 2i + 3j \leq r. \quad (8)$$

Vamos encontrar as bases dos espaços $\mathcal{L}(rP_\infty)$, com $0 < r < 8$.

- $D = 7P_\infty$
  De (8) temos

  $$\frac{X^iY^j}{Z^{i+j}} \in \mathcal{L}(7P_\infty) \Longleftrightarrow 2i + 3j \leq 7.$$

Variando-se i e j e usando a equação da curva, conseguimos a seguinte base de $\mathcal{L}(7P_\infty)$

$$\mathcal{B}_1 = \left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}\right\}.$$

De acordo com (3), a matriz geradora do código é da forma

$$M = [G_i(P_j)],\ i = 1, ..., 7,\ j = 1, ..., 8,$$

com $\{G_i\}$ uma base de $\mathcal{L}(7P_\infty)$. Neste caso, considerando-se

$G_1 = 1,\ G_2 = \frac{X}{Z},\ G_3 = \frac{Y}{Z},\ G_4 = \frac{X^2}{Z^2}, G_5 = \frac{Y^2}{Z^2},$
$G_6 = \frac{XY}{Z^2},\ G_7 = \frac{X^2Y}{Z^3}$

temos

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 & \alpha & 1 & 1 \\ 0 & 0 & \alpha & \alpha^2 & 1 & 1 & \alpha^2 & \alpha \end{bmatrix}.$$

Assim, obtemos um código de Goppa C_1 com parâmetros $(n, k, d) = (8, 7, 2)$.

- $D = 6P_\infty$
  Possui base $\mathcal{B}_2 = \left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY}{Z^2}\right\}$, gerando um $(8, 6, 2)-$código.
- $D = 5P_\infty$
  Possui base $\mathcal{B}_3 = \left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}, \frac{Y^2}{Z^2}\right\}$, gerando um $(8, 5, 3)-$código.
- $D = 4P_\infty$
  Possui base $\mathcal{B}_4 = \left\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}\right\}$, gerando um $(8, 4, 4)-$código.
- $D = 3P_\infty$
  Possui base $\mathcal{B}_5 = \left\{1, \frac{X}{Z}, \frac{Y}{Z}\right\}$, gerando um $(8, 3, 5)-$código.
- $D = 2P_\infty$
  Possui base $\mathcal{B}_6 = \left\{1, \frac{X}{Z}\right\}$, gerando um $(8, 2, 6)-$código.

Vamos apresentar um modo de se fazer o puncionamento do código com parâmetros $(8, 7, 2)$ apresentado anteriormente. O objetivo deste puncionamento é a obtenção de códigos racionais com parametros $(4, 4, 1), (4, 3, 2), (4, 2, 3), (4, 1, 4)$. Podemos trocar o gerador $\frac{Y^2}{Z^2}$ por $\frac{X^3}{Z^3}$ e reescrever os geradores como

$G_1 = 1,\ G_2 = \frac{X}{Z},\ G_3 = \frac{X^2}{Z^2},\ G_4 = \frac{X^3}{Z^3}, G_5 = \frac{Y}{Z},$
$G_6 = \frac{XY}{Z^2},\ G_7 = \frac{X^2Y}{Z^3}.$

Reescrevendo os pontos racionais da curva

$P_\infty = (0:1:0)$ $P_1 = (0:0:1)$ $P_2 = (1:\alpha:1)$
$P_3 = (\alpha:\alpha^2:1)$ $P_4 = (\alpha^2:\alpha^2:1)$ $P_5 = (0:1:1)$
$P_6 = (1:\alpha^2:1)$ $P_7 = (\alpha:\alpha:1)$ $P_8 = (\alpha^2:\alpha:1)$

a matriz geradora do código fica da forma

$$M = \left[\begin{array}{c|c} M_1 & M_2 \\ \hline M_3 & \end{array}\right],$$

onde
$M_1 = [G_i(P_j)],\ i = 1, 2, 3, 4,\ j = 1, 2, 3, 4;$
$M_2 = [G_i(P_j)],\ i = 1, 2, 3, 4,\ j = 5, 6, 7, 8;$
$M_3 = [G_i(P_j)],\ i = 5, 6, 7,\ j = 1, ..., 8.$
Desta forma

$$M_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & \alpha \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

dá origem a um código racional com parâmetros $(4, 4, 1)$ e, retirando-se as linhas de baixo para cima, dá origem a códigos racionais com parâmetros $(4, 3, 2), (4, 2, 3), (4, 1, 4)$ respectivamente.
Cada palavra código do código original é da forma

$$v = v' + v''$$

onde

$$v' = (\textstyle\sum_1^4 a_i G_i(P_1), ..., \sum_1^4 a_i G_i(P_4), 0, 0, 0, 0)$$

$$v'' = (\textstyle\sum_5^7 a_i G_i(P_1), ..., \sum_5^7 a_i G_i(P_4), 0, 0, 0, 0) +$$

$$(0, 0, 0, 0, \textstyle\sum_1^7 a_i G_i(P_5), ..., \sum_1^7 a_i G_i(P_8))$$

Para o puncionamento, troque v por v' e ignore as 4 últimas coordenadas. Este raciocínio pode ser usado para obtenção dos outros códigos racionais.

IV. Conclusões

Dada uma curva eliptica maximal $\mathcal{C}$, tomando-se divisores com um ponto base da forma $D = rP_\infty$, os códigos de Goppa associados à curva, em sua maioria, possuem parâmetros $(n, r, d = n - r)$, onde $n = \mathcal{C}(k) - 1$.

Referências

[1] Judy L. Walker, *Codes and Curves*. AMS Press, 2000.
[2] Kenji Ueno, *An Introduction to Algebraic Geometry*. AMS Press, 1997.
[3] José Felipe Voloch, *Códigos Corretores de Erros*. IMPA, 1987.
[4] Jéfferson L.R. Bastos, *Forma Combinada de Conjunto de Sinais e Códigos de Goppa através da Geometria algébrica*. Tese de Doutorado (FEEC - UNICAMP), 2007.