Projeto de Códigos de Reticulado LDPC Multinível Irregulares e com Uso de *Shaping*

Paulo Ricardo Branco da Silva, Roberto Augusto Philippi Martins e Danilo Silva

***Resumo*— Códigos de reticulado são ferramentas poderosas tanto para atingir a capacidade do canal AWGN quanto em diversos problemas de teoria da informação multiterminal. Em particular, códigos de reticulado multinível baseados em códigos LDPC binários parecem promissores por apresentar um bom desempenho sob uma decodificação multi-estágio de baixa complexidade. Este artigo apresenta duas contribuições ao projeto de reticulados LDPC: o projeto de distribuições de graus irregulares para decodificação multi-estágio e o uso de *shaping* para reduzir a potência de transmissão. Os ganhos obtidos por estas duas modificações são avaliados via simulações.**

Palavras-Chave*— Códigos de reticulado, códigos LDPC irregulares, códigos multinível, Construção D′, *shaping

***Abstract*— Lattice codes are powerful tools for achieving the capacity of the AWGN channel as well as for many multiterminal information theory problems. In particular, multilevel lattice codes based on binary LDPC codes are attractive due to their good performance under low-complexity multistage decoding. This paper presents two contributions to the design of LDPC lattices: the design of irregular degree distributions for multistage decoding and the use of shaping to reduce the transmission power. The gains obtained by these two modifications are evaluated via simulations.**

***Keywords*— Lattice codes, irregular LDPC codes, multilevel codes, Construction D′, shaping**

I. Introdução

Códigos de reticulado são estruturas matemáticas elegantes e poderosas que não apenas são capazes de alcançar a capacidade do canal AWGN mas também se mostram um ingrediente-chave em muitos problemas recentes da teoria da informação multiterminal (veja, por exemplo, [1] e referências ali citadas). Entretanto, construir códigos de reticulado poderosos que sejam implementáveis com baixa complexidade ainda é um problema desafiador.

Uma direção promissora é a construção de reticulados multinível através das Construções D e D′ [2], as quais se baseiam em uma família de L códigos lineares binários aninhados usados em conjunto com modulação 2^L-PAM. A primeira (segunda) construção descreve um reticulado através das matrizes geradoras (de verificação de paridade) dos códigos componentes aninhados. Uma grande vantagem destas construções é admitir uma decodificação multi-estágio (MSD) [3], [4] de baixa complexidade, em que cada código componente é individualmente decodificado sobre o corpo binário.

Exemplos importantes das Construções D e D′, respectivamente, são os reticulados polares [5]—os quais são mostrados atingir a capacidade do canal AWGN com complexidade $O(Ln\log n)$, onde n é a dimensão do reticulado—e os reticulados LDPC [6]. Até recentemente, havia uma lacuna de desempenho e complexidade entre os reticulados produzidos por ambas as construções. Esta lacuna foi eliminada em [7] com uma generalização da Construção D′ que permite um projeto mais flexível de códigos LDPC aninhados, bem como a introdução de uma codificação sequencial que permite obter complexidade $O(Ln)$ com reticulados LDPC.

Os resultados apresentados em [7], entretanto, consideram apenas o projeto de reticulados LDPC *regulares* para transmissão sobre um canal *sem* restrição de potência. Neste artigo, estendemos os resultados de [7] considerando o projeto de reticulados LDPC *irregulares* e *com* o uso de *shaping* para transmissão em um canal com restrição de potência.

Embora reticulados LDPC irregulares tenham sido propostos previamente em [8], o projeto apresentado em tal artigo baseia-se em uma decodificação conjunta, de complexidade elevada, enquanto o projeto apresentado no presente artigo considera uma decodificação multi-estágio. Com relação ao uso de *shaping*, não temos conhecimento de métodos existentes que se apliquem a reticulados LDPC multinível genéricos. Em particular, o método proposto em [9] requer um reticulado de um único nível com uma estrutura especial (triangular) da matriz geradora, o que não é exigido neste artigo.

Como demonstrado por resultados de simulação, os reticulados irregulares projetados neste artigo possuem um desempenho superior aos regulares. Além disso, o uso de *shaping* permite uma redução considerável de potência de transmissão em comparação ao caso sem *shaping*, resultando em um ganho de SNR. Combinadas, as duas melhorias proporcionam um ganho de aproximadamente $0,7116$ dB com relação ao desempenho do nosso melhor projeto de reticulado LDPC regular sem *shaping*.

II. Preliminares

A. Reticulados

Um reticulado $\Lambda \subseteq \mathbb{R}^n$ é um subgrupo discreto de $\mathbb{R}^n$. Como consequência, pode ser descrito pelo conjunto $\Lambda = \{\mathbf{uG},\ \mathbf{u} \in \mathbb{Z}^n\}$, onde $\mathbf{G} \in \mathbb{R}^{n\times n}$ é uma matriz geradora. Uma região fundamental de Λ é um conjunto $\mathcal{R}_\Lambda \subseteq \mathbb{R}^n$ tal que qualquer $\mathbf{x} \in \mathbb{R}^n$ pode ser *unicamente* expresso como $\mathbf{x} = \boldsymbol{\lambda} + \mathbf{r}$, onde $\boldsymbol{\lambda} \in \Lambda$ e $\mathbf{r} \in \mathcal{R}_\Lambda$. Toda região fundamental tem o mesmo volume, denotado por $V(\Lambda)$. Uma região fundamental $\mathcal{R}_\Lambda$ define um quantizador $Q_\Lambda : \mathbb{R}^n \to \Lambda$ e uma operação modulo-Λ $\mathbb{R}^n \to \mathcal{R}_\Lambda$ dados por $Q_\Lambda(\mathbf{x}) = \boldsymbol{\lambda}$ e $\mathbf{x} \bmod \Lambda = \mathbf{r}$, respectivamente, onde $\mathbf{x} = \boldsymbol{\lambda}+\mathbf{r}$. Em particular,

Paulo Ricardo Branco da Silva, Roberto Augusto Philippi Martins e Danilo Silva, Centro Tecnológico, Universidade Federal de Santa Catarina, Florianópolis-SC, Brasil, E-mails: paulo.branco@posgrad.ufsc.br, roberto.apm@grad.ufsc.br, danilo.silva@ufsc.br.

a região de Voronoi de Λ em torno da origem é definida como $\mathcal{V}_\Lambda \triangleq \{\mathbf{x} \in \mathbb{R}^n : \arg\min_{\boldsymbol{\lambda}\in\Lambda} \|\mathbf{x}-\boldsymbol{\lambda}\| = \mathbf{0}\}$, com empates decididos arbitrariamente mas tais que $\mathcal{V}_\Lambda$ seja uma região fundamental. A probabilidade de erro $P_e(\Lambda,\sigma^2)$ de um reticulado $\Lambda \subseteq \mathbb{R}^n$ é definida 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 $\mathcal{V}_\Lambda$. Um sub-reticulado $\Lambda' \subseteq \Lambda$ é um subconjunto de Λ que também é um reticulado. Se Λ e $\Lambda' \subseteq \Lambda$ são reticulados, então $\mathcal{C} = \Lambda \cap \mathcal{R}_{\Lambda'}$ é dito ser um código de reticulado aninhado. Note que $|\mathcal{C}| = V(\Lambda')/V(\Lambda)$.

B. Modelo de Canal

Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado e seja $\Lambda_s \subseteq \Lambda$ um sub-reticulado com região de Voronoi $\mathcal{V}_{\Lambda_s}$, denominado reticulado de *shaping*. Seja $\mathcal{X} = (\Lambda + \mathbf{d}) \cap \mathcal{V}_{\Lambda_s}$ um código de reticulado deslocado por um vetor de *dither* $\mathbf{d} \in \mathbb{R}^n$. A saída do canal é $\mathbf{y} = \mathbf{x} + \mathbf{z}$, onde $\mathbf{x} \in \mathcal{X}$ é o vetor transmitido e $\mathbf{z} \in \mathbb{R}^n$ é um vetor de ruído gaussiano branco de variância σ^2 por componente. Define-se $P = \frac{1}{n}\mathrm{E}[\|\mathbf{x}\|^2]$ e $\mathrm{SNR} = P/\sigma^2$.

Seja $\mathcal{C} = \Lambda \cap \mathcal{R}_{\Lambda_s}$ um código de reticulado, onde $\mathcal{R}_{\Lambda_s}$ é uma região fundamental de Λ_s que define alguma operação módulo-Λ_s conveniente. É possível expressar $\mathbf{x}$ como

$$\mathbf{x} = \mathbf{c} + \mathbf{d} + \boldsymbol{\lambda}_s \tag{1}$$

onde $\mathbf{c} \in \mathcal{C}$ é uma palavra-código e $\boldsymbol{\lambda}_s \in \Lambda_s$ é um vetor de *shaping* escolhido tal que $\mathbf{x} \in \mathcal{V}_{\Lambda_s}$.

Segundo a abordagem de [1, Cap. 9], o receptor primeiramente calcula o vetor

$$\mathbf{y}_{\text{eff}} = \alpha\mathbf{y} - \mathbf{d} = \boldsymbol{\lambda} + \mathbf{z}_{\text{eff}} \tag{2}$$

onde $\boldsymbol{\lambda} = \mathbf{c} + \boldsymbol{\lambda}_s \in \Lambda$,

$$\mathbf{z}_{\text{eff}} = (\alpha - 1)\mathbf{x} + \alpha\mathbf{z} \tag{3}$$

é o ruído efetivo e $\alpha = \mathrm{SNR}/(1+\mathrm{SNR})$ é um coeficiente de escalonamento MMSE. Em seguida, um decodificador (quantizador) para Λ é aplicado em (2). A probabilidade de erro na recuperação de $\boldsymbol{\lambda}$ tem como limite superior $P_e(\Lambda, \sigma^2_{\text{eff}})$, onde

$$\sigma^2_{\text{eff}} = (\alpha-1)^2 P + \alpha^2\sigma^2 \tag{4}$$

é a variância por componente de $\mathbf{z}_{\text{eff}}$. De posse de $\boldsymbol{\lambda}$, obtém-se finalmente $\mathbf{c} = \boldsymbol{\lambda} \bmod \Lambda_s$.

Conforme mostrado em [10], [1], a aplicação do escalonamento MMSE resulta em um melhor desempenho para SNR finita, permitindo que a capacidade do canal AWGN seja alcançada para qualquer SNR.

1) Decodificação Simplificada: Uma forma prática de implementar a decodificação de $\boldsymbol{\lambda} \in \Lambda$ em (2), seguindo a abordagem em [4], é primeiramente realizar uma redução módulo um sub-reticulado mais simples $\Lambda' \subseteq \Lambda_s$.

Mais precisamente, calcula-se

$$\mathbf{r} = \mathbf{y}_{\text{eff}} \bmod \Lambda' = \mathbf{c}_c + \mathbf{z}_{\text{eff}} \bmod \Lambda' \tag{5}$$

onde $\mathbf{c}_c = \boldsymbol{\lambda} \bmod \Lambda'$. Note que, se $\Lambda' = q\mathbb{Z}^n$, com $\mathcal{R}_{\Lambda'} = [0,q)^n$, então a operação módulo-Λ' pode ser implementada simplesmente pela redução modulo-q (em $\mathbb{R}$) de cada componente. Em seguida, $\mathbf{c}_c \in \mathcal{C}_c$ é decodificado aplicando-se um decodificador para o código de reticulado $\mathcal{C}_c \triangleq \Lambda \cap \mathcal{R}_{\Lambda'}$ no canal (5). Nesse contexto, $\mathcal{C}_c$ é denominado *código de canal*. A probabilidade de erro tem como limite superior $P_e(\mathcal{C}_c, \sigma^2_{\text{eff}})$, onde $P_e(\mathcal{C}_c,\sigma^2)$ denota a probabilidade de erro do código $\mathcal{C}_c$ em um canal módulo-Λ' sujeito a ruído AWGN de variância σ^2. De posse de $\mathbf{c}_c$, obtém-se finalmente $\mathbf{c} = \mathbf{c}_c \bmod \Lambda_s$, o que decorre do fato de que $\Lambda_s \supseteq \Lambda'$.

Concretamente, isto significa que a eliminação do ruído pode ser realizada de forma prática efetivamente ignorando a região de *shaping*, através da decodificação de $\mathcal{C}_c$ [11].

C. 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 $\mathbf{H}_\ell = \begin{bmatrix}\mathbf{h}_1^T & \cdots & \mathbf{h}_{m_\ell}^T\end{bmatrix}^T$ 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′ [2] resulta no reticulado

$$\Lambda = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{H}_j\mathbf{x}^{\mathrm{T}} \equiv \mathbf{0} \pmod{2^{\ell+1}},\ 0 \le \ell < L\}. \tag{6}$$

Observa-se que $\Lambda = \mathcal{C} + 2^L\mathbb{Z}^n$, onde $\mathcal{C} = \Lambda \cap [0,2^L)^n$ 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.

1) Construção D′ Generalizada: A Construção D′ exige que as matrizes $\mathbf{H}_\ell$ sejam aninhadas, i.e., $\mathbf{H}_\ell$ deve ser uma submatriz de $\mathbf{H}_{\ell-1}$. Conforme mostrado em [7], é possível relaxar esta restrição de aninhamento de matrizes preservando as características da Construção D′, desde que os códigos componentes continuem aninhados. Para isto, basta escolher matrizes $\mathbf{H}_\ell \in \mathbb{Z}^{m_\ell \times n}$ que satisfaçam

$$\mathbf{H}_\ell \equiv \mathbf{F}_\ell\mathbf{H}_{\ell-1} \pmod{2^\ell} \tag{7}$$

para algum $\mathbf{F}_\ell \in \mathbb{Z}^{m_\ell \times m_{\ell-1}}$, $\ell = 1,\ldots,L-1$. Nesse caso, o resultado definido por (6) é dito ser obtido pela Construção D′ Generalizada aplicada a $\mathbf{H}_0,\ldots,\mathbf{H}_{L-1}$.

2) Particionamento de Equações de Paridade: Conforme proposto em [7], uma maneira prática de construir matrizes $\mathbf{H}_0,\ldots,\mathbf{H}_{L-1}$ satisfazendo (7) é construir $\mathbf{H}_{\ell-1}$ através da partição das linhas de $\mathbf{H}_\ell$, para $\ell = L-1,\ldots,1$.

Como exemplo, particionamos $\mathbf{H}_2$ em $\mathbf{H}_1$, e $\mathbf{H}_1$ em $\mathbf{H}_0$:

$$\mathbf{H}_2 = \begin{bmatrix}1&1&1&1&1&1&1&1\end{bmatrix}$$
$$\mathbf{H}_1 = \begin{bmatrix}1&0&0&1&0&1&1&0\\0&1&1&0&1&0&0&1\end{bmatrix}$$
$$\mathbf{H}_0 = \begin{bmatrix}0&0&0&1&0&1&0&0\\1&0&0&0&0&0&1&0\\0&1&0&0&0&0&0&1\\0&0&1&0&1&0&0&0\end{bmatrix}.$$

Um propriedade importante desta abordagem é que todas as matrizes produzidas possuem exatamente os mesmos pesos de colunas.

D. Codificação e Decodificação Multi-Estágio

Seja $\mathcal{C} = \Lambda \cap [0, 2^L)^n$ um código de reticulado, onde Λ é um reticulado produzido pela Construção D′ (generalizada). Conforme mostrado em [7], qualquer $\mathbf{c} \in \mathcal{C}$ pode ser expresso como $\mathbf{c} = \sum_{\ell=0}^{L-1} 2^\ell \mathbf{c}_\ell$, onde cada $\mathbf{c}_\ell \in \mathcal{C}_\ell(\mathbf{s}_\ell)$ é um elemento de um código de *coset*

$$\mathcal{C}_\ell(\mathbf{s}_\ell) \triangleq \left\{\mathbf{v} \in \{0,1\}^n : \mathbf{H}_\ell \mathbf{v}^{\mathrm{T}} \equiv \mathbf{s}_\ell \pmod 2\right\} \tag{8}$$

e os vetores $\mathbf{s}_\ell \in \{0,1\}^{m_\ell}$ são dados por $\mathbf{s}_0 = \mathbf{0}$ e

$$\mathbf{s}_\ell = \frac{-\mathbf{H}_\ell \sum_{i=0}^{\ell-1} 2^i \mathbf{c}_i^{\mathrm{T}}}{2^\ell} \bmod 2, \quad \ell = 1, \ldots, L-1. \tag{9}$$

De acordo com [7], o código $\mathfrak{a}lC$ admite também uma decodificação multi-estágio. Sejam $\mathbf{c} \in \mathcal{C}$ e $\mathbf{r} = \mathbf{c} + \mathbf{z} \bmod 2^L$, onde $\mathbf{z}$ é um vetor de ruído branco gaussiano com variância σ^2 por componente. Supondo que os vetores $\mathbf{c}_i$ tenham sido corretamente decodificados para $i = 0, 1, \ldots, \ell-1$, calcula-se

$$\mathbf{r}_\ell = \left(\frac{\mathbf{r} - \sum_{i=0}^{\ell-1} 2^i \mathbf{c}_i}{2^\ell}\right) \bmod 2 \tag{10}$$

$$= \left(\mathbf{c}_\ell + \frac{\mathbf{z}}{2^\ell}\right) \bmod 2 \tag{11}$$

de onde $\mathbf{c}_\ell \in \mathcal{C}_\ell(\mathbf{s}_\ell)$ pode ser recuperado pela decodificação do código de *coset* $\mathcal{C}_\ell(\mathbf{s}_\ell)$ em um canal módulo-2 sujeito a ruído aditivo $\mathbf{z}/2^\ell$. Alternativamente, pode-se calcular $\mathbf{c}_\ell = \bar{\mathbf{c}}_\ell + \mathbf{v}_\ell$, onde $\mathbf{v}_\ell \in \mathcal{C}_\ell(\mathbf{s}_\ell)$ é qualquer vetor do código de *coset* e $\bar{\mathbf{c}}_\ell \in \mathcal{C}_\ell = \mathcal{C}_\ell(\mathbf{0})$. Nesse caso, a decodificação pode ser realizada usando o código linear $\mathcal{C}_\ell$.

Consequentemente, a probabilidade de erro está limitada por

$$P_e(\mathcal{C}, \sigma^2) \le \sum_{\ell=0}^{L-1} P_e(\mathcal{C}_\ell, (\sigma/2^\ell)^2) \tag{12}$$

onde $P_e(\mathcal{C}_\ell, (\sigma/2^\ell)^2)$ denota a probabilidade de erro de $\mathcal{C}_\ell$ no canal (11).

Note que este método pode ser diretamente aplicado no canal (5) fazendo-se $\Lambda' = 2^L\mathbb{Z}^n$ e substituindo-se $\mathcal{C}$, $\mathbf{c}$, $\mathbf{z}$ e σ por $\mathcal{C}_c$, $\mathbf{c}_c$, $\mathbf{z}_{\text{eff}}$ e σ_{eff}, respectivamente.

III. Uso de Shaping

Nesta seção, apresentamos uma forma prática de aplicar *shaping* no sinal transmitido, adaptando a abordagem em [11].

Considere as definições da seção II-B. Embora o código de canal $\mathcal{C}_c = \Lambda \cap \mathcal{R}_{\Lambda'}$ possa, em princípio, ser projetado ignorando o reticulado de *shaping* Λ_s, o projeto de Λ_s depende da escolha de Λ, uma vez que $\Lambda_s \subseteq \Lambda$. Uma forma prática de desacoplar o problema, no caso em que Λ é um reticulado multinível, é deixando o último nível sem codificação e aplicando *shaping* apenas neste último nível [11].

Mais precisamente, suponha que Λ seja um reticulado de L níveis produzido pela Construção D′ (generalizada) e que $\Lambda' = 2^L\mathbb{Z}^n$, com $\mathcal{R}_{\Lambda'} = [0, 2^L)^n$, de forma que $\mathcal{C}_c = \Lambda \cap [0, 2^L)^n$. Suponha que o último nível, $L-1$, seja não-codificado, i.e., $\mathcal{C}_{c,L-1} = \{0,1\}^n$. Além disso, suponha que Λ_s satisfaz $2^L\mathbb{Z}^n \subseteq \Lambda_s \subseteq 2^{L-1}\mathbb{Z}^n$, i.e., $\Lambda_s = 2^{L-1}\mathcal{C}_s + 2^L\mathbb{Z}^n$, onde $\mathcal{C}_s \subseteq \{0,1\}^n$ é um código linear, denominado código de *shaping*, e que $\mathcal{R}_{\Lambda_s} \subseteq \mathcal{R}_{\Lambda'}$, de forma que $\mathcal{C} = \Lambda \cap \mathcal{R}_{\Lambda_s} \subseteq \mathcal{C}_c$. Suponha também que $\mathbf{d} = (d, \ldots, d)$, onde $d = -(2^L - 1)/2$.

Desta forma, dado $\mathbf{c} = \sum_{\ell=0}^{L-1} 2^\ell \mathbf{c}_\ell \in \mathcal{C}$, a operação de *shaping* definida em (1) pode ser realizada calculando-se

$$\mathbf{x} = \mathbf{c}_c + \mathbf{d} \tag{13}$$

onde $\mathbf{c}_c = \sum_{\ell=0}^{L-1} 2^\ell \mathbf{c}_{c,\ell}$,

$$\mathbf{c}_{c,\ell} = \mathbf{c}_\ell, \quad \ell = 0, \ldots, L-1$$
$$\mathbf{c}_{c,L-1} = \mathbf{c}_{L-1} + \mathbf{c}_s \bmod 2$$

e $\mathbf{c}_s \in \mathcal{C}_s$ é escolhido de forma a minimizar $\|\mathbf{x}\|^2$.

Note que, como $\|\mathbf{x}\|^2 = \sum_{j=1}^n x_j^2$, onde

$$x_j = d + \sum_{\ell=0}^{L-2} 2^\ell c_{\ell,j} + 2^{L-1}(c_{L-1,j} + c_{s,j} \bmod 2) \tag{14}$$

só depende de $c_{s,j}$ (e não de $c_{s,j'}$, $j' > j$), o cálculo de $\mathbf{c}_s$ pode ser resolvido de forma eficiente pelo algoritmo de Viterbi aplicado à treliça que representa $\mathcal{C}_s$, usando $x_j^2|_{c_{s,j}}$ como métrica associada ao j-ésimo símbolo (a qual pode ser interpretada como a distância euclidiana entre o símbolo transmitido x_j e o "símbolo recebido" $0 \in \mathbb{R}$).

Concretamente, $\mathcal{C}_s$ é especificado por uma matriz de verificação de paridade $\mathbf{H}_s \in \{0,1\}^{m_s \times n}$, enquanto $\mathcal{C}$ é especificado pela escolha de uma matriz $(\mathbf{H}_s^T)^\dagger \in \{0,1\}^{m_s \times n}$ inversa à esquerda de $\mathbf{H}_s^T$, i.e., tal que $(\mathbf{H}_s^T)^\dagger \mathbf{H}_s^T = \mathbf{I}$. Mais precisamente, para $\mathbf{c}_c \in \mathcal{C}_c$, a operação

$$\mathbf{c} = \mathbf{c}_c \bmod \Lambda_s \tag{15}$$

é definida por

$$\mathbf{c}_\ell = \mathbf{c}_{c,\ell}, \quad \ell = 0, \ldots, L-1$$
$$\mathbf{c}_{L-1} = \mathbf{c}_{c,L-1} \mathbf{H}_s^T (\mathbf{H}_s^T)^\dagger \bmod 2$$

o que por sua vez define $\mathcal{C} = \mathcal{C}_c \bmod \Lambda_s$.[1] Em particular, $R = \frac{1}{n}\log_2|\mathcal{C}| = R_c - R_s$, onde $R_c = \frac{1}{n}\log_2|\mathcal{C}_c|$ e $R_s = \frac{1}{n}\log_2|\mathcal{C}_s| = 1 - \frac{m_s}{n}$.

IV. Projeto de Códigos LDPC Irregulares Aninhados via EXIT Charts

Nesta seção discutimos a otimização das distribuições de graus para códigos lineares aninhados construídos através do particionamento de equações de paridade.

A. Projeto para um Único Código

Um código LDPC pode ser caracterizado pelas distribuições de graus $\lambda(x) = \sum_{i=2}^{d_v} \lambda_i x^{i-1}$ para nós de variável e $\rho(x) = \sum_{i=2}^{d_c} \rho_i x^{i-1}$ para nós de paridade, onde λ_i (ρ_i) representa a fração de arestas conectadas a nós de variável (paridade) com peso i. A taxa de projeto de um código LDPC com distribuições $\lambda(x)$ e $\rho(x)$ é dada por

$$R = 1 - \frac{\sum_i \rho_i / i}{\sum_i \lambda_i / i}. \tag{16}$$

Considere a decodificação via *belief propagation* em um canal simétrico com entrada binária. O desempenho de

[1] Na prática, se $\mathbf{c}_{L-1} = \mathbf{u}_{L-1}(\mathbf{H}_s^T)^\dagger \bmod 2$, onde $\mathbf{u}_{L-1} \in \{0,1\}^{m_s}$ é o vetor de dados do último nível, então $\mathbf{c}_{L-1}$ não precisa ser regenerado pelo receptor, que pode recuperar diretamente $\mathbf{u}_{L-1} = \mathbf{c}_{c,L-1}\mathbf{H}_s^T \bmod 2$.

um *ensemble* (família) de códigos LDPC com as mesmas distribuições de graus pode ser analisado através de curvas conhecidas como *EXIT (extrinsic information transfer) charts*. A partir destas funções é possível determinar condições para o bom desempenho de um *ensemble*, o que por sua vez nos permite projetar as distribuições $\lambda(x)$ e $\rho(x)$.

Para $I, I_C \in [0,1]$, sejam as funções

$$v(I, I_C) \triangleq \sum_i \lambda_i v_i(I, I_C) \tag{17}$$

$$v_d(I, I_C) \triangleq J\left(\sqrt{(d-1)[J^{-1}(I)]^2 + [J^{-1}(I_C)]^2}\right) \tag{18}$$

$$c(I) \triangleq 1 - \sum_i \rho_i J\left(\sqrt{(i-1)[J^{-1}(1-I)]^2}\right) \tag{19}$$

onde

$$J(\sigma) = 1 - \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} e^{-(\ell-\sigma^2/2)^2/(2\sigma^2)} \log_2\left(1+e^{-\ell}\right) d\ell.$$

Conforme mostrado em [12], assumindo uma aproximação gaussiana, $v(I, I_C)$ ($c(I)$) corresponde à informação mútua extrínseca média da mensagem de saída de um nó de variável (paridade) quando a mensagem de entrada possui informação mútua extrínseca média I, onde I_C é a capacidade do canal. A condição para o sucesso da decodificação é que, a cada iteração do algoritmo, a informação mútua cresça, isto é, $v(c(I), I_C) \geq I$.

Assumindo esta condição de progresso (e incluindo também a condição técnica de estabilidade $\lambda_2 < 1/\rho'(1)$ [12], onde $\rho'(x)$ denota a derivada de $\rho(x)$), desejamos maximizar a taxa de projeto do código para um dado $\rho(x)$, o que nos leva ao seguinte problema de otimização linear:

$$\begin{aligned} \max_{\lambda(x)} \quad & \sum_i \lambda_i/i \\ \text{s.t.} \quad & \lambda_i \geq 0, \quad \sum_i \lambda_i = 1, \quad \lambda_2 < 1/\rho'(1) \\ & \sum_i \lambda_i v_i(c(I), I_C) \geq I, \ \forall I \in [0,1]. \end{aligned}$$

B. Projeto de Códigos Aninhados

Por definição, no particionamento de equações de paridade, a matriz $\mathbf{H}_\ell$ do código $\mathcal{C}_\ell$ conserva a distribuição de graus de variável da matriz $\mathbf{H}_{\ell+1}$ do código $\mathcal{C}_{\ell+1}$, de taxa maior, para $\ell = 0, 1, \ldots, L-2$, isto é, $\lambda_0(x) = \cdots = \lambda_{L-1}(x) = \lambda(x)$. Isto significa que a taxa de $\mathcal{C}$ é dada por

$$R = \sum_{\ell=0}^{L-1} R_\ell = L - \frac{\sum_{\ell=0}^{L-1}\sum_i \rho_{\ell,i}/i}{\sum_i \lambda_i/i}. \tag{20}$$

Assumindo $\rho_0(x), \ldots, \rho_{L-1}(x)$ fixos, observamos que a função objetivo da otimização, $\sum_i \lambda_i/i$, continua a mesma que no caso de um único código. No entanto, as restrições precisam ser alteradas para que se exija um bom desempenho de todos os códigos simultaneamente.

Mais precisamente, o problema de otimização linear se torna

$$\begin{aligned} \max_{\lambda(x)} \quad & \sum_i \lambda_i/i \\ \text{s.t.} \quad & \lambda_i \geq 0, \quad \sum_i \lambda_i = 1, \quad \lambda_2 < 1/\max_\ell\{\rho'_\ell(1)\} \\ & \sum_i \lambda_i v_i(c^{(\ell)}(I), I_C^{(\ell)}) \geq I, \ \forall I \in [0,1], \forall \ell \end{aligned}$$

onde $c^{(\ell)}(I)$ denota a função em (19) para a distribuição $\rho_\ell(x)$ e $I_C^{(\ell)}$ denota a capacidade do canal (11).

Note que $I_C^{(\ell)}$ pode ser calculada numericamente a partir da densidade condicional do canal (11), dada por

$$p(r_\ell|c_\ell) = \sum_{k\in\mathbb{Z}} \frac{1}{\sqrt{2\pi}\sigma_\ell} \exp\left(-\frac{(r_\ell - c_\ell - k)^2}{2\sigma_\ell^2}\right) \tag{21}$$

onde $c_\ell \in \{0,1\}$, $r_\ell \in [0,2)$ e $\sigma_\ell = \sigma/2^\ell$, $\ell = 0, \ldots, L-1$.

V. RESULTADOS

Esta seção discute o projeto de códigos de reticulado LDPC multinível irregulares e com uso de *shaping*. Para fins de comparação, projetamos também códigos multinível convencionais (MLC). Embora o desempenho de códigos MLC seja tipicamente superior ao de códigos de reticulado, códigos MLC não possuem a estrutura algébrica necessária para serem empregados em algumas aplicações multiterminais [1]. Idealmente, desejamos construir códigos de reticulado com desempenho próximo ao de códigos MLC convencionais.

Utilizamos $\Lambda' = 4\mathbb{Z}^n$ e $\mathcal{C}_c$ construído por meio de $\mathcal{C}_0, \mathcal{C}_1 \subseteq \{0,1\}^n$. Como código de *shaping* $\mathcal{C}_s$ utilizamos o código convolucional de taxa $R_s = 0,5$ apresentado em [11], o qual foi escolhido pela disponibilidade das matrizes $\mathbf{H}_s^T$ e $(\mathbf{H}_s^T)^\dagger$.

Para $\mathcal{C}_c$ utilizam-se 1) códigos de reticulado construídos via Construção D′ Generalizada, em particular via o particionamento de equações de paridade, e 2) códigos MLC com códigos componentes construídos independentemente através do algoritmo PEG [13]. Em 1) é utilizada a decodificação de reticulado (Reticulado) discutida na subseção II-D; em 2) é utilizada a decodificação multi-estágio padrão - MSD (MLC).

A eficiência espectral $R = R_0 + R_1 + R_2$, onde $R_2 = 1 - R_s$ é a taxa do nível de *shaping*, é projetada para probabilidade de erro $P_e = 10^{-3}$ e tamanho de bloco $n = 2048$ por meio da regra do expoente de erro [3, Subseção IV.C]. Para $R_s = 0,5$, encontramos aproximadamente $R = 1,6$ bits/dimensão.

O projeto individual das taxas R_0 e R_1 é baseado na regra da igualdade de probabilidades de erro [3, Subseção IV.E]. Mais precisamente, deseja-se escolher taxas R_0 e R_1 para as quais $P_e(\mathcal{C}, \sigma_{\text{eff}}) \leq \sum_{\ell=0}^{2} P_e(\mathcal{C}_\ell, (\sigma_{\text{eff}}/2^\ell)^2) \leq 10^{-3}$ e $P_e(\mathcal{C}_0, \sigma_{\text{eff}}) \approx P_e(\mathcal{C}_1, \sigma_{\text{eff}}/2)$. Inicialmente, são fixados valores de R_0 e R_1 tal que $R = R_0 + R_1 + R_2$, e é feita uma varredura sobre $\rho_0(x)$, $\rho_1(x)$ e σ a fim de encontrar $\lambda(x)$ que resulte nas taxas R_0 e R_1 estipuladas. De posse de $\lambda(x)$, são construídos os códigos $\mathcal{C}_0$ e $\mathcal{C}_1$, os quais são testados via simulação. O processo é repetido até que as probabilidades de erro desejadas sejam obtidas.

Casos de simulação com e sem *shaping* (c/ sh. e s/ sh.) e com $\mathcal{C}_0$ e $\mathcal{C}_1$ regulares (reg.) e irregulares (irreg.) são

TABELA I

TAXAS DOS CÓDIGOS COMPONENTES ($R_0/R_1/R_2$).

	MLC	Reticulado
Reg.	0,2075 / 0,9063 / 0,5 (c/ sh.) 0,6387 / 0,9790 / — (s/ sh.)	0,2036 / 0,9102 / 0,5 (c/ sh.) 0,6304 / 0,9878 / — (s/ sh.)
Irreg.	0,2334 / 0,8804 / 0,5 (c/ sh.) —	0,2036 / 0,9102 / 0,5 (c/ sh.) 0,6387 / 0,9795 / — (s/ sh.)

utilizados. Para os códigos regulares, selecionamos $d_v = 3$. Para o caso irregular sem *shaping* com decodificação de reticulado, a distribuição de graus de variável é $\lambda(x) = 0,0111x^3 + 0,5372x^4 + 0,0080x^{12} + 0,1969x^{13} + 0,2467x^{21}$, enquanto para o caso com *shaping*, $\lambda(x) = 0,0172x^3 + 0,9024x^4 + 0,0717x^{19} + 0,0087x^{20}$. A distribuição de graus $\rho(x)$ não é informada, pois varia segundo a construção da matriz $\mathbf{H}$ realizada pelo algoritmo PEG [13], o qual depende exclusivamente de $\lambda(x)$. Na tabela I apresentamos as taxas de todos os casos de simulação avaliados.

Na Figura 1, é apresentada a curva de probabilidade de erro de bloco P_e em função de E_b/N_0 para códigos regulares, onde $\sigma^2 = N_0/2$ e $E_b/N_0 = \text{SNR}/2R$. O uso de *shaping* resulta em ganho de desempenho ($0,6585$ dB entre as curvas com decodificação de reticulado). A Figura 1 demonstra a relação entre o *shaping* e a decodificação. Sem *shaping*, a decodificação de reticulado degrada o desempenho. Como esta decodificação supõe ruído equivalente gaussiano e como o uso de *shaping* aproxima a distribuição de probabilidade do ruído efetivo à gaussiana, a diferença de desempenho entre as decodificações MSD e de reticulado é praticamente eliminada.

Na Figura 2, nota-se a diferença de desempenho em função do uso de códigos irregulares. Para o caso sem *shaping*, ocorre um ganho de $0,1667$ dB e para os códigos com *shaping* e decodificação de reticulado o ganho é de $0,0531$ dB. Os pequenos valores se devem à restrição $\lambda_0(x) = \lambda_1(x) = \lambda(x)$ para códigos aninhados $\mathcal{C}_0$ e $\mathcal{C}_1$, os quais teriam distribuições $\lambda_0(x)$ e $\lambda_1(x)$ ótimas diferentes se projetados independentemente. A fim de aumentar os ganhos na utilização de códigos irregulares, estamos pesquisando métodos distintos ao particionamento de equações de paridade, os quais permitiriam $\lambda_0(x) \neq \lambda_1(x)$.

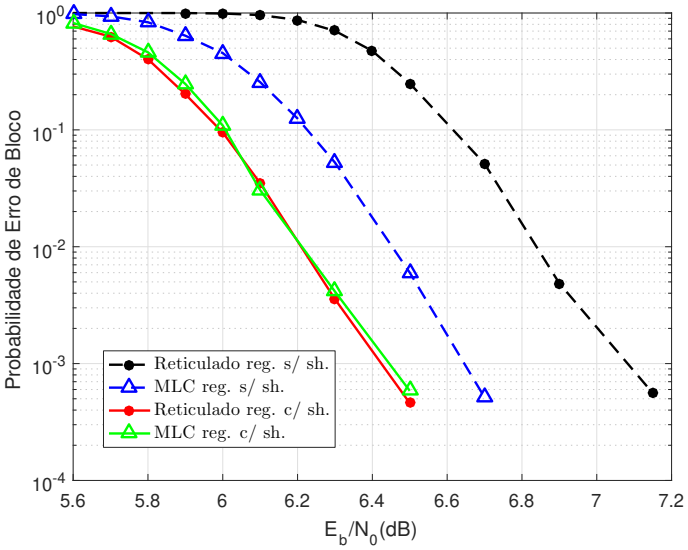

Fig. 1. Probabilidade de erro de bloco em função de E_b/N_0 para códigos regulares. Verifica-se o ganho produzido pelo uso de *shaping*.

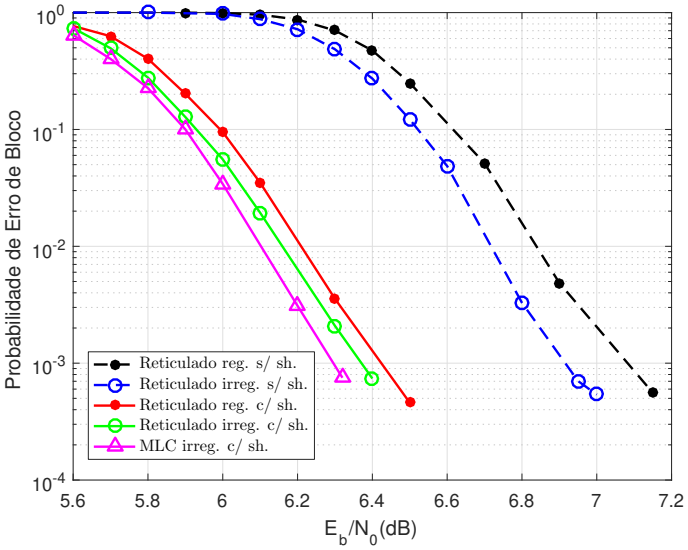

Fig. 2. Probabilidade de erro de bloco em função de E_b/N_0. Observa-se o pequeno ganho resultante do uso de códigos irregulares.

REFERÊNCIAS

[1] R. Zamir, *Lattice Coding for Signals and Networks*. Cambridge, UK: Cambridge University Press, 2014.

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

[3] 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, Jul. 1999.

[4] G. D. Forney, 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.

[5] Y. Yan, L. Liu, C. Ling, and X. Wu, "Construction of capacity-achieving lattice codes: Polar lattices," Nov. 2014. Available: http://arxiv.org/abs/1411.0187

[6] M.-R. Sadeghi, A. 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.

[7] P. R. B. da Silva and D. Silva, "Low-Complexity Multilevel LDPC Lattices and a Generalization of Construction D'," in *2018 IEEE International Symposium on Information Theory*, Jun. 2018, pp. 1–5.

[8] I.-J. Baik and S.-Y. Chung, "Irregular low-density parity-check lattices," in *2008 IEEE International Symposium on Information Theory*, Jul. 2008, pp. 2479–2483.

[9] H. Khodaiemehr, D. Kiani, and M. R. Sadeghi, "LDPC Lattice Codes for Full-Duplex Relay Channels," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 536–548, Feb. 2017.

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

[11] G. D. Forney, "Trellis shaping," *IEEE Transactions on Information Theory*, vol. 38, no. 2, pp. 281–300, Mar. 1992.

[12] T. J. Richardson and R. L. Urbanke, *Modern Coding Theory*. Cambridge University Press, 2008.

[13] X.-Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.