Codificação de Rede na Camada Física via Reticulados

Danilo Silva

***Resumo*— Codificação de rede na camada física (PNC) é uma estratégia de cooperação em redes sem fio que utiliza a interferência como um auxílio—ao invés de um obstáculo—para a comunicação. Uma forma promissora de PNC baseada em reticulados aninhados tem atraído significativamente a atenção da comunidade devido a suas inúmeras vantagens teóricas e práticas. Este artigo convidado sumariza alguns dos resultados recentes nessa área obtidos pelo autor e seus colaboradores (Feng, Silva & Kschischang, *IEEE Trans. Inf. Theory*, 2013). Especificamente, é apresentada uma abordagem algébrica para PNC, baseada na teoria de módulos, a qual se aplica a qualquer par de reticulados aninhados. São fornecidas expressões para a probabilidade de erro e critérios de projeto para reticulados genéricos, os quais são também particularizados para reticulados baseados na Construção A.**

***Palavras-Chave*— Comunicações cooperativas, redes sem fio, codificação de rede, reticulados aninhados.**

***Abstract*— Physical-layer network coding (PNC) is a relaying strategy for wireless networks that exploits interference as an aid—rather than an obstacle—to communications. A promising type of PNC based on nested lattices is attracting significant attention due to its several advantages, both theoretical and practical. This invited paper summarizes some of the recent work in this area obtained by the author and his collaborators (Feng, Silva & Kschischang, *IEEE Trans. Inf. Theory*, 2013). Specifically, an algebraic framework for PNC is presented, based on module theory, which is applicable to any pair of nested lattices. Error probability expressions and design criteria are derived for general lattices and then specialized for lattices based on Construction A.**

***Keywords*— Cooperative communications, wireless networks, network coding, nested lattices.**

I. Introdução

Codificação de rede na camada física (PNC) é uma nova estratégia de cooperação em redes sem fio que explora de forma inteligente a interferência entre usuários, com o objetivo de aumentar as taxas de informação alcançáveis. Proposta independentemente em [1]–[3], a essência da PNC é fazer uso da sobreposição de sinais em um canal de acesso múltiplo para extrair evidência—na forma de equações lineares—sobre as mensagens (digitais) às quais os sinais estão associados. A evidência extraída pode então ser encaminhada para outros destinatários, os quais podem recuperar as mensagens desejadas resolvendo-se um sistema linear.

O exemplo mais proeminente de PNC considera o canal bidirecional com relay (TRWC), em que dois usuários desejam trocar mensagens através de um relay, conforme ilustrado na Fig. 1. Suponha que os usuários 1 e 2 transmitem simultaneamente os sinais $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{C}^n$, correspondentes às mensagens

Danilo Silva: Departamento de Engenharia Elétrica, Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil. E-mail: danilo@eel.ufsc.br. Este trabalho foi parcialmente financiado pelo CNPq (475482/2012-3).

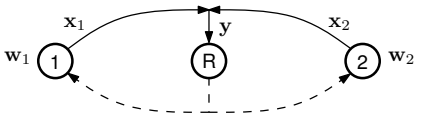

Fig. 1. Canal bidirecional com relay.

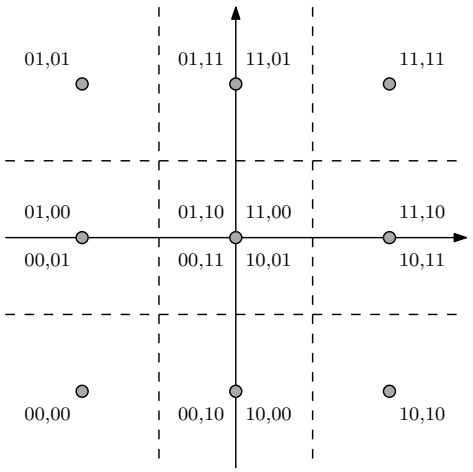

Fig. 2. Constelação recebida quando $h_1 = 1$, $h_2 = 1$.

$\mathbf{w}_1, \mathbf{w}_2 \in W = \{0,1\}^k$, respectivamente. Suponha que o relay deseja obter o XOR entre as mensagens, $\mathbf{u} = \mathbf{w}_1 \oplus \mathbf{w}_2$ (pois esta é uma evidência útil para ambos os usuários se posteriormente transmitida através de difusão). O problema, portanto, é como decodificar esta função a partir do sinal recebido $\mathbf{y} = h_1\mathbf{x}_1 + h_2\mathbf{x}_2 + \mathbf{z}$, onde $h_1, h_2 \in \mathbb{C}$ são ganhos do canal e $\mathbf{z} \in \mathbb{C}^n$ é ruído gaussiano.

Suponha que os dois usuários utilizem a modulação 4-QAM sem codificação, com mapeamento

$$00 \to -1 - i, \quad 10 \to 1 - i, \quad 01 \to -1 + i, \quad 11 \to 1 + i$$

onde $i = \sqrt{-1}$, e suponha que $h_1 = h_2 = 1$. A constelação recebida é mostrada na Fig. 2. Pode-se ver que é possível decodificar o XOR usando as regiões de decisão ilustradas na figura: embora não seja possível determinar $(\mathbf{w}_1, \mathbf{w}_2)$, não há ambiguidade sobre $\mathbf{u} = \mathbf{w}_1 \oplus \mathbf{w}_2$.

O exemplo acima, no entanto, torna-se limitado para tratar canais mais genéricos. Por exemplo, se $h_1 = 1$ e $h_2 = i$, isto é o canal aplica uma rotação no segundo sinal, surgem ambiguidades no cálculo do XOR, sendo preciso que o relay seja capaz de decodificar outras combinações lineares (no caso, não sobre um corpo finito mas sobre o anel de inteiros gaussianos $\mathbb{Z}[i]$). Além da escolha da combinação linear mais adequada, outras questões envolvem o aumento da eficiência espectral e a integração com a codificação de canal.

A abordagem moderna para PNC, denominada neste artigo de codificação de rede via reticulados (*lattice network coding*), foi introduzida por Nazer e Gastpar em [4], sob a alcunha de *compute-and-forward*. Baseados nos resultados de Erez e Zamir [5], os quais utilizaram reticulados aninhados para atingir a capacidade do canal gaussiano, Nazer e Gastpar foram capazes de demonstrar taxas alcançáveis superiores a quaisquer outros esquemas PNC que não exigem conhecimento dos ganhos do canal (CSI) nos transmissores (apenas no receptor). Os resultados em [4] deixam claro que os coeficientes da combinação linear inteira a ser decodificada devem ser escolhidos livremente pelo relay, com o objetivo de aproximar da melhor forma possível os ganhos aplicados pelo canal (que não serão, em geral, inteiros).

O presente artigo revisa e sumariza os principais resultados de [6], onde é apresentada uma abordagem algébrica para o problema de PNC. Diferentemente dos resultados de teoria da informação em [4], os quais são restritos a uma construção específica de reticulados (de dimensão assintoticamente grande), nossa abordagem é válida para quaisquer reticulados complexos de quaisquer dimensões (inclusive sobre outros anéis de inteiros complexos como os inteiros de Eisenstein $\mathbb{Z}[\omega]$). Mostramos que a escolha do par de reticulados aninhados unicamente determina a estrutura algébrica do espaço de mensagens (qualquer outra estrutura resultaria em ambiguidades). Além disso, desenvolvemos uma estimativa da probabilidade de erro de decodificação, a qual resulta em critérios geométricos para o projeto de reticulados. Tais resultados são particularizados para construções importantes de reticulados baseados em códigos, especificamente, a Construção A Complexa e a Construção A Levantada.

Nossa abordagem algébrica já tem sido usada por outros autores para obter resultados importantes em PNC. Especificamente, os trabalhos [7], [8] utilizam nossa abordagem para determinar taxas alcançáveis e estimativas de probabilidade de erro para reticulados construídos sobre $\mathbb{Z}[\omega]$, demonstrando ganhos em relação a reticulados sobre $\mathbb{Z}[i]$.

II. Codificação de Rede na Camada Física

Esta seção apresenta uma formulação do problema da *codificação de rede na camada física* (PNC), bem como o modelo de canal adotado neste trabalho. Essencialmente, o objetivo da PNC é tirar proveito de um canal de múltiplo acesso para extrair combinações lineares dos pacotes transmitidos. Tais combinações lineares podem ser posteriormente repassadas para uma camada superior (que implementa codificação de rede tradicional) para realizar a comunicação fim-a-fim.

A. Modelo do Canal

Considere um canal de múltiplo acesso com L transmissores (que podem ser fontes ou *relays*) e um único receptor (que pode ser um *relay* ou um destino) sujeito a desvanecimento de bloco e ruído aditivo gaussiano branco. As entradas do canal são denotadas por $\mathbf{x}_1, \ldots, \mathbf{x}_L \in \mathbb{C}^n$ e a saída do canal é dada por

$$\mathbf{y} = \sum_{\ell=1}^{L} h_\ell \mathbf{x}_\ell + \mathbf{z} \tag{1}$$

onde $h_1, \ldots, h_L \in \mathbb{C}$ são coeficientes de desvanecimento e $\mathbf{z} \sim \mathcal{CN}(\mathbf{0}, N_0\mathbf{I}_n)$ é um vetor aleatório complexo conjuntamente gaussiano e circularmente simétrico. Assume-se que os coeficientes de desvanecimento são perfeitamente conhecidos no receptor mas *desconhecidos* nos transmissores.

Por simplicidade, assumiremos que todos os transmissores são idênticos, com potência média de transmissão dada por

$$P \triangleq \frac{1}{n} E\left[\|\mathbf{x}_\ell\|^2\right]. \tag{2}$$

Valores de potência assimétricos podem ser incorporados escalonando-se os coeficientes h_ℓ. Por conveniência, definimos $\mathsf{SNR} \triangleq P/N_0$.

B. Formulação do Problema

Seja T um anel comutativo com identidade $1 \neq 0$ e seja W um T-módulo finito, chamado de *espaço de mensagens* ou *espaço ambiente*. Assume-se que cada transmissor ℓ possui uma mensagem $\mathbf{w}_\ell \in W$ a ser transmitida e que o receptor deseja receber a combinação T-linear de mensagens dada por

$$\mathbf{u} = \sum_{\ell=1}^{L} a_\ell \mathbf{w}_\ell \in W \tag{3}$$

onde $a_\ell \in T$ são os coeficientes da combinação linear.

Por simplicidade, assumiremos que todos os transmissores são idênticos, embora essa restrição possa ser removida. Um *esquema PNC T-linear* de comprimento n consiste de um codificador

$$\mathcal{E} : W \to \mathbb{C}^n$$

idêntico para cada transmisor ℓ, o qual codifica uma mensagem $\mathbf{w}_\ell \in W$ em um vetor transmitido $\mathbf{x}_\ell = \mathcal{E}(\mathbf{w}_\ell) \in \mathbb{C}^n$, e um decodificador

$$\mathcal{D} : \mathbb{C}^n \times \mathbb{C}^L \times T^L \to W$$

que calcula, a partir do vetor recebido $\mathbf{y} \in \mathbb{C}^n$, do vetor de ganhos de canal $\mathbf{h} = (h_1, \ldots, h_L) \in \mathbb{C}^L$ e do vetor de coeficientes $\mathbf{a} = (a_1, \ldots, a_L) \in T^L$, uma estimativa $\hat{\mathbf{u}} = \mathcal{D}(\mathbf{y} \mid \mathbf{h}, \mathbf{a})$ da combinação linear de mensagens dada por (3).

Assumiremos que as mensagens $\mathbf{w}_1, \ldots, \mathbf{w}_L$ são independentes e distribuidas uniformemente sobre W. Seja

$$\mathsf{R}_{\mathsf{mes}} \triangleq \frac{1}{n} \log_2 |W| \tag{4}$$

a *taxa de mensagem* (ou eficiência espectral) do codificador, medida em bits por dimensão complexa, e seja $P_e(\mathbf{h}, \mathbf{a}) = \Pr[\hat{\mathbf{u}} \neq \mathbf{u}]$ a probabilidade de erro de decodificação.

Dados n e $\mathsf{R}_{\mathsf{mes}}$, deseja-se projetar um esquema PNC tal que, para quaisquer SNR, $\mathbf{h}$ e $\mathbf{a}$ fixos, a probabilidade de erro $P_e(\mathbf{h}, \mathbf{a})$ seja a menor possível. Naturalmente, para um dado esquema PNC e uma dada realização de canal $(\mathsf{SNR}, \mathbf{h})$, $P_e(\mathbf{h}, \mathbf{a})$ poderá ser maior ou menor dependendo da escolha de $\mathbf{a}$. Assim, um problema relacionado consiste na determinação do vetor $\mathbf{a}$ ótimo em função de $(\mathsf{SNR}, \mathbf{h})$. Uma vez fixado um método para a determinação de $\mathbf{a}$, também é possível avaliar a probabilidade de erro média de um esquema PNC considerando um modelo probabilístico para $\mathbf{h}$.

C. Taxas Alcançáveis

Mencionamos agora um resultado importante sobre taxas alcançáveis em PNC, o qual foi obtido por Nazer e Gastpar [4] usando reticulados aninhados e métodos de teoria da informação. No que segue, utilizaremos $\langle p \rangle$ para denotar o ideal de um anel T gerado pelo elemento $p \in T$.

Teorema 1 ([4]): Para qualquer $\epsilon > 0$, qualquer n suficientemente grande, e qualquer inteiro primo p suficientemente grande (tal que $n/p \to 0$ quando $n \to \infty$), existe um esquema PNC $\mathbb{Z}[i]$-linear de comprimento n, com espaço de mensagens $W = (\mathbb{Z}[i]/\langle p \rangle)^k$ para algum k, tal que, para qualquer vetor de ganhos $\mathbf{h} \in \mathbb{C}^L$, a equação correspondente ao vetor de coeficientes $\mathbf{a} \in \mathbb{Z}[i]^L$ pode ser decodificada com $P_e(\mathbf{h}, \mathbf{a}) < \epsilon$ desde que $R_{\mathsf{comp}}(\mathbf{h}, \mathbf{a}) > \mathsf{R}_{\mathsf{mes}}$, onde

$$R_{\mathsf{comp}}(\mathbf{h}, \mathbf{a}) \triangleq \max_{\alpha \in \mathbb{C}} \log_2 \left(\frac{\mathsf{SNR}}{\|\alpha \mathbf{h} - \mathbf{a}\|^2 \mathsf{SNR} + |\alpha|^2} \right).$$

O valor ótimo de α na expressão acima é dado por

$$\alpha_{\mathsf{opt}} = \frac{\mathbf{a}\mathbf{h}^{\mathsf{H}} \mathsf{SNR}}{\|\mathbf{h}\|^2 \mathsf{SNR} + 1} \tag{5}$$

o que resulta em

$$R_{\mathsf{comp}}(\mathbf{h}, \mathbf{a}) = \log_2 \left(\frac{\mathsf{SNR}}{\mathbf{a}\mathbf{M}\mathbf{a}^{\mathsf{H}}} \right) \tag{6}$$

onde $\mathbf{M} = \mathsf{SNR}\mathbf{I}_L - \frac{\mathsf{SNR}^2}{\mathsf{SNR}\|\mathbf{h}\|^2 + 1} \mathbf{h}^{\mathsf{H}} \mathbf{h}$.

As taxas alcançáveis mencionadas no teorema acima assumem reticulados de dimensão assintoticamente grande, gerados de forma aleatória e com complexidade de decodificação potencialmente ilimitada. Não fica claro a partir destes resultados como projetar e decodificar com baixa complexidade esquemas PNC de comprimento finito. Esta será nossa principal motivação para o desenvolvimento a seguir.

III. Codificação de Rede via Reticulados

A *codificação de rede via reticulados* (LNC) é uma forma de PNC que utiliza pontos de um reticulado para representar mensagens. Esta seção apresenta uma abordagem para LNC que admite o uso de quaisquer reticulados (inclusive sobre anéis de inteiros complexos), generalizando a abordagem em [4]. A característica principal de um reticulado é ser fechado com relação a combinações lineares (com coeficientes inteiros), isto é, uma combinação linear de pontos de um reticulado resulta em um ponto do reticulado. Esta é a propriedade fundamental explorada na LNC, a qual permite fazer uso do canal para calcular combinações lineares de mensagens.

A. Estrutura Algébrica

Seja T um sub-anel discreto de $\mathbb{C}$ e seja W um T-módulo finito. Em sua forma mais abrangente, um esquema LNC é especificado simplesmente por um T-reticulado $\Lambda \subseteq \mathbb{C}^n$ (isto é, um T-submódulo discreto de $\mathbb{C}^n$) *compatível* com W, isto é, tal que existe um homomorfismo sobrejetor de T-módulos $\varphi : \Lambda \to W$.

O homomorfismo φ pode ser visto como um rotulamento (linear) de todos os pontos de Λ pelas mensagens em W. Assim, uma mensagem $\mathbf{w} \in W$ pode ser codificada através da escolha de qualquer ponto $\boldsymbol{\lambda} \in \Lambda$ tal que $\varphi(\boldsymbol{\lambda}) = \mathbf{w}$. A linearidade de φ garante a compatibilidade entre operações T-lineares em $\mathbb{C}^n$ e as mesmas operações em W, uma vez que, para todos $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \Lambda$ e todos $a_1, a_2 \in T$,

$$\varphi\left(a_1 \boldsymbol{\lambda}_1 + a_2 \boldsymbol{\lambda}_2\right) = a_1 \varphi(\boldsymbol{\lambda}_1) + a_2 \varphi(\boldsymbol{\lambda}_2).$$

Portanto, se $\mathbf{x}_1, \ldots, \mathbf{x}_L \in \Lambda$ são os sinais transmitidos correspondentes a $\mathbf{w}_1, \ldots, \mathbf{w}_L \in W$ (em particular, $\varphi(\mathbf{x}_\ell) = \mathbf{w}_\ell$, $\ell = 1, \ldots, L$), então, ao menos no caso ideal $\mathbf{h} = \mathbf{a} \in T^L$ e $\mathbf{z} = 0$, a decodificação de $\mathbf{u} = \sum_\ell a_\ell \mathbf{w}_\ell$ pode ser feita simplesmente aplicando-se φ ao vetor recebido $\mathbf{y} = \sum_\ell a_\ell \mathbf{x}_\ell$.

Seja $\Lambda' \subseteq \Lambda$ o núcleo de φ, i.e., $\Lambda' = \{\boldsymbol{\lambda} \in \Lambda : \varphi(\boldsymbol{\lambda}) = \mathbf{0}\}$. Pelo Primeiro Teorema do Isomorfismo [9], sabemos que Λ' é um T-submódulo de Λ (portanto um T-reticulado), o quociente Λ/Λ' é um T-módulo, e $\Lambda/\Lambda' \cong W$. Assim, podemos interpretar a codificação como um mapeamento entre mensagens e *cosets* de Λ' em Λ, pois todo elemento de uma *coset* $\boldsymbol{\lambda} + \Lambda'$ é rotulado com a mesma mensagem $\varphi(\boldsymbol{\lambda})$.

Inversamente, dado qualquer T-reticulado $\Lambda' \subseteq \Lambda$ (com a mesma dimensão de Λ), sabemos que Λ/Λ' é um T-módulo (finito), com homomorfismo $\Lambda \to \Lambda/\Lambda'$ dado pela projeção natural $\boldsymbol{\lambda} \mapsto \boldsymbol{\lambda} + \Lambda'$. Assim, podemos escolher o espaço de mensagens como $W \cong \Lambda/\Lambda'$. Portanto, um esquema LNC pode ser igualmente especificado pelo par de T-reticulados aninhados $\Lambda \subseteq \mathbb{C}^n$ e $\Lambda' \subseteq \Lambda$. Nesse contexto, Λ e Λ' são chamados de reticulados *fino* e *grosso*, respectivamente.

Uma questão natural é como encontrar um quociente de reticulados Λ/Λ' tal que $\Lambda/\Lambda' \cong W$ ou, inversamente, como determinar a estrutura algébrica de Λ/Λ'. Esta questão é respondida no seguinte teorema, o qual faz uso do teorema de estrutura para módulos finitamente gerados sobre um domínio de ideais principais (PID) [9, p. 462] e da forma normal de Smith.

Teorema 2: Seja T um PID e seja Λ/Λ' um quociente finito de T-reticulados. Então existem matrizes geradoras $\mathbf{G}_\Lambda$ e $\mathbf{G}_{\Lambda'}$ para Λ e Λ', respectivamente, tais que

$$\mathbf{G}_{\Lambda'} = \begin{bmatrix} \mathrm{diag}(\pi_1, \ldots, \pi_k) & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{n-k} \end{bmatrix} \mathbf{G}_\Lambda$$

onde $\pi_1, \ldots, \pi_k \in T$ satisfazem $\pi_1 \mid \pi_2 \mid \cdots \mid \pi_k$. Neste caso, o mapeamento $\varphi : \Lambda \to T/\langle \pi_1 \rangle \times \cdots \times T/\langle \pi_k \rangle$ dado por $\varphi(\mathbf{r}\mathbf{G}_\Lambda) = (r_1 + \langle \pi_1 \rangle, \ldots, r_k + \langle \pi_k \rangle)$ é um homomorfismo sobrejetor de T-módulos com núcleo Λ'.

Exemplos de PIDs relevantes para PNC são os inteiros gaussianos $\mathbb{Z}[i]$ e os inteiros de Eisenstein $\mathbb{Z}[\omega]$, onde $\omega = e^{i2\pi/3}$.

B. Codificação e Decodificação

Até agora consideramos apenas a estrutura algébrica do quociente Λ/Λ'. A seguir completamos a especificação de um esquema LNC de forma que possa satisfazer restrições de potência e possa ser usado em um canal sujeito a ruído e a ganhos não necessariamente inteiros.

Primeiramente, faz-se necessário revisar alguns conceitos sobre reticulados. Uma *região fundamental* de Λ é qualquer região $\mathcal{R}_\Lambda \subseteq \mathbb{C}^n$, com $\mathbf{0} \in \mathcal{R}_\Lambda$, tal que $\{\boldsymbol{\lambda} + \mathcal{R}_\Lambda : \boldsymbol{\lambda} \in \Lambda\}$

forma uma partição de $\mathbb{C}^n$. Um *quantizador de reticulado* é qualquer função $\mathcal{Q}_\Lambda : \mathbb{C}^n \to \Lambda$ tal que $\mathcal{Q}_\Lambda(\mathbf{0}) = \mathbf{0}$ e $\mathcal{Q}_\Lambda(\boldsymbol{\lambda}+\mathbf{x}) = \boldsymbol{\lambda}+\mathcal{Q}_\Lambda(\mathbf{x})$, para todo $\boldsymbol{\lambda} \in \Lambda$. Dada uma região fundamental e/ou um quantizador, define-se a operação

$$\mathbf{x} \bmod \Lambda \triangleq (\mathbf{x}+\Lambda) \cap \mathcal{R}_\Lambda = \mathbf{x} - \mathcal{Q}_\Lambda(\mathbf{x}).$$

De posse dos conceitos acima, podemos completar a especificação de um esquema PNC. Seja $\mathcal{R}_{\Lambda'}$ uma região fundamental de Λ'. O codificador $\mathcal{E} : W \to \mathbb{C}^n$ é dado por

$$\mathbf{x}_\ell = \mathcal{E}(\mathbf{w}_\ell) \triangleq \varphi^{-1}(\mathbf{w}_\ell) \cap \mathcal{R}_{\Lambda'} = \tilde{\varphi}(\mathbf{w}_\ell) \bmod \Lambda'$$

onde $\tilde{\varphi} : W \to \Lambda$ é alguma imersão tal que $\varphi(\tilde{\varphi}(\mathbf{w})) = \mathbf{w}$, para todo $\mathbf{w} \in W$. O papel de $\mathcal{R}_{\Lambda'}$, também chamada de região de formatação (*shaping region*), é controlar a potência de transmissão.

Seja $\mathcal{Q}_\Lambda$ um quantizador para Λ. O decodificador $\mathcal{D} : \mathbb{C}^n \times \mathbb{C}^L \times T^L$ é dado por

$$\hat{\mathbf{u}} = \mathcal{D}(\mathbf{y} \mid \mathbf{h}, \mathbf{a}) \triangleq \varphi(\mathcal{Q}_\Lambda(\alpha \mathbf{y})) \tag{7}$$

onde $\alpha \in \mathbb{C}$ é um fator de escalonamento escolhido em função de $\mathbf{h}$ e $\mathbf{a}$. O papel de $\mathcal{Q}_\Lambda$ é eliminar o ruído com alta probabilidade, enquanto o parâmetro α auxilia na aproximação de $\mathbf{h}$ pelos coeficientes inteiros $\mathbf{a}$.

O funcionamento do decodificador pode ser explicado através do conceito de *canal equivalente*. Seja $\mathbf{u} = \sum_\ell a_\ell \mathbf{w}_\ell$ a combinação linear a ser decodificada, e seja $\boldsymbol{\lambda} = \sum_\ell a_\ell \mathbf{x}_\ell$. Observe que $\varphi(\boldsymbol{\lambda}) = \mathbf{u}$. Consequentemente, temos o canal equivalente $\alpha\mathbf{y} = \boldsymbol{\lambda} + \mathbf{n}$, onde

$$\mathbf{n} = \sum\nolimits_{\ell=1}^{L} (\alpha h_\ell - a_\ell)\mathbf{x}_\ell + \alpha \mathbf{z} \tag{8}$$

é chamado de *ruído efetivo*.

Proposição 1:

$$P_e(\mathbf{h}, \mathbf{a}) = \min_{\alpha \in \mathbb{C}} \Pr[\mathcal{Q}_\Lambda(\mathbf{n}) \notin \Lambda'].$$

Vemos, portanto, que o desempenho do sistema depende da capacidade do decodificador de eliminar o ruído efetivo, o qual consiste de uma mistura entre ruído gaussiano e *auto-interferência* provocada pela imperfeição na quantização de $\mathbf{h}$ através de $\mathbf{a}$.

Embora a formulação acima seja genérica, as escolhas ótimas para $\mathcal{R}_{\Lambda'}$ e $\mathcal{Q}_\Lambda$ são dadas pela região de Voronoi

$$\mathcal{R}_{\Lambda'} = \{\mathbf{x} \in \mathbb{C}^n : \|\mathbf{x} - \mathbf{0}\| \leq \|\mathbf{x} - \boldsymbol{\lambda}\|, \boldsymbol{\lambda} \in \Lambda\}$$

e pelo quantizador de mínima distância euclidiana

$$\mathcal{Q}_\Lambda(\mathbf{x}) = \operatorname*{argmin}_{\lambda \in \Lambda} \|\mathbf{x} - \boldsymbol{\lambda}\|$$

os quais assumiremos no restante deste artigo.

Vale a pena mencionar que, para reduzir ainda mais a potência transmitida (assim como facilitar cálculos de probabilidade de erro), é comum a utilização de um reticulado deslocado por um vetor de *dither* $\mathbf{d}_\ell \in \mathbb{C}^n$. Nesse caso, o codificador e o decodificador são modificados para

$$\mathcal{E}(\mathbf{w}_\ell \mid \mathbf{d}_\ell) \triangleq (\mathbf{d}_\ell + \tilde{\varphi}(\mathbf{w}_\ell)) \bmod \Lambda'$$

$$\mathcal{D}(\mathbf{y} \mid \mathbf{h}, \mathbf{a}, \{\mathbf{d}_\ell\}) \triangleq \varphi\left(\mathcal{Q}_\Lambda\left(\alpha\mathbf{y} - \sum_{\ell=1}^{L} a_\ell \mathbf{d}_\ell\right)\right)$$

de tal forma que a Proposição 1 se mantém inalterada.

IV. Análise de Desempenho para Reticulados de Dimensão Finita

Nesta seção, apresentamos uma estimativa da probabilidade de erro de decodificação para $\mathbb{Z}[i]$-reticulados de dimensão finita. Este resultado é baseado no limitante da união, de forma análoga a resultados clássicos de teoria de comunicações, porém a dificuldade aqui é maior devido ao fato de que o ruído efetivo não é necessariamente gaussiano. Para derivar o limitante assumimos que o reticulado grosso é da forma $\Lambda' = \gamma\mathbb{Z}[i]^n$, para algum $\gamma \in \mathbb{C}$, e que a estratégia de *dithering* é utilizada nos transmissores, de forma a tornar a estatística do ruído efetivo mais tratável.

Definimos a *distância mínima* de um quociente de reticulados Λ/Λ' como

$$d(\Lambda/\Lambda') \triangleq \min_{\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \Lambda : \boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2 \notin \Lambda'} ||\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2|| = \min_{\boldsymbol{\lambda} \in \Lambda \setminus \Lambda'} ||\boldsymbol{\lambda}||$$

onde $\Lambda \setminus \Lambda'$ denota a diferença de conjuntos $\{\boldsymbol{\lambda} \in \Lambda : \boldsymbol{\lambda} \notin \Lambda'\}$. Note que $d(\Lambda/\Lambda')$ corresponde à norma dos vetores de mínima norma em $\Lambda \setminus \Lambda'$. Seja $K(\Lambda/\Lambda')$ o número destes vetores de mínima norma.

Definimos o *ganho de codificação nominal* de Λ/Λ' como

$$\gamma_c(\Lambda/\Lambda') \triangleq \frac{d^2(\Lambda/\Lambda')}{V(\Lambda)^{1/n}}$$

onde $V(\Lambda)$ denota o volume de uma região fundamental de Λ. Note que $\gamma_c(\Lambda/\Lambda')$ é invariante a escalonamento.

Teorema 3: Se $\Lambda' = \gamma\mathbb{Z}[i]$, onde $\gamma \in \mathbb{C}$, então uma estimativa da probabilidade de erro do decodificador (7) é

$$P_e(\mathbf{h}, \mathbf{a}) \lessapprox K(\Lambda/\Lambda') \exp\left(-\frac{3}{2}\gamma_c(\Lambda/\Lambda') 2^{-\mathsf{R}_{\mathsf{mes}}} \frac{\mathsf{SNR}}{\mathbf{a}\mathbf{M}\mathbf{a}^{\mathsf{H}}}\right)$$

onde o valor ótimo de α é dado por (5).

É interessante observar que, segundo o resultado acima, o vetor de coeficientes $\mathbf{a}$ que minimiza a probabilidade de erro é o mesmo que maximiza a taxa de computação (6).

Note também que apenas os parâmetros $\mathsf{R}_{\mathsf{mes}}$, $K(\Lambda/\Lambda')$ e $\gamma_c(\Lambda/\Lambda')$ dependem de Λ/Λ'. Conclui-se que, para uma dada eficiência espectral $\mathsf{R}_{\mathsf{mes}}$, deve-se projetar um quociente de reticulados que maximize $\gamma_c(\Lambda/\Lambda')$ e (em segundo plano) minimize $K(\Lambda/\Lambda')$. Em particular, se $\Lambda = \mathbb{Z}[i]^n$ e $\Lambda' = \pi\mathbb{Z}[i]^n$, então $\mathsf{R}_{\mathsf{mes}} = \frac{2}{n}\log_2|\pi|$ e $\gamma_c(\Lambda/\Lambda') = 1$ para todo $\pi \in \mathbb{Z}[i]^*$, correspondendo a uma modulação sem codificação.

V. Construções de Reticulados Aninhados

Nesta seção, adaptamos algumas construções conhecidas de reticulados baseados em códigos para produzir quocientes de reticulados que possuem uma estrutura algébrica simples e um alto ganho de codificação nominal, ao mesmo tempo em que podem ser decodificados utilizando métodos tradicionais.

A. Construção A Complexa

Seja π um primo em T. Observe que $T/\langle\pi\rangle$ é um corpo finito. Seja $\sigma : T \to T/\langle\pi\rangle$ a projeção natural dada por $\sigma(x) = x + \langle\pi\rangle$ e seja $\tilde{\sigma} : T/\langle\pi\rangle \to T$ uma imersão tal que $\sigma(\tilde{\sigma}(a)) = a$, para todo $a \in T/\langle\pi\rangle$. Considere as extensões componente-a-componente $\sigma : T^n \to (T/\langle\pi\rangle)^n$ e $\tilde{\sigma} : (T/\langle\pi\rangle)^n \to T^n$.

Seja $\mathcal{C}$ um código linear (n,k) sobre $T/\langle\pi\rangle$. O T-reticulado construído a partir de $\mathcal{C}$ através da *Construção A Complexa* [10] é dado por

$$\Lambda \triangleq \{\boldsymbol{\lambda} \in T^n : \sigma(\boldsymbol{\lambda}) \in \mathcal{C}\}.$$

Seja $\Lambda' = \pi T^n \subseteq \Lambda$. Pode-se mostrar que $\Lambda/\Lambda' \cong (T/\langle\pi\rangle)^k \cong \mathcal{C}$, com homomorfismo $\varphi : \Lambda \to \mathcal{C}$ dado por $\varphi(\boldsymbol{\lambda}) = \sigma(\boldsymbol{\lambda})$ onde, por simplicidade, estamos considerando o espaço de mensagens como sendo o próprio código $\mathcal{C}$.

Definimos a *norma euclidiana* de um vetor $\mathbf{v} \in (T/\langle\pi\rangle)^n$ e a *norma euclidiana mínima* de um código $\mathcal{C} \subseteq (T/\langle\pi\rangle)^n$ como

$$w_E(\mathbf{v}) \triangleq \sqrt{\sum\nolimits_{j=1}^{n} |v_i|^2} \qquad w_E(\mathcal{C}) \triangleq \min_{\mathbf{c}\in\mathcal{C}:\mathbf{c}\neq 0} w_E(\mathbf{c})$$

onde a magnitude de um elemento $a \in T/\langle\pi\rangle$ é definida como

$$|a| \triangleq |\tilde{\sigma}(a) \bmod \pi T|.$$

Note que, na expressão acima, a definição da operação $\bmod$ é consistente com a teoria de reticulados, isto é, $x \bmod \pi T$ retorna o elemento de menor norma (magnitude) em $x + \pi T$.

Com essas definições, é possível mostrar que

$$\gamma_c(\Lambda/\Lambda') = \frac{w_E^2(\mathcal{C})}{|\pi|^{2(1-k/n)}}$$

$$K(\Lambda/\Lambda') = \begin{cases} A_E(\mathcal{C})\left(2/\log_2|\pi|\right)^{w_E^2(\mathcal{C})}, & |\pi| \leq 2 \\ A_E(\mathcal{C}), & |\pi| > 2 \end{cases}$$

onde $A_E(\mathcal{C})$ denota o número de palavras de $\mathcal{C}$ de norma euclidiana mínima $w_E(\mathcal{C})$. Consequentemente, o desempenho de um código $\mathcal{C}$ para PNC através desta construção será dado principalmente por $w_E^2(\mathcal{C})$.

Além disso, pode-se mostrar que a decodificação de mínima distância em Λ/Λ' pode ser realizada através de uma busca no código $\mathcal{C}$ usando uma métrica modificada:

$$\begin{aligned}\varphi(\mathcal{Q}_\Lambda(\mathbf{x})) &= \operatorname*{argmin}_{\mathbf{c}\in\mathcal{C}} \|\mathbf{x} - \tilde{\sigma}(\mathbf{c}) \bmod \pi T^n\|^2 \\ &= \operatorname*{argmin}_{\mathbf{c}\in\mathcal{C}} \sum_{j=1}^{n} |x_j - \tilde{\sigma}(c_j) \bmod \pi T|^2 .\end{aligned}$$

A separabilidade da expressão acima, resultante da estrutura de produto cartesiano do reticulado grosso, simplifica significativamente a decodificação, permitindo, por exemplo, o uso do algoritmo de Viterbi.

B. Construção A Levantada

Seja p um primo em $\mathbb{Z}$. Observe que $\mathbb{Z}/\langle p\rangle$ é um corpo finito. Podemos interpretar $\mathbb{Z}/\langle p\rangle$ como um subconjunto de $\mathbb{Z}[i]/\langle p\rangle$ através do isomorfismo $(\mathbb{Z}/\langle p\rangle)[i] \cong \mathbb{Z}[i]/\langle p\rangle$. Da mesma forma, podemos interpretar $(\mathbb{Z}/\langle p\rangle)^n$ como um subconjunto de $(\mathbb{Z}[i]/\langle p\rangle)^n$.

Seja $\mathcal{C}$ um código linear (n,k) sobre $\mathbb{Z}/\langle p\rangle$. Considere o código levantado $\bar{\mathcal{C}} = \mathcal{C} + i\mathcal{C} \subseteq \mathbb{Z}[i]/\langle p\rangle$. Observe que $\bar{\mathcal{C}}$ é um $\mathbb{Z}[i]/\langle p\rangle$-módulo (e portanto também um $\mathbb{Z}[i]$-módulo), embora não necessariamente um espaço vetorial, pois $\mathbb{Z}[i]/\langle p\rangle$ não necessariamente é um corpo finito.

O $\mathbb{Z}[i]$-reticulado construído a partir de $\mathcal{C}$ através da *Construção A Levantada* é dado por

$$\Lambda \triangleq \{\boldsymbol{\lambda} \in \mathbb{Z}[i]^n : \sigma(\boldsymbol{\lambda}) \in \bar{\mathcal{C}}\}$$

onde $\sigma : \mathbb{Z}[i] \to \mathbb{Z}[i]/\langle p\rangle$ é a projeção natural mencionada na seção anterior. Note que esta construção pode ser intepretada como a Construção A Complexa a partir de um código levantado $\bar{\mathcal{C}}$.

Todos as definições e resultados da seção anterior se mantém substituindo-se $\mathcal{C}$ por $\bar{\mathcal{C}}$, $T = \mathbb{Z}[i]$ e $\pi = p$ (inclusive para $p = 2$). Observe que $w_E(\bar{\mathcal{C}}) = w_E(\mathcal{C})$ e $A_E(\bar{\mathcal{C}}) = 2A_E(\mathcal{C})$.

Além disso, a decodificação de mínima distância em Λ/Λ' torna-se ainda mais simples, separando-se em duas buscas independentes no código $\mathcal{C}$:

$$\varphi(\mathcal{Q}_\Lambda(\mathbf{x}_\mathsf{R} + i\mathbf{x}_\mathsf{I})) = \hat{\mathbf{c}}(\mathbf{x}_\mathsf{R}) + i\hat{\mathbf{c}}(\mathbf{x}_\mathsf{I}), \quad \mathbf{x}_\mathsf{R}, \mathbf{x}_\mathsf{I} \in \mathbb{R}^n$$

$$\hat{\mathbf{c}}(\mathbf{x}) = \operatorname*{argmin}_{\mathbf{c}\in\mathcal{C}} \sum_{j=1}^{n} |x_j - \tilde{\sigma}(c_j) \bmod p\mathbb{Z}|^2, \quad \mathbf{x} \in \mathbb{R}^n$$

onde se assume que $\tilde{\sigma}$ é tal que $\tilde{\sigma}(a) \in \mathbb{Z}$ para todo $a \in \mathbb{Z}/\langle p\rangle$.

Em particular, para $p = 2$, $\mathcal{C}$ é um código linear binário e $w_E(\mathcal{C})$ é igual à mínima distância de Hamming de $\mathcal{C}$.

VI. Conclusão

Neste artigo, descrevemos uma abordagem algébrica completamente genérica para a codificação de rede via reticulados. Esta abordagem nos permitiu desenvolver limitantes para a probabilidade de erro de diversas classes de reticulados, assim como encontrar os parâmetros geométricos e combinatoriais que determinam seu desempenho.

Exemplos específicos e resultados experimentais foram omitidos por falta de espaço e podem ser encontrados em [6].

Referências

[1] S. Zhang, S.-C. Liew, and P. P. Lam, "Hot topic: Physical layer network coding," in *Proc. ACM Int. Conf. Mobile Compu. and Netw.*, Los Angeles, CA, USA, Sep. 24–29, 2006, pp. 358–365.

[2] P. Popovski and H. Yomo, "The anti-packets can increase the achievable throughput of a wireless multi-hop network," in *Proc. of IEEE Int. Conf. on Commun.*, Istanbul, Turkey, Jun. 11–15, 2006, pp. 3885–3890.

[3] B. Nazer and M. Gastpar, "Computing over multiple-access channels with connections to wireless network coding," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, USA, Jul. 9–14, 2006, pp. 1354–1358.

[4] ——, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.

[5] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.

[6] C. Feng, D. Silva, and F. R. Kschischang, "An algebraic approach to physical-layer network coding," *IEEE Trans. Inf. Theory*, 2013, to be published. [Online]. Available: http://arxiv.org/abs/1108.1695

[7] S. Qifu and J. Yuan, "Lattice network codes based on Eisenstein integers," in *Proc. 20012 IEEE Int. Conf. on Wireless and Mobile Comput.*, Barcelona, Spain, Oct. 2012, pp. 225–231.

[8] N. E. Tunali, K. R. Narayanan, J. J. Boutros, and Y.-C. Huang, "Lattices over Eisenstein integers for compute-and-forward," in *Proc. Allerton Conf. Commun., Control, and Comput.*, Monticello, IL, Oct. 2012, pp. 33–40.

[9] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed. John Wiley & Sons, Inc., 2004.

[10] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York: Springer-Verlag, 1999.