

CONSTRUÇÃO DE EMPACOTAMENTOS ESFÉRICOS VIA CÓDIGOS DE CLASSES LATERAIS GENERALIZADOS

Antonio de Andrade e Silva¹ e Reginaldo Palazzo Jr.^{2,3}

¹Departamento de Matemática, CCEN – UFPb, 58.059-900, J. Pessoa, Pb.

²Departamento de Telemática, FEEC – UNICAMP, CP 6101, 13081-970, Campinas, SP, Brasil.
palazzo@dt.fee.unicamp.br.

Resumo - Neste trabalho propomos uma construção de empacotamentos esféricos tendo como base códigos de bloco sobre o grupo \mathbb{Z}_q . Esta construção é uma generalização da construção proposta por Costa e Silva e Palazzo [4]. Tabela e exemplos são incluídos com os melhores empacotamentos esféricos obtidos através desta construção. Nas dimensões 68 e 72, um novo recorde de densidades foi alcançado.

Abstract - We propose a construction scheme for sphere packing arrangements based on block codes over the \mathbb{Z}_q group. This scheme is a generalization of the one proposed by Costa e Silva and Palazzo [4]. A table and examples are included with results from the best sphere packings obtained with this construction. In dimensions 68 and 72 a new density record is achieved.

Palavras-chave: Empacotamento de esferas, códigos de bloco, códigos sobre grupos, códigos de classes laterais.

1. INTRODUÇÃO

A primeira proposta de construção de um reticulado Λ em \mathbb{R}^N utilizando um código linear foi apresentada por Leech e Sloane [10]. Desde então, novos métodos de construção de reticulados utilizando códigos lineares foram apresentados, [1], [4], [7], [8], [9], e [12]. Para maiores detalhes sobre empacotamentos esféricos e reticulados sugerimos ao leitor a referência [2].

Os métodos propostos invariavelmente utilizam do seguinte procedimento. Seja $C = [N, k, d]_p$ um código linear sobre $\mathbb{Z}_p \cong GF(p)$, onde p é um número primo. Se identificarmos \mathbb{Z}_p com o subconjunto $\mathbb{N}_p = \{0, 1, \dots, p-1\} \subset \mathbb{Z}$, então

$$\Lambda = \bigcup_{c \in C} (l(c) + p\mathbb{Z}^N),$$

é um reticulado em \mathbb{R}^N consistindo da união de p^k classes laterais à esquerda de $p\mathbb{Z}^N$, onde $\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$ é um grupo de rótulos, $l: \mathbb{Z}_p^N \rightarrow [\mathbb{Z}/p\mathbb{Z}]^N$ e $c \in C$.

Os principais métodos de construção de novos empacotamentos esféricos, usando reticulados conhecidos, consistem da união de um número finito de elementos de uma partição. Mais precisamente, sejam Γ e Λ reticulados em \mathbb{R}^N tal que Λ é um subreticulado de Γ . Então Λ induz uma partição Γ/Λ

de Γ em $[\Gamma : \Lambda]$ classes laterais de Λ . Seja $[\Gamma/\Lambda]$ um sistema de representantes de classes laterais de Λ em Γ . Dado $H \subset [\Gamma/\Lambda]$, $\mathbf{L}_N = H + \Lambda$ é um empacotamento esférico em \mathbb{R}^N e é um reticulado se, e somente se, H é um subgrupo de $[\Gamma/\Lambda]$ com a operação de adição módulo Λ . De um modo geral, $\mathbf{L}_{Nn} = H + \Lambda^n$ é um empacotamento esférico em \mathbb{R}^{Nn} e é um reticulado se, e somente se, H é um subgrupo de $[\Gamma^n/\Lambda^n]$ com a operação de adição módulo Λ^n , onde Γ^n/Λ^n é isomorfo a $(\Gamma/\Lambda)^n$.

Por exemplo, sejam $\Gamma = \mathbb{Z}$ e $\Lambda = 2\mathbb{Z}$ reticulados em \mathbb{R} tal que Λ é um subreticulado de Γ e $[\Gamma/\Lambda] = \{0, 1\}$ um sistema de representantes de classes laterais de Λ em Γ . Então $\mathbf{L}_4 = H + \Lambda^4$ é um reticulado em \mathbb{R}^4 que tem Λ^4 como um subreticulado e por sua vez é um subreticulado de Γ^4 , onde o subgrupo selecionado é dado por $H = \{(0, 0, 0, 0), (1, 1, 0, 0)\} \subset [\Gamma/\Lambda]^4$. Sob esta construção, \mathbf{L}_4 apresenta um ganho de codificação fundamental de 1.51 [dB], portanto mais denso do que Γ ou Γ^4 (veja parte 1 do Exemplo 1).

Chamamos a atenção para o fato de que a construção de empacotamentos esféricos da forma \mathbf{L}_{Nn} que sejam mais densos do que Γ para a utilização em esquemas de quantização e/ou codificação de canais com ruído gaussiano branco aditivo com faixa limitada, torna-se impraticável quando a ordem da partição Γ/Λ for muito grande. Infelizmente, não se conhece nenhum método sistemático de selecionar o subgrupo H de $[\Gamma/\Lambda]^n$ de modo que o empacotamento esférico $\mathbf{L}_{Nn} = H + \Lambda^n$ seja mais denso do que Γ^n .

Seja r a ordem da partição Γ/Λ e $r = \prod_{i=0}^{m-1} q_i$, onde $q_i = p_i^{n_i}$, com p_i números primos distintos, $0 \leq i \leq m-1$ e $n_0 + \dots + n_{m-1} \leq N$. Como Γ/Λ é um grupo comutativo finito, existe um refinamento da partição Γ/Λ em uma cadeia de partições de m -níveis e q_i -maneiras, [5],

$$\Lambda_0/\Lambda_1/\dots/\Lambda_{m-1}/\Lambda_m,$$

onde

$$\Lambda_0 = \Gamma, \Lambda_m = \Lambda, \Lambda_i = [\Lambda_i/\Lambda_{i+1}] + \Lambda_{i+1}$$

e

$$|\Lambda_i/\Lambda_{i+1}| = q_i, 0 \leq i \leq m-1.$$

³Este trabalho foi financiado em parte pela Fundação de Amparo à Pesquisa do Estado de São Paulo, FAPESP, No. 95/4720-8, e em parte pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico, CNPq, No. 301416/85-0.

Assim, um método alternativo de construção de empacotamentos esféricos da forma $L_{Nn} = H + \Lambda_m^n$ é considerar o subconjunto H de $[\Lambda_0/\Lambda_m]^n$ definido por $H = \sum_{i=0}^{m-1} H_i$, onde H_i são subconjuntos de $[\Lambda_i/\Lambda_{i+1}]^n$, $0 \leq i \leq m-1$. É claro que L_{Nn} é um reticulados se, e somente se, cada H_i é um subgrupo de $[\Lambda_i/\Lambda_{i+1}]^n$, $0 \leq i \leq m-1$. Uma vez que Λ_i/Λ_{i+1} é isomorfo ao grupo de rótulos \mathbb{Z}_{q_i} , $0 \leq i \leq m-1$, os conjuntos H_i podem ser identificados com códigos C_i sobre \mathbb{Z}_{q_i} . Assim, cada palavra-código $\mathbf{c}_i \in C_i$ será identificada com um elemento $h_i \in H_i$ e $\sum_{i=0}^{m-1} h_i$ é o representante de alguma classe lateral de Λ_m^n em Λ_0^n . Portanto, L_{Nn} é a união de todas as classes laterais de Λ_m^n .

Este trabalho é constituído da seguinte forma. Na Seção 2, apresentamos uma construção multicamada, que estende a proposta de [4], com o objetivo de obter empacotamentos esféricos com o maior ganho de codificação fundamental possível em \mathbb{R}^{Nn} . Na Seção 3, com o propósito de completudeza, um algoritmo de decodificação com distância limitada é exibido para a decodificação dos reticulados obtidos através desta construção. Na Seção 4, como resultado da construção sendo proposta, apresentamos empacotamentos esféricos conhecidos e novos, onde nas dimensões 68 e 72 um novo recorde de densidades foi alcançado.

2. CONSTRUÇÃO DE EMPACOTAMENTOS ESFÉRICOS

Os resultados desta seção estendem a proposta de [4], para qualquer número r , onde $r = \prod_{i=0}^{m-1} q_i$ é a decomposição de r em fatores primos distintos. Com o propósito de completudeza, apresentamos as provas de todos os resultados que foram estendidos. Para maiores detalhes, [3].

Sejam Γ e Λ reticulados em \mathbb{R}^N tal que Λ é um subreticulado de Γ . Então Λ induz uma partição Γ/Λ de ordem r e $r\Gamma \subseteq \Lambda$. Se

$$[\Gamma/\Lambda] = \left\{ \sum_{i=0}^{m-1} a_i \mathbf{g}_i : a_i \in \mathbb{N}_{q_i} \right\},$$

onde $\mathbf{g}_i \in \Gamma$, $\mathbf{g}_i \notin \Lambda$ e $\mathbb{N}_{q_i} = \{0, \dots, q_i - 1\}$, é um sistema de representantes de classes laterais fixo de Λ em Γ . Então uma cadeia de partições

$$\Lambda_0/\Lambda_1/\dots/\Lambda_{m-1}/\Lambda_m,$$

com m -níveis e q_i -maneiras, pode ser definida como um refinamento de Γ/Λ , fazendo

$$\Lambda_0 = \Gamma, \Lambda_m = \Lambda \text{ e } \Lambda_i = [\Lambda_i/\Lambda_{i+1}] + \Lambda_{i+1},$$

onde

$$[\Lambda_i/\Lambda_{i+1}] = \{a_i \mathbf{g}_i : a_i \in \mathbb{N}_{q_i}, \mathbf{g}_i \in \Lambda_i, \mathbf{g}_i \notin \Lambda_{i+1}\}$$

e

$$|\Lambda_i/\Lambda_{i+1}| = q_i, 0 \leq i \leq m-1,$$

com $\mathbb{Z}_{q_i} \simeq \Lambda_i/\Lambda_{i+1}$, $0 \leq i \leq m-1$ um grupo de rótulos.

Definição 1 Sejam $\Lambda_0/\Lambda_1/\dots/\Lambda_{m-1}/\Lambda_m$ uma cadeia de partições de reticulados em \mathbb{R}^N , com m -níveis e q_i -maneiras, e C_0, \dots, C_{m-1} códigos de bloco sobre \mathbb{Z}_{q_i} cada um de comprimento n . Fixado $\alpha_i \in [\Lambda_i/\Lambda_{i+1}] - \{0\}$, $0 \leq i \leq m-1$, define-se um empacotamento esférico L_{Nn} em \mathbb{R}^{Nn} como o conjunto

$$L_{Nn} \triangleq \left\{ \sum_{i=0}^{m-1} (\mathbf{c}_i \otimes \alpha_i) : \mathbf{c}_i \in C_i, 0 \leq i \leq m-1 \right\} + \Lambda_m^n$$

$$= \bigcup_{\mathbf{c}_i \in C_i} \left(\sum_{i=0}^{m-1} (\mathbf{c}_i \otimes \alpha_i) + \Lambda_m^n \right),$$

onde para cada $\mathbf{c}_i = (c_{i1}, \dots, c_{in}) \in C_i$, $\mathbf{c}_i \otimes \alpha_i \triangleq (c_{i1}\alpha_i, \dots, c_{in}\alpha_i)$, com as palavras-código \mathbf{c}_i vistas como um vetor real de componentes $c_{ij} \in \mathbb{N}_{q_i}$: $0 \leq i \leq m-1$; $1 \leq j \leq n$ e a união sendo sobre todos os códigos C_0, \dots, C_{m-1} .

Chamamos a atenção de que o empacotamento esférico L_{Nn} é periódico, no sentido de que ele é invariante sob deslocamento de múltiplos inteiros dos vetores básicos de Λ_m^n . O arranjo periódico L_{Nn} é chamado de código de classe lateral generalizado [6], e denotado por

$$L_{Nn} = \sum_{i=0}^{m-1} (C_i \otimes [\Lambda_i/\Lambda_{i+1}]) + \Lambda_m^n.$$

Dados $\mathbf{l} \in L_{Nn}$, $\mathbf{l} = \sum_{i=0}^{m-1} (\mathbf{c}_i \otimes \alpha_i) + \lambda_m$, com $\mathbf{c}_i \in C_i$, $\lambda_m \in \Lambda_m^n$ e $\alpha_i \in [\Lambda_i/\Lambda_{i+1}] - \{0\}$. Então,

$$\mathbf{l} = \sum_{i=0}^{m-1} (c_{i1}\alpha_i, \dots, c_{in}\alpha_i) + (\lambda_{m1}, \dots, \lambda_{mn})$$

$$= \left(\sum_{i=0}^{m-1} (c_{i1}\alpha_i), \dots, \sum_{i=0}^{m-1} (c_{in}\alpha_i) \right) + (\mathbf{v}_1 D, \dots, \mathbf{v}_n D)$$

Portanto, $\mathbf{l} = (\mathbf{u}_1 B, \dots, \mathbf{u}_n B) + VD$, onde $\mathbf{u}_k = (c_{0k}, \dots, c_{(m-1)k})$, $1 \leq k \leq n$, é a m -upla formada da k -ésima componente de cada palavra-código $\mathbf{c}_i \in C_i$, $0 \leq i \leq m-1$, isto é, \mathbf{u}_k é um rótulo de alguma classe lateral à esquerda de Λ_m em Λ_0 , B é uma matriz $m \times N$ cujas linhas são os vetores $\alpha_0, \dots, \alpha_{m-1}$, isto é, $B = \{\mathbf{g}_i : 0 \leq i \leq m-1\}$, pois $\alpha_i = a \mathbf{g}_i$, $a \in \mathbb{N}_{q_i} - \{0\}$, $V = \{\mathbf{v}_k : 1 \leq k \leq n\}$ é uma matriz $m \times N$ cujas linhas são os vetores $\mathbf{v}_k \in \mathbb{Z}^N$, $1 \leq k \leq n$, e $D = M_m^t$, onde M_m é uma matriz geradora para o reticulado Λ_m . Assim,

$$\mathbf{l} = UB + VD,$$

onde $U = \{\mathbf{u}_k : 1 \leq k \leq n\}$ é uma matriz $n \times m$ cujas linhas são os vetores $\mathbf{u}_k \in \mathbb{N}_{q_i}^m$. Isto significa que a i -ésima linha do produto UB é uma combinação linear das linhas de B com escalares da i -ésima linha de U . Por essa razão, vamos considerar

$$L_{Nn} = \left\{ \sum_{i=0}^{m-1} (\mathbf{c}_i \otimes \mathbf{g}_i) : \mathbf{c}_i \in C_i, 0 \leq i \leq m-1 \right\} + \Lambda_m^n.$$

Isto exhibe explicitamente \mathbf{L}_{Nn} como a união de $\prod_{i=0}^{m-1} |C_i|$ classes laterais de Λ_m^n , onde $|C_i|$ é a cardinalidade do código C_i . Em particular, se $q_i = q$ e os códigos C_i , $0 \leq i \leq m-1$, são lineares, isto é, subgrupos de \mathbb{Z}_q^n , então o empacotamento esférico \mathbf{L}_{Nn} é um reticulado em \mathbb{R}^{Nn} (Teorema 2). Neste caso,

$$\mathbf{c}_i + \mathbf{c}_j = \mathbf{c}_i \oplus \mathbf{c}_j + q(\mathbf{c}_i \circ \mathbf{c}_j),$$

onde "+" é a soma ordinária em \mathbb{R}^N , " \oplus " é soma em \mathbb{Z}_q e " \circ " é definida por

$$\mathbf{c}_i \circ \mathbf{c}_j \triangleq \left(\lfloor \frac{1}{q}(c_{i1} + c_{j1}) \rfloor, \dots, \lfloor \frac{1}{q}(c_{in} + c_{jn}) \rfloor \right),$$

sendo $\lfloor x \rfloor$ o maior inteiro menor ou igual a x . No caso em que $q = 2$, temos

$$\lfloor \frac{1}{2}(c_{ik} + c_{jk}) \rfloor = c_{ik}c_{jk}, \quad 1 \leq k \leq n.$$

Note que, quando \mathbb{Z}_q é substituído pelo corpo de Galois \mathbb{F}_q , a soma acima apresenta restrições, pois neste caso a soma depende da característica do corpo. Uma alternativa é considerar os códigos C_i como sendo quasilineares, [11]. Se $q_i = q$ e os códigos C_i , $0 \leq i \leq m-1$, são lineares, então temos o seguinte resultado.

Teorema 2 Se $q_i = q$ e os códigos C_i , $0 \leq i \leq m-1$, são lineares, então \mathbf{L}_{Nn} é um reticulado em \mathbb{R}^{Nn} .

Prova. É claro que $\mathbf{0} \in \mathbf{L}_{Nn}$. Dado $\mathbf{l} = UB + \lambda_m \in \mathbf{L}_{Nn}$. Então,

$$\mathbf{l} = ((1-q)U)B + (qU)B + \lambda_m.$$

Assim, existe $\mathbf{l}' = ((q-1)U)B - \lambda'_m \in \mathbf{L}_{Nn}$, onde $\lambda'_m = (qU)B + \lambda_m \in \Lambda_m^n$, pois $q\Lambda_0 \subseteq \Lambda_m$, tal que $\mathbf{l} + \mathbf{l}' = \mathbf{0}$. Dados $\mathbf{l}, \mathbf{l}' \in \mathbf{L}_{Nn}$: $\mathbf{l} = UB + \lambda_m$ e $\mathbf{l}' = U'B + \lambda'_m$. Então,

$$\begin{aligned} \mathbf{l} + \mathbf{l}' &= UB + \lambda_m + U'B + \lambda'_m \\ &= (U + U')B + \lambda_m + \lambda'_m. \end{aligned}$$

Como $U + U' = U \oplus U' + q(U \circ U')$ e $\mathbf{c}_i \oplus \mathbf{c}'_i = \bar{\mathbf{c}}_i \in C_i$ temos que

$$\mathbf{l} + \mathbf{l}' = \bar{U}B + \bar{\lambda}_m \in \mathbf{L}_{Nn},$$

pois, $\bar{U} = U \oplus U'$ e $\bar{\lambda}_m = q(U \circ U')B + \lambda_m + \lambda'_m \in \Lambda_m^n$. Portanto, \mathbf{L}_{Nn} é um subgrupo de \mathbb{R}^{Nn} . ■

O teorema a seguir determina uma cota da mínima distância euclidiana quadrática dos empacotamentos esféricos da Definição 1.

Teorema 3 $\min_{0 \leq i \leq m-1} \{d_H(C_i)d_{\min}^2(\Lambda_i), d_{\min}^2(\Lambda_m)\} \leq d_{\min}^2(\mathbf{L}_{Nn}) \leq d_{\min}^2(\Lambda_m)$. Em particular, se $C_0 \subseteq \dots \subseteq C_{m-1}$ e $q_i = q$, $0 \leq i \leq m-1$, então

$$d_{\min}^2(\mathbf{L}_{Nn}) = \min_{0 \leq i \leq m-1} \{d_H(C_i)N(\Lambda_i), d_{\min}^2(\Lambda_m)\}.$$

Corolário 4 Se $C_0 \subseteq \dots \subseteq C_{m-1}$ e $q_i = q$, $0 \leq i \leq m-1$, então dados $\mathbf{l} \in \mathbf{L}_{Nn}$: $\mathbf{l} = UB + \lambda_m$ e $\mathbf{u}_k \neq \mathbf{0}$, para algum k : $1 \leq k \leq n$, temos que $N(\mathbf{l}) = d_{\min}^2(\mathbf{L}_{Nn})$ se, e somente se, $w_H(\mathbf{c}_i) = d_H(C_i)$ e $d_{\min}^2(\mathbf{L}_{Nn}) = d_H(C_i)d_{\min}^2(\Lambda_i)$, $0 \leq i \leq m-1$, onde $\mathbf{u}_k = (c_{0k}, \dots, c_{m-1k}) \neq \mathbf{0}$ implica que $\mathbf{c}_i \neq \mathbf{0}$ para algum i : $0 \leq i \leq m-1$. ■

O cálculo do coeficiente de erro $E(\mathbf{L}_{Nn})$ do reticulado \mathbf{L}_{Nn} em \mathbb{R}^{Nn} é feito através da função Téta de Jacobi, $\theta_{\mathbf{L}_{Nn}}(z)$, [2], isto é,

$$\theta_{\mathbf{L}_{Nn}}(z) = \sum_{j=1}^K \sum_{\lambda \in \Lambda_m^n} q^{N(\lambda + \mathbf{h}_j - \mathbf{h}_1)},$$

onde $q = e^{i\pi z}$, $\mathbf{h}_j \in \left\{ \sum_{i=0}^{m-1} (\mathbf{c}_i \otimes \mathbf{g}_i) : \mathbf{c}_i \in C_i \right\}$ e $K = \prod_{i=0}^{m-1} |C_i|$, pois \mathbf{L}_{Nn} é um empacotamento periódico.

Com o propósito de comparação, será conveniente normalizar o coeficiente de erro para duas dimensões, isto é,

$$\tilde{E}(\mathbf{L}_{Nn}) \triangleq \frac{2}{Nn} E(\mathbf{L}_{Nn}).$$

Como o empacotamento esférico \mathbf{L}_{Nn} em \mathbb{R}^{Nn} é periódico, a densidade \mathbf{L}_{Nn} é dada por

$$\Delta(\mathbf{L}_{Nn}) \triangleq \prod_{i=0}^{m-1} |C_i| \frac{V(\mathbf{E}_\rho(0))}{V(\Lambda_m^n)},$$

onde $\rho = \frac{1}{2}d_{\min}(\mathbf{L}_{Nn})$. Consequentemente, a densidade de centros de \mathbf{L}_{Nn} é dada por

$$\delta(\mathbf{L}_{Nn}) \triangleq \prod_{i=0}^{m-1} |C_i| \frac{\rho^{Nn}}{V(\Lambda_m^n)}.$$

O ganho de codificação fundamental do empacotamento esférico \mathbf{L}_{Nn} em \mathbb{R}^{Nn} é dado, [6], por

$$\gamma(\mathbf{L}_{Nn}) \triangleq \frac{d_{\min}^2(\mathbf{L}_{Nn})}{[V(\mathbf{L}_{Nn})]^{\frac{2}{Nn}}},$$

onde $V(\mathbf{L}_{Nn})$ é o volume da região de Voronoi em \mathbf{L}_{Nn} . Para calcular o ganho de codificação fundamental devemos encontrar o volume de uma região de Voronoi de \mathbf{L}_{Nn} . Como \mathbf{L}_{Nn} é periódico, basta considerar apenas um período, o qual corresponde a uma região congruente à região fundamental básica de Λ_m^{Nn} , pois \mathbf{L}_{Nn} é a união de $\prod_{i=0}^{m-1} |C_i|$ classes laterais à esquerda de Λ_m^{Nn} . Assim, esta região contém $\prod_{i=0}^{m-1} |C_i|$ centros de esferas, uma vez que as regiões de Voronoi destes centros cobrem esta região. Desse modo, temos que

$$V(\mathbf{L}_{Nn}) = \frac{V(\Lambda_m^n)}{\prod_{i=0}^{m-1} |C_i|} = \frac{V(\Lambda_m^n)}{\prod_{i=0}^{m-1} |C_i|}.$$

Portanto, o ganho de codificação fundamental de \mathbf{L}_{Nn} é dado por

$$\gamma(\mathbf{L}_{Nn}) = \left(\prod_{i=0}^{m-1} |C_i| \right)^{\frac{2}{Nn}} \frac{d_{\min}^2(\mathbf{L}_{Nn})}{V(\Lambda_m^n)^{\frac{2}{Nn}}}.$$

Neste caso, temos a seguinte relação

$$\delta(\mathbf{L}_{Nn}) = \left(\frac{\gamma(\mathbf{L}_{Nn})}{4} \right)^{\frac{Nn}{2}}$$

Note que, o ganho de codificação fundamental $\gamma(\mathbf{L}_{Nn})$ mede uma componente do ganho de potência que pode ser alcançado usando uma constelação de sinais S com base no reticulado \mathbf{L}_{Nn} relativo a uma constelação de sinais com base em \mathbb{Z}^{Nn} .

3. DECODIFICAÇÃO

Com o propósito de completeza, apresentamos nesta seção o algoritmo de decodificação, [4], para os empacotamentos esféricos \mathbf{L}_{Nn} de \mathbb{R}^{Nn} obtidos com a construção multicamada da Seção 2. Este algoritmo pode ser usado para a quantização de vetores e/ou para a decodificação de códigos reticulados, isto é, um subconjunto finito de pontos de um reticulado, para um canal gaussiano. Para maiores detalhes sobre codificações e algoritmos de decodificações de reticulados, [2] ou [3].

Um algoritmo de decodificação por máxima verossimilhança ou simplesmente algoritmo ML para um reticulado Γ em \mathbb{R}^N é um algoritmo que, dado $\mathbf{x} \in \mathbb{R}^N$, encontra um ponto de Γ mais próximo de \mathbf{x} do que qualquer outro ponto de Γ , isto é, dado $\mathbf{x} \in \mathbb{R}^N$ existe $\lambda \in \Gamma$ tal que $N(\mathbf{x} - \lambda) \leq N(\mathbf{x} - \lambda')$ para todo $\lambda' \in \Gamma$, $\lambda \neq \lambda'$, onde $N(\mathbf{x})$ denota a norma do vetor \mathbf{x} . Assim, uma região de decisão de um algoritmo de decodificação por ML para Γ é essencialmente uma região de Voronoi para Γ , salvo ambiguidade envolvida em resolver empate na fronteira. Note que, se $\Phi(\lambda)$ é o ponto mais próximo de Γ para $\mathbf{x} \in \mathbb{R}^N$, então $\mathbf{r} + \Phi(\lambda - \mathbf{r})$ é o ponto mais próximo de $\mathbf{r} + \Gamma$ para $\mathbf{x} \in \mathbb{R}^N$. Portanto, um algoritmo de decodificação por ML de um reticulado Γ pode ser usado como um algoritmo de decodificação por ML de uma translação de Γ . Como a medida de distância de um reticulado Γ em \mathbb{R}^N é invariante por translação temos que o algoritmo por ML para Γ em \mathbb{R}^N é invariante por translação.

Um algoritmo de decodificação com distância limitada para um empacotamento esférico Γ em \mathbb{R}^N é um algoritmo com a seguinte propriedade: dado $\mathbf{x} \in \mathbb{R}^N$ se existe $\lambda \in \Gamma$ tal que $N(\mathbf{x} - \lambda) < d_{\min}^2(\Gamma)/4$, então \mathbf{x} será decodificado como λ . A seguir apresentamos um algoritmo de decodificação com distância limitada ou algoritmo de decodificação por estágio, [4], para os empacotamentos esféricos \mathbf{L}_{Nn} em \mathbb{R}^{Nn} obtidos através da construção proposta na Seção 2.

Algoritmo A^a : Dado $\mathbf{r} \in \mathbb{R}^{Nn}$.

Passo 0 - Faça $\mathbf{r}_0 = \mathbf{r}$ e decodifique \mathbf{r}_0 no ponto $(\hat{c}_0 \otimes \mathbf{g}_0) + \hat{\lambda}_1$ mais próximo do reticulado $\Gamma_0 = (C_0 \otimes [\Lambda_0/\Lambda_1]) + \Lambda_1^n$ em \mathbb{R}^{Nn} ;

Passo 1 - Faça $\mathbf{r}_1 = \mathbf{r}_0 - (\hat{c}_0 \otimes \mathbf{g}_0)$ e decodifique \mathbf{r}_1 no ponto $(\hat{c}_1 \otimes \mathbf{g}_1) + \hat{\lambda}_2$ mais próximo do reticulado $\Gamma_1 = (C_1 \otimes [\Lambda_1/\Lambda_2]) + \Lambda_2^n$ em \mathbb{R}^{Nn} ;

⋮

Passo (m-1) - Faça $\mathbf{r}_{m-1} = \mathbf{r}_{m-2} - (\hat{c}_{m-2} \otimes \mathbf{g}_{m-2})$ e decodifique \mathbf{r}_{m-1} no ponto $(\hat{c}_{m-1} \otimes \mathbf{g}_{m-1}) + \hat{\lambda}_m$

mais próximo do reticulado $\Gamma_{m-1} = (C_{m-1} \otimes [\Lambda_{m-1}/\Lambda_m]) + \Lambda_m^n$ em \mathbb{R}^{Nn} .

Portanto, \mathbf{r} será decodificado como $\hat{\mathbf{l}} = \hat{U}B + \hat{\lambda}_m \in \mathbf{L}_{Nn}$, pois $\mathbf{r}_{m-1} = \mathbf{r} - \sum_{i=0}^{m-2} (\hat{c}_i \otimes \mathbf{g}_i)$.

O próximo resultado é uma extensão para o empacotamento esférico \mathbf{L}_{Nn} de um resultado semelhante para reticulados em [4], onde omitiremos as demonstrações (veja [13] para maiores detalhes).

Lema 5 Se $q_i = q$ e os códigos $C_i, : 0 \leq i \leq m-1$, são lineares, então o algoritmo A^a é invariante por translação.

Teorema 6 Dado $\mathbf{r} \in \mathbb{R}^{Nn}$, se $C_0 \subseteq \dots \subseteq C_{m-1}, : q_i = q, : 0 \leq i \leq m-1$, e existe $\mathbf{l} \in \mathbf{L}_{Nn}$ tal que $N(\mathbf{r} - \mathbf{l}) < \frac{d_{\min}^2(\mathbf{L}_{Nn})}{4}$, então \mathbf{r} será decodificado corretamente pelo algoritmo A^a .

O conjunto de pontos $\mathbf{r} \in \mathbb{R}^{Nn}$ que mapeia para o ponto 0 é chamado a região de decisão, isto é,

$$R^a(\mathbf{0}) = \{\mathbf{r} \in \mathbb{R}^{Nn} : N(\mathbf{r}) \leq d_{\min}^2(\mathbf{L}_{Nn})/4\},$$

do algoritmo A^a . Pelo Lema 5 todas as regiões de decisão $R^a(\mathbf{l})$ são congruentes e, $R^a(\mathbf{l}) = \mathbf{l} + R^a(\mathbf{0})$ para todo $\mathbf{l} \in \mathbf{L}_{Nn}$. Neste caso, $R^a(\mathbf{0})$ é uma região fundamental para \mathbf{L}_{Nn} . Como as esferas $E_\rho(\mathbf{0})$ de centro $\mathbf{0} \in \mathbf{L}_{Nn}$ e raio $\rho = d_{\min}(\mathbf{L}_{Nn})/2$, devem tocar-se, temos que existem pontos de norma igual a ρ^2 na fronteira de $R^a(\mathbf{0})$. O número de pontos na fronteira de $R^a(\mathbf{0})$ com norma igual a ρ^2 é o coeficiente de erro efetivo de \mathbf{L}_{Nn} e, denotaremos por $E_e(\mathbf{L}_{Nn})$. Em geral, $E_e(\mathbf{L}_{Nn}) \geq E(\mathbf{L}_{Nn})$. Assim, A^a é um algoritmo subótimo, ou equivalentemente, A^a é um algoritmo de decodificação com distância limitada para o empacotamento esférico \mathbf{L}_{Nn} em \mathbb{R}^{Nn} .

O próximo resultado é uma extensão para o reticulado \mathbf{L}_{Nn} de um resultado semelhante para reticulados em [4]. Omitiremos a demonstração, porém, a mesma pode ser encontrada em [13].

Teorema 7 Se $C_0 \subseteq \dots \subseteq C_{m-1}$ e $q_i = q, 0 \leq i \leq m-1$, então o coeficiente de erro efetivo $E_e(\mathbf{L}_{Nn})$ é dado por

$$E_e(\mathbf{L}_{Nn}) =$$

$$= \sum_{d_{\min}^2(\mathbf{L}_{Nn}) = d_H(C_i)d_{\min}^2(\Lambda_i)} (E(C_i)E(\Lambda_{i+1}))^{d_H(C_i)} + E_m,$$

onde

$$E_m = \begin{cases} nE(\Lambda_m), & \text{se } d_{\min}^2(\Lambda_m) = d_{\min}^2(\mathbf{L}_{Nn}) \\ 0, & \text{se } d_{\min}^2(\Lambda_m) > d_{\min}^2(\mathbf{L}_{Nn}) \end{cases}$$

A seguir, iremos apresentar o cálculo aproximado da complexidade de decodificação do algoritmo A^a para o empacotamento esférico L_{Nn} . Para maiores detalhes e exemplos, ver [4].

Primeiro. Dado $\mathbf{r}_i = (r_{i1}, \dots, r_{in})$, $r_{ij} \in \mathbb{R}^N$, $0 \leq i \leq m-1$, $1 \leq j \leq n$, então para cada $i = 0, \dots, m-1$, o algoritmo escolhe um $c_{ij} \in \mathbb{N}_{q_i}$ que esteja mais próximo de cada uma das componentes r_{ij} de \mathbf{r}_i , $1 \leq j \leq n$, isto é,

$$d_{ij} \triangleq \min \{N(\mathbf{r}_{ij} - ((c_{ij}\mathbf{g}_i) + \lambda_{(i+1)j}))\}.$$

Note que d_{ij} é a mínima distância euclidiana quadrática de cada classe lateral à esquerda de Λ_{i+1} em Λ_i da componente recebida \mathbf{r}_{ij} , $1 \leq j \leq n$.

Segundo. Para cada $i = 0, \dots, m-1$, seja $\tilde{\mathbf{c}}_i = (\tilde{c}_{i1}, \dots, \tilde{c}_{in})$ uma aproximação para a palavra-código $\mathbf{c}_i = (c_{i1}, \dots, c_{in}) \in C_i$. Então um algoritmo de decodificação suave para decodificar C_i , (Apêndice de [7] ou [15]), é usado para corrigir erros em $\tilde{\mathbf{c}}_i$, e a palavra resultante é uma palavra-código $\hat{\mathbf{c}}_i \in C_i$. isto é,

$$d_i \triangleq \min \{N(\mathbf{r}_i - ((\mathbf{c}_i \otimes \mathbf{g}_i) + \lambda_{i+1}))\}.$$

Como a norma é uma medida de distância aditiva e

$$\min \left(\sum_{i=0}^{m-1} X_i \right) = \sum_{i=0}^{m-1} (\min X_i),$$

temos que

$$d_i = \sum_{j=1}^n d_{ij}, \quad 0 \leq i \leq m-1.$$

Finalmente, como o algoritmo A^a para L_{Nn} usa apenas a palavra código $\mathbf{c}_i \in C_i$ para minimizar d_i e

$$\begin{aligned} \Gamma_i &= \{\mathbf{c}_i \otimes \mathbf{g}_i : \mathbf{c}_i \in C_i\} + \Lambda_{i+1}^n = \bigcup_{\mathbf{c}_i \in C_i} (\mathbf{c}_i \otimes \mathbf{g}_i + \Lambda_{i+1}^n) \\ &= \bigcup_{\mathbf{c}_i \in C_i} \{(c_{i1}\mathbf{g}_i + \lambda_{i1}, \dots, c_{in}\mathbf{g}_i + \lambda_{in}) : \lambda_{ij} \in \Lambda_{i+1}\}, \end{aligned}$$

$0 \leq i \leq m-1$, a complexidade para decodificar Γ_i é dada aproximadamente por

$$N_D(\Gamma_i) = n(N_D(\Lambda_i/\Lambda_{i+1}) + 1) + N_D(C_i),$$

onde $N_D(\Lambda_i/\Lambda_{i+1})$ é a complexidade do algoritmo ML usado para decodificar a partição Λ_i/Λ_{i+1} , (Apêndice [7]), e $N_D(C_i)$ é a complexidade do algoritmo com decisão suave por ML usado para decodificar C_i . Portanto, a complexidade para o algoritmo A^a para L_{Nn} é dada por

$$N_D^a(L_{Nn}) \triangleq \sum_{i=0}^{m-1} N_D(\Gamma_i) + mnN,$$

onde mnN refere-se aos passos do algoritmo A^a que calcula cada \mathbf{r}_i a ser decodificado em relação a Γ_i , no passo subsequente.

A complexidade normalizada é dada por

$$\tilde{N}_D^a(L_{Nn}) = \frac{2}{nN} N_D^a(L_{Nn}).$$

A relação de degradação de desempenho em $[dB]$ por redução de complexidade em [oitavas], [4], do reticulado L_{Nn} é dada por

$$\beta(L_{Nn}) \triangleq -\frac{\Delta(L_{Nn})}{\log_2 \left(\frac{N_D^a(L_{Nn})}{N_D(L_{Nn})} \right)}$$

$$\text{e } \Delta(L_{Nn}) \approx 0.22 \log_2 \left(\frac{E_e(L_{Nn})}{E(L_{Nn})} \right).$$

Note que um algoritmo de decodificação misto pode alcançar o melhor compromisso entre desempenho e complexidade, isto é, no primeiro passo do algoritmo A^a usamos um decodificador com decisão suave por ML e um decodificador com decisão abrupta subótimo nos passos subsequentes. Para comparações do algoritmo A^a com outros algoritmos, ver [3].

4. EXEMPLOS

Nesta seção apresentaremos alguns exemplos de empacotamentos esféricos como ilustrações da construção multicamada da Seção 2, bem como a obtenção de seus principais parâmetros. Para mais exemplos e comparações, ver [4].

Exemplo 8 Seja $\Lambda_0/\Lambda_1/\Lambda_2$ uma cadeia de partições, com 2-níveis e 2-maneiras, onde $\Lambda_0 = \mathbb{Z}^2$ é o reticulado cúbico em \mathbb{R}^2 com uma matriz geradora

$$M_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

e $\Lambda_i = T_2^i(\Lambda_0)$, $i = 1, 2$, os subreticulados de Λ_0 induzidos pelo endomorfismo T_2 de Λ_0 definido pela matriz

$$[T_2] = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

que escala Λ_0 por $\sqrt{2}$ e rotaciona por 45° . Neste caso,

$$\begin{aligned} \mathbf{g}_0 &= (1, 0), \quad \mathbf{g}_1 = (1, 1), \quad d_{\min}^2(L_{2n}) = \min_{0 \leq i \leq 1} \{2^i d_H(C_i), 4\}, \quad V(L_{2n}) = 2^{2n-k} e \\ \gamma(L_{2n}) &= 2^{\frac{k-2n}{n}} d_{\min}^2(L_{2n}), \quad \text{onde } k = k_0 + k_1. \end{aligned}$$

Usaremos a notação $[n, k, d]_q$ para um código sobre $GF(q)$, com comprimento n , dimensão k e distância de Hamming d .

(1) Para os códigos $C_0 = [2, 1, 2]_2$ e $C_1 = [2, 2, 1]_2$, Tabela-I de [14], temos

$$d_{\min}^2(L_4) = 2, \quad V(L_4) = 2 : e : \gamma(L_4) = 1.51[dB],$$

$$\begin{aligned} E(L_4) &= \sum_{w_H(\mathbf{c}_0)=d_H(C_0)} M^{(0)}(\mathbf{c}_0) + \\ &+ \sum_{w_H(\mathbf{c}_1)=d_H(C_1)} M^{(1)}(\mathbf{c}_1) \\ &= M^{(0)}(\mathbf{c}_0) + 2M^{(1)}(\mathbf{c}_1). \end{aligned}$$

Para $\mathbf{c}_0 = (11)$, obtemos

$$\begin{aligned} M^{(0)}(\mathbf{c}_0) &= \\ &= \sum_{\substack{\mathbf{c}_1 \in C_1 \\ w_H(\mathbf{c}_1 * \mathbf{c}_0) = w_H(\mathbf{c}_1)}} \prod_{k=1}^2 [E^{(0)}(\mathbf{c}_{0k} \mathbf{g}_0 + \mathbf{c}_{1k} \mathbf{g}_1 + \Lambda_2)] \\ &= E^{(0)}(\mathbf{g}_0 + \Lambda_2)^2 + 2E^{(0)}(\mathbf{g}_0 + \Lambda_2) \times \\ &\quad E^{(0)}(\mathbf{g}_0 + \mathbf{g}_1 + \Lambda_2) + E^{(0)}(\mathbf{g}_0 + \mathbf{g}_1 + \Lambda_2)^2 \\ &= 2^2 + 2 \cdot 2 \cdot 2 + 2^2 = 16. \end{aligned}$$

e

$$M^{(1)}(\mathbf{c}_1) = E^{(1)}(\Lambda_2)^{d_H(C_1)} = 4^1 = 4.$$

Logo,

$$\begin{aligned} E(\mathbf{L}_4) &= 24 :: e :: \tilde{E}(\mathbf{L}_4) = 12. \\ E_e(\mathbf{L}_4) &= E^{(0)}(C_0)E^{(0)}(\Lambda_1)^{d_H(C_0)} + \\ &\quad E^{(1)}(C_1)E^{(1)}(\Lambda_2)^{d_H(C_1)} \\ &= 4^2 + 2 \cdot 4^1 = 24 :: e :: \tilde{E}_e(\mathbf{L}_4) = 12. \end{aligned}$$

Finalmente,

$$\begin{aligned} N_D^a(\mathbf{L}_4) &= 2(N_D(\Lambda_0/\Lambda_1) + 1) + N_D(C_0) + \\ &\quad + 2(N_D(\Lambda_1/\Lambda_2) + 1) + N_D(C_1) + 8 \\ &= 6 + 4 + 6 + 2 + 8 = 26. \end{aligned}$$

Note que \mathbf{L}_4 é similar ao reticulado do tabuleiro de xadrez \mathbf{D}_4 em \mathbb{R}^4 , [2].

- (2) Para os códigos $C_0 = [4, 1, 4]_2$ e $C_1 = [4, 3, 2]_2$, Tabela-I de [14], obtemos

$$d_{\min}^2(\mathbf{L}_8) = 4, : V(\mathbf{L}_8) = 2^4,$$

$$\gamma(\mathbf{L}_8) = 3,01[dB], : \tilde{E}(\mathbf{L}_8) = 60, : \tilde{E}_e(\mathbf{L}_8) = 92$$

$$e :: N_D^a(\mathbf{L}_8) = 52.$$

Como $N_D(\mathbf{L}_8) = 72$, [2], temos que a relação de degradação de desempenho em [dB] por redução de complexidade em [oitavas] do reticulado \mathbf{L}_8 é dada por

$$\beta(\mathbf{L}_8) = 0.29.$$

Note que \mathbf{L}_8 é similar ao reticulado de Gosset \mathbf{E}_8 em \mathbb{R}^8 , [2].

Exemplo 9 Seja $\Lambda_0/\Lambda_1 \cdots / \Lambda_m$ uma cadeia de partições, com m -níveis e 3- e/ou 4-maneyras, onde $\Lambda_0 = \mathbf{A}_2$ é o reticulado hexagonal em \mathbb{R}^2 com uma matriz geradora

$$M_0 = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}$$

e $\Lambda_i = T_3^i(T_4^j(\Lambda_0))$, $i, j = 0, 1, \dots, m$, os subreticulados de Λ_0 induzidos pelos endomorfismos T_3 e T_4 de Λ_0 definidos pelas matrizes, [2],

$$[T_3] = \begin{bmatrix} \frac{3}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{3}{2} \end{bmatrix} \cdots e \cdots [T_4] = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}.$$

Usando as cadeias de partições do reticulado hexagonal \mathbf{A}_2 , reproduzimos todos os empacotamentos esféricos da Tabela-VIII de [9]. Como um exemplo, seja $\Lambda_0/\Lambda_1/\Lambda_2$ uma cadeia de partições, com 2-níveis, onde $\Lambda_0 = \mathbf{A}_2$, $\Lambda_1 = T_4(\Lambda_0)$ e $\Lambda_2 = T_3(\Lambda_1)$. Então para os códigos $C_0 = [18, 9, 8]_4$, $C'_0 = [30, 15, 12]_4$, Tabela-VI de [9], e $C_1 = [18, 17, 2]_3$, $C'_1 = [30, 26, 3]_3$, Tabela-V de [9], obtemos os empacotamentos esféricos \mathbf{L}_{36} e \mathbf{L}_{60} , que são os mais densos em suas dimensões.

Seja $\Lambda_0/\Lambda_1 \cdots / \Lambda_m$ uma cadeia de partições, com m -níveis e 4-maneyras, onde $\Lambda_0 = \mathbf{D}_4$ é o reticulado do tabuleiro de xadrez em \mathbb{R}^4 com uma matriz geradora

$$M_0 = \begin{bmatrix} 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

e $\Lambda_i = T_4^i(\Lambda_0)$, $i = 0, 1, \dots, m$, os subreticulados de Λ_0 induzidos pelo endomorfismo T_4 de Λ_0 definido pela matriz

$$[T_4] = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}.$$

Usando os melhores códigos quaternários conhecidos, Tabela-VI de [9], e a cadeia de partições do reticulado \mathbf{D}_4 , obtemos uma variedade de empacotamentos esféricos mostrados na Tabela 1, onde os códigos $C_i = [n, k_i, d_i]_4$ nas quatro colunas da tabela são provenientes da Tabela-VI de [9]. Na quinta coluna, está o ganho de codificação fundamental $\gamma(\mathbf{L}_{Nn})$, em [dB], dos empacotamentos propostos e na sexta coluna γ_{cs} e γ_{kp} representam o ganho de codificação fundamental, em [dB], dos melhores empacotamentos da Tabela 3.1 de [2] e da Tabela-VIII de [9], respectivamente. Finalmente, na sétima coluna temos a dimensão dos empacotamentos \mathbf{L}_{Nn} .

Nas dimensões 68 e 72, os empacotamentos esféricos obtidos (Tabela 1) são mais densos do que os correspondentes da Tabela VIII de [9]. As densidades de centros destes empacotamentos esféricos são $\delta(\mathbf{L}_{68}) \approx 2^{24.95}$ e $\delta(\mathbf{L}_{72}) \approx 2^{30.73}$, respectivamente. Os empacotamentos esféricos obtidos com esta construção dependem muito dos códigos e dos endomorfismos a serem utilizados, uma vez que a utilização de códigos com distâncias de Hamming maiores para os primeiros níveis da partição implica em melhores empacotamento dos subcódigos para um endomorfismo apropriado. Para maiores detalhes veja [13].

C_0	C_1	C_2	C_3	$\gamma(L_{N_n})[dB]$	$\gamma[dB]$	N_n
[2, 1, 2]	[2, 2, 1]	[2, 2, 1]	[2, 2, 1]	3.01	3.01cs	L_8
[3, 2, 2]	[3, 3, 1]	[3, 3, 1]	[3, 3, 1]	3.51	3.63cs	L_{12}
[4, 1, 4]	[4, 3, 2]	[4, 4, 1]	[4, 4, 1]	4.52	4.52cs	L_{16}
[5, 2, 4]	[5, 4, 2]	[5, 5, 1]	[5, 5, 1]	5.12	5.12cs	L_{20}
[6, 3, 4]	[6, 5, 2]	[6, 6, 1]	[6, 6, 1]	5.52	6.02cs	L_{24}
[7, 3, 4]	[7, 6, 2]	[7, 7, 1]	[7, 7, 1]	5.38	5.81cs	L_{28}
[8, 1, 8]	[8, 4, 4]	[8, 7, 2]	[8, 8, 1]	6.02	6.28cs	L_{32}
[9, 1, 9]	[9, 5, 4]	[9, 8, 2]	[9, 9, 1]	6.19	6.38kp	L_{36}
[10, 2, 8]	[10, 6, 4]	[10, 9, 2]	[10, 10, 1]	6.62	6.62cs	L_{40}
[11, 2, 8]	[11, 7, 4]	[11, 10, 2]	[11, 11, 1]	6.71	6.98cs	L_{44}
[12, 3, 8]	[12, 8, 4]	[12, 11, 2]	[12, 12, 1]	7.02	7.78cs	L_{48}
[13, 4, 8]	[13, 9, 4]	[13, 12, 2]	[13, 13, 1]	7.30	7.30kp	L_{52}
[14, 5, 8]	[14, 10, 4]	[14, 13, 2]	[14, 14, 1]	7.53	7.52kp	L_{56}
[15, 6, 8]	[15, 11, 4]	[15, 14, 2]	[15, 15, 1]	7.73	7.77kp	L_{60}
[16, 1, 16]	[16, 7, 8]	[16, 12, 4]	[16, 15, 2]	8.10	8.10cs	L_{64}
[17, 1, 17]	[17, 8, 8]	[17, 13, 4]	[17, 16, 2]	8.23	8.01kp	L_{68}
[18, 1, 18]	[18, 9, 8]	[18, 13, 4]	[18, 17, 2]	8.59	8.16kp	L_{72}
[19, 9, 8]	[19, 14, 4]	[19, 18, 2]	[19, 19, 1]	8.16	8.24kp	L_{76}
[20, 2, 16]	[20, 10, 8]	[20, 15, 4]	[20, 19, 2]	8.43	8.73cs	L_{80}
[21, 3, 16]	[21, 10, 8]	[21, 16, 4]	[21, 20, 2]	8.53	8.54kp	L_{84}
[22, 3, 16]	[22, 11, 8]	[20, 17, 4]	[22, 21, 2]	8.62	8.58kp	L_{88}
[23, 3, 16]	[23, 12, 8]	[23, 18, 4]	[23, 22, 2]	8.70	8.72kp	L_{92}
[24, 4, 16]	[24, 13, 8]	[24, 19, 4]	[24, 23, 2]	8.91	9.29cs	L_{96}
[25, 5, 16]	[25, 14, 8]	[25, 20, 4]	[25, 24, 2]	9.09	9.07kp	L_{100}

Tabela 1. Empacotamentos esféricos obtidos de partições do reticulado D_4 .

5. CONCLUSÕES

Neste trabalho foi proposta uma construção multinível para a obtenção de empacotamentos esféricos ou reticulados com expressões explícitas para os seus principais parâmetros. Os empacotamentos esféricos obtidos com esta construção dependem dos códigos e dos endomorfismos a serem utilizados, uma vez que a utilização de códigos com distâncias de Hamming maiores para os primeiros níveis da partição implica em melhores empacotamento dos subcódigos para um endomorfismo apropriado. Nas dimensões 68 e 72, um novo recorde de densidades foi alcançado.

REFERÊNCIAS

- [1] A.R. Calderbank and N.J.A. Sloane, "New trellis codes based on lattices and cosets," *IEEE Trans. Inform. Theory*, vol. 33, pp. 177-195, 1987.
- [2] J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups*, New York, Springer-Verlag, 1988.
- [3] M.A.O. Costa e Silva, *Reticulados e suas Partições Aplicados a Codificação sobre Canais AWGN Limitados em Faixa*, Tese de Doutorado, FEE-UNICAMP, 1991.
- [4] M.A.O. Costa e Silva e R. Palazzo, Jr., "A bounded-distance decoding algorithm for lattices based on generalized code formula," *IEEE Trans. Inform. Theory*, vol. 40, pp. 2075-2082, 1994.
- [5] D.S. Dummit and R.M. Foote, *Abstract Algebra*, New Jersey, Prentice Hall, 1991.
- [6] G.D. Forney, Jr., "Coset codes I: Introduction and geometrical classification," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1123-1151, 1988.
- [7] G.D. Forney, Jr., "Coset codes II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152-1187, 1988.
- [8] G.D. Forney, Jr., "A bounded-distance decoding algorithm for the Leech lattices, with generalizations," *IEEE Trans. Inform. Theory*, vol. 35, pp. 906-909, 1989.
- [9] F.R.Kschischang and S. Pasupathy, "Some ternary and quaternary codes and associated sphere packings," *IEEE Trans. Inform. Theory*, vol. 38, pp. 227-246, 1992.
- [10] J. Leech and N.J.A. Sloane, "Sphere packings and error correcting codes," *Canad. J. Math.*, vol. 23, pp. 718-745, 1971.
- [11] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. New York: North-Holland, 1977.
- [12] A.A. e Silva e R. Palazzo, Jr., "Construção de reticulados via fórmula de códigos p-ários generalizado," *XIII Simpósio Brasileiro de Telecomunicações*, Águas de Lindóia, São Paulo, 1995.
- [13] A.A. e Silva, *Uma Contribuição à Classe dos Códigos Geometricamente Uniformes*, Tese de Doutorado, FECC-UNICAMP, 1996.

- [14] T. Verhoeff, "An updated table of minimum-distance bounds for binary codes, *IEEE Trans. Inform. Theory*, vol. 33, pp. 665-680, 1987.
- [15] J.K. Wolf, "Efficient maximum likelihood decoding of linear block codes using trellis," *IEEE Trans. Inform. Theory*, vol. 24, pp. 76-80, 1978.