Códigos de bloco espaço-tempo sobre anéis de inteiros algébricos

Antonio Aparecido de Andrade

***Resumo*— No presente trabalho apresentamos um estudo de códigos de bloco espaço-tempo via corpos de números. Neste sentido, definimos uma família que extende os códigos de bloco espaço-tempo obtidos por Damen e Viterbo.**

***Palavras-Chave*— Corpos de números, códigos de bloco espaço-tempo.**

***Abstract*— In this work we present a study of space-time block codes via number fields. In this sense, we define a family that extends the space-time block codes obtained by Damen and Viterbo.**

***Keywords*— Number fields, space-time block code.**

I. Introdução

A alta capacidade de um sistema de múltiplas antenas e a necessidade de transmitir através de canais altas taxas de dados com melhor desempenho têm motivado a pesquisa sobre o processamento de sinais pressupondo muitas antenas transmissoras-receptoras [1]-[6].

O termo código espaço-tempo é usado para descrever sinais bi-dimensionais associados a sistemas de múltiplas antenas. Um código de bloco espaço-tempo (STBC) $n \times l$ $(l \geq n)$ $\mathcal{C}$ é dado por um número finito de matrizes $n \times l$ com entradas complexas [5].

Deste modo, neste trabalho apresentamos novas construções de códigos de bloco espaço-tempo via corpos de números fazendo uso dos anéis de inteiros desses corpos.

Este trabalho é organizado da seguinte maneira. Na Seção II, faremos uma breve revisão de extensões de corpos. Na Seção III, damos os fatos básicos sobre corpos quadráticos e ciclotômicos. Na Seção IV, faremos uma revisão do anel dos inteiros algébricos de um corpo de números. Na Seção V, apresentamos o conceito de código de bloco espaço-tempo. Na Seção VI, definimos uma nova família de códigos de bloco espaço-tempo via corpos de números. Na Seccão VII, definimos novas estruturas de códigos de bloco espaço-tempo via corpos ciclotômicos. Na Seção VIII, damos nossas conclusões.

II. Extensões de Corpos

Nesta seção, apresentamos fatos básicos envolvendo a teoria de corpos. Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos. Se $\mathbb{K} \subseteq \mathbb{L}$ dizemos que $\mathbb{L}$ é uma *extensão de corpos* de $\mathbb{K}$. Neste caso, $\mathbb{L}$ tem uma estrutura natural de um espaço vetorial sobre $\mathbb{K}$. A dimensão de $\mathbb{L}$ como um espaço vetorial sobre $\mathbb{K}$ é chamado o *grau* de $\mathbb{L}$ sobre $\mathbb{K}$, e é denotado por $[\mathbb{L} : \mathbb{K}]$. Se $[\mathbb{L} : \mathbb{K}]$ é finito, dizemos que $\mathbb{L}$ é uma *extensão finita* de $\mathbb{K}$. Observamos que, se $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ são corpos então $[\mathbb{M} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}] \cdot [\mathbb{M} : \mathbb{L}]$ e que $[\mathbb{L} : \mathbb{K}] = 1$ se, e somente se, $\mathbb{K} = \mathbb{L}$.

Definição 1: Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos. Um elemento $\alpha \in \mathbb{L}$ é chamado *algébrico* sobre $\mathbb{K}$ se existe um polinômio $f(x) \in \mathbb{K}[x] - \{0\}$ tal que $f(\alpha) = 0$.

Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos, $\alpha \in \mathbb{L}$ algébrico sobre $\mathbb{K}$ e o homomorfismo de anéis $\varphi : \mathbb{K}[x] \to \mathbb{L}$ definido por $\varphi(f(x)) = f(\alpha)$, onde $f(x) \in \mathbb{K}[x]$. A imagem de φ é dada por

$$\mathbb{K}[\alpha] = \{f(\alpha) \ : \ f(x) \in \mathbb{K}[x]\},$$

ou seja, $\mathbb{K}[\alpha]$ é o conjunto das expressões polinomiais $\sum_{i=0}^{n} a_i \alpha^i$, com $a_i \in \mathbb{K}$. Sendo $\mathbb{K}$ um corpo, temos que $\mathbb{K}[x]$ é um domínio principal, e assim, o $Ker(\varphi)$ é um ideal principal não nulo de $\mathbb{K}[x]$, o qual é gerado por um polinômio mônico $p(x) \in \mathbb{K}[x]$. Logo, temos que $\mathbb{K}[x]/\langle p(x)\rangle \simeq \mathbb{K}[\alpha]$. Assim, o quociente $\mathbb{K}[x]/\langle p(x)\rangle$ é um domínio, pois $\mathbb{K}[\alpha]$ é um domínio. Portanto, temos que $\langle p(x)\rangle$ é um ideal primo. Deste modo, temos que $p(x)$ é iredutível, de onde segue que $\mathbb{K}[x]/\langle p(x)\rangle$ é um corpo, e pelo isomorfismo φ temos que $\mathbb{K}[\alpha]$ é um corpo.

O polinômio mônico $p(x)$ que gera o $Ker(\varphi)$ e tem α como raiz é unicamente determinado por α. Logo, temos que $p(x)$ é o polinômio irredutível de menor grau que tem α como raiz. Este polinômio é chamado de *polinômio mínimo* de α sobre $\mathbb{K}$. Neste caso, temos que $\mathbb{K}[\alpha]$ é uma extensão de grau n sobre $\mathbb{K}$, onde n é o grau do polinômio mínimo de α sobre $\mathbb{K}$, pois $\mathbb{K}[\alpha]$ é o conjunto das expressões polinomiais de grau menor ou igual a n, com coeficientes em $\mathbb{K}$ e como α é algébrico sobre $\mathbb{K}$, temos que $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de $\mathbb{K}[\alpha]$ sobre $\mathbb{K}$.

Chamamos de *corpo de frações* de α, ao conjunto

$$\mathbb{K}(\alpha) = \{f(\alpha)/g(\alpha) : f(x), g(x) \in \mathbb{K}[x], \ g(\alpha) \neq 0\}.$$

Sendo α algébrico, temos que o corpo $\mathbb{K}[\alpha]$ coincide com o corpo $\mathbb{K}(\alpha)$.

Definição 2: Seja $\mathbb{K}$ um corpo. Uma função σ de $\mathbb{K}$ em $\mathbb{C}$ é chamada uma *imersão* se σ é um homomorfismo injetivo.

Teorema 1: [7, Corollary, 2.4] Se $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$, então existe $\alpha \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\alpha)$ e α é chamado de elemento primitivo.

Teorema 2: [7, Theorem 1, 2.4] Se $\mathbb{K} = \mathbb{Q}(\alpha)$ é uma extensão finita de $\mathbb{Q}$ de grau n, então existem exatamente n imersões distintas $\sigma_1, \ldots, \sigma_n$ de $\mathbb{K}$ em $\mathbb{C}$.

Definição 3: Sejam $\mathbb{K}$ uma extensão de $\mathbb{Q}$ de grau n, $\sigma_1, \ldots, \sigma_n$ as imersões de $\mathbb{K}$ em $\mathbb{C}$ e α um elemento de $\mathbb{K}$.

Departamento of Matemática - Ibilce - Unesp, Rua Cristovão Colombo, 2265, 15054-000, São José do Rio Preto, SP, Brasil, E-mail: andrade@ibilce.unesp.br. Este trabalho foi parcialmente financiado pela FAPESP - 02/07473-7.

Os elementos $\sigma_i(\alpha)$, para $i = 1, 2, \cdots, n$, são chamados de *conjugados* de α.

Exemplo 1: Em $\mathbb{Q}(\sqrt{5})$ temos que, $\sqrt{5}$ e $-\sqrt{5}$ são conjugados.

Definição 4: Uma extensão finita de $\mathbb{Q}$ é chamado de um *corpo de números*.

Temos, pelo Teorema 1 que um corpo de números $\mathbb{K}$ é da forma $\mathbb{Q}(\alpha)$ para algum elemento $\alpha \in \mathbb{K}$. Sendo o polinômio mínimo de α sobre $\mathbb{Q}$ é de grau n, temos que

$$\mathbb{Q}(\alpha) = \{a_0 + \cdots + a_{n-1}\alpha^{n-1} : \ a_i \in \mathbb{Q}, \ i = 0, \cdots, n-1\},$$

e esta representação é única, ou seja, $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base do espaço vetorial $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.

Se o polinômio mínimo de α sobre $\mathbb{Q}$ têm todas as raízes $\alpha = \alpha_1, \alpha_2, \cdots, \alpha_n$ em $\mathbb{K}$, dizemos que $\mathbb{K}$ é uma *extensão de Galois* de $\mathbb{Q}$. Neste caso, o conjunto dos automorfismos

$$Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma : \mathbb{K} \to \mathbb{K} \mid \sigma(x) = x, \quad \forall x \in \mathbb{Q}\}$$

é um grupo, chamado *grupo de Galois* de $\mathbb{K}$ sobre $\mathbb{Q}$. Se o grupo de Galois é *abeliano* (*cíclico*) dizemos que a extensão é *abeliana* (*cíclica*).

Definição 5: Sejam $\mathbb{K}$ um corpo de números de grau n, $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ as n imersões de $\mathbb{K}$ em $\mathbb{C}$ e $\alpha \in \mathbb{K}$. O *traço* de α sobre $\mathbb{Q}$ é definido como

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

e a *norma* de α sobre $\mathbb{K}$ é definida como

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

III. Corpos quadráticos e ciclotômicos

Nesta seção, apresentamos os corpos quadráticos e os corpos ciclotômicos. Esses corpos desempenham um papel fundamental na Teoria Algébrica dos Números, uma vez que é possível caracterizar o anel dos inteiros algébricos e, conseqüentemente, seu discriminante.

Definição 6: Um *corpo quadrático* é uma extensão de grau 2 de $\mathbb{Q}$.

Proposição 1: [7, Proposition 1, 2.5] Todo corpo quadrático é da forma $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.

Definição 7: Seja $\mathbb{K}$ um corpo. Um elemento $\xi \in \mathbb{K}$ é chamado uma raiz n-ésima da unidade se $\xi^n = 1$, para $n \geq 1$, um inteiro.

Segue da Definição 7 que as raízes n-ésimas da unidade são raízes do polinômio $x^n - 1$. Seja $U = \{\xi^{r_1}, \cdots, \xi^{r_n}\}$ o conjunto de todas as raízes distintas de $x^n - 1$ em $\mathbb{K}$. Como $(\xi^i\xi^j)^n = (\xi^i)^n(\xi^j)^n = (\xi^n)^i(\xi^n)^j = 1$ e $\left(\frac{\xi^i}{\xi^j}\right)^n = \frac{(\xi^i)^n}{(\xi^j)^n} = \frac{(\xi^n)^i}{(\xi^n)^j} = 1$, segue que o conjunto U é um grupo multiplicativo. Como todo grupo multiplicativo finito num corpo é cíclico [8], segue que U é um grupo cíclico. Assim, podemos representar as n raízes n-ésimas da unidade por $\xi, \xi^2, \cdots, \xi^n = 1$, onde ξ é um gerador do grupo U. As raízes n-ésimas primitivas da unidade são os geradores do grupo U, isto é, os elementos ξ^k com $mdc(k, n) = 1$, para $k = 1, 2, \cdots, n$. O número das raízes n-ésimas primitivas da unidade é dado por

$$\varphi(n) = \#\{0 < m < n : \ mdc(m, n) = 1, \ m, \ n \in \mathbb{Z}\},$$

onde φ é a função de Euler.

Definição 8: Dado n um inteiro positivo, definimos ξ_n como sendo $e^{\frac{2\pi i}{n}}$ e o corpo $\mathbb{Q}(\xi_n)$ é chamado o $n-$ésimo corpo ciclotômico.

Definição 9: Se n é um inteiro positivo, o polinômio $\phi_n(x) = \prod_{j=1, \, mdc(j,n)=1}^{n} (x - \xi_n^j)$ é chamado de $n-$ésimo polinômio ciclotômico e $x^n - 1 = \prod_{d|n} \phi_d(x)$.

Como consequência temos que

$$\phi_n(x) = \frac{x^n - 1}{\prod_{d|n, \, d<n} \phi_d(x)}.$$

Assim $\phi_1(x) = x - 1$, $\phi_2(x) = \frac{x^2 - 1}{\phi_1(x)} = \frac{x^2 - 1}{x - 1} = x + 1$, $\phi_3(x) = \frac{x^3 - 1}{\phi_1(x)} = \frac{x^3 - 1}{x - 1} = x^2 + x + 1$, e , $\phi_4(x) = \frac{x^4 - 1}{\phi_1(x)\phi_2(x)} = \frac{(x^2 - 1)(x^2 + 1)}{(x - 1)(x + 1)} = x^2 + 1$. Quando $n = p$, onde p é um número primo, temos que

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.$$

Este polinômio é chamado de *p-ésimo polinômio ciclotômico*. Quando $n = p^r$, onde r é um número inteiro maior que 1 e p é um número primo, temos que

$$x^{p^r} - 1 = \phi_1(x)\phi_p(x)\phi_{p^2}(x) \cdots \phi_{p^{r-1}}(x)\phi_{p^r}(x) \ \ e$$
$$x^{p^{r-1}} - 1 = \phi_1(x)\phi_p(x)\phi_{p^2}(x) \cdots \phi_{p^{r-1}}(x).$$

Logo $\phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \cdots + x^{p^{r-1}} + 1$. Este polinômio é chamado de *p^r-ésimo polinômio ciclotômico*.

Teorema 3: [8, Theorem 6, VIII-3] Se ζ_n é uma raiz n-ésima primitiva da unidade, então $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$.

Exemplo 2: Se $\mathbb{K} = \mathbb{Q}(\zeta)$, onde $\zeta = i$ é uma raiz quarta da unidade, então $[\mathbb{K} : \mathbb{Q}] = 2$ e $p(x) = x^2 + 1$ é o polinômio mínimo de ξ.

IV. Inteiros algébricos

Nesta seção, apresentamos os conceitos básicos de Teoria Algébrica dos Números que serão utilizados como ferramentas para a construção dos códigos de bloco espaço-tempo.

Definição 10: Seja $\mathbb{K}$ um corpo de números de grau finito. Um elemento $\alpha \in \mathbb{K}$ é chamado *inteiro algébrico* (ou simplesmente inteiro) sobre $\mathbb{Z}$ se existirem $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Esta equação é chamada de equação de dependência integral de α.

Exemplo 3: O elemento $\alpha = \sqrt{5} \in \mathbb{Q}(\sqrt{5})$ é inteiro sobre $\mathbb{Z}$ e a equação de dependência integral é dada por $\alpha^2 - 5 = 0$.

Definição 11: Seja $\mathbb{K}$ um corpo de números de grau n. O conjunto $\mathcal{O}_K$ dos elementos de $\mathbb{K}$ que são inteiros sobre $\mathbb{Z}$ é um anel chamado *anel dos inteiros* de $\mathbb{K}$.

Teorema 4: [7, Corollary, 2.7] Seja $\mathbb{K}$ um corpo de números de grau n. O anel dos inteiros $\mathcal{O}_K$ de $\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n, isto é, $\mathcal{O}_K$ possui uma base consistindo de n elementos sobre $\mathbb{Z}$.

Definição 12: Seja $\mathbb{K}$ um corpo de números de grau n. Uma base de $\mathbb{L}$ sobre $\mathbb{Q}$ contida em $\mathcal{O}_K$ é chamada de *base integral* de $\mathbb{K}$.

Teorema 5: [7, Corollary, 2.6] Seja $\mathbb{K}$ um corpo de números de grau n.

1) Se $\alpha \in \mathbb{K}$, então $T(\alpha),\ N(\alpha) \in \mathbb{Q}$.
2) Se $\alpha \in \mathcal{O}_K$ então $T(\alpha),\ N(\alpha) \in \mathbb{Z}$.

Exemplo 4: Seja $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. As raízes do polinômio $x^2 - 2$ são $\alpha_1 = \sqrt{2}$ e $\alpha_2 = -\sqrt{2}$. Assim, para todo $\alpha = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ temos os homomorfismos dedinidos por $\sigma_1(\alpha) = a + b\sqrt{2}$ e $\sigma_2(\alpha) = a - b\sqrt{2}$, e deste modo, temos que $T(\alpha) = 2a$ e $N(\alpha) = a^2 - 2b^2$.

Teorema 6: [7, Theorem 1, 2.5] Se $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ é um corpo de números quadrático, onde $d \in \mathbb{Z}$ é livre de quadrados, então o anel dos inteiros algébricos $\mathcal{O}_K$ de $\mathbb{K}$ é dado por:

1) $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ se $d \equiv 2$ ou $3(mod\ 4)$;
2) $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ se $d \equiv 1(mod\ 4)$.

Definição 13: Sejam $\mathbb{K}$ um corpo de números de grau n e $\{\alpha_1, \cdots, \alpha_n\} \subset \mathbb{K}$. Definimos o discriminante do conjunto $\{\alpha_1, \cdots, \alpha_n\}$ por

$$D(\alpha_1, \cdots, \alpha_n) = det(T(\alpha_i \alpha_j)).$$

Exemplo 5: Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{11})$ e $\{1, \sqrt{11}\} \subset \mathbb{K}$. Assim,

$$\begin{aligned} D(1, \sqrt{11}) &= det \begin{pmatrix} T(1) & T(\sqrt{11}) \\ T(\sqrt{11}) & T(\sqrt{11})^2 \end{pmatrix} \\ &= det \begin{pmatrix} 2 & 0 \\ 0 & 22 \end{pmatrix} = 44. \end{aligned}$$

Proposição 2: [7, Proposition 1, 2.7] Seja $\mathbb{K}$ um corpo de números de grau n. Se $\{\beta_1, \beta_2, \cdots, \beta_n\}$ é um conjunto de elementos de $\mathbb{L}$ tal que $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, onde $a_{ij} \in \mathbb{K}$, para $i = 1, \cdots, n$, então $D(\beta_1, \cdots, \beta_n) = (det(a_{ij}))^2 D(\alpha_1, \cdots, \alpha_n)$.

Exemplo 6: Pelo Exemplo 5, vimos que o $D(1, \sqrt{11})$ de $\mathbb{Q}(\sqrt{11})$ é igual a 44. Agora, considerando outra base de $\mathbb{K}$, por exemplo $\{2 - \sqrt{11}, 1 + \sqrt{11}\}$, segue pela Proposição 2, que

$$\begin{aligned} D(2 - \sqrt{11}, 1 + \sqrt{11}) &= \det \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}^2 D(1, \sqrt{11}) \\ &= (3)^2 44. \end{aligned}$$

Teorema 7: [7, Proposition 2, 2.7] Se $\mathbb{K}$ é um corpo de números de grau n, então o discriminante de $\mathbb{K}$ independe da base e pertence a $\mathbb{Z}$.

Proposição 3: [7, Example 1, 5.3] Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z}$ é livre de quadrados. Se $d \equiv 2(modulo\ 4)$ ou $d \equiv 3(modulo\ 4)$ então o discriminante de $\mathcal{O}_K$, onde $\mathcal{O}_K$ é o anel dos inteiros de $\mathbb{K}$ sobre $\mathbb{Z}$, é $4d$.

Proposição 4: [7, Example 1, 5.3] Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z}$ é livre de quadrados. Se $d \equiv 1(modulo\ 4)$ então o discriminante de $\mathcal{O}_K$, onde $\mathcal{O}_K$ é o anel dos inteiros de $\mathbb{K}$ sobre $\mathbb{Z}$, é d.

Exemplo 7: Seja $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. Como $5 \equiv 1(modulo\ 4)$, temos pelo Teorema 6, que $\left\{1, \frac{1}{2} + \frac{\sqrt{5}}{2}\right\}$ é uma base de $\mathbb{K}$. Assim, pela Proposição 4, temos que

$$\begin{aligned} D\left(1, \frac{1+\sqrt{5}}{2}\right) &= \det \begin{pmatrix} T(1) & T\left(\frac{1+\sqrt{5}}{2}\right) \\ T\left(\frac{1+\sqrt{5}}{2}\right) & T\left(\frac{1+\sqrt{5}}{2}\right)^2 \end{pmatrix} \\ &= \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+5}{2} \end{pmatrix} = 1 + 5 - 1 = 5. \end{aligned}$$

Proposição 5: [7, Proposition 3, 2.7] Seja $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita de corpos e $\sigma_1, \cdots, \sigma_n$ $\mathbb{K}$-isomorfismos de $\mathbb{L}$. Se $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, então

$$D(\alpha_1, \cdots, \alpha_n) = det(\sigma_i(\alpha_j))^2 \neq 0.$$

Exemplo 8: Se $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})$, então existem dois $\mathbb{Q}-$isomorfismos, σ_1, σ_2, onde $\sigma_1(a + b\sqrt{3}) = a + b\sqrt{3}$ e $\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$. Como $\{1, \sqrt{3}\}$ é uma base de $\mathbb{Q}(\sqrt{3})$ sobre $\mathbb{Q}$ segue que

$$D(1, \sqrt{3}) = det \begin{pmatrix} 1 & 1 \\ \sqrt{3} & -\sqrt{3} \end{pmatrix}^2 = (-2\sqrt{3})^2 = 12.$$

Teorema 8: [9, Theorem 2.6] Se ξ_n é uma raiz n-ésima primitiva da unidade, então $\mathbb{Z}[\zeta_n]$ é o anel dos inteiros de $\mathbb{Q}(\zeta_n)$.

Teorema 9: [9, p. 11] Se ζ_n é uma raiz n-ésima primitiva da unidade, então o discriminante absoluto de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é dado por

$$D(1, \zeta_n, \cdots, \zeta_n^{\varphi(n)-1}) = \pm \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

V. CÓDIGOS DE BLOCO ESPAÇO-TEMPO

Seja S uma constelação n-dimensional contendo $2^m = M$ sinais. A cada m-upla de bits de entrada, associamos um sinal $x = (x_1, \cdots, x_n)$ sobre S. Quando x é enviado pelo canal gaussiano, a ação do ruído faz com que o sinal recebido seja

$$r = x + \beta,$$

onde $\beta = (\beta_1, \cdots, \beta_n)$ é um processo aleatório gaussiano. Quando um sinal x é transmitido através de um canal com ruído Rayleigh com desvanecimento, o sinal recebido é

$$r = \alpha * x + \beta,$$

onde $\beta = (\beta_1, \cdots, \beta_n)$ é um vetor ruído, cujas componentes são variáveis aleatórias independentes com distribuição gaussiana, média 0 e variância N_0, $\alpha = (\alpha_1, \cdots, \alpha_n)$ são os coeficientes de desvanecimento com segundo momento unitário e $*$ representa o produto componente a componente. Em geral, os M sinais são escolhidos de uma constelação finita S, que é obtida a partir de um reticulado Λ. Em particular, os pontos da constelação são escolhidos nas primeiras camadas do reticulado, de forma que o conjunto de sinais se aproxima

da forma esférica. A eficiência espectral é medida em número de bits por duas dimensões,

$$\eta = \frac{2m}{n}$$

e a relação sinal ruído é dado por

$$SNR = \frac{E_b}{N_0},$$

onde E_b é a energia média por bit e $N_0/2$ é a densidade espectral de potência. Um demodulador de máxima verossimilhança deverá minimizar a métrica

$$m(x|r) = \sum_{i=1}^{n} |r_i - x_i|^2$$

para o canal gaussiano, e

$$m(x|r,\alpha) = \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2,$$

para o canal Rayleigh com desvanecimento. Depois disto, é feita uma estimativa $\hat{x}$ do sinal enviado x e a suposta sequência de bits enviada é obtida. Dados x e $y \in \Lambda$, denotamos por $P(x \longrightarrow y)$ a probabilidade de que quando x é transmitido, o ponto y seja detectado, ou seja, que o ponto recebido esteja mais próxima de y do que de x, na respectiva métrica. A probabilidade de erro na constelação S tomada a partir de Λ é dada por

$$P_e(S) \leq P_e(\Lambda) \leq \sum_{x \neq y} P(x \longrightarrow y).$$

Em cada tipo de canal, a expressão acima possibilita a obtenção de fórmula explícita para a probabilidade de erro, conforme vemos nos ítens que seguem.

- **Canal gaussiano:** a probabilidade de erro de símbolo é limitada superiormente por

$$P_e \leq \frac{\tau}{2} erfc\left(\frac{d_{min}/2}{\sqrt{2N_0}}\right),$$

onde τ é o número de vizinhos e d_{min} é a menor distância na constelação. O ganho de codificação é dado por

$$\gamma = \frac{d_{min}^2}{v(\Lambda)^{2/n}},$$

onde $v(\Lambda)$ é o volume do reticulado, e representa o ganho de potência com relação a $\mathbb{Z}^n$, podendo ser obtido a partir da densidade de centro dada por

$$\delta = (\gamma/4)^{n/2}.$$

- **Canal Rayleigh com desvanecimento:** a probabilidade de erro de símbolo par a par com alta relação sinal-ruído satisfaz

$$P_e(S) \leq \frac{1}{2} \prod_{x_i \neq y_i} \frac{1}{\frac{(x_i - y_i)^2}{8N_0}} = \frac{1}{2} \frac{1}{\left(\frac{\eta E_b}{8N_0}\right)^l d_p^l(x,y)^2},$$

onde E_b é a energia média por bit, l é a diversidade, $\eta = \frac{2m}{n}$ é a eficiência espectral e $d_p^2(x,y)$ é a distância l-produto normalizada de x a y, dada por

$$d_p^2(x,y) = \frac{\prod_{x_i \neq y_i} (x_i - y_i)^2}{(\frac{E}{n})^l},$$

onde $E = E(||x||^2)$ é a energia média por ponto da constelação.

Como o interesse é pelo caso $l = n$, omitiremos a notação l.

Definição 14: A *diversidade* de uma constelação é a distância mínima de Hamming entre quaisquer dois pontos distintos da constelação.

Seja

$$K_s = \sum_{x \in S} \frac{1}{d_p^2(x,0)}.$$

A probabilidade de erro de símbolo satisfaz

$$P_e(S) \leq \frac{1}{2} \frac{K_s}{\left(\frac{\eta E_b}{8N_0}\right)^n}.$$

Para minimizar a probabilidade de erro, precisamos:

1) maximizar a diversidade;
2) minimizar K_S, que equivale a simultaneamente maximizar a distância produto mínima e minimizar o número de vizinhos produto.

Seja um vetor símbolo de informação $\mathbf{s} = (s_1, s_2, \cdots, s_q)$, onde $q \geq 1$ e s_j, para $j = 1, 2, \cdots, q$, pertence a uma dada constelação.

Definição 15: Um *código de bloco espaço-tempo* associa cada vetor símbolo de informação $\mathbf{s}$ a uma matriz $T \times M$, denotada por $\mathbf{X}(s)$, onde M símbolos codificados x_{tm} $(m = 1, 2, \cdots, M)$ são transmitidos simultaneamente de todas antenas transmissoras no tempo t $(t = 1, 2, \cdots, T)$.

Para atingir altas eficiências num sistema de transmissão de dados necessitamos de múltiplas antenas no transmissor e no receptor. Neste caso, o sinal recebido é dado por

$$Y_{T \times N} = X_{T \times M} H_{M \times N} + W_{T \times N},$$

onde X é a palavra transmitida, H é a matriz canal (conhecida pelo receptor), W o ruído Gaussiano, M é o número de antenas transmissoras, N é o número de antenas receptoras [3].

Exemplo 9: Como um exemplo de *código espaço-tempo* com duas antenas transmissoras e duas antenas receptoras temos

$$\mathcal{C} = \left\{ X = \begin{bmatrix} s_1 & s_2 \\ s_3 & s_4 \end{bmatrix} \ : \ s_1, s_2, s_3, s_4 \in S \subset \mathbb{C} \right\},$$

onde S é uma constelação de sinais.

Considerando a decodificação por máxima verossimilhança e a tentativa de minimizar a probabilidade de erro de que $\mathbf{s}_2$ seja recebido dado que $\mathbf{s}_1$ foi enviado, temos os seguintes critérios:

1) **Critério do posto:** o posto mínimo r de $\mathbf{X}(s_1) - \mathbf{X}(s_2)$ tomadas sobre todos os pares (s_1, s_2) é o ganho de diversidade e deve ser maximizado.

2) **Critério do determinante:** Se $\mathbf{A} = \mathbf{X}(s_1) - \mathbf{X}(s_2)$, então o mínimo de $(\prod_{j=1}^{r} \lambda_j)^{1/r}$, tomado sobre todos os pares de palavras código distintas, é o ganho do código e deve ser maximizado, onde λ_j, para $j = 1, 2, \cdots, r$, são os autovalores de $\mathbf{A}\mathbf{A}^H$, onde $\mathbf{A}^H$ denota a matriz transposta conjugada de $\mathbf{A}$.

Exemplo 10: Seja o código definido por

$$\mathcal{C}_{Alamouti} = \left\{ X(s) = \begin{bmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{bmatrix} \ : \ s_1, \ s_2 \in \mathbb{C} \right\},$$

onde s^* denota o conjugado complexo de s. Este código é chamado código de Alamouti [1] e satisfaz os critérios acima.

Exemplo 11: Seja o código definido por

$$\mathcal{C}_{Damen} = \left\{ X_{2,\psi}(s) = \frac{1}{\sqrt{2}} \begin{bmatrix} s_1 + \psi s_2 & \alpha(s_3 + \psi s_4) \\ \alpha(s_3 - \psi s_4) & s_1 - \psi s_2 \end{bmatrix} \right\},$$

onde $\alpha^2 = \psi$ e $\psi = e^{i\lambda}$. O parâmetro λ é real e deve ser otimizado. Este código possui taxa e diversidade máximas [3].

Exemplo 12: Seja o código definido por

$$\mathcal{C}_{Viterbo} = \left\{ X(s) = \begin{bmatrix} s_1 + s_2\alpha & s_3 + s_4\alpha \\ \gamma(s_3 + s_4\overline{\alpha}) & s_1 + s_2\overline{\alpha} \end{bmatrix} \right\},$$

onde $s_1, s_2, s_3, s_4 \in \mathbb{Z}[i]$, $\gamma \in \mathbb{C}$, $\alpha = \frac{1+\sqrt{5}}{2}$ e $\overline{\alpha} = \frac{1-\sqrt{5}}{2}$. Este código possui taxa máxima e é chamado de código de ouro [6].

VI. Códigos de bloco espaço-tempo sobre corpos de números

Sejam $\mathbb{L} = \mathbb{Q}(\sqrt{d}, \alpha)$ uma extensão quadrática de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ e $\mathcal{O}_K$ o anel dos inteiros de $\mathbb{K}$, onde d é um inteiro livre de quadrados e $\alpha \in \mathbb{C}$. Temos que o anel dos inteiros de $\mathbb{L}$ é dado por $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, $\mathbb{L} = \{s_1 + s_2\alpha \mid s_1, s_2 \in \mathbb{Q}(\sqrt{d})\}$ é uma extensão quadrática relativa de $\mathbb{K}$ com polinômio mínimo $p(x) = x^2 + ax + b \in \mathbb{K}[x]$ e que $\{1, \alpha\}$ é uma base integral de $\mathbb{L}$ sobre $\mathbb{K}$. Para todo inteiro algébrico $z = s_1 + s_2\alpha \in \mathcal{O}_L$, com $s_1, s_2 \in \mathcal{O}_K$, a norma relativa é dada por

$$N(z) = (s_1 + s_2\alpha)(s_1 + s_2\overline{\alpha}) = s_1^2 + s_2^2 + s_1 s_2(\alpha + \overline{\alpha}) \in \mathcal{O}_K.$$

O corpo $\mathbb{L} = \{s_1 + s_2\sqrt{d} + s_3\alpha + s_4\alpha\sqrt{d} \ : \ s_1, s_2, s_3, s_4 \in \mathbb{Q}\}$ é uma extensão absoluta sobre $\mathbb{Q}$ com base integral $\{1, \sqrt{d}, \alpha, \alpha\sqrt{d}\}$ sobre $\mathbb{Q}$.

Definição 16: Definimos o *código infinito* $\mathcal{C}_\alpha$ como o conjunto das matrizes da forma

$$\mathcal{C}_\alpha = \left\{ X(s) = \begin{bmatrix} s_1 + s_2\alpha & s_3 + s_4\alpha \\ \gamma(s_3 + s_4\overline{\alpha}) & s_1 + s_2\overline{\alpha} \end{bmatrix} \right\},$$

onde $s_1, s_2, s_3, s_4 \in \mathcal{O}_K$, $\gamma \in \mathbb{C}$ e $\overline{\alpha}$ é o conjugado de α sobre $\mathbb{K}$.

Temos que $\mathcal{C}_\alpha$ é um código linear, uma vez que $X_1 + X_2 \in \mathcal{C}_\alpha$ para todo $X_1, X_2 \in \mathcal{C}_\alpha$ e se tomarmos os símbolos de informações s_1, s_2, s_3, s_4 sobre uma constelação finita de sinais $S \subseteq \mathcal{O}_K$ temos um *código finito* $\mathcal{C}$. Definimos o *determinante mínimo* de $\mathcal{C}_\alpha$ como

$$d_{min}(\mathcal{C}_\alpha) = min_{X \in \mathcal{C}_\alpha, X \neq 0} \mid det(X) \mid^2$$

e o determinante mínimo do código $\mathcal{C}$ como

$$d_{min}(\mathcal{C}_\alpha) = min_{X_1, X_2 \in \mathcal{C}_\alpha, X_1 \neq X_2} \mid det(X_1 - X_2) \mid^2 .$$

Observação 1: Se tomarmos $d = -1$, $\gamma = \alpha$ e $\alpha = e^{i\psi}$ temos que o código $\mathcal{C}_\alpha$ é o código de Damen e se tomarmos $d = -1$, $\alpha = \frac{1+\sqrt{5}}{2}$ temos que o código $\mathcal{C}_\alpha$ é o código de ouro de Viterbo.

Definição 17: Seja $\mathbb{L}$ um corpo de números.

1) Uma *involução* $\phi : \mathbb{L} \longrightarrow \mathbb{L}$ é uma aplicação aditiva e multiplicativa tal que ϕ^2 é a identidade de $\mathbb{L}$.
2) O conjunto $K = \{x \in \mathbb{L} | \phi(x) = x\}$ é um corpo, chamado *corpo fixo da involução*.

Temos que $[\mathbb{L} : \mathbb{K}] \leq 2$. Supondo que $[\mathbb{L} : \mathbb{K}] = 2$, pelo Teorema 1, temos que $\mathbb{L} = \mathbb{K}[\alpha]$, para algum $\alpha \in \mathbb{L}$.

Definição 18: Definimos o *código infinito* $\mathcal{C}_\phi$ como o conjunto das matrizes da forma

$$\mathcal{C}_\phi = \left\{ X(s) = \begin{bmatrix} s_1 + s_2\alpha & s_3 + s_4\alpha \\ \gamma(s_3 + s_4\overline{\alpha}) & s_1 + s_2\overline{\alpha} \end{bmatrix} \right\},$$

onde $s_1, s_2, s_3, s_4 \in \mathcal{O}_K$, $\gamma \in \mathbb{C}$ e $\overline{\alpha}$ é o conjugado de α sobre $\mathbb{K}$.

VII. Códigos de bloco espaço-tempo sobre corpos ciclotômicos

Sejam $\mathbb{L} = \mathbb{Q}(\zeta_n)$ e $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, onde ζ_n é uma raiz n-ésima primitiva da unidade. Temos que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, onde φ é a função de Euler, $\mathbb{L} = \{s_1 + s_2\zeta \mid s_1, s_2 \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})\}$ é uma extensão quadrática relativa de $\mathbb{K}$ com polinômio mínimo $p(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1 \in \mathbb{K}[x]$, o anel dos inteiros de $\mathbb{L}$ é $\mathcal{O}_L = \mathbb{Z}[\zeta_n]$, $\{1, \zeta_n\}$ é uma base integral de $\mathbb{L}$ sobre $\mathbb{K}$, $[\mathbb{K} : \mathbb{Q}] = \varphi(n)/2$, $\mathcal{O}_K = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ é o anel dos inteiros de $\mathbb{K}$ e que $\{\zeta_n^j + \zeta_n^{-j}\}$, para $j = 1, 2, \cdots, \varphi(n)/2$, é uma base integral de $\mathbb{K}$ sobre $\mathbb{Q}$.

Para todo inteiro algébrico $z = s_1 + s_2\zeta_n \in \mathcal{O}_L$, com $s_1, s_2 \in \mathcal{O}_K$, sua norma relativa é dada por

$$N(z) = (s_1 + s_2\zeta_n)(s_1 + s_2\zeta_n^{-1}) = s_1^2 + s_2^2 + s_1 s_2(\zeta_n + \zeta_n^{-1}),$$

que é um elemento de $\mathcal{O}_K$. O corpo $\mathbb{L} = \{s_0 + s_1\zeta_n + \cdots + s_{\varphi(n)-1}\zeta_n^{\varphi(n)-1} \ : \ s_0, s_1, \cdots, s_{\varphi(n)-1} \in \mathbb{Q}\}$ é uma extensão absoluta de $\mathbb{Q}$ com base integral $\{1, \zeta_n, \cdots, \zeta_n^{\varphi(n)-1}\}$.

Definição 19: Definimos o *código infinito* $\mathcal{C}_{\zeta_n}$ como o conjunto das matrizes da forma

$$\mathcal{C}_{\zeta_n} = \left\{ X(s) = \begin{bmatrix} s_1 + s_2\zeta_n & s_3 + s_4\zeta_n \\ \gamma(s_3 + s_4\zeta_n^{-1}) & s_1 + s_2\zeta_n^{-1} \end{bmatrix} \right\},$$

onde $s_1, s_2, s_3, s_4 \in \mathcal{O}_K$, $\gamma \in \mathbb{C}$ e ζ_n^{-1} é o conjugado de ζ_n sobre $\mathbb{K}$.

Se γ é um elemento transcendente sobre $\mathbb{K}$ então

$$det(X(s)) = N(s_1 + s_2\zeta_n) - \gamma N(s_3 + s_4\zeta_n) \neq 0.$$

Por outro lado, temos que

$$\begin{aligned} X(s) &= \begin{bmatrix} s_1 + s_2\zeta_n & s_3 + s_4\zeta_n \\ \gamma(s_3 + s_4\zeta_n^{-1}) & s_1 + s_2\zeta_n^{-1} \end{bmatrix} \\ &= \begin{bmatrix} s_1 + s_2\zeta_n & 0 \\ 0 & s_1 + s_2\zeta_n^{-1} \end{bmatrix} \\ &+ \begin{bmatrix} s_3 + s_4\zeta_n & 0 \\ 0 & s_3 + s_4\zeta_n^{-1} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ \gamma & 0 \end{bmatrix}. \end{aligned}$$

Assim, se γ não é uma norma algébrica de qualquer elemento de $\mathbb{L}$, então o conjunto das matrizes $X(s)$ é uma álgebra de divisão [2]. Deste modo, para satisfazer o critério do posto devemos ter que $det(X) \neq 0$.

VIII. CONCLUSÕES

Neste trabalho apresentamos construções de códigos de bloco espacço-tempo via corpos de números. Tais construções são muito similares as apresentadas por Damen e Viterbo, mas são muito mais gerais e nesta família bons exemplos podem ser obtidos.

AGRADECIMENTOS

Agradecemos a FAPESP, Processo 02/07473-7, pelo apoio.

REFERÊNCIAS

[1] Alamouti, S.M. "A simple transmit diversity technique for wireless communications," *IEEE Select. Areas Commun.*, Vol. 16, pp. 1451-1458, Oct. 1998.

[2] Belfiore, J.-C. and Rekaya, G. "Quaternionic lattices for space-time coding." *Proceedings of the Information Theory Workshop, IEEE*, Paris 31 March - 4 April 2003, ITW 2003.

[3] Damen, M.O., Tewfik, A. and Belfiore, J.C. "A constructions of a space-time code based on number theory." *IEEE Trans. Inform. Theory*, Vol.49, N.5, pp. 1037-1113, May 2003.

[4] Gamal, H. and Damen, M.O. "Universal space-time coding." *IEEE Trans. Inform. Theory*, Vol. 49, No. 5, pp. 1097-1119, May 2003.

[5] 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, No. 10, pp. 2596-2616, October 2003.

[6] Belfiore, J.-C, Rekaya, G. and Viterbo, E. "The golden code: 2×2 full-rate space-time code with non-vanishing determinants."To appear, 2005.

[7] Samuel, P. *Algebraic theory of numbers.* Paris, Herman 1967.

[8] Lang, S. *Álgebra.* Addison-Wesley Publishing Company, 1972.

[9] Washington, L.C. *Introduction to Ciclotomic Fields.* Springer-Verlag, 1982.