Reticulados LDPC com Codificação e Decodificação Eficiente e uma Generalização da Construção D′

Paulo Ricardo Branco da Silva e Danilo Silva

***Resumo*— Neste artigo são propostos algoritmos de codificação e decodificação com tempo linear para reticulados LDPC multinível baseados na Construção D′. Além disso, uma generalização da Construção D′ é proposta, a qual resulta em uma nova classe de reticulados multinível. A partir desta construção, são projetados reticulados LDPC que alcançam desempenho comparável ao de reticulados polares no canal AWGN sem restrição de potência.**

***Palavras-Chave*— Construção D′, reticulados, códigos LDPC, códigos multinível, decodificação multiestágio.**

***Abstract*— We propose linear-time encoding and decoding algorithms for multilevel LDPC lattices based on Construction D′. Moreover, a generalization of Construction D′ is proposed which leads to a new class of multilevel lattices. Based on this construction, two-level LDPC lattices are designed that achieve performance comparable to that of polar lattices in the power-unconstrained AWGN channel.**

***Keywords*— Construction D′, lattices, LDPC codes, multilevel codes, multistage decoding.**

I. Introdução

Um dos principais desafios na área de codificação de canal é encontrar códigos capazes de alcançar a capacidade do canal com ruído aditivo gaussiano branco (AWGN) e que possam ser codificados e decodificados de forma computacionalmente eficiente. Uma ferramenta poderosa para esse fim são os códigos de reticulado, os quais também são úteis para diversas outras aplicações (veja [1] e suas referências).

Um código de reticulado $\mathcal{C} = \Lambda \cap \mathcal{R}$ consiste da intersecção entre um reticulado $\Lambda \in \mathbb{R}^n$ (arranjo regular de pontos no espaco euclidiano) e uma região delimitadora $\mathcal{R} \subseteq \mathbb{R}^n$. Sabe-se que Λ deve ser escolhido como um reticulado *bom* para codificação AWGN (empacotamento), ou seja, a região de Voronoi em torno de cada ponto deve conter uma esfera com fração de volume suficientemente grande para minimizar a probabilidade de erro [1]. Conjuntamente, a escolha dos pontos do reticulado deve minimizar o consumo de potência para uma dada taxa de informação. Uma solução é escolher $\mathcal{R}$ como uma região aproximadamente esférica, possivelmente a região de Voronoi de um sub-reticulado [2]; outra é escolher uma região mais simples, como um hipercubo, mas utilizar as palavras de $\mathcal{C}$ de forma não-equiprovável, de forma a aproximar uma distribuição esférica em n dimensões [3].

Recentemente, ambos os problemas foram simultaneamente resolvidos pela primeira vez com o uso de códigos de reticulado baseados em códigos polares [4]. O esquema proposto utiliza uma codificação multinível de códigos binários com decodificação multiestágio, o que permite uma implementação eficiente sob modulação 2^L-PAM, com complexidade de decodificação $O(Ln \log n)$. Em contraste, a maioria dos reticulados propostos na literatura para esse fim são p-ários (onde p é primo) [1], exigindo códigos lineares p-ários com modulação p-PAM, o que dificulta tanto o projeto dos códigos quanto sua implementação para $p > 2$. A codificação multinível com decodificação multiestágio é útil pois reaproveita a experiência acumulada na teoria e prática de códigos binários.

Apesar de provadamente assintoticamente ótimos, códigos polares são computacionalmente menos eficientes que códigos LDPC, os quais podem ser decodificados com complexidade linear pelo algoritmo *Belief Propagation* [5]. Assim, construir reticulados LDPC multinível com desempenho comparável ao dos reticulados polares parece ser um problema importante.

Reticulados multinível são construídos algebricamente através da Construção D e da Construção D′. Descrevem o reticulado a partir das matrizes geradoras e das matrizes de verificação de paridade, respectivamente, dos códigos componentes [6]. A primeira é usada na construção dos reticulados polares em [4]. Reticulados LDPC multinível com a Construção D′ foram propostos em [7] e estudados posteriormente em [8]; no entanto, estes trabalhos consideram apenas uma decodificação conjunta dos códigos componentes, a qual tem complexidade exponencial em L. A decodificação multiestágio de reticulados LDPC é considerada em [9], mas a construção proposta se baseia na Construção D, essencialmente inviabilizando uma codificação eficiente.

Este artigo propõe reticulados LDPC com codificação e decodificação eficientes. Um desafio de projeto é que a Construção D′ tradicional exige não apenas códigos componentes aninhados, mas também matrizes de verificação de paridade aninhadas, uma restrição que aparentemente se mostra incompatível com o projeto ótimo de distribuição de graus. Para contornar este problema, uma nova Construção D′ é proposta que relaxa essa restrição. Esta contribuição pode ser de interesse independente do ponto de vista matemático.

Resultados de simulação mostram que os reticulados propostos atingem desempenho ligeiramente superior ao dos reticulados polares, e isto com complexidade de codificação e decodificação de apenas $O(Ln)$. Embora este artigo trate apenas do problema da codificação AWGN sem restrição de potência, os resultados podem, em princípio, ser estendidos para o cenário com restrição de potência através das técnicas em [2] ou [3]. Provas são omitidas por limitação de espaço.

II. Conceitos Básicos

A seguir revisamos conceitos básicos sobre reticulados e seu uso em comunicações. Para maiores detalhes, veja [1], [6].

Paulo Ricardo Branco da Silva e Danilo Silva¸ Centro Tecnológico, Universidade Federal de Santa Catarina, Florianópolis-SC, Brasil, E-mails: pauloricardo.branco@gmail.com, danilo@eel.ufsc.br.

A. Reticulados

Um reticulado $\Lambda \in \mathbb{R}^n$ é um subgrupo discreto de $\mathbb{R}^n$. Isto significa que é fechado sob combinações lineares inteiras e que pode ser definido pelo conjunto $\Lambda = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} = \mathbf{uG},\ \mathbf{u} \in \mathbb{Z}^n\}$ e pela operação de soma $+$, onde $\mathbf{G} \in \mathbb{R}^{n\times n}$ é uma matriz geradora de Λ.

Um quantizador de reticulado de mínima distância euclidiana $\mathcal{Q}_\Lambda : \mathbb{R}^n \to \Lambda$ é definido por $\mathbf{x} \mapsto \arg\min_{\boldsymbol{\lambda}\in\Lambda} \|\mathbf{x} - \boldsymbol{\lambda}\|$, com empates decididos de forma sistemática. A região de Voronoi de Λ (em torno de $\mathbf{0}$) é definida como $\mathcal{V}(\Lambda) \triangleq \{\mathbf{x} \in \mathbb{R}^n : \mathcal{Q}_\Lambda(\mathbf{x}) = \mathbf{0}\}$, cujo volume é denotado por $V(\Lambda)$. A operação modulo-Λ é definida como

$$\mathbf{x} \bmod \Lambda \triangleq \mathbf{x} - \mathcal{Q}_\Lambda(\mathbf{x}) \in \mathcal{V}(\Lambda). \tag{1}$$

B. Figuras de Mérito

Define-se a probabilidade de erro $P_e(\Lambda, \sigma^2)$ de um reticulado $\Lambda \subseteq \mathbb{R}^n$ como sendo a probabilidade de um vetor aleatório gaussiano $\mathbf{z} \in \mathbb{R}^n$ com componentes independentes de média nula e variância σ^2 se situar fora de $\mathcal{V}(\Lambda)$.

Já que a densidade de Λ é inversamente proporcional a $V(\Lambda)$, pode-se definir a razão volume-ruído (VNR) como [1]

$$\gamma_\Lambda(\sigma) \triangleq \frac{V(\Lambda)^{2/n}}{2\pi \mathrm{e}\sigma^2}. \tag{2}$$

Como mostrado em [10], [1], se $P_e(\Lambda, \sigma^2) \approx 0$, então necessariamente $\gamma_\Lambda(\sigma) > 1$. Este limite fundamental é conhecido como *limitante da esfera*. Por outro lado, para todo $\sigma^2 > 0$ e todo $P_e > 0$, existe uma sequência de reticulados com $P_e(\Lambda, \sigma^2) \le P_e$ tal que $\lim_{n\to\infty} \gamma_\Lambda(\sigma) = 1$. Tais reticulados são ditos bons para codificação AWGN.

C. Codificação sem Restrição de Potência

Uma forma prática de abordar o problema da codificação AWGN sem restrição de potência é através da partição em dois níveis proposta por Forney [10]. Dado um reticulado $\Lambda \subseteq \mathbb{R}^n$, escolhe-se primeiramente um sub-reticulado $\Lambda' \subseteq \Lambda$ tal que a operação modulo-Λ' (assim como a enumeração de elementos de Λ') seja de fácil implementação. Dessa forma, Λ pode ser particionado como $\Lambda = \mathcal{C} + \Lambda'$, onde $\mathcal{C} = \Lambda \cap \mathcal{V}(\Lambda')$.

Para transmitir um ponto $\mathbf{x} \in \Lambda$, escolhe-se independentemente $\mathbf{c} \in \mathcal{C}$ e $\boldsymbol{\lambda}' \in \Lambda'$ e transmite-se $\mathbf{x} = \mathbf{c} + \boldsymbol{\lambda}'$. Seja $\mathbf{y} = \mathbf{x} + \mathbf{z}$ a saída do canal, onde $\mathbf{z} \in \mathbb{R}^n$ é ruído aditivo. A decodificação a partir de $\mathbf{y}$ procede da seguinte maneira. Primeiramente, calcula-se

$$\mathbf{y} \bmod \Lambda' = \mathbf{c} + \mathbf{z} \bmod \Lambda' \tag{3}$$

eliminando a influência de $\boldsymbol{\lambda}'$. Em seguida, aplica-se um decodificador para $\mathcal{C}$ para o canal equivalente modulo-Λ' descrito acima, obtendo a estimativa $\hat{\mathbf{c}} \in \mathcal{C}$. Finalmente, $\hat{\mathbf{c}}$ é subtraído de $\mathbf{y}$, resultando em

$$\mathbf{y}' = \mathbf{y} - \hat{\mathbf{c}} = (\mathbf{c} - \hat{\mathbf{c}}) + \boldsymbol{\lambda}' + \mathbf{z} \tag{4}$$

e um decodificador para Λ' é aplicado, obtendo a estimativa $\hat{\boldsymbol{\lambda}}' \in \Lambda'$ e consequentemente $\hat{\mathbf{x}} = \hat{\mathbf{c}} + \hat{\boldsymbol{\lambda}}'$.

Pode-se mostrar que

$$P_e(\Lambda, \sigma^2) \le P_e(\mathcal{C}, \sigma^2) + P_e(\Lambda', \sigma^2) \tag{5}$$

onde $P_e(\mathcal{C}, \sigma^2)$ é a probabilidade de erro para o código $\mathcal{C}$ quando usado no canal em (3).

D. Construção D′

Seja $\mathcal{C}_0 \subseteq \mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_{L-1} \subseteq \mathbb{F}_2^n$ uma família de códigos lineares aninhados, onde, para $\ell = 0, \ldots, L-1$, $\mathcal{C}_\ell$ tem dimensão k_ℓ, taxa $R_\ell = k_\ell/n$ e $m_\ell = n - k_\ell$ equações de paridade. Por conveniência, definimos $m_L = 0$.

Seja $\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$ o homomorfismo de redução natural, extensível componente-a-componente, e sejam $\mathbf{h}_1, \ldots, \mathbf{h}_{m_L-1} \in \{0,1\}^n$ e

$$\mathbf{H}_\ell = \begin{bmatrix} \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{m_\ell} \end{bmatrix} \tag{6}$$

tais que $\varphi(\mathbf{H}_\ell) \in \mathbb{F}_2^{m_\ell \times n}$ seja a matriz de verificação de paridade de $\mathcal{C}_\ell$, para $\ell = 0, \ldots, L-1$.

A aplicação da Construção D′ [6] resulta no reticulado

$$\Lambda = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{h}_j \mathbf{x}^{\mathrm{T}} \equiv \mathbf{0} \pmod{2^{\ell+1}}, \\ m_{\ell+1} < j \le m_\ell,\ 0 \le \ell \le L-1\}. \tag{7}$$

Observa-se que $\Lambda = \mathcal{C} + 2^L\mathbb{Z}^n$, onde

$$\mathcal{C} = \Lambda \cap [0, 2^L)^n \tag{8}$$

é um código de reticulado. Em particular, temos que $V(\Lambda) = 2^{n(L-R)}$ onde $R = \frac{1}{n}\log_2|\mathcal{C}| = R_0 + \cdots + R_{L-1}$.

Se $\mathbf{H}_0, \ldots, \mathbf{H}_{L-1}$ são esparsas, i.e., se $\mathcal{C}_0, \ldots, \mathcal{C}_{L-1}$ são códigos LDPC, então Λ é dito ser um reticulado LDPC.

III. Descrições Alternativas para a Construção D′

Nesta seção são fornecidas descrições alternativas para a Construção D′, as quais são centrais para o restante do artigo. As proposições 1 e 2 são resultados que derivamos a partir da definição da Construção D′.

Proposição 1 (Descrição matricial): Seja Λ um reticulado definido por (7). Então

$$\Lambda = \left\{\mathbf{x} \in \mathbb{Z}^n : \mathbf{H}_\ell \mathbf{x}^{\mathrm{T}} \equiv 0 \pmod{2^{\ell+1}},\ 0 \le \ell \le L-1\right\}. \tag{9}$$

Lema 1: Sejam $\mathbf{H}_0, \ldots, \mathbf{H}_{L-1}$ matrizes satisfazendo (6). Se $\mathbf{H}_{\ell-1}\mathbf{x}^T \equiv 0 \pmod{2^\ell}$, então $\mathbf{H}_\ell \mathbf{x}^T \equiv 0 \pmod{2^\ell}$.

Proposição 2 (Codificação sequencial): Seja $\mathcal{C}$ um código de reticulado definido por (8). Todo vetor $\mathbf{x} \in \mathcal{C}$ pode ser gerado sequencialmente da seguinte forma. Para cada $\ell = 0, 1, \ldots, L-1$, escolhe-se $\mathbf{x}_\ell \in \{0,1\}^n$ satisfazendo

$$\mathbf{H}_\ell \mathbf{x}_\ell^{\mathrm{T}} \equiv \mathbf{s}_\ell \pmod 2 \tag{10}$$

onde $\mathbf{s}_\ell \in \{0,1\}^{m_\ell}$ é calculado como

$$\mathbf{s}_\ell = \left(\frac{-\mathbf{H}_\ell \sum_{i=0}^{\ell-1} 2^i \mathbf{x}_i^{\mathrm{T}}}{2^\ell}\right) \bmod 2 \tag{11}$$

e assumindo $\mathbf{s}_0 = \mathbf{0}$. Finalmente, faz-se $\mathbf{x} = \sum_{\ell=0}^{L-1} 2^\ell \mathbf{x}_\ell$.

Alternativamente, pode-se descrever o procedimento mencionado na Proposição 2 como sendo a escolha, para $\ell = 0, \ldots, L-1$, de $\mathbf{x}_\ell \in \mathcal{C}_\ell(\mathbf{s}_\ell)$, onde

$$\mathcal{C}_\ell(\mathbf{s}_\ell) = \{\mathbf{x}_\ell \in \{0,1\}^n : \mathbf{H}_\ell \mathbf{x}_\ell^{\mathrm{T}} \equiv \mathbf{s}_\ell \pmod 2\}. \tag{12}$$

IV. CODIFICAÇÃO E DECODIFICAÇÃO

Nesta seção, mostramos que, se códigos componentes admitem codificação e decodificação eficientes, então a mesma afirmação é válida para o código de reticulado correspondente.

A. Codificação Sistemática

Seja $\ell \in \{0, \ldots, L-1\}$ e suponha que, para $i = 0, \ldots, \ell-1$, os vetores $\mathbf{x}_i \in \mathcal{C}(\mathbf{s}_i)$ tenham sido previamente calculados. Dado um vetor de informação $\mathbf{u} \in \{0,1\}^{k_\ell}$, deseja-se determinar o vetor $\mathbf{p} \in \{0,1\}^{m_\ell}$ tal que $\mathbf{x}_\ell = \begin{bmatrix}\mathbf{u} & \mathbf{p}\end{bmatrix} \in \mathcal{C}_\ell(\mathbf{s}_\ell)$.

Primeiramente, note que $\mathbf{s}_\ell$ em (11) sempre pode ser calculado eficientemente, uma vez que $\mathbf{H}_\ell$ é uma matriz esparsa.

Suponha que, possivelmente através de permutações de linha e coluna, $\mathbf{H}_\ell$ possa ser expressa na forma

$$\mathbf{H}_\ell = \begin{bmatrix}\mathbf{A} & \mathbf{B} & \mathbf{T} \\ \mathbf{C} & \mathbf{D} & \mathbf{E}\end{bmatrix} \tag{13}$$

onde $\mathbf{A} \in \{0,1\}^{(m_\ell-g)\times(n-m_\ell)}$, $\mathbf{B} \in \{0,1\}^{(m_\ell-g)\times g}$, $\mathbf{T} \in \{0,1\}^{(m_\ell-g)\times(m_\ell-g)}$ é triangular inferior, $\mathbf{C} \in \{0,1\}^{g\times(n-m_\ell)}$, $\mathbf{D} \in \{0,1\}^{g\times g}$ e $\mathbf{E} \in \{0,1\}^{g\times(m_\ell-g)}$. Para o caso $\mathbf{s}_\ell = \mathbf{0}$, i.e., quando se deseja obter $\mathbf{H}_\ell \mathbf{x}_\ell^{\mathrm{T}} \equiv \mathbf{0} \pmod 2$, é mostrado em [11] que o cálculo de $\mathbf{p}$ pode ser realizado com complexidade $O(n + g^2)$. Tal complexidade pode ainda ser reduzida para $O(n)$ caso $\mathbf{H}_\ell$ admita uma estrutura especial quase-cíclica, o que de fato se verifica em praticamente todos os códigos LDPC utilizados na prática [12].

Para $\mathbf{s}_\ell$ genérico, podemos reescrever (10) como

$$\mathbf{H}'_\ell {\mathbf{x}'_\ell}^{\mathrm{T}} \equiv \mathbf{0} \pmod 2, \tag{14}$$

onde $\mathbf{H}'_\ell = \begin{bmatrix}-\mathbf{s}_\ell & \mathbf{H}_\ell\end{bmatrix}$ e $\mathbf{x}'_\ell = \begin{bmatrix}1 & \mathbf{x}_\ell\end{bmatrix}$. Assim, observamos que $\mathbf{H}'_\ell$ pode ainda ser expressa na forma (13), com o primeiro bloco de colunas substituído por $\begin{bmatrix}\mathbf{A}' \\ \mathbf{C}'\end{bmatrix} = \begin{bmatrix}-\mathbf{s}_\ell & \mathbf{A} \\ & \mathbf{C}\end{bmatrix}$, enquanto $\mathbf{x}'_\ell = \begin{bmatrix}\mathbf{u}' & \mathbf{p}\end{bmatrix}$, com $\mathbf{u}' = \begin{bmatrix}1 & \mathbf{u}\end{bmatrix}$, o que não altera a ordem de complexidade. Na verdade, assumindo que $\mathbf{s}_\ell$ já tenha sido calculado, observa-se facilmente das Tabelas I e II de [11] que as únicas alterações no algoritmo de [11] são o acréscimo de apenas m_ℓ adições.

Sob essas hipóteses, conclui-se que o código de reticulado $\mathcal{C}$ admite codificação sistemática com complexidade $O(Ln)$.

B. Decodificação Multi-Estágio

Seja $\mathbf{x} = \sum_{\ell=0}^{L-1} 2^\ell \mathbf{x}_\ell \in \mathcal{C}$ o vetor transmitido, onde $\mathbf{x}_\ell \in \{0,1\}^n$, e $\mathbf{y} = \mathbf{x}+\mathbf{z}$ o vetor recebido, onde $\mathbf{z}$ é um vetor de ruído gaussiano branco de variância σ^2 por componente.

A decodificação multi-estágio de $\mathcal{C}$ pode ser feita da seguinte forma, a qual é inspirada em [10]. Suponha que os vetores $\mathbf{x}_\ell$ tenham sido corretamente decodificados para $i = 0, 1, \ldots, \ell-1$. Calcula-se

$$\mathbf{y}_\ell = \left(\frac{\mathbf{y} - \sum_{i=0}^{\ell-1} 2^i \mathbf{x}_i}{2^\ell}\right) \bmod 2. \tag{15}$$

É fácil ver que

$$\mathbf{y}_\ell = \left(\mathbf{x}_\ell + \frac{\mathbf{z}}{2^\ell}\right) \bmod 2 \tag{16}$$

o que pode ser interpretado como a transmissão de $\mathbf{x}_\ell \in \mathcal{C}_\ell(\mathbf{s}_\ell)$ através de um canal modulo-2 sujeito a ruído aditivo $\mathbf{z}/2^\ell$. Em particular, a decodificação de máxima verossimilhança seria dada por $\hat{\mathbf{x}}_\ell = \operatorname{argmax}_{\mathbf{x}_\ell \in \mathcal{C}_\ell(\mathbf{s}_\ell)} p(\mathbf{y}_\ell|\mathbf{x}_\ell)$.

Para se decodificar com baixa complexidade e desempenho próximo do ótimo, é possível usar o algoritmo iterativo *Belief Propagation*, o qual possui complexidade $O(n)$ para matrizes esparsas e um número fixo de iterações. O algoritmo tem como entrada um vetor $\mathbf{LLR} \in \mathbb{R}^n$ com a *log-likelihood ratio* (LLR) de cada componente $y_{\ell j}$ do vetor recebido $\mathbf{y}_\ell$, definida como

$$\mathrm{LLR}_j = \ln\left(\frac{p(y_{\ell j}|x_{\ell j}=0)}{p(y_{\ell j}|x_{\ell j}=1)}\right), \quad j = 1, \ldots, n. \tag{17}$$

Porém, o algoritmo assume palavras códigos $\mathbf{x}_\ell$ pertencentes a um código linear, e não a um código afim como $\mathcal{C}_\ell(\mathbf{s}_\ell)$.

Podemos reaproveitar este algoritmo para o problema em questão fazendo uso do código linear alongado $\mathcal{C}'_\ell \subseteq \mathbb{F}_2^{n+1}$ definido pela matriz de verificação de paridade $\mathbf{H}'_\ell = \begin{bmatrix}-\mathbf{s}_\ell & \mathbf{H}_\ell\end{bmatrix}$, a qual continua sendo uma matriz esparsa. Nesse caso, as palavras códigos admissíveis devem ser restringidas às da forma $\mathbf{x}'_\ell = \begin{bmatrix}1 & \mathbf{x}_\ell\end{bmatrix}$, conforme (14). Para impor esta restrição, é suficiente fornecer como vetor de LLRs o vetor

$$\mathbf{LLR}' = \begin{bmatrix}\infty & \mathbf{LLR}\end{bmatrix} \tag{18}$$

indicando que se tem certeza de que o primeiro símbolo da palavra código é igual a 1.

Conclui-se que a decodificação de $\mathcal{C}$ pode ser realizada com complexidade $O(Ln)$. Pelo limitante da união, a probabilidade de erro satisfaz

$$P_e(\mathcal{C}, \sigma^2) \leq P_e(\mathcal{C}_0, \sigma^2) + \cdots + P_e(\mathcal{C}_{L-1}, \sigma^2) \tag{19}$$

onde $P_e(\mathcal{C}_\ell, \sigma^2)$ é a probabilidade de erro de $\mathcal{C}_\ell$ no canal (16).

V. GENERALIZAÇÃO DA CONSTRUÇÃO D′

Uma grande limitação da Construção D′ é a necessidade de que não apenas os códigos componentes, mas também as matrizes $\mathbf{H}_\ell$ sejam aninhadas, i.e., $\mathbf{H}_\ell$ deve ser uma submatriz de $\mathbf{H}_{\ell-1}$. Isto dificulta o projeto de códigos LDPC, pois exige, por exemplo, que o grau médio dos nós de variável do código $\mathcal{C}_{\ell-1}$ seja significativamente superior ao do código $\mathcal{C}_\ell$, o que entra em conflito com o projeto ótimo de códigos LDPC.

A princípio, poderíamos eliminar completamente esta restrição e redefinir a Construção D′ pela expressão (9). Porém, com essa abordagem não haveria garantia da cardinalidade de $\mathcal{C}$, muito menos da possibilidade de codificação sequencial, o que descaracterizaria a construção.

Ao invés disso, podemos relaxar a restrição de aninhamento de matrizes $\mathbf{H}_\ell$ e ainda assim preservar as características da Construção D′. O ingrediente crucial é o Lema 1: se esta propriedade é válida, então a codificação sequencial (Proposição 2) torna-se possível e a cardinalidade de $|\mathcal{C}|$ se mantém como consequência imediata desta.

A forma mais simples de satisfazer a propriedade do Lema 1 é exigindo que $\mathbf{H}_\ell$ seja uma submatriz de $\mathbf{H}_{\ell-1}$. No entanto, é fácil ver que, para que a propriedade seja satisfeita, basta que $\mathbf{H}_\ell \equiv \mathbf{F}\mathbf{H}_{\ell-1} \pmod{2^\ell}$, onde $\mathbf{F}$ é alguma matriz inteira.

Definição 1 (Construção D′ Generalizada): Seja $\mathbf{H}_\ell \in \mathbb{Z}^{m_\ell \times n}$ para $\ell = 0, \ldots, L-1$, tal que $\mathbf{H}_\ell \equiv \mathbf{F}_\ell \mathbf{H}_{\ell-1} \pmod{2^\ell}$, para algum $\mathbf{F}_\ell \in \mathbb{Z}^{m_\ell \times m_{\ell-1}}$. O reticulado

$$\Lambda = \left\{ \mathbf{x} \in \mathbb{Z}^n : \mathbf{H}_\ell \mathbf{x}^{\mathrm{T}} \equiv 0 \pmod{2^{\ell+1}},\ 0 \le \ell \le L-1 \right\}$$

é dito ser obtido pela Construção D′ generalizada aplicada a $\mathbf{H}_0, \ldots, \mathbf{H}_{L-1}$. Equivalentemente, $\Lambda = \mathcal{C} + 2^L \mathbb{Z}^n$, onde $\mathcal{C} = \Lambda \cap [0, 2^L)^n$ é um código de reticulado.

É imediato verificar que o conjunto Λ definido acima é de fato um reticulado.

A ênfase da Definição 1 está nas matrizes $\mathbf{H}_\ell$, ao invés dos códigos componentes. A interpretação através de códigos componentes aninhados pode ser recuperada tomando-se $\mathcal{C}_\ell \subseteq \mathbb{F}_2^n$ como o espaço nulo de $\varphi(\mathbf{H}_\ell) \in \mathbb{F}_2^{m_\ell \times n}$. Possui, portanto, dimensão $k_\ell = n - m_\ell$, para $\ell = 0, \ldots, L-1$. Claramente, temos $\mathcal{C}_0 \subseteq \mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_{L-1}$.

O principal resultado desta seção é o teorema a seguir.

Teorema 3: Seja $\mathcal{C}$ um código de reticulado satisfazendo a Definição 1. Então $\mathcal{C}$ admite codificação sequencial segundo a Proposição 2. Além disso, $R = \frac{1}{n}\log_2|\mathcal{C}| = \sum_{i=0}^{L-1} R_\ell$, onde $R_\ell = k_\ell/n = (n - m_\ell)/n$.

É fácil ver que os resultados da Seção IV se mantém válidos para a Construção D′ generalizada.

VI. Particionamento de Equações de Paridade

No projeto de códigos LDPC, a grande vantagem da Construção D′ generalizada está em permitir que os códigos componentes possuam distribuições de graus idênticas (ou próximas). Por exemplo, podemos escolher todos os códigos componentes como códigos LDPC regulares com grau de nó de variável $d_v = 3$, o que de antemão sabemos que resultará em um desempenho razoavelmente bom. Isto é impossível de obter com a Construção D′ tradicional.

Sejam $\mathbf{h}_j^{(\ell)}$ e $\mathbf{f}_j^{(\ell)}$ a j-ésima linha das matrizes $\mathbf{H}_\ell$ e $\mathbf{F}_\ell$, para todo ℓ. Para que os graus de nós de variável do código $\mathcal{C}_\ell$ sejam iguais aos do código $\mathcal{C}_{\ell-1}$ basta que (i) para todo j, não ocorra soma de coeficientes não-nulos na combinação linear $\mathbf{h}_j^{(\ell)} = \mathbf{f}_j^{(\ell)} \mathbf{H}_{\ell-1}$, isto é, que os coeficientes não-nulos das linhas de $\mathbf{H}_{\ell-1}$ efetivamente somadas estejam em posições disjuntas, e além disso que (ii) cada linha de $\mathbf{H}_{\ell-1}$ seja somada uma única vez em todo o cálculo de $\mathbf{H}_\ell$. Esta última condição equivale a exigir que cada coluna de $\mathbf{F}$ tenha exatamente um coeficiente não-nulo. Vale notar que, seguindo essa regra, é suficiente que todas as matrizes $\mathbf{H}_\ell$ e $\mathbf{F}_\ell$ sejam binárias.

Uma forma prática de satisfazer a regra descrita acima é seguir o caminho inverso: começar da matriz $\mathbf{H}_{L-1}$ e produzir cada $\mathbf{H}_{\ell-1}$ a partir de $\mathbf{H}_\ell$ através do particionamento de equações de paridade. Mais precisamente, cada linha de $\mathbf{H}_{\ell-1}$ é transformada em duas ou mais linhas $\mathbf{H}_\ell$, com coeficientes não-nulos em posições disjuntas, de tal forma que, quando estas linhas são somadas, obtém-se a linha original de $\mathbf{H}_{\ell-1}$.

Matematicamente, seja $\mathcal{P}(\mathbf{H}) = (\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m)$ a função que mapeia uma matriz $\mathbf{H} \in \{0,1\}^{m \times n}$ aos conjuntos $\mathcal{P}_j$, $j = 1, 2, \ldots, m$, cada qual constituído pelos índices das posições não-nulas da j-ésima linha de $\mathbf{H}$. Particionar cada j-ésima linha de $\mathbf{H}$ em t_j linhas significa produzir uma nova matriz $\mathbf{H}' \in \{0,1\}^{m' \times n}$ tal que $\mathcal{P}(\mathbf{H}') = (\mathcal{P}_1^{(1)}, \ldots, \mathcal{P}_1^{(t_1)}, \ldots, \mathcal{P}_m^{(1)}, \ldots, \mathcal{P}_m^{(t_m)})$, onde $\mathcal{P}_j^{(1)}, \ldots, \mathcal{P}_j^{(t_j)}$ formam uma partição de $\mathcal{P}_j$, para todo j. Em particular, $|\mathcal{P}(\mathbf{H}')| = m' = \sum_{j=1}^m t_j$.

Verifica-se para quaisquer $\mathbf{H}$ e $\mathbf{H}'$ satisfazendo a definição acima que existe uma matriz $\mathbf{F} \in \{0,1\}^{m \times m'}$ tal que $\mathbf{H} = \mathbf{F}\mathbf{H}'$. Ou seja, as posições não-nulas da j-ésima linha de $\mathbf{F}$ são os índices das linhas de $\mathbf{H}'$ correspondentes a $\mathcal{P}_j^{(1)}, \ldots, \mathcal{P}_j^{(t_j)}$. Além disso, observa-se que os pesos das colunas de $\mathbf{H}'$ são idênticos aos de $\mathbf{H}$, em virtude da definição de partição.

A. Exemplos

Em ambos os exemplos a seguir, seja

$$\mathbf{H}_0 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

1) Combinação linear genérica: Sejam

$$\mathbf{F}_1 = \begin{bmatrix} 5 & 48 & 21 & 88 \\ 29 & 49 & 31 & 13 \end{bmatrix}$$

$$\mathbf{F}_2 = \begin{bmatrix} 3 & 7 \end{bmatrix}$$

$$\mathbf{H}_1 = \mathbf{F}_1 \mathbf{H}_0 \bmod 2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\mathbf{H}_2 = \mathbf{F}_2 \mathbf{H}_1 \bmod 4 = \begin{bmatrix} 3 & 2 & 3 & 3 & 2 & 2 & 2 & 3 \end{bmatrix}.$$

A Construção D′ generalizada aplicada às matrizes $\mathbf{H}_0$, $\mathbf{H}_1$ e $\mathbf{H}_2$ produz um código de reticulado $\mathcal{C}$ com $L = 3$ níveis e taxa $R = \frac{1}{n}\log_2|\mathcal{C}| = \frac{1}{8}\log_2(2^{4+6+7}) = 2.125$.

2) Particionamento de Equações de Paridade: Começando pela matriz

$$\mathbf{H}_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

podemos particioná-la em

$$\mathbf{H}_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

a qual por sua vez é particionada em $\mathbf{H}_0$. Note que $\mathbf{H}_2 = \mathbf{F}_2\mathbf{H}_1 \bmod 4$ e $\mathbf{H}_1 = \mathbf{F}_1\mathbf{H}_0 \bmod 2$, onde $\mathbf{F}_2 = \begin{bmatrix} 1 & 1 \end{bmatrix}$ e

$$\mathbf{F}_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

A Construção D′ generalizada aplicada às matrizes $\mathbf{H}_0$, $\mathbf{H}_1$ e $\mathbf{H}_2$ produz um código de reticulado com a mesma taxa do exemplo anterior. Note que todas estas matrizes são binárias e que cada coluna delas possui o mesmo peso (igual a 1).

VII. Resultados de Simulação

Esta seção discute o projeto de reticulados LDPC com $L = 2$ níveis codificados, bem como seu desempenho em um canal AWGN sem restrição de potência.

Construímos um reticulado $\Lambda = \mathcal{C} + 4\mathbb{Z}^n$ com a Construção D′ generalizada aplicada às matrizes $\mathbf{H}_0 \in \{0,1\}^{m_0 \times n}$ e $\mathbf{H}_1 \in \{0,1\}^{m_1 \times n}$, referentes aos códigos aninhados $\mathcal{C}_0 \subseteq \mathcal{C}_1$. Fixados n, m_0 e m_1, o código $\mathcal{C}_1$ foi escolhido como um

código LDPC regular de grau de variável $d_v = 3$ e matriz de verificação de paridade $\mathbf{H}_1$ obtida via PEG [12]. Por sua vez, $\mathbf{H}_0$ foi obtida do particionamento aleatório das linhas de $\mathbf{H}_1$. O particionamento foi feito de modo a manter a maior regularidade possível dos graus de paridade.

Para possibilitar a comparação com os resultados de [4], foram desenvolvidos códigos com os mesmos parâmetros de projeto, isto é, com $n \leq 1024$ e probabilidade de erro de bloco $P_e \leq 10^{-5}$. Mais precisamente, escolheu-se $n = 1020$.

O projeto de m_0 e m_1, ou, equivalentemente, das taxas R_0 e R_1, foi baseado na estimativa de probabilidade de erro obtida com a combinação dos limitantes (5) e (19), i.e.,

$$P_e(\Lambda, \sigma^2) \leq P_e(\mathcal{C}_0, \sigma^2) + P_e(\mathcal{C}_1, \sigma^2) + P_e(4\mathbb{Z}^n, \sigma^2). \quad (20)$$

Utilizando o critério de igualdade de probabilidades de erro [13], deseja-se obter $P_e(\mathcal{C}_0, \sigma^2) = P_e(\mathcal{C}_1, \sigma^2) = P_e(4\mathbb{Z}^n, \sigma^2) = 10^{-5}/3$.

Visto que o nível 2 (não-codificado) admite um simples decodificador de reticulado modulo-$4\mathbb{Z}^n$ (essencialmente um detector QAM), é fácil calcular a variância σ^2 do ruído observado no receptor que resulta na probabilidade de erro de bloco desejada, a qual foi obtida para $\sigma^2 = 0.1142$.

As taxas dos códigos foram encontradas num processo iterativo de projeto e simulação. Com $R_1 = 0.2471$ se alcançou probabilidade de erro $10^{-5}/3$ para σ^2. Para $\mathcal{C}_0$, um desempenho de erro semelhante foi obtido com $R_0 = 0.8902$, resultando na taxa total $R = 1.1373$ bits/dimensão, referente a VNR $= 1.6949$ (2.2914 dB).

A Fig. 1 mostra a probabilidade de erro em função da VNR para o reticulado construído com o particionamento de equações de paridade. Realizamos a comparação com o nosso melhor reticulado LDPC obtido com a Construção D′ tradicional, o qual é composto por códigos irregulares projetados por meio de *EXIT charts* [12] de comprimento $N = 5000$ e taxas $R_0 = 0.2$ e $R_1 = 0.9$. Apesar do maior comprimento, a taxa total se mostra menor e a curva de probabilidade de erro significativamente pior, o que motiva o desenvolvimento de construções alternativas à Construção D′.

A curva de desempenho do reticulado LDPC projetado com a nova construção possui taxa de declínio mais acentuada que a dos reticulados polares de [4], cruzando-a em torno de $P_e = 3 \times 10^{-5}$ (VNR $= 2.177$ dB). Para $P_e = 10^{-5}$, o desempenho é ligeiramente superior ao de [4] e ainda com a vantagem de permitir codificação e decodificação mais eficientes.

VIII. Conclusão

Propusemos uma nova construção baseada na Construção D′, a partir da qual obtivemos curvas de probabilidade de erro semelhantes às de [4] com o uso de algoritmos de codificação e decodificação computacionalmente mais eficientes.

Observamos que a extensão da abordagem proposta para mais de dois níveis ocorre naturalmente através da alteração do projeto para uma nova variância de ruído. Acreditamos igualmente que, a menos de algumas pequenas alterações no projeto e nas expressões de taxa, os resultados obtidos para o canal real se estendam para o complexo.

Além dos acréscimos sugeridos, pretendemos incorporar em trabalhos futuros a análise de probabilidade de erro com restrição de potência e a utilização de códigos mais estruturados e de melhor performance, como os LDPCs quasi-cíclicos com distribuições de graus irregulares otimizadas.

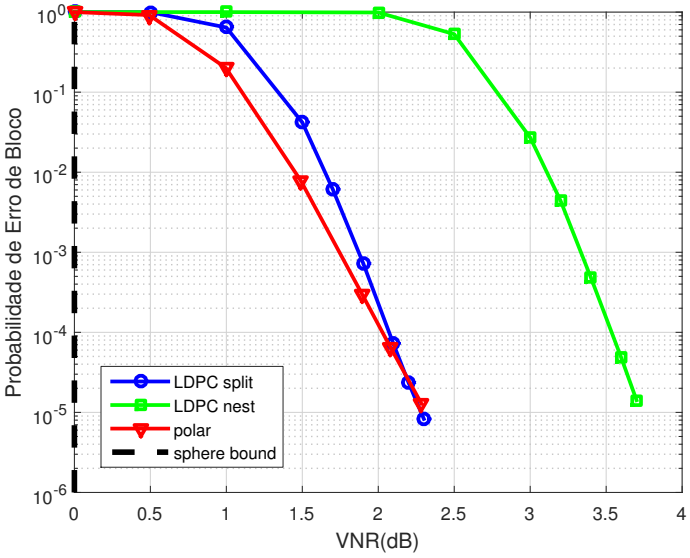

Fig. 1. Probabilidade de erro de bloco em função da VNR dos códigos de reticulado: LDPC via particionamento de equações de paridade (*LDPC split*), LDPC via Construção D′ (*LDPC nest*) e polares (*polar*). O limitante em negro se refere à VNR = 0 dB, isto é, ao limitante da esfera (*sphere bound*).

Referências

[1] R. Zamir, *Lattice Coding for Signals and Networks*, 1st ed., P. Meyler, S. Marsh, and M. Balashova, Eds. Cambridge, UK: Cambridge University Press, 2014.

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

[3] C. Ling and J.-C. Belfiore, "Achieving AWGN channel capacity with lattice gaussian coding," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 5918–5929, Oct. 2014.

[4] Y. Yan, L. Liu, C. Ling, and X. Wu, "Construction of capacity-achieving lattice codes: polar codes," Sep. 2015, online. [Online]. Available: https://arxiv.org/abs/1411.0187v3

[5] T. Richardson and R. Urbanke, *Modern Coding Theory*, P. Meyler, Ed. Cambridge, UK: Cambridge University Press, 2008.

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

[7] M.-R. Sadeghi, A. H. Banihashemi, and D. Panario, "Low-density parity-check lattices: construction and decoding analysis," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4481–4495, Oct. 2006.

[8] I.-J. Baik and S.-Y. Chung, "Irregular low-density parity-check lattices," in *IEEE International Symposium on Information Theory, 2008*, Toronto, Canada, Jul. 2008, pp. 1–5.

[9] A. Vem, Y.-C. Huang, and K. R. Narayanan, "Multilevel lattices based on spatially-coupled LDPC codes with applications," in *IEEE International Symposium on Information Theory*, Honolulu, HI, Jul. 2014, pp. 1–5.

[10] G. D. F. Jr., M. D. Trott, and S. Y. Chung, "Sphere-bound-achieving coset codes and multilevel coset codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 820–850, May 2000.

[11] T. J. Richardson and R. L. Urbanke, "Efficient encoding of Low-Density Parity-Check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 638–656, Feb. 2001.

[12] D. Declerq, M. Fossorier, and E. Biglieri, *Channel Coding: Theory, Algorithms, and Applications*, 1st ed. Oxford, UK: Academic Press, 2014.

[13] U. Wachsmann, R. F. H. Fischer, and J. B. Huber, "Multilevel codes: Theoretical concepts and practical design rules," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1361–1391, July 1999.