Códigos Temporais Perfeitos 2×2 Provenientes de Constelações de Sinais HEX

Edson Donizete de Carvalho e Antonio Aparecido de Andrade

***Resumo*— Neste trabalho apresentamos uma nova construção de códigos temporais perfeitos 2×2 a partir de constelações HEX. Este código tem taxa máxima, diversidade máxima, seu determinante mínimo não tende a zero, e possui a propriedade de ter a mesma energia média de transmissão por antenas.**

***Palavras-Chave*— Álgebra cíclica, álgebra de divisão, código perfeito, forma cúbica.**

***Abstract*— In this work we propose a new 2×2 perfect space-time codes from HEX constellation. This code has full rate, full diversity, nonvanishing constant minimum determinant and uniform average transmitted energy per antenna.**

***Keywords*— Cyclic algebra, division algebra, perfect codes, cubic shaping.**

I. INTRODUÇÃO

Códigos temporais são usados em canais de comunicações móveis, na qual as transmissões de informações parte de M antenas transmissoras e é recebida por N antenas receptoras. Estes canais são afetados por múltiplos percursos de propagação, podendo alterar de maneira significativa a amplitude do sinal, as variações de amplitude e fase do canal sofrem alterações com a variação da distância e do posicionamento entre transmissor e receptor, comportamento este conhecido como *desvanecimento*. As perdas em propagações, variações no tempo, ruídos, e no desvanecimento, dificultam a obtenção de altas taxas de transmissões [1].

Por outro lado, o que dificulta o projeto de códigos que minimizem a probabilidade de erro no receptor é quando é imposto uma taxa de tranmsissão mais elevada. Uma boa estratégia para a resolução de tal problema é a utilização de técnicas de *diversidade*, fornecendo réplicas de informações ao receptor, ou seja, para cada período de tempo $t = T$, tomamos y_{mt}, para $m = 1, \cdots, M$, sinais que são transmitidos simultaneamente, a partir das M antenas. Estes canais de comunicações são considerados perfeitos, isto é, a distribuição da probabilidade de erro é homogênea. Em cada período de tempo t o sinal recebido x_t^j, a partir da antena j, é dado por

$$x_t^j = \sum_{i=1}^{n} h_{i,j} y_{mt} + w_t^j, \tag{1}$$

com $h_{i,j}$ sendo o ganho do canal entre a antena transmissora i e a antena receptora j, e w_t^j é o ruído introduzido pelo canal. Pelo fato do canal ser perfeito, as informações recebidas podem ser avaliadas através da métrica de decisão acumulada dada por

$$\sum_{t=1}^{l} \sum_{j=1}^{m} |x_t^j - \sum_{i=1}^{n} h_{i,j} y_{mt}|^2, \tag{2}$$

sobre todas as palavras códigos

$$y_1^1 y_1^2 \cdots y_1^m y_2^1 y_2^2 \cdots y_2^m \cdots y_l^1 y_l^2 \cdots y_l^m,$$

e decide em favor da palavra código que minimiza esta soma.

Denotando por X a matriz de sinal recebida de ordem $N \times M$, por Y a matriz de codificação de ordem $N \times T$, por H a matriz que representa os caminhos entre as antenas no canal de ordem $T \times M$, e por W a matriz que representa o ruído de ordem $N \times M$, tem-se que este modelo de transmissão pode ser definido pela igualdade matricial

$$X = YH + W. \tag{3}$$

Para minimizar a métrica de decisão acumulada definida na Equação (2), que decide em favor da palavra código que minimiza tal soma, equivale a avaliar o posto da matriz Y dada pela igualdade matricial dada na Equação (3).

Critério do posto: Se $s_1 \neq s_j$, para todo $j = 2, 3, \cdots, k$, onde $s = (s_1, s_2, \cdots, s_k)$ é um vetor símbolo de informação, então devemos maximizar o posto r da matriz $Y(s_1) - Y(s_j)$, tomados sobre todos os pares distintos (s_1, s_j), ou seja, equivale maximizar a diversidade.

Neste trabalho, estamos interessados nos código que possuam a propriedade de que o determinante associado a suas palavras códigos não tende a zero, sem a normalização, ou seja, quando existe uma cota inferior para o determinante mínimo, e que não dependa do tamanho da constelação. Em outras palavras, impomos que o determinante mínimo do código seja constante para altos valores de eficiência espectral.

Fixar o determinante mínimo é um dos principais parâmetros introduzidos pelos *códigos perfeitos* em [2], o outro está relacionado com forma geométrica que a constelação assume.

Para otimizar a energia eficiente destes códigos, requer que as palavras códigos sejam dadas na forma Rv, onde R é a matriz unitária, que codifica os símbolos de informações e v é o vetor que contém símbolos de informações QAM ou HEX. Referimos a este tipo de constelação, de *forma cúbica*, dado que a matriz aplicada sobre os vetores contém valores discretos, que podemos interpretar como uma matriz geradora de pontos de um reticulado. Caso, a constelação seja QAM tem-se reticulados na forma cúbica $\mathbb{Z}^n$ e se for HEX tem-se reticulados na forma A_2^n. Em [2], Oggier e et. all construíram códigos perfeitos em dimensões 2×2 e 4×4

Edson Donizete de Carvalho, Departamento de Matemática, FEIS-UNESP, Ilha Solteira - SP, Brasil, E-mail: edson@mat.feis.unesp.br.

Antonio Aparecido de Andrade, Departamento de Matemática, IBILCE-UNESP, São José do Rio Preto - SP, Brasil, E-mail: andrade@ibilce.unesp.br.

a partir de constelações QAM e de dimensões 3×3 e 6×6 a partir de constelações HEX. Com base nestes fatos, neste trabalho, propomos uma nova construção, de códigos perfeitos de dimensão 2×2 para constelação HEX. O trabalho possui a seguinte distribuição de seções. Na Seção II fornecemos os conceitos preliminares de códigos temporais. Na Seção III são dados os conceitos de álgebras cíclicas e de códigos perfeitos. Na Seção IV apresentamos nossa construção de códigos perfeitos 2×2 a partir da constelação HEX, e finalmente na Seção V damos nossas conclusões finais.

II. Exposição do Problema

Hassibi em [3] introduziu o conceito de códigos temporais de bloco linear, isto é, códigos que comprimem as informações no espaço e no tempo. São estes códigos que estamos considerando neste trabalho. Caso, esses códigos tenham a propriedade de que a quantidade dos símbolos transmitidos seja a mesma dos símbolos de informações recebidos, dizemos que o código tem *taxa máxima*.

Oggier et. all [2] e Belfiore et. all [4] construiram códigos a partir do espaço de matrizes quadradas, ou seja, quando $M = T$. Estes códigos chamados de "Square Codes", possuem M graus de liberdade, e usam símbolos de informação QAM (Quadrature Amplitude Modulation). Além disso, pelo fato das palavras códigos serem formadas por matrizes quadradas, tem-se pelo critério do posto que o código tem diversidade máxima se

$$|det(X_i - X_j)|^2 \neq 0,$$

para todo $X_i \neq X_j \in \mathcal{C}$. A partir da linearidade destes códigos, podemos simplificar o critério do posto avaliando apenas o seguinte determinante

$$|det(X)|^2 \neq 0,$$

sobre todas palavras códigos não nulas $X \in \mathcal{C}$.

Quando o código tem diversidade máxima, a próxima etapa é maximizar o ganho de codificação, que é definido pelo *determinante mínimo* do código. Deste modo, considerando códigos infinitos $\mathcal{C}_\infty$, o determinante mínimo do código é dado por

$$\delta_{min}(\mathcal{C}_\infty) = min_{0 \neq X \in \mathcal{C}_\infty} |det(X)|^2.$$

Porém, o determinante mínimo depende da eficiência espectral, podendo tender a zero quando a constelação de sinais torna-se muito grande.

III. Álgebras Cíclicas e Códigos Temporais

Por meio da teoria algébrica dos números Oggier et. all [2] e Belfiore et. all [4], [5] obtiveram bons parâmetros para os códigos temporais. Os leitores que não estiverem familarizados com conceitos de teoria algébrica dos números recomendamos fazer uma leitura preliminar do Apêndice I.

Nesta direção, eles mostraram que uma boa alternativa é considerar o espaço das matrizes complexas $\mathcal{M}_n(\mathbb{C})$ de ordem $n \times n$ como um ambiente natural para os códigos temporais $\mathcal{C}$, e que apresentem uma estrutura de reticulado de posto máximo, e além disso, mostraram que quando o código $\mathcal{C}$ possui posto máximo o ganho de codificação é proporcional ao *determinante mínimo*.

Agora, se considerarmos corpos de números K e F tal que K seja uma extensão cíclica de grau n sobre F, cujo grupo de Galois seja dado por $Gal(K/F) =< \sigma >$, então podemos definir uma álgebra cíclica $\mathcal{A} = (K/F, \sigma, \gamma)$ de grau n dada por

$$\mathcal{A} = 1K \oplus uK \oplus \cdots \oplus u^{n-1}K, \tag{4}$$

satisfazendo a condição de que $u \in \mathcal{A}, ux = u\sigma(x)$ para todo $x \in K$ e $u^n = \gamma \in F^* = F - \{0\}$. Assim, um elemento $a = x_0 + ux_1 + \ldots + u^{n-1}x_{n-1} \in \mathcal{A}$, pode ser identificado pela matriz X ([2] e [6]), dada por

$$X = \begin{pmatrix} x_0 & \gamma\sigma(x_{n_1}) & \gamma\sigma^2(x_{n_2}) & \ldots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n_1}) & \ldots & \gamma\sigma^{n-1}(x_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & \sigma(x_{n_2}) & \sigma^2(x_{n_3}) & \ldots & \sigma^{n-1}(x_1) \end{pmatrix}. \tag{5}$$

A. Taxa Máxima e Diversidade Máxima

Esta subseção tem como objetivo mostrar como podemos obter uma codificação a partir das álgebras cíclicas. Note que todos os coeficientes das matrizes X da forma da Equação (5) estão em K, quando K é considerado como um espaço vetorial de dimensão n sobre F. Assim, cada x_i é uma combinação linear de n elementos em F. Os símbolos de informações são tomados a partir de F. Se considerarmos uma constelação QAM então a constelação pode ser vista como um subconjunto de $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ (anel de inteiros de Gauss), sendo que $i^2 = -1$. Como $\mathbb{Z}[i] \subset \mathbb{Q}(i)$, tomamos $F = \mathbb{Q}(i)$. De forma similar, os símbolos HEX podem ser vistos como um subconjunto de $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$ (anel de inteiros de Eisenstein), sendo que $\omega = e^{\frac{2i\pi}{3}} = \frac{-1+i\sqrt{3}}{2}$, a raiz terceira primitiva da unidade. Como $\mathbb{Z}[\omega] \subset \mathbb{Q}(\omega)$, tomamos $F = \mathbb{Q}(\omega)$.

Usando a mesma termologia usada em [7] dizemos que $\mathcal{C}$ é um código temporal, se $\mathcal{C}$ é da forma

$$\mathcal{C}_\infty = \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_{n_1}) & \ldots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \ldots & \gamma\sigma^{n-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & \sigma(x_{n_2}) & \ldots & \sigma^{n-1}(x_1) \end{pmatrix} \right\}. \tag{6}$$

Cada palavra código X contém n coeficientes x_i, com cada um dos simbolos sendo uma combinação linear de n símbolos de informações. Ou seja, os códigos temporais obtidos a partir destas álgebras cíclicas tem taxa máxima.

Definição 1: O determinte da matriz da Equação (5) (que também é o mesmo determinante da matriz da Equação (6)) é chamado de norma reduzida do elemento x, onde $x \in \mathcal{A}$.

A seguir descrevemos uma seqüência de resultados bem conhecidos na literatura, que auxíliará na determinação do determinante mínimo do código $\mathcal{C}$ que propomos na Seção IV.

Teorema 1: [2] Se $\mathcal{A} = (K/F, \sigma, \gamma)$ é uma álgebra cíclica, então a norma reduzida de $x \in \mathcal{A}$ pertence a F.

Corolário 1 [2] Seja $\mathcal{A} = (K/F, \sigma, \gamma)$ uma álgebra cíclica, sendo que $\gamma \in \mathcal{O}_F$, com base dada por $\{1, e, \ldots, e^{n-1}\}$. Se

$x = x_0 + ex_1 + \cdots + e^{n-1}x_{n-1} \in \mathcal{A}$, onde $x_k \in \mathcal{O}_K$, para $k = 0, \ldots, n-1$, então a norma reduzida de x pertence a $\mathcal{O}_F$.

Uma álgebra cíclica é dita ser uma *álgebra de divisão*, se todos seus elementos são inversíveis, assim todas as palavras códigos tem determinante não nulo. Note que se trata de um importante critério algébrico para verificar se um código $\mathcal{C}_\infty$ satisfaz o critério do posto.

O próximo teorema garante quando uma álgebra cíclica é uma álgebra de divisão.

Teorema 2 ([6], Theorem 11.12, p. 184): Uma álgebra cíclica $\mathcal{A} = (K/F, \sigma, \gamma)$ de grau n é uma álgebra de divisão se, e somente se, o menor fator $t \in \mathbb{Z}_+$ de n tal que γ^t é a norma de algum elemento de K^* é n.

Corolário 2 [2] O determinante mínimo do código infinito com $\mathcal{I} = \mathcal{O}_K$ definido na Equação (6), quando $F = \mathbb{Q}(i)$ ou $\mathbb{Q}(\omega)$, é dado por

$$\delta_{min}(\mathcal{C}_{\mathcal{O}_K}) = 1.$$

B. Códigos Temporais Perfeitos

Em [2], Oggier et. all construíram uma classe especial de códigos temporais denominada de *Códigos Temporais Perfeitos*. Na construção destes códigos foram considerados espaços de matrizes do tipo $M \times M$ indentificadas por álgebras cíclicas de divisão, garantindo diversidade máxima. Tal construção teve como focos principais garantir uma cota inferior para o determinante mínimo do código e de que a constelação de sinais tenha forma cúbica, seja ela QAM ou HEX.

A seguir damos a definição formal de códigos temporais perfeitos.

Definição 2: Um código temporal de bloco $M \times M$ é chamado *código perfeito*, se as seguintes condições são satisfeitas:

1) tem taxa máxima, isto é, o código faz uso de M^2 símbolos de informações, seja QAM ou HEX,
2) o determinante do código infinito é não-nulo (em particular o critério do posto é satisfeito),
3) o reticulado real de dimensão $2M^2$ gerado pelas palavras-códigos é dado por $\mathbb{Z}^{2M^2}$ ou $A_2^{M^2}$, e
4) todos os símbolos codificados na matriz código tem a mesma energia média.

IV. Códigos Temporais Perfeitos Proveniente de Símbolos HEX

Em [2], Oggier et. all mostraram que encontrar constelações que sejam dadas na forma cúbica equivale procurar um ideal $\mathcal{I}$ que represente a versão rotacionada dos reticulados $\mathbb{Z}[i]^n$ ou $\mathbb{Z}[\omega]^n$. Estes reticulados são obtidos a partir de reticulados algébricos complexos, conforme a seguinte definição.

Definição 3: Dizemos que o conjunto

$$\Lambda^c = \{x = \lambda M : \lambda \in \mathbb{Z}[i]^n\} \tag{7}$$

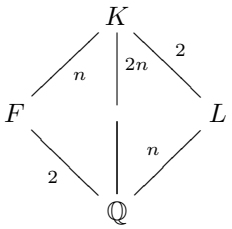
definido sobre $\mathbb{Z}[i]$ é um *reticulados complexo*, onde $M \in M_n(\mathbb{C})$ é a matriz geradora do reticulado, MM^H é a *matriz Gram*, e H denota a transposta conjugada.

De forma similar defini-se um reticulado complexo sobre $\mathbb{Z}[\omega]$.

Porém, caso desejamos obter um reticulado algébrico complexo que seja da forma cúbica, precisamos que a matriz M seja da forma de uma matriz R unitária, como descrevemos na Seção II.

Neste sentido, sejam K uma extensão de Galois de $F = \mathbb{Q}(i)$ (respectivamente, $F = \mathbb{Q}(\omega)$) de grau n, e $\mathcal{O}_K$ o anel de inteiros de K. Seja L um corpo de números totalmente real de grau n com discriminante coprimo com F, isto é, $mdc(d_F, d_L) = 1$. Tomando a composição $K = FL$ de F e L (ou seja, o menor corpo que contém ambos, ver figura), tem-se que

$$d_K = d_L^2 d_F^n, \tag{8}$$



com $d_K = -4$ se $K = \mathbb{Q}(i)$ e $d_K = -3$ se $K = \mathbb{Q}(\omega)$.

Sejam $\{\sigma_k\}_{k=1}^n$ o grupo de Galois $Gal(K/F)$ e $\Lambda^c(I)$ o reticulado algébrico complexo correspondente ao ideal $I \subset \mathcal{O}_K$ obtido pelo mergulho de K em $\mathbb{C}^n$ definido por

$$\sigma : K \longrightarrow \mathbb{C}^n$$

$$x \longmapsto \sigma(x) = (\sigma_1(x), \ldots, \sigma_n(x)).$$

Uma base de $\Lambda^c(I)$ é obtido através do mergulho σ a uma base $\{\alpha_k\}_{k=1}^n$ de $\mathcal{I}$. Consequentemente, a sua matriz Gram é dada por:

$$G = \begin{cases} Tr_{K/\mathbb{Q}(i)}(\nu_k \overline{\nu_l})_{k,l=1}^n \\ \\ Tr_{K/\mathbb{Q}(\omega)}(\nu_k \tau(\nu_l))_{k,l=1}^n, \end{cases}$$

a função traço é definida por

$$Tr_{K/\mathbb{Q}(i)} : K \times K \longrightarrow \mathbb{Q}(i)$$

$$(x, y) \longmapsto Tr_{K/\mathbb{Q}(i)}(x\overline{y}),$$

com $\overline{x}$ denotando a conjugação complexa de x, ou também é dada por,

$$Tr_{K/\mathbb{Q}(\omega)} : K \times K \longrightarrow \mathbb{Q}(\omega)$$

$$(x, y) \longmapsto Tr_{K/\mathbb{Q}(\omega)}(x\tau(y)),$$

com τ denotando a conjugação em $\mathbb{Q}(\omega)$ dada por $\tau(\omega) = \omega^2$.

A. O reticulado $\mathbb{Z}[\omega]^2$

Em [2], Oggier et. all propuseram uma família de códigos perfeitos para 2 antenas de transmissão, para símbolos codificados a partir de $\mathbb{Z}[i]$. Para tal consideraram extensões de corpos $K/\mathbb{Q}(i)$ de grau 2 sobre $\mathbb{Q}(i)$, com $K = \mathbb{Q}(i, \sqrt{p})$ para p um inteiro primo da forma $p \equiv 5 \ (mod\, 8)$.

Assim, nessa seção, propomos um procedimento de construção de códigos perfeitos com 2 antenas de transmissões, porém com símbolos codificados a partir de $\mathbb{Z}[\omega]$.

Seja p um inteiro primo e consideremos extensões de corpos $K/\mathbb{Q}(\omega)$ de grau 2 sobre $\mathbb{Q}(\omega)$, com $K = \mathbb{Q}(\omega, \sqrt{p})$. Podemos ver K como um espaço vetorial sobre $\mathbb{Q}(\omega)$, ou sendo

$$K = \{a + b\sqrt{p} | a, b \in \mathbb{Q}(\omega)\}.$$

O seu grupo de Galois $Gal(K/\mathbb{Q}(\omega)) =< \sigma >$ é gerado por $\sigma : \sqrt{p} \mapsto -\sqrt{p}$. Seja $\mathcal{A} = (K/\mathbb{Q}(\omega), \sigma, \gamma)$ a sua correspondente álgebra cíclica.

Agora, propomos um método para encontrar convenientes ideais $\mathcal{I} \in \mathcal{O}_K$ que sejam versões rotacionadas do reticulado $\mathbb{Z}[\omega]^2$ quando $p \equiv 1 \ (mod\, 12)$. Para isso, seja $\Lambda^c(\mathcal{I})$ um reticulado algébrico complexo com base $\{v_1, v_2\}$. Para obtermos um ideal $\mathcal{I}$ que seja a versão rotacionada do reticulado $\mathbb{Z}[\omega]^2$, procuramos encontrar um ideal $\mathcal{I}$ tal que o reticulado complexo $\Lambda^c(\mathcal{I})$ seja unimodular (matriz unitária). Por definição um reticulado unimodular coincide com o seu dual.

Definição 5: O reticulado dual $\Lambda^c(\mathcal{I})^\perp$ de $\Lambda^c(\mathcal{I})$ é definido por $\Lambda^c(\mathcal{I})^\perp = \{x = a_1v_1 + a_2v_2, a_1, a_2 \in \mathbb{Q}(\omega) | < x, y > \in \mathbb{Z}[\omega], \forall y \in \Lambda^c(\mathcal{I})\}$, ou sendo o produto escalar entre dois vetores é dado pelo correspondente traço entre os números algébricos, isto é,

$$< x, y >= Tr_{K/\mathbb{Q}(\omega)}(x\overline{y}),$$

onde por abuso de notação, denotamos $\overline{y} = \tau(y)$ e $\tau \in Gal(K/\mathbb{Q}(\omega))$ sendo diferente da identidade.

Para que possamos obter um reticulado complexo dual definimos o codiferente [ver [2]], que é dado por

$$D^{-1}_{K/F} = \{x \in K | \forall \alpha \in \mathcal{O}_K, Tr_{K/F}(x\alpha) \in \mathcal{O}_F\}.$$

Lema 1 Tem-se que $\Lambda^c(\mathcal{I})^\perp = \Lambda^c(\mathcal{I}^\perp)$, sendo que

$$\mathcal{I}^\perp = \overline{\mathcal{I}^{-1}\mathcal{D}^{-1}_{K/\mathbb{Q}(\omega)}}.$$

Demonstração: Seja $x \in \overline{\mathcal{I}^{-1}\mathcal{D}^{-1}_{K/\mathbb{Q}(\omega)}}$. Para todo $y \in \mathcal{I}$ precisamos mostrar que $Tr_{K/\mathbb{Q}(\omega)}(x\overline{y}) \in \mathbb{Z}[\omega]$. Desde que $x = \overline{uv}$, com $u \in \mathcal{I}^{-1}$ e $v \in \mathcal{D}^{-1}_{K/\mathbb{Q}(\omega)}$, segue que $x\overline{y} = \overline{uyv}$ com $uy \in \mathcal{O}_L$. Agora, pela definição de $\mathcal{D}^{-1}_{K/\mathbb{Q}(\omega)}$ o resultado segue.

Se $K = \mathbb{Q}(\omega, \sqrt{p})$, com $p \equiv 1 \ (mod\, 6)$, então p se fatora em $\mathcal{O}_K$ da forma

$$(p)\mathcal{O}_K = \beta^2\overline{\beta}^2, \tag{9}$$

com β e $\overline{\beta}$ sendo ideais primos conjugados. Note que se $p \equiv 1 \ (mod\, 12)$, então obviamente $p \equiv 1 \ (mod\, 6)$.

Proposição 1: O $\mathbb{Z}[\omega]$-reticulado $\frac{1}{\sqrt{p}}\Lambda^c(\beta)$ é unimodular.
Demonstração: Como $\mathcal{D}_{K/\mathbb{Q}(\omega)} = \mathcal{D}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}} = (\sqrt{p})\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$, segue que o resultado é válido se $p \equiv 1 \ (mod\, 4)$ [2]. Mas como $p \equiv 1 \ (mod\, 12)$, o resultado segue. Agora, fazendo uso do Lema 1 e da Equação (9), tem-se que o dual de β é dado por

$$\beta^\perp = \overline{\beta^{-1}}(\sqrt{p})^{-1} = \frac{1}{p}\beta.$$

Além disso, o reticulado dual é dado por

$$\left(\frac{1}{\sqrt{p}}\Lambda^c(\beta)\right)^\perp = \sqrt{p}\left(\Lambda^c(\beta)^\perp\right) = \frac{1}{\sqrt{p}}\Lambda^c(\beta),$$

o que conclui a demonstração.

B. Construção de Códigos Perfeitos de Dimensão 2 Provenientes de Constelações HEX

Seja a álgebra cíclica

$$\mathcal{A} = (K/\mathbb{Q}, \sigma, \omega), \quad \text{com} \quad K = \mathbb{Q}(\omega, \sqrt{13}). \tag{10}$$

Como $13 \equiv 1 \ (mod\, 12)$, segue pela Equação (9) e pela Proposição 1 que existe um ideal $\mathcal{I}$ de norma 13 em K que é uma versão rotacionada de $\mathbb{Z}[\omega]$. Com o intuito de exibir este ideal, precisamos da seguinte proprosição.

Proposição 2: Tem-se que $\mathbb{Q}(\omega, \sqrt{13}) = \mathbb{Q}(i\sqrt{3} + \sqrt{13})$.
Demostração: Como $\mathbb{Q}(\omega, \sqrt{13}) = \mathbb{Q}(\frac{-1+i\sqrt{3}}{2}, \sqrt{13}) = \mathbb{Q}(i\sqrt{3} + \sqrt{13})$, segue que é suficiente provar que $\mathbb{Q}(i\sqrt{3} + \sqrt{13}) = \mathbb{Q}(i\sqrt{3}, \sqrt{13})$. Claramente, $\mathbb{Q}(i\sqrt{3} + \sqrt{13}) \subset \mathbb{Q}(i\sqrt{3}, \sqrt{13})$. Agora, mostramos que $\mathbb{Q}(i\sqrt{3}, \sqrt{13}) \subset \mathbb{Q}(i\sqrt{3}+\sqrt{13})$. Como $(i\sqrt{3}+\sqrt{13})^3 = (-6+10\sqrt{13})+36i\sqrt{3}$ e $(i\sqrt{3} + \sqrt{13})^3 - 36(i\sqrt{3} + \sqrt{13}) = -6 - 26\sqrt{13} \in \mathbb{Q}(i\sqrt{3} + \sqrt{13})$, segue que $\sqrt{13} \in \mathbb{Q}(i\sqrt{3} + \sqrt{13})$. Por outro lado, $(i\sqrt{3}+\sqrt{13})^3 - 10(i\sqrt{3}+\sqrt{13}) = i\sqrt{3} \in \mathbb{Q}(i\sqrt{3}+\sqrt{13})$. Portanto, $L = \mathbb{Q}(\omega, \sqrt{13}) = \mathbb{Q}(i\sqrt{3} + \sqrt{13})$.

Se $\theta = i\sqrt{3} + \sqrt{13}$, então $\{1, \theta, \theta^2, \theta^3\}$ é uma base integral de $\mathbb{Q}(\theta)$ e $p(x) = x^4 - 20x^2 + 256$ é o polinômio minimal associado a θ. No intuito, de exibirmos o ideal $\mathcal{I}$ em $\mathcal{O}_K$, enunciaremos o próximo teorema.

Teorema 3 (Teorema de Kummer): Sejam A um anel de Dedekind, F seu corpo de frações, K uma extensão separável de grau $n, \mathcal{O}_K$ o anel de inteiros de K sobre A tal que $\mathcal{O}_K = A[\beta]$, para algum $\beta \in K$ e P um ideal primo não nulo de A. Se $f(x)$ é o polinômio minimal de β sobre F e $f_1, \ldots, f_r$ são polinômios mônicos em $A[x]$, tal que a fatoração de $\overline{f}$ em polinômios irredutíveis distintos em $(A/P)[x]$ seja dada por

$$\overline{f} = \overline{f}_1^{e_1} \ldots \overline{f}_r^{e_r},$$

então os ideais primos, dois a dois distintos, $Q_1, \ldots, Q_r$ de $\mathcal{O}_K$, que estão acima de P, são dados por $Q_j = (A/P)[\overline{\beta}_j]$, onde $\overline{\beta}_j$ é raíz de $\overline{f(x)}_j$, e

1) $P\mathcal{O}_K = Q_1^{e_1} \ldots Q_r^{e_r}$, sendo que $Q_j = P\mathcal{O}_K + f(\beta)\mathcal{O}_L$, para $j = 1, \ldots, r$,
2) $e(Q_j/P) = e_j$, para $j = 1, \ldots, r$ e
3) $f(Q_j/P) = grau f_j$, para $j = 1, \ldots, r$.

Agora, tomando $p(x)(mod13)$, tem-se que

$$p(x)(mod13) = (x+6)^2(x+7)^2 = (x+6)^2(x-6)^2.$$

Com isto, $\overline{p(x)} = \overline{p_1(x)}^2\overline{p_2(x)}^2$ é a fatoração de $\overline{p(x)}$ em polinômios irredutíveis em $\mathbb{Z}/13\mathbb{Z}$. Logo, pelo Teorema de Kummer, tem-se que

$$13\mathcal{O}_K = \mathcal{P}_1.\mathcal{P}_2,$$

com $\mathcal{P}_1 = \langle 13, \theta + 6\rangle$ e $\mathcal{P}_2 = \langle 13, \theta - 6\rangle$.

Teorema 4: Se considerarmos o espaço das matrizes de ordem 2 formada pelas matrizes X, obtidas pela correspondente identificação da álgebra cíclica dada na Equação (6), dadas por

$$X = \frac{1}{\sqrt{13}} \begin{bmatrix} \alpha(a+b\theta) & \alpha(c+d\theta) \\ \omega\overline{\alpha}(c+d\overline{\theta}) & \overline{\alpha}(a+b\overline{\theta}) \end{bmatrix}$$

sendo que a, b, c, d são símbolos HEX, $\theta = \frac{1+\sqrt{13}}{2}$, $\overline{\theta} = \frac{1-\sqrt{13}}{2}$, $\alpha = \langle\mathcal{P}_1\rangle$, e $\overline{\alpha} = \overline{\langle\mathcal{P}_1\rangle} = \langle\mathcal{P}_2\rangle$, então o espaço das matrizes X definem um código perfeito de dimensão 2.

Demostração: Nesse sentido, mostramos que as condições da Definição 2 são verificadas. Note que o código tem taxa máxima, contem 4 símbolos de informações HEX a, b, c, d, e assim a condição (1) é satisfeita. A condição (2), pelo critério do posto, também é verificada (Apêndice III). Agora, calculamos o determinante mínimo. Antes, observamos que o ideal β na Equação (9) é principal para $p \equiv 1\ (mod\,6)$. Desde que $N(\beta) = 13$, segue que equivale a encontrar um elemento $\alpha \in \beta$ tal que a norma absoluta $N_{K/\mathbb{Q}}(\alpha) = 13$. Usando o fato de que $13 = u^2 - uv + v^2$, para $u = 4, v = 3 \in \mathbb{Z}$, tem-se o elemento $\alpha = \sqrt{4+3\omega}$. Note que a matriz geradora do reticulado pode ser reduzida a forma unitária. O determinante $det(X)$ é dado por

$$\frac{1}{13}.N_{K/\mathbb{Q}(\omega)}(\alpha)(N_{K/\mathbb{Q}(\omega)}(a+b\theta) - \omega N_{K/\mathbb{Q}(\omega)}(c+d\theta)). \quad (11)$$

O segundo termo na Equação (11) assume valores em $\mathbb{Z}[\omega]$ e seu módulo mínimo é igual a 1 (com $a = 1, b = c = d = 0$). Assim concluímos que $\delta_{min}(C_\infty)$ é dado por

$$min_{0\neq X\in C}|det(X)|^2 = \frac{1}{13^2}|N_{K/\mathbb{Q}(\omega)}(\alpha)|^2 = |4+3\omega|^2 = \frac{1}{13},$$

o que garante que a condição (2) é veficada. A condição (3) segue da Subseção A da Seção IV. Note que o fator ω na segunda linha da palavra-código X garante a energia média de transmissão, uma vez que $|\omega|^2 = 1$. Desta forma a condição (4) está provada.

V. Conclusões

Neste trabalho apresentamos uma nova construção de códigos temporais perfeitos 2×2 a partir de constelações HEX. O que estimula a procura de novas construções de códigos temporais perfeitos para dimensões 4×4 a partir de constelações HEX e de dimensões 3×3 e 6×6 a partir de constelações QAM.

Agradecimentos

Os autores agradecem a FAPESP pelo suporte financeiro 2007/56052-8.

Referências

[1] Damen, M.O; Tewfik, A. and Belfiore, J.C; *A Construction of a Space-Time Code Based on Number Theory*, IEEE Trans. Inform. Theory, vol.48, No.3 (2002), pp 753-760.

[2] Oggier, F; Rekaya, G. and Belfiori, J.C.; *Perfect Space-Time Block Codes* in IEEE Trans. Inform. Theory, vol.52, No. 9, pp 3885-3902 (2006).

[3] Hassibi, B. and Hochwald, B.M.; *High-Rate Codes that are Linear in Space and Time*, IEEE Trans. Inform. Theory, vol. 48, No 7, pp. 1804-1824 (2002).

[4] Belfiore, J.C.; Rekaya, G. and Viterbo, E; *The Golden Code: A* 2×2 *Full Rate Space-Time Code with non Vanishing Determinants*, IEEE Trans. Inform. Theory, vol. 51, No.4, pp. 1432-1436 (2005).

[5] Belfiore, J.C. and Rekaya, G.; *Quaternionic Lattices for Space-Time Coding* in Proc. IEEE Inf. Theory Workshop (ITW 2003), Paris, France, 31 Mar-Apr.4 (2003).

[6] Albert, A.A; *Sctruture of Algebras*, in. AMS Colloquim Pub. XXIV, AMS, Providence, 1961.

[7] Sethuraman, B.A.; Rajan, B.S. and Shashidhar, V.; *Full Diversity, high-rate space-time block codes from division algebras*, IEEE Trans. Inform. Theory, vol.49, pp 2596-26162, vol.11 (2003).

[8] Gras, G.; *Class Field Theory* , Berlin, Germany: Springer-Varlag, (2003).

Apêndice I
Teoria Algébrica dos Números: Definições Básicas

Um corpo de números K é um corpo contendo os racionais Q que é um espaço vetorial de dimensão finita sobre Q. Sejam dois corpos de números $F \subseteq K$, onde K pode ser visto como um espaço vetorial de dimensão finita n sobre F. Neste caso, dizemos que K é uma *extensão de corpos* de F que denotamos por K/F. Podemos obter uma extensão de corpos K/F, a partir de um polinômio $p(x)$ de grau n, ou seja, quando K é o menor corpo que contém F e todas raizes $\theta_1, \ldots, \theta_n$ de $p(x)$. Neste caso, dizemos que a extensão de corpos K/F é uma *extensão Galosiana*, e denotamos por $Gal(K/F) = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ seu grupo de Galois. Dizemos que uma extensão K/F é abeliana (cíclica) se seu grupo de Galois é abeliano (cíclico).

A norma e o traço de um elemento $x \in K$ são definidos, respectivamente, por

$$Tr_{K/F}(x) = \sum_{k=1}^{n} \sigma_k(x) \quad \text{e} \quad N_{K/F}(x) = \prod_{k=1}^{n} \sigma_k(x).$$

Se $F = \mathbb{Q}$, então um elemento $\alpha \in K$ é chamado de inteiro sobre $\mathbb{Z}$ se existe um polinômio $p(x) \in \mathbb{Z}[x]$, não nulo, tal que $p(\alpha) = 0$. O conjunto dos elementos com esta propriedade formam um anel que chamamos de anel de inteiros e denotamos por $\mathcal{O}_K$. Este anel tem uma $\mathbb{Z}$-base que denotamos por $\{\omega_1, \ldots, \omega_n\}$. Um importante invariante associado ao corpo K, é o seu *discriminante* que é definido por $d_K = det(Tr_{K/\mathbb{Q}}(\omega_i\omega_j))_{i,j=1}^n$.

Apêndice II
Símbolo da Norma de Hasse

O símbolo da norma de Hasse é derivado da teoria de classe de corpos. Sejam K/F uma extensão de corpos de números do tipo abeliana, K_ν o complemento de K em relação a uma valorização ν, e o mergulho de K em K_ν denotado por i_ν.

Definição 6: A aplicação

$$\left(\frac{\bullet, K/F}{\nu}\right) : K^* \longrightarrow Gal(K/F),$$

definida por

$$x \longmapsto \left(\frac{i_\nu(x), K/F}{\nu}\right)$$

é chamada de *símbolo da norma de Hasse*.

A principal propriedade deste símbolo é que podemos calcular se um elemento é norma local.

Teorema 5: [8] Tem-se que $\left(\frac{\bullet, K/F}{\nu}\right) = 1$ se, e somente se, x é uma norma local no lugar ν para K/F.

Uma outra importante propriedade deste símbolo é a sua linearidade dada pelo próximo teorema.

Teorema 6: [8] Vale a propriedade $\left(\frac{xy, K/F}{\nu}\right) = \left(\frac{x, K/F}{\nu}\right)\left(\frac{y, K/F}{\nu}\right)$.

O próximo teorema fornece como é dado o símbolo nos lugares não-ramificados.

Teorema 7: [8] Se ν não é ramificado em K/F, então para todo $x \in F^*$, tem-se que

$\left(\frac{x, K/F}{\nu}\right) = \left(\frac{K/F}{\nu}\right)\left(\frac{K/F}{\nu}\right)^{v(x)}$ onde $\left(\frac{K/F}{\nu}\right)$ denota o Frobenius de ν para K/F (para os nossos propósitos é um elemento do grupo de galois $Gal(K/F)$ (maiores detalhes ver [8]) e $v(x)$ denota a valorização de x.

Corolário 3 [8] Em um lugar não ramificado, a unidade é sempre uma norma.

O próximo teorema fornece a propriedade da *fórmula produto do símbolo da norma de Hasse*.

Teorema 8: Seja K/F uma extensão finita. Para cada $x \in F^*$, tem-se que

$$\prod_\nu \left(\frac{y, K/F}{\nu}\right) = 1,$$

com o produto definido sobre todos os lugares de ν.

Pelo Corolário 3, tem-se que a unidade é sempre uma norma local de um lugar que não é ramificado. O nosso interesse é mostrar que uma unidade γ não é uma norma. Forçamos uma contradição em lugar ramificado. Para isto, começamos com a fórmula produto, simplificando todos os termos exceto em dois termos no produto sobre todos os primos, e tomamos o produto entre dois termos iguais a 1.

$$\left(\frac{\gamma, K/F}{\nu}\right)\left(\frac{x, K/F}{\nu}\right) = 1, \quad x \in K^*.$$

O primeiro termo envolve γ, e o outro mostramos ser diferente de 1. Assim, como o produto é 1, segue que γ não é uma norma. Para simplificar a fórmula, introduzimos um elemento $y \in L$ tal que $y\gamma$ é uma unidade local em um primo ramificado e calculamos a fórmula produto

$$\prod_v \left(\frac{y\gamma, K/F}{\nu}\right) = 1.$$

APÊNDICE III
ω NÃO É UMA NORMA EM $K = \mathbb{Q}(\omega, \sqrt{13})/\mathbb{Q}(\omega)$

O objetivo deste apêndice é mostrar que ω não é uma norma em $\mathbb{Q}(\omega, \sqrt{13})/\mathbb{Q}(\omega)$, que para isso usamos a ramificação dos primos que aparecem em $\mathbb{Q}(\omega, \sqrt{13})/\mathbb{Q}(\omega)$.

Proposição 3: A unidade ω não é uma norma na extensão de corpos $\mathbb{Q}(\omega, \sqrt{13})/\mathbb{Q}(\omega)$.

Demonstração: Tem-se que $13 = (1 - 3\omega)(4 + 3\omega) = p_{13}q_{13}$. Mostramos que ω não é uma norma local em p_{13}, e assim não é uma norma em $\mathbb{Q}(\omega)$. Seja o sistema

$$\begin{cases} y \equiv 1 \ (mod\, 1 - 3\omega) \\ \\ \omega y \equiv 1 \ (mod\, 4 + 3\omega), \end{cases} \tag{12}$$

com $y \in \mathbb{Z}[\omega]$. Tem-se que $y = 13 + 3\omega$ é uma solução do sistema (12), sendo que $(y)\mathbb{Z}[\omega] = p_{217}$. Seja $\left(\frac{y\gamma, K/F}{\nu}\right)$ o símbolo da norma de Hasse. Pela fórmula produto tem-se que

$$\prod_v \left(\frac{y\gamma, K/F}{\nu}\right) = \prod_v \left(\frac{y\gamma, K/F}{\nu}\right) \prod_v \left(\frac{y\gamma, L/K}{\nu}\right),$$

e que $\prod_v \left(\frac{y\gamma, K/F}{\nu}\right) = 1$, com o primeiro produto tomado sobre os primos que ramificam e o segundo sobre os primos que não ramificam. O produto sobre os primos não ramificados fica $\left(\frac{y\gamma, K/F}{p_{13}}\right)\left(\frac{y\gamma, K/F}{q_{13}}\right)$, uma vez que a ramificação em K/F é somente em 13. Agora, vejamos como é o produto sobre os primos não ramificados. Como $y \in p_{217}$, segue que sua valorização é zero para $\nu \neq p_{217}$. Como a valorização é zero para todos os lugares, segue que $\prod_{v,\, n\ ramif}\left(\frac{y\gamma, K/F}{\nu}\right) = \prod_{v,\, n\ ramif}\left(\frac{\gamma, K/F}{\nu}\right)\left(\frac{y, K/F}{\nu}\right) = \left(\frac{y, K/F}{p_{217}}\right)$. Assim, o produto dado pela fórmula produto fica simplificado como $\left(\frac{\omega, K/F}{p_{13}}\right)\left(\frac{y, K/F}{p_{13}}\right)\left(\frac{y\omega, K/F}{q_{13}}\right)\left(\frac{y, K/F}{p_{217}}\right) = 1$. O segundo e o terceiro termos são iguais a 1, pela escolha de y no sistema (12). Finalmente, tem-se que $\left(\frac{\omega, K/F}{p_{13}}\right)\left(\frac{y\omega, K/F}{p_{217}}\right) = 1$. Como p_{217} é inerte, segue que o segundo termo é diferente de 1, e com isto $\left(\frac{\omega, K/F}{p_{13}}\right) \neq 1$. Portanto, ω não é uma norma em p_{13}, o que conclui a demonstração.