Forma Combinada de Conjunto de Sinais e Códigos de Goppa através da Geometria Algébrica

Jefferson Luiz Rocha Bastos e Reginaldo Palazzo Jr.

***Resumo*— Neste trabalho propomos a construção de conjuntos de sinais e codigos na forma combinada atraves do uso dos codigos algebrico-geometricos. Esta proposta tem como fundamentação a utilização da topologia, como uma primeira abordagem, associada a cada bloco do modelo tradicional de sistemas de comunicações digitais ao inves da de espaço metrico. Mostramos que a forma natural de obtenção da forma combinada vem atraves do conhecimento do genero da superficie (invariante topologico).**

***Palavras-Chave*— Topologia, Codigos de Goppa, Genero da superficie, Forma Combinada Modulaçaõ/Codificação.**

***Abstract*— In this paper we propose a construction of signal sets and codes in the combined form by using algebraic-geometric codes. The foundantion of this proposal makes use of the topology, as a first approach, associated with each block in the traditional model of a comuunication system instead of the metric space approach. We show that the natural way of obtaining such a combined form is when the genus of the surface (topological invariant) is known.**

***Keywords*— Topology, Goppa Codes, Genus of a Surface, Combined Form Coding/Modulation.**

I. Introdução

Todo projetista de sistemas de comunicações faz uso das premissas de que o novo sistema deve ser mais confiável e menos complexo que os sistemas conhecidos. Nesta direção, a estrutura de espaço vetorial é fortemente utilizada ao projetar cada bloco no modelo tradicional de um sistema de comunicações de modo a alcançar os objetivos mencionados. Inerente à estrutura de espaço vetorial encontramos uma medida de distância, isto é, uma métrica. Esta métrica pode ser discreta ou contínua, dependendo se o espaço vetorial é discreto ou contínuo. Diante disso, cada bloco do modelo tradicional de um sistema de comunicações pode ser visto como um espaço métrico.

Como um espaço métrico dá origem a uma topologia, então podemos associar à cada bloco do sistema de comunicações o correspondente espaço topológico (superfície). Com isso, a nossa proposta passa a ser então a de projetar o sistema de comunicações sob o ponto de vista topológico. A razão para tal proposta está relacionada com o fato de que ela fornece um importante invariante geométrico, denominado *característica de Eüler*, esta intimamente relacionada com o gênero da superfície. Como consequência do conhecimento do gênero da superfície, podemos obter a caracterização algébrica desta superfície através do seu grupo fundamental. Portanto, se dispusermos do gênero da superfície associado à cada bloco poderemos estabelecer as condições a serem satisfeitas entre os diferentes espaços topológicos e, consequentemente, alcançar os objetivos mencionados anteriormente.

Em [1] analisamos e estabelecemos as condições necessárias e suficientes para que a proposta de primeiramente projetar o sistema de comunicações sob o ponto de vista topológico e em seguida fazer uso apropriado do espaço métrico associado seja factível. Todavia, não foram considerados em [1] os projetos dos codificadores e decodificadores de canal.

Dessa forma, é objetivo deste trabalho apresentar uma proposta de projeto do codificador combinado com o modulador, sob o enfoque de espaço topológico. Como consequência, estaremos utilizando a importância do invariante gênero da superfície, e ao mesmo tempo realçando e estabelecendo a importância dos códigos algébrico-geométricos, como sendo o paradigma para o projeto do bloco codificador de canal.

Este trabalho está organizado da seguinte forma. Na Seção II, apresentamos uma breve revisão do problema de mergulho de canais discretos sem memória em superfícies compactas orientadas. Consideramos o caso do canal simétrico binário na entrada e oito-ário na saída e seus possíveis mergulhos. Na Seção III, apresentamos os elementos essenciais sobre curvas e códigos de Goppa. Na Seção IV, apresentamos em detalhes as derivações dos códigos de Goppa sobre uma curva Hermitiana de gênero 1 para diferentes divisores. Neste contexto, mostramos como obter um sub-código de Goppa casado ao código de Goppa trivial (modulação). Esta é a forma combinada código-modulação. Na Seção V, desenvolvemos os mesmos procedimentos, porém para a curva de Hurwitz de gênero 1, como uma alternativa no sentido de comparações entre os sistemas de comunicações a serem projetados.

II. Definições e Conceitos Relacionados a Grafos e Superfícies

Nesta seção apresentamos os principais conceitos, definições e resultados relacionados à identificação da estrutura geométrica das superfícies associadas aos mergulhos de um canal discreto sem memória, quando visto como um grafo.

Definição 2.1: [3] Um grafo G' é dito *mergulhado* em uma superfície Ω quando quaisquer dois de seus ramos não se cruzam, a não ser em um vértice. O complemento de G' em Ω é chamado de *região*. Uma região homeomorfa (equivalência topológica) a um disco aberto é chamada *2-células*; se a região toda é uma 2-células, o mergulho é dito ser um *mergulho 2-*

Jefferson Luiz Rocha Bastos, Departamento de Matemática, IBILCE-UNESP,S. J. Rio Preto, Brasil, E-mail: jefferson@mat.ibilce.unesp.br

Reginaldo Palazzo Jr., Departamento de Telemática, FEEC-UNICAMP, Campinas, Brasil, E-mail: palazzo@dt.fee.unicamp.br. Este trabalho foi financiado pela FAPESP, CNPq e PROCAD-CAPES.

células. É de conhecimento geral que se G' é conectado, então o mergulho mínimo é um mergulho 2-células.

Um *grafo completo biparticionado* com m e n vértices, denotado por $K_{m,n}$, é um grafo consistindo de dois conjuntos distintos de vértices com m e n vértices, onde cada vértice de um conjunto está conectado através de ramos a todo vértice do outro conjunto.

Um invariante topológico importante de grafos e superfícies é a caracaterística de Eüler. Com isso, temos

Teorema 1: [4] Para $m, n \geq 2$, a característica de Eüler do grafo completo biparticionado $K_{m,n}$ é dada por $\chi\left(K_{m,n}\right) = 2[(m+n-mn/2)/2]$, onde $[a]$ denota o maior inteiro menor que ou igual ao número real a.

O primeiro procedimento, quando do mergulho de um grafo completo biparticionado em uma superfície, é determinar o valor mínimo da característica de Eüler da referida superfície. Se não existem restrições quanto ao mergulho ser um mergulho 2-células, então o mergulho pode ser realizado em qualquer superfície compacta orientada com característica maior ou igual à característica de Eüler. Por outro lado, quando o mergulho é 2-células, sabemos que existe também um valor máximo para a característica de Eüler da superfície dada. Como estamos interessados em mergulho 2-células de um grafo completo biparticionado $K_{m,n}$, então os valores mínimo e máximo do gênero das correspondentes superfícies terão que ser determinados. Esses valores são dados por:

- (i) O gênero mínimo, [5], de uma superfície compacta orientada é $g_m\left(K_{m,n}\right) = \{(m-2)(n-2)/4\}$, para $m, n \geq 2$, onde $\{a\}$ denota o menor inteiro maior que o número real a.
- (ii) O gênero máximo, [6], de uma superfície compacta orientada é $g_M\left(K_{m,n}\right) = [(m-1)(n-1)/2]$, para $m, n \geq 1$, onde $[a]$ denota o maior inteiro menor que o número real a.

A importância desses limitantes vem com o seguinte resultado:

Teorema 2: [3] Se um grafo G' tem um mergulho 2-células em superfícies de gênero g_m e g_M, então para todo inteiro g, $g_m \leq g \leq g_M$, G' tem um mergulho 2-células em uma superfície de gênero g.

Proposição 2.1: [3] Se Ω é um g-toro, denotado por gT, então o número de regiões α de $\mathfrak{F}_{mn}^{\alpha}$ é $\alpha = 2 - 2g - m - n + mn$.

A. Mergulhos do canal $\mathcal{C}_{2,8}$

Como um exemplo típico do processo sendo proposto, consideraremos o mergulho do grafo completo biparticionado $K_{2,8}$ em superfícies compactas orientadas. Associado a esses grafos temos o canal discreto sem memória $C_{2,8}$.

Canal $C_{2,8}\,[8,2]$: O quantizador de 8-níveis para o canal binário na entrada corresponde ao canal $C_{2,8}\,[8,2]$. Este canal e alguns de seus mergulhos são mostrados na Fig. 1.

O mergulho mínimo do canal $C_{2,8}[8,2]$ ocorre com gênero $g_m = 0$ (esfera). Isto é mostrado na Fig. 1 para $\mathcal{S} = 8R_4$, portanto uma tesselação regular.

Na segunda linha da Fig. 1 são mostrados dois mergulhos em $2T$ (bitoro, $g = 2$), um dos mergulhos com cinco regiões $(2R_4 + 3R_8)$, duas delas com quatro arestas e três delas com oito arestas, e o segundo mergulho com quatro regiões cada com oito arestas $(4R_8)$. Note que o último mergulho é uma tesselação regular. Na primeira linha da Fig. 1 são mostrados três mergulhos. O mais a esquerda é um toro ($g = 1$) com seis regiões, quatro delas com quatro arestas e duas delas com oito arestas. O mergulho mais a direita é um $3T$ (tritoro, $g = 3$) com duas regiões, uma delas com doze arestas e a outra com vinte arestas. Neste caso, o conjunto de superfícies compactas orientadas nas quais o canal $C_{2,8}\,[8,2]$ pode ser mergulhado é $\mathcal{A} = \{\mathcal{S}(8), T(6), 2T(4), 3T(2)\}$.

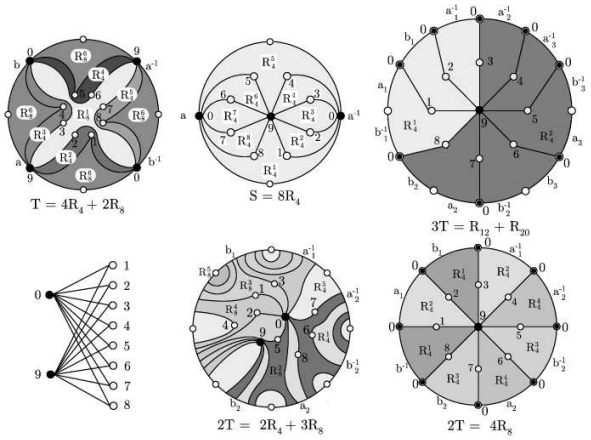

Fig. 1. Canal $C_{2,8}\,[8,2]$ e alguns de seus mergulhos

Neste ponto, chamamos a atenção do leitor ao fato de que uma vez que conhecemos o conjunto dos possíveis mergulhos do canal $C_{2,8}\,[8,2]$, e correspondentemente o conjunto dos gêneros das superfícies associadas, podemos através disso projetar a constelação de sinais associada ao código de Goppa trivial. Esta constelação é obtida através de curvas algébricas cujo gênero é especificado para cada caso contido no conjunto $\mathcal{A}$. O código corretor de erros a ser utilizado é um subcódigo do código de Goppa trivial, satisfazendo as características do canal $C_{2,8}\,[8,2]$.

Sabemos de [2] que o melhor desempenho é atingido para constelações de sinais em espaços com curvatura constante negativa, equivalentemente, em superfícies com o maior gênero possível. No caso do canal $C_{2,8}\,[8,2]$, o melhor desempenho é, portanto, atingido para $g = 3$. Todavia, iremos considerar, como caso ilustrativo, o caso em que $g = 1$ na especificação dos códigos de Goppa. Isto será realizado nas Seções IV e V.

III. Curvas e Códigos de Goppa

Seja k um corpo e $\overline{k}$ seu fecho algébrico.

Definição 3.1: O plano projetivo $\mathbb{P}^2(k)$ é definido como

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

onde $(X_1, X_2, X_3) \sim (Y_1, Y_2, Y_3) \iff \exists\ a \in k^*;\ X_i = aY_i,\ i = 1, 2, 3$.

Como os pontos de $\mathbb{P}^2(k)$ são classes de equivalência, iremos usar a notação $(X : Y : Z)$ para representar estes elementos.

Definição 3.2: Seja $F(X,Y,Z) \in k[X,Y,Z]$ um polinômio homogêneo de grau d. A curva projetiva associada ao polinômio F consiste do conjunto $\mathcal{X}(k) = \{(x:y:z) \in \overline{k}^3 |\ F(x,y,z) = 0\}$.

Podemos também associar a uma curva o seu gênero, denotado por $g(\mathcal{X})$ que satisfaz

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

A igualdade em (1) é atingida quando a curva for não singular, isto é, quando for válida a condição $F(x,y,z) = F_X(x,y,z) = F_Y(x,y,z) = F_Z(x,y,z) = 0$, implicando que $(x,y,z) = (0,0,0)$, onde $F_X,\ F_Y,\ F_Z$ são as derivadas parciais de F com relação às variáveis X, Y e Z, respectivamente.

Definição 3.3: 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 por $\mathcal{X}(K) = \{(x:y:z) \in K^3 |\ F(x,y,z) = 0\}$.

Com relação aos conjuntos definidos anteriormente vale o seguinte resultado.

Teorema 3.1: Seja $\mathcal{X}$ uma curva projetiva não singular definida sobre um corpo finito $k = \mathbb{F}_q$. Então o limitante superior do número de pontos racionais é dado por $\#\mathcal{X}(\mathbb{F}_q) \leq 1 + q + \lfloor 2g\sqrt{q} \rfloor$, onde $g = g(\mathcal{X})$.

Definição 3.4: Seja $\mathcal{X}$ uma curva definida em $\mathbb{F}_q$. Um divisor D em $\mathcal{X}$ 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 escrevemos $D \geq 0$.

Definimos o grau de um divisor como sendo $deg(D) = \sum n_Q deg(Q)$, e o suporte de um divisor como sendo o conjunto $supp(D) = \{Q |\ n_Q \neq 0\}$.

Definição 3.5: Seja $F(X,Y,Z)$ um polinômio que define uma curva plana projetiva $\mathcal{X}$ sobre $\mathbb{F}_q$. O corpo das funções racionais em $\mathcal{X}$ é o conjunto $\mathbb{F}_q(\mathcal{X})$ dado por

$$\left(\left\{ \frac{g(X,Y,Z)}{h(X,Y,Z)} \right\} \cup \{0\} \right) / \sim,$$

onde $g/h \sim g'/h' \leftrightarrow gh' - g'h \in \langle F \rangle$, e g, h são homogêneos de mesmo grau.

Definição 3.6: Seja $\mathcal{X}$ uma curva e $f = \frac{g}{h} \in \mathbb{F}_q(\mathcal{X})$. O divisor de f é definido como $div(f) = \sum P - \sum Q$, onde $\sum P$ é o divisor da interseção $\mathcal{X} \cap \mathcal{X}_g$ e $\sum Q$ é o divisor $\mathcal{X} \cap \mathcal{X}_h$.

Definição 3.7: Seja D um divisor sobre uma curva não singular. O espaço das funções racionais associadas a D é o conjunto $\mathcal{L}(D) = \{f \in \mathbb{F}_q(\mathcal{X}) |\ div(f) + D \geq 0\} \cup \{0\}$.

O conjunto da Definição 3.7 é um espaço vetorial finitamente gerado sobre $\mathbb{F}_q$. Com isso, temos o seguinte resultado.

Teorema 3.2 (Teorema de Riemann-Roch): Seja $\mathcal{X}$ uma curva plana projetiva não singular de gênero g definida sobre $\mathbb{F}_q$ e D um divisor em $\mathcal{X}$. Então $dim\mathcal{L}(D) \geq deg(D) + 1 - g$. Mais ainda, se $deg(d) > 2g - 2$, então $dim\mathcal{L}(D) = deg(D) + 1 - g$.

Com isso, podemos definir os códigos algébricos-geométricos da seguinte forma. Considere $\mathcal{X}$ uma curva plana projetiva não singular 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 $\mathcal{P} \cap supp(D) = \emptyset$, então

Definição 3.8: O código algébrico-geométrico associado a $\mathcal{X}$, $\mathcal{P}$ e D é $\mathcal{C}(\mathcal{X}, \mathcal{P}, D) = \{(f(P_1), ..., f(P_n)) |\ f \in \mathcal{L}(D)\} \in \mathbb{F}_q^n$.

Os parâmetros (n, k, d) do código $\mathcal{C}(\mathcal{X}, \mathcal{P}, D)$ são dados pelo seguinte resultado.

Teorema 3.3: Seja $\mathcal{X}$ uma curva plana, projetiva, não singular, 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 $2g - 2 < deg(D) < n$. Então o código algébrico-geométrico $\mathcal{C}(\mathcal{X}, \mathcal{P}, D)$ é linear de comprimento n, dimensão $k = deg(D) + 1 - g$ e distância mínima $d \geq n - deg(D)$.

IV. Códigos de Goppa sobre uma Curva Hermitiana

A curva Hermitiana $\mathcal{X}$ é uma curva definida pelo polinômio homogêneo

$$F(X,Y,Z) = ZY^2 + Z^2Y + X^3. \quad (2)$$

Como o grau de $F(X,Y,Z)$ é 3 e as raízes são distintas, então de (1) temos que o gênero desta curva é dado por $g(\mathcal{X}) = 1$. Além disso, $F(X,Y,Z)$ é uma curva maximal em $\mathbb{F}_4$, isto é, a quantidade de pontos racionais da curva atinge a cota máxima dada por $\mathcal{X}(\mathbb{F}_4) = 1 + 4 + 2.1.2 = 9$, veja Teorema 3.1. Nesta direção, vamos considerar $\mathbb{F}_4 = \frac{\mathbb{F}_2[t]}{\langle t^2 + t + 1 \rangle} = \{0, 1, \alpha, \alpha^2\}$, onde $\alpha = \overline{t}$ e, portanto, satisfaz $\alpha^2 = \alpha + 1$.

Os pontos racionais dessa curva são:

$$\begin{array}{lll} P_\infty = (0:1:0) & P_1 = (0:0:1) & P_2 = (0:1:1) \\ P_3 = (1:\alpha:1) & P_4 = (1:\alpha:1) & P_5 = (\alpha:\alpha:1) \\ P_6 = (\alpha^2:\alpha^2:1) & P_7 = (\alpha^2:\alpha:1) & P_8 = (\alpha:\alpha^2:1) \end{array}$$

Usando o Teorema 3.3 e considerando $\mathcal{P} = \{P_1, ..., P_8\}$ e $D = rP_\infty$ temos que, se $0 < deg(D) < 8$, o código em consideração será um $(8, deg(D), d)-$código com distância mínima $8 - deg(D) \leq d \leq 8 - deg(D) + 1$ (note que $g(\mathcal{X}) = 1$).

A seguir, iremos considerar os códigos de Goppa correspondentes aos divisores $D = rP_\infty$, com $1 \leq r \leq 7$.

A. Caso 1: $D = 7P_\infty$

Neste caso temos que encontrar uma base para o espaço vetorial

$$\mathcal{L}(7P_\infty) = \{f \in \mathbb{F}_4(\mathcal{X});\ div(f) + 7P_\infty \geq 0\}.$$

Vamos procurar bases da forma $(\frac{X^iY^j}{Z^{i+j}})$ uma vez que temos

$$div(\frac{X^iY^j}{Z^{i+j}}) = (3j+i)P_1 + iP_2 - (2i+3j)P_\infty.$$

Assim,

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

Variando-se i e j, conseguimos os seguintes elementos: $\{1, \frac{X}{Z}, \frac{X^2}{Z^2}, \frac{X^3}{Z^3}, \frac{Y}{Z}, \frac{Y^2}{Z^2}, \frac{XY}{Z^2}, \frac{X^2Y}{Z^3}\}$.

Tendo como base a equação que define a curva, isto é, a equação (2), temos $\frac{Y^2}{Z^2} + \frac{Y}{Z} + \frac{X^3}{Z^3} = 0$, isto é, os elementos acima são linearmente dependentes. Podemos, então, retirar o elemento $\frac{X^3}{Z^3}$ do conjunto acima. Os elementos restantes são LIs e, de acordo com o resultado em [8], a matriz geradora do código é da forma $M = [G_i(P_j)],\ i = 1, ..., 7,\ j = 1, ..., 8$, onde os G_i´s formam uma base de $\mathcal{L}(7P_\infty)$. Consequentemente, a matriz verificação de paridade é, portanto, dada por

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Assim, conseguimos construir um código de Goppa com parâmetros $(8, 7, 2)$.

B. Caso 2: $D = 6P_\infty$

Neste caso, notamos que $div(\frac{X^2Y}{Z^3}) = 5P_1 + 2P_2 - 7P_\infty$ e, consequentemente que X^2Y/Z^3 não pertence à base do espaço vetorial $\mathcal{L}(6P_\infty)$. Logo, a base deste espaço vetorial é dada pelo conjunto $\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY}{Z^2}\}$.

A matriz verificação de paridade é dada por

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

Consequentemente, temos um código de Goppa com parâmetros $(8, 6, 2)$.

C. Caso 3: $D = 5P_\infty$

Neste caso temos $div(\frac{Y^2}{Z^2}) = 6P_1 - 6P_\infty$. Com isso, notamos que $\frac{Y^2}{Z^2} \notin \mathcal{L}(5P_\infty)$. Logo, a base do correspondente espaço vetorial é então dada por $\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}, \frac{XY}{Z^2}\}$.

A matriz verificação de paridade é dada por

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

Assim, um código de Goppa com parâmetros $(8, 5, 3)$ é obtido.

D. Caso 4: $D = 4P_\infty$

Neste caso temos $div(\frac{XY}{Z^2}) = 4P_1 + P_2 - 5P_\infty$. Com isso, notamos que $\frac{XY}{Z^2} \notin \mathcal{L}(4P_\infty)$. Logo, a base do correspondente espaço vetorial é então dada por $\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}\}$.

A matriz verificação de paridade é dada por

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

Assim, um código de Goppa $(8, 4, 4)$ é obtido.

E. Caso 5: $D = 3P_\infty$

Neste caso temos $div(\frac{X^2}{Z^2}) = 2P_1 + 2P_2 - 4P_\infty$. Com isso, notamos que $\frac{X^2}{Z^2} \notin \mathcal{L}(3P_\infty)$. Logo, a base do correspondente espaço vetorial é, então, dada por $\{1, \frac{X}{Z}, \frac{Y}{Z}\}$.

A matriz verificação de paridade é dada por

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

Assim, um código de Goppa $(8, 3, 5)$ é obtido.

F. Caso 6: $D = 2P_\infty$

Neste caso temos $div(\frac{Y}{Z}) = 3P_1 - 3P_\infty$. Com isso, notamos que $\frac{X^2}{Z^2} \notin \mathcal{L}(2P_\infty)$. Logo, a base do correspondente espaço vetorial é, então, dada por $\{1, \frac{X}{Z}\}$.

A matriz verificação de paridade é dada por

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

Logo, um código de Goppa $(8, 2, 6)$ é obtido.

G. Caso 7: $D = P_\infty$

Neste caso temos um código de Goppa $(8, 1, 8)$ cuja matriz geradora é dada por

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

V. Código de Goppa sobre uma Curva de Hurwitz

Em [7] é mostrado que o modelo não singular da curva

$$X^nY + Y^nZ + Z^nX = 0$$

é maximal em $\mathbb{F}_{q^2}$ se, e somente se, $q+1 \equiv 0\ mod(n^2-n+1)$. Tomando-se $q = 2,\ n = 2$ vemos que a condição anterior é satisfeita. Consequentemente, a curva é definida por $X^2Y + Y^2Z + Z^2X = 0$, em $\mathbb{F}_4$. Esta curva é não singular, com gênero $g(\mathcal{X}) = 1$ e, assim como ocorre com a curva Hermitiana, a curva de Hurwitz é maximal com nove pontos racionais, veja Teorema 3.1.

Os pontos racionais dessa curva são:

$$\begin{array}{lll} P_1 = (0:1:0) & P_2 = (1:0:0) & P_3 = (0:0:1) \\ P_4 = (1:\alpha:1) & P_5 = (1:\alpha^2:1) & P_6 = (\alpha:1:1) \\ P_7 = (\alpha^2:1:1) & P_8 = (\alpha:\alpha:1) & P_9 = (\alpha^2:\alpha^2:1) \end{array}.$$

Nosso interesse é determinar uma base para o espaço vetorial cujos elementos são da forma $\frac{X^iY^j}{Z^{i+j}}$. Após algumas manipulações algébricas chegamos a

$$div\left(\frac{X^iY^j}{Z^{i+j}}\right) = (2i+j)P_3 + (j-i)P_2 - (2j+i)P_1.$$

Pensando-se na construção da matriz geradora do código e nas bases como acima, temos que tratar de divisores da forma $D = rP_1 + sP_2$ e assim temos

$$(\frac{X^iY^j}{Z^{i+j}}) \in \mathcal{L}(D) \Longleftrightarrow 2j + i \leq r \text{ e } i \leq j + s.$$

Assim, tomando-se $\mathcal{P} = \{P_3, ..., P_9\}$ e $D = rP_1 + sP_2$ temos que, se $0 < deg(D) = r + s < 7$, o código será um $(7, deg(D), d)$-código com $7 - deg(D) \leq d \leq 7 - deg(D) + 1$.

A. *Caso* $deg(D) = r + s = 6$

Neste caso a dimensão do espaço é 6 e, portanto, devemos ter seis elementos LIs da forma $\left(\frac{X^iY^j}{Z^{i+j}}\right)$. Temos a seguinte tabela para observar:

r	s	condição
0	6	$2j + i \leq 0,\ i \leq j + 6$
1	5	$2j + i \leq 1,\ i \leq j + 5$
2	4	$2j + i \leq 2,\ i \leq j + 4$
3	3	$2j + i \leq 3,\ i \leq j + 3$
4	2	$2j + i \leq 4,\ i \leq j + 2$
5	1	$2j + i \leq 5,\ i \leq j + 1$
6	0	$2j + i \leq 6,\ i \leq j + 0$

Nas três primeiras linhas da tabela não conseguimos encontrar seis elementos que sejam LIs. Temos, então, as seguintes possibilidades:

1) $2j + i \leq 3,\ i \leq j + 3$*:* Neste caso conseguimos os elementos $\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2}{Z^2}, \frac{X^3}{Z^3}\}$ que são LIs e formam uma base de $\mathcal{L}(3P_1 + 3P_2)$. A matriz geradora é então dada por

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

que nos dá um $(7, 6, 1)$-código de Goppa.

2) $2j + i \leq 4,\ i \leq j + 2$*:* Neste caso conseguimos os elementos $\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2}{Z^2}, \frac{Y^2}{Z^2}\}$ que são LIs e formam uma base de $\mathcal{L}(4P_1 + 2P_2)$. A matriz geradora na forma padrão é dada por

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

que nos dá um $(7, 6, 1)$-código de Goppa.

3) $2j + i \leq 5,\ i \leq j + 1$*:* Neste caso conseguimos os elementos $\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY^2}{Z^3}\}$ que são LIs e formam uma base de $\mathcal{L}(5P_1 + P_2)$. A matriz verificação de paridade é dada por

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

o que nos dá um $(7, 6, 2)$-código de Goppa.

4) $2j + i \leq 6,\ i \leq j + 0$*:* Conseguimos a base $\{1, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY^2}{Z^3}, \frac{Y^3}{Z^3}\}$ e matriz geradora

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

que nos fornece um $(7, 6, 1)$-código de Goppa.

B. $deg(D) = r + s = 5$

Assim como no caso anterior, temos a seguinte tabela

r	s	condição
0	5	$2j + i \leq 0,\ i \leq j + 5$
1	4	$2j + i \leq 1,\ i \leq j + 4$
2	3	$2j + i \leq 2,\ i \leq j + 3$
3	2	$2j + i \leq 3,\ i \leq j + 2$
4	1	$2j + i \leq 4,\ i \leq j + 1$
5	0	$2j + i \leq 5,\ i \leq j + 0$

Consideraremos os seguintes casos.

1) $2j + i \leq 3,\ i \leq j + 2$*:* A base do correspondente espaço vetorial é $\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{X^2}{Z^2}\}$, cuja matriz geradora na forma padrão é dada por

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

o que nos dá um $(7, 5, 2)$-código de Goppa (gerador com peso 2)

2) $2j + i \leq 4,\ i \leq j + 1$*:* A base do correspondente espaço vetorial é $\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{Y^2}{Z^2}\}$, cuja matriz geradora na forma padrão é dada por

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

que nos dá um $(7, 5, 2)$-código de Goppa.

3) $2j + i \leq 5,\ i \leq j + 0$*:* A base do correspondente espaço vetorial é $\{1, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{Y^2}{Z^2}, \frac{XY^2}{Z^3}\}$, cuja matriz geradora é dada por

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

que nos fornece um $(7, 5, 1)$-código de Goppa (somando-se as 4 últimas linhas obtemos um gerador de peso 2).

C. Caso $deg(D) = r + s = 4$

Assim como no caso anterior, temos a tabela

r	s	condição
0	4	$2j + i \leq 0,\ i \leq j + 4$
1	3	$2j + i \leq 1,\ i \leq j + 3$
2	2	$2j + i \leq 2,\ i \leq j + 2$
3	1	$2j + i \leq 3,\ i \leq j + 1$
4	0	$2j + i \leq 4,\ i \leq j + 0$

Iremos considerar os seguintes casos.

1) $2j + i \leq 2,\ i \leq j + 2$*:* A base do correspondente espaço vetorial é $\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{X^2}{Z^2}\}$, cuja matriz geradora na forma padrão é dada por

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

o que nos dá um $(7, 4, 3)$-código de Goppa.

2) $2j + i \leq 3,\ i \leq j + 1$*:* A base do correspondente espaço vetorial é $\{1, \frac{X}{Z}, \frac{Y}{Z}, \frac{XY}{Z^2}\}$, cuja matriz geradora na forma padrão é dada por

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

que nos dá um $(7, 4, 3)$-código de Goppa.

3) $2j + i \leq 4,\ i \leq j + 0$*:* A base do correspondente espaço vetorial é $\{1, \frac{Y}{Z}, \frac{XY}{Z^2}, \frac{Y^2}{Z^2}\}$, cuja matriz geradora na forma padrão é dada por

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

que nos fornece um $(7, 4, 3)-$código de Goppa.

D. Caso $deg(D) = r + s = 3$

Assim como no caso anterior, temos a tabela

r	s	condição
0	3	$2j + i \leq 0,\ i \leq j + 3$
1	2	$2j + i \leq 1,\ i \leq j + 2$
2	1	$2j + i \leq 2,\ i \leq j + 1$
3	0	$2j + i \leq 3,\ i \leq j + 0$

Iremos considerar os seguintes casos.

1) $2j+i \leq 2,\ i \leq j+1$*:* A base do espaço é formada pelos elementos $\{1, \frac{X}{Z}, \frac{Y}{Z}\}$ com matriz geradora na forma padrão

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

que nos dá um $(7, 3, 4)-$código de Goppa.

2) $2j + i \leq 3,\ i \leq j + 0$*:* A base do espaço é formada pelos elementos $\{1, \frac{Y}{Z}, \frac{XY}{Z^2}\}$ com matriz geradora

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

que nos fornece um $(7, 3, 4)$-código de Goppa (somando-se as 2 últimas linhas temos um gerador de peso 4).

E. Caso $deg(D) = r + s = 2$

Temos a tabela

r	s	condição
0	2	$2j + i \leq 0,\ i \leq j + 2$
1	1	$2j + i \leq 1,\ i \leq j + 1$
2	0	$2j + i \leq 2,\ i \leq j + 0$

Iremos considerar os seguintes casos.

1) $\mathcal{L}(P_1 + P_2)$*:* Este espaço é gerado pelo conjunto $\{1, \frac{X}{Z}\}$ que nos fornece a matriz geradora

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

dando origem a um $(7, 2, 5)$-código de Goppa.

2) $\mathcal{L}(2P_1)$*:* Este espaço é gerado pelo conjunto $\{1, \frac{Y}{Z}\}$ que nos fornece a matriz geradora na forma padrão

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

dando origem a um $(7, 2, 5)$-código de Goppa.

REFERÊNCIAS

[1] R.G. Cavalcante, H. Lazari, J.D. Lima, e R. Palazzo Jr., "A new approach to the design of digital communication systems,"*American Mathematical Society, DIMACS Series*, pp. 1-32, August 2005.

[2] R.G. Cavalcante, e R. Palazzo Jr., "Performance analysis of M-PSK signal constellations in Riemannian varieties," *Lecture Notes in Computer Science*, Springer-Verlag, 2003.

[3] J.D. de Lima, e R. Palazzo Jr., "Embedding discrete memoryless channels on compact and minimal surfaces," *IEEE Information Theory Workshop*, Bangalore, India, pp. 20-25, October 2002.

[4] D. König, *Theirue der Endlichen und Unendlichen Graphen*, Leipzig, 1936, reprinted, Chelsea, New York, 1950.

[5] G. Ringel, Das Geschlecht des Vollständigen paaren Graphen, *Abh. Math. Sem. Univ. Hamburg*, **28** (1965), 139-150.

[6] R.D. Ringeisen, Determining all Compact Orientable 2-manifolds upon which $K_{m,n}$ has 2-cell Embeddings, *Journal Combinatorial Theory*, **12** (1972), 101-104.

[7] A. Aguglia, G. Gabor, e F. Torres, "Plane maximal curves,"*Acta Arithmeticae*, **98** (2001), No. 2, 165-179.

[8] J. Walker, *Codes and Curves*, American Mathematical Society, 2000.