Um estudo de reticulados obtidos via Construção B

Grasiele C. Jorge, Antonio A. Campello Jr., Sueli I. R. Costa

***Resumo*— Neste trabalho apresentamos uma generalização da chamada Construção B de [3] para classes de códigos q-ários com $q \in \mathbb{N}$ e algumas relações entre as Construções A e B. Mostramos que o reticulado obtido via Construção B de um código q-ário possui qD_n como sub-reticulado e pode ser visto alternativamente como a Construção A de um código $2q$-ário. Por fim, estudamos uma adaptação do algoritmo "Sphere decoding" para reticulados obtidos via Construção B de códigos q-ários, q primo, na métrica da soma.**

***Palavras-Chave*— Códigos q-ários, Construção A, Construção B, Reticulados inteiros.**

***Abstract*— In this work we present a generalization of the so called Construction B of [3] for classes of q-ary codes with $q \in \mathbb{N}$ and also some relations between the Constructions A and B. We show that the lattice obtained from a q-ary code via Construction B has qD_n as sub-lattice and can alternatively be viewed as the Construction A of a $2q$-ary code. Finally, we study an adaptation of the "Sphere decoding" algorithm for lattices obtained via Construction B from q-ary codes, q prime, in the sum metric.**

***Keywords*— q-ary codes, Construction A, Construction B, Integer lattices.**

I. Preliminares

O uso de códigos corretores de erros e reticulados em teoria da informação e criptografia "pós-quântica" vem sendo cada vez mais explorado [9], [15]. Uma classe de reticulados muito utilizada nos estudos relacionados a estas duas vertentes é a classe dos reticulados q-ários. Um dos principais problemas envolvendo reticulados e, em particular reticulados q-ários, é o da decodificação, um problema computacional NP-difícil [10].

Um *reticulado* $\Lambda \subseteq \mathbb{R}^n$ é um subgrupo aditivo discreto. Equivalentemente, podemos definir um reticulado como um conjunto discreto de pontos em $\mathbb{R}^n$, gerado por combinações lineares inteiras de $m \leq n$ vetores linearmente independentes $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbb{R}^n$ [3]. O conjunto $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_m\}$ é chamado de *base* para Λ. Uma matriz $\boldsymbol{G}$ contendo uma base do reticulado em suas linhas é chamada de *matriz geradora do reticulado*. A matriz $\boldsymbol{G}\boldsymbol{G}^t$, onde t denota a matriz transposta, é chamada de *matriz de Gram*. O determinante de qualquer matriz de Gram associada a um reticulado Λ não varia e é chamado de *determinante do reticulado* e denotado por $\det(\Lambda)$. Dizemos que $\Lambda^* \subseteq \Lambda$ é um sub-reticulado se Λ^* é um reticulado. Como Λ e Λ^* são grupos aditivos, temos associado o grupo quociente Λ/Λ^* e vale que $|\Lambda/\Lambda^*| = \det(\Lambda^*)^{1/2}/\det(\Lambda)^{1/2}$ [12]. Decodificar um vetor $\boldsymbol{y} \in \mathbb{R}^n$ em um reticulado Λ com relação à uma métrica d, é encontrar o ponto de Λ mais próximo de $\boldsymbol{y}$ em relação à esta métrica [3]. Neste trabalho faremos o estudo de reticulados na métrica de soma que pode ser associada a canais com ruído aditivo de Laplace [5].

Reticulados q-ários constituem uma classe de reticulados diretamente associada à códigos lineares sobre o anel $\mathbb{Z}_q$, dos inteiros reduzidos módulo q. Dado $q \in \mathbb{N}$, um *código linear q-ário* $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ é um subgrupo aditivo de $\mathbb{Z}_q^n$. Quando q não é primo, não podemos garantir a existência de uma base, apenas de um conjunto de geradores para $\boldsymbol{C}$.

Podemos definir um *reticulado q-ário* Λ, como um reticulado satisfazendo $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$ para algum $q \in \mathbb{N}$ [9]. Equivalentemente, um reticulado q-ário Λ pode ser definido via Construção A [3], [11].

Proposição 1: [3] Considere a aplicação sobrejetora

$$\begin{aligned} \phi :\ \mathbb{Z}^n &\longrightarrow \mathbb{Z}_q^n \\ (x_1, \cdots, x_n) &\longmapsto (\overline{x_1}, \cdots, \overline{x_n}), \end{aligned} \tag{1}$$

onde $\overline{x_i}$ é obtido de x_i por redução módulo q para todo $i = 1, \cdots, n$. Temos que $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ é um código linear q-ário se, e somente se, $\phi^{-1}(\boldsymbol{C}) \subseteq \mathbb{Z}^n$ é um reticulado em $\mathbb{R}^n$. Além disso, $q\mathbb{Z}^n \subseteq \phi^{-1}(\boldsymbol{C})$. □

Definição 1: Chamamos de *Construção A* a aplicação ϕ que relaciona um código $q-$ário $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ a um reticulado $\phi^{-1}(\boldsymbol{C})$ e chamamos o reticulado $\Lambda_A(C) = \phi^{-1}(\boldsymbol{C})$ de *reticulado q-ário* associado ao código $\boldsymbol{C}$.

Proposição 2: [3] Se $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ é um código q-ário, então $\Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n \simeq \boldsymbol{C}$. □

Geometricamente, um reticulado q-ário $\Lambda_A(\boldsymbol{C})$ pode ser visto como o conjunto de pontos obtidos através das translações dos pontos de $\Lambda_A(\boldsymbol{C})$ no hipercubo $[0, q)^n$ por vetores inteiros múltiplos de q. Os pontos do reticulado contidos no hipercubo $[0, q)^n$ são identificados com os pontos do código $\boldsymbol{C}$.

Com base nas relações entre um código q-ário e o reticulado q-ário associado pela Construção A, é possível relacionar a decodificação no reticulado q-ário na métrica da soma com a decodificação no código q-ário associado na métrica de Lee [2].

II. Construção B estendida

A Construção B é apresentada em [3] para classes de códigos binários e ternários. Neste trabalho, estendemos tal construção para classes de códigos lineares $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$, $q \in \mathbb{N}$. Como veremos no que se segue, reticulados obtidos via Construção B em códigos q-ários são $2q$-ários.

Definição 2: Sejam $q = 2^r b$, onde $b \in \mathbb{N}$ ímpar e $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ um código linear q-ário tal que

$$2^r \text{ divide } \sum_{i=1}^{n} c_i \text{ para todo } \overline{\boldsymbol{c}} = (\overline{c_1}, \cdots, \overline{c_n}) \in \boldsymbol{C}. \tag{2}$$

Departamento de Matemática Aplicada, Departamento de Matemática, IMECC-Unicamp, Campinas-SP, Brasil E-mails: grajorge@ime.unicamp.br, campello@ime.br, sueli@ime.unicamp.br. Este trabalho foi parcialmente financiado pelo CNPq (140239/2009-0), CAPES (2548/2010), FAPESP (2009/18337-6), CNPq (309561/2009-4) e FAPESP (2007/56052-8)

Definimos a *Construção B estendida* para o código $\boldsymbol{C}$ como em (2) por

$$\Lambda_B(\boldsymbol{C}) = \{\boldsymbol{z} = \boldsymbol{c} + q\boldsymbol{w};\ \boldsymbol{w} \in \mathbb{Z}^n,\ \overline{\boldsymbol{c}} \in C \text{ e } \ 2^{r+1} \text{ divide } \sum_{i=1}^{n} z_i\}. \quad (3)$$

Observação 1: Para q ímpar, o código $\boldsymbol{C}$ não possui nenhuma restrição dada pela Equação (2). Quando q é par, se não colocarmos restrição no código, poderão existir elementos do código que não geram nenhum ponto do reticulado $\Lambda_B(\boldsymbol{C})$. De fato, se $q = 2^r b$ com $r > 0$, b é ímpar e existe $\overline{\boldsymbol{c}} \in C$ tal que 2^r não divide $\sum_{i=1}^{n} c_i$, então $\sum_{i=1}^{n} c_i = 2^a t$ com $a < r$ e t ímpar. Desta forma, para todo $\boldsymbol{w} \in \mathbb{Z}^n$, temos que se $\boldsymbol{z} = \boldsymbol{c} + q\boldsymbol{w}$ então $\sum_{i=1}^{n} z_i = \sum_{i=1}^{n} c_i + 2^r b \sum_{i=1}^{n} w_i = 2^a(t + 2^{r-a} b \sum_{i=1}^{n} w_i)$ não é divisível por 2^{r+1}.

Exemplo 1: Seja $\boldsymbol{C} = \langle(\overline{1}, \overline{3})\rangle \subseteq \mathbb{Z}_6^2$ um código linear 6-ário satisfazendo a Equação (2). A Figura 1 representa o reticulado $\Lambda_B(\boldsymbol{C})$.

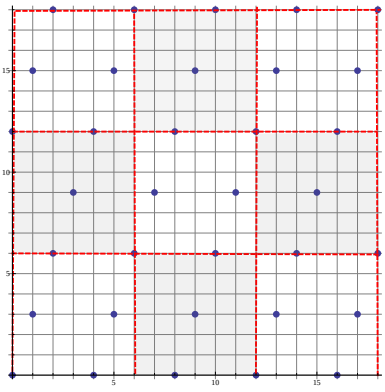

Fig. 1. Reticulado $\Lambda_B(\boldsymbol{C})$ com $\boldsymbol{C} \subseteq \mathbb{Z}_6^2$

Notemos que $\Lambda_B(\boldsymbol{C})$ é um reticulado 12-ário, isto é, $12\mathbb{Z}^2 \subseteq \Lambda_B(\boldsymbol{C})$. Os pontos do reticulado em $[6, 12) \times [0, 6)$ são obtidos dos pontos do código $\boldsymbol{C}$ que não estão em $[0, 6) \times [0, 6)$, transladados pelo vetor $(6, 0)$.

Geometricamente, o reticulado $\Lambda_B(\boldsymbol{C})$ pode ser visto como descrito a seguir: particionamos $\mathbb{R}^n$ através de cópias do hipercubo $[0, q)^n$ e colorimos alternadamente os hipercubos como em um tabuleiro de xadrez. No hipercubo $[0, q)^n$, marcamos os pontos de $\boldsymbol{C}$ que estão no reticulado. No hipercubo vizinho $[6, 12) \times [0, 6)^{n-1}$, marcamos os pontos de $\boldsymbol{C}$ que não estão no reticulado, transladados pelo vetor $(6, 0, \cdots, 0)$. Repetimos os pontos destes dois hipercubos em cada hipercubo de cor equivalente. A união destes pontos é o reticulado $\Lambda_B(\boldsymbol{C})$.

Exemplo 2: [3] Uma versão escalonada, $2E_8$, do reticulado E_8 é obtida via Construção B do código binário

$$\boldsymbol{C} = \{(\overline{0}, \cdots, \overline{0}), (\overline{1}, \cdots, \overline{1})\} \subseteq \mathbb{Z}_2^8.$$

Consideraremos a seguir apenas códigos $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ satisfazendo as restrições da Equação (2).

Proposição 3: Nas condições acima, $\Lambda_B(\boldsymbol{C})$ é um reticulado se, e somente se, $\boldsymbol{C}$ é um código linear q-ário.

Demonstração: Seja $\boldsymbol{C}$ um código linear. Pela demonstração da Proposição 1, temos que $\phi^{-1}(\boldsymbol{C})$ é um grupo aditivo, onde ϕ é dada pela Equação (1). É claro que $\Lambda_B(\boldsymbol{C})$ é um subgrupo aditivo de $\phi^{-1}(\boldsymbol{C})$. Logo, $\Lambda_B(\boldsymbol{C})$ é um reticulado em $\mathbb{R}^n$. Agora, se $\Lambda_B(\boldsymbol{C})$ é um reticulado, mostremos que $\boldsymbol{C}$ é um código linear. Sejam $\overline{\boldsymbol{a}}, \overline{\boldsymbol{b}} \in \boldsymbol{C}$. Existem alguns casos a analisar, porém, abordamos apenas um deles, já que os demais são análogos. Suponha $\boldsymbol{a} \in \Lambda_B(\boldsymbol{C})$ e $\boldsymbol{b} \notin \Lambda_B(\boldsymbol{C})$. Temos $\boldsymbol{b} + q\boldsymbol{e}_1 \in \Lambda_B(\boldsymbol{C})$ e, do fato de $\Lambda_B(\boldsymbol{C})$ ser reticulado, segue que $\boldsymbol{a} - \boldsymbol{b} - q\boldsymbol{e}_1 \in \Lambda_B(\boldsymbol{C})$, ou seja, existe $\overline{\boldsymbol{c}} \in \boldsymbol{C}$ tal que $\boldsymbol{a} - \boldsymbol{b} - q\boldsymbol{e}_1 = \boldsymbol{c} + q\boldsymbol{t}$ para algum $\boldsymbol{t} \in \mathbb{Z}^n$. Assim, $\overline{\boldsymbol{a}} - \overline{\boldsymbol{b}} = \overline{\boldsymbol{c}} \in \boldsymbol{C}$. Portanto, $\boldsymbol{C}$ é um código linear. □

A proposição seguinte mostra que o reticulado obtido via Construção B em um código q-ário $\boldsymbol{C}$ é um sub-reticulado do reticulado obtido pela Construção A no mesmo código $\boldsymbol{C}$.

Proposição 4: Seja $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ um código linear q-ário, $q = 2^r b$, b ímpar. Temos que $\Lambda_B(\boldsymbol{C}) \subseteq \Lambda_A(\boldsymbol{C})$ e $|\Lambda_A(\boldsymbol{C})/\Lambda_B(\boldsymbol{C})| = 2$.

Demonstração: É fácil ver que $\Lambda_B(\boldsymbol{C}) \subseteq \Lambda_A(\boldsymbol{C})$. Seja $\overline{\overline{\boldsymbol{x}}} \in \Lambda_A(\boldsymbol{C})/\Lambda_B(\boldsymbol{C})$. Temos que $\boldsymbol{x} = \boldsymbol{c} + q\boldsymbol{t}$ para $\overline{\boldsymbol{c}} \in \boldsymbol{C}$ e $\boldsymbol{t} \in \mathbb{Z}^n$. Se $\boldsymbol{x} \in \Lambda_B(\boldsymbol{C})$, então $\overline{\overline{\boldsymbol{x}}} = \overline{\overline{\boldsymbol{0}}}$ em $\Lambda_A(\boldsymbol{C})/\Lambda_B(\boldsymbol{C})$. Agora, se $\boldsymbol{x} \notin \Lambda_B(\boldsymbol{C})$, então $\overline{\overline{\boldsymbol{x}}} \neq \overline{\overline{\boldsymbol{0}}}$. Mostremos que para todo $\boldsymbol{y} = \boldsymbol{c}_1 + q\boldsymbol{s} \in \Lambda_A(\boldsymbol{C}) - \Lambda_B(\boldsymbol{C})$ com $\overline{\boldsymbol{c}_1} \in C$ e $\boldsymbol{s} \in \mathbb{Z}^n$, temos que $\overline{\overline{\boldsymbol{y}}} = \overline{\overline{\boldsymbol{x}}}$. De fato, primeiro notemos que como $\overline{\boldsymbol{c}}, \overline{\boldsymbol{c}_1} \in \boldsymbol{C}$, segue que $\sum_{i=1}^{n} c_i = 2^r a$ e $\sum_{i=1}^{n} c_{1_i} = 2^r d$ para $a, d \in \mathbb{Z}$. Como $\boldsymbol{x}, \boldsymbol{y} \notin \Lambda_B(C)$, então 2^{r+1} não divide $\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} c_i + q\sum_{i=1}^{n} t_i = 2^r(a + b\sum_{i=1}^{n} t_i)$ e 2^{r+1} não divide $\sum_{i=1}^{n} y_i = \sum_{i=1}^{n} c_{1_i} + q\sum_{i=1}^{n} s_i = 2^r(d + b\sum_{i=1}^{n} s_i)$. Segue então que $(a + b\sum_{i=1}^{n} t_i)$ e $(d + b\sum_{i=1}^{n} s_i)$ são números ímpares e então 2^{r+1} divide $2^r(a + b\sum_{i=1}^{n} t_i - d - b\sum_{i=1}^{n} s_i) = \sum_{i=1}^{n} x_i - \sum_{i=1}^{n} y_i$, o que implica que $\boldsymbol{x} - \boldsymbol{y} \in \Lambda_B(\boldsymbol{C})$. Portanto, $\Lambda_A(\boldsymbol{C})/\Lambda_B(\boldsymbol{C}) = \left\{\overline{\overline{0}}, \overline{\overline{x}}\right\}$. □

Exemplo 3: Seja $\boldsymbol{C} = \langle(\overline{1}, \overline{7})\rangle \subseteq \mathbb{Z}_9^2$. Os pontos em preto na Figura 2 representam os pontos do reticulado $\Lambda_B(\boldsymbol{C})$ e a união dos pontos pretos e cinzas representa os pontos do reticulado $\Lambda_A(\boldsymbol{C})$.

Observação 2: Como $|\Lambda_A(\boldsymbol{C})/\Lambda_B(\boldsymbol{C})| = 2$, segue que podemos particionar o reticulado $\Lambda_A(\boldsymbol{C})$ como duas cópias do reticulado $\Lambda_B(\boldsymbol{C})$. Desta forma, se o reticulado $\Lambda_B(\boldsymbol{C})$ possuir um algoritmo eficiente de decodificação, podemos decodificar eficientemente $\Lambda_A(\boldsymbol{C})$ utilizando a decodificação por classes de [3].

Exemplo 4: Considere o código $\boldsymbol{C} \subseteq \mathbb{Z}_2^8$ do Exemplo 2. Temos que $\Lambda_B(\boldsymbol{C}) = 2E_8$ e $\Lambda_A(\boldsymbol{C})/\Lambda_B(\boldsymbol{C}) = \{\overline{(0, \cdots, 0)}, \overline{(2, 0, \cdots, 0)}\}$. Dado um vetor recebido $\boldsymbol{y} \in \mathbb{R}^n$, vamos decodificar $\boldsymbol{y}$ em $\Lambda_A(\boldsymbol{C})$. Primeiro decodificamos $\boldsymbol{y}$ em

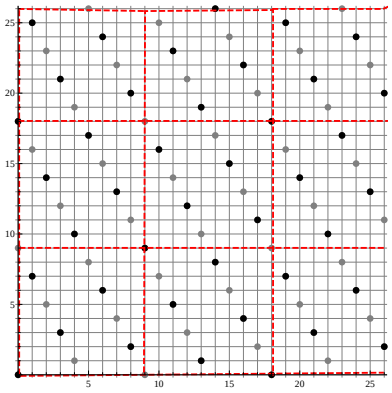

Fig. 2. $\boldsymbol{C} = \langle(\overline{1}, \overline{7})\rangle$

$\Lambda_B(\boldsymbol{C}) = 2E_8$, obtendo $\boldsymbol{z}_1 \in \Lambda_A(\boldsymbol{C})$. Em seguida, decodificamos o vetor $\boldsymbol{y} - (2, 0, \cdots, 0)$ em $\Lambda_B(\boldsymbol{C}) = 2E_8$, obtendo z_2. Então, fazemos $\boldsymbol{z}_2^* = \boldsymbol{z}_2 + (2, 0, \cdots, 0)$ e calculamos o mínimo entre $d(\boldsymbol{y}, \boldsymbol{z}_1)$ e $d(\boldsymbol{y}, \boldsymbol{z}_2^*)$. Portanto, utilizamos duas vezes o algoritmo de decodificação de $\Lambda_B(\boldsymbol{C})$ para decodificar $\Lambda_A(\boldsymbol{C})$.

Consideremos o reticulado padrão D_n, definido em [3] da seguinte forma:

$$D_n = \{(x_1, \cdots, x_n) \in \mathbb{Z}^n \quad \text{tal que} \quad x_1 + \cdots + x_n \text{ é par}\}. \tag{4}$$

Proposição 5: Sejam $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ um código q-ário e D_n o reticulado definido em (4). Temos que $qD_n \subseteq \Lambda_B(\boldsymbol{C})$ e $|\Lambda_B(\boldsymbol{C})/qD_n| = |\boldsymbol{C}|$.

Demonstração: É fácil ver que $qD_n \subseteq \phi^{-1}(\boldsymbol{0})$, onde ϕ é dada pela Eq. (1) e 2^{r+1} divide $\sum_{i=1}^{n} qd_i$, pois $\boldsymbol{d} = (d_1, \ldots, d_n) \in D_n$. Então $qD_n \subseteq \Lambda_B(\boldsymbol{C})$. Consideremos o grupo quociente $\Lambda_B(\boldsymbol{C})/qD_n$. Provaremos que cada elemento de $\boldsymbol{C}$ define uma classe diferente neste quociente. Primeiro, notemos que se $\boldsymbol{x}_1 = \boldsymbol{c}_1 + q\boldsymbol{w}_1, \boldsymbol{x}_2 = \boldsymbol{c}_1 + q\boldsymbol{w}_2 \in \Lambda_B(\boldsymbol{C})$, então $\boldsymbol{x}_1 - \boldsymbol{x}_2 = q(\boldsymbol{w}_1 - \boldsymbol{w}_2)$. Assim, $\sum_{i=1}^{n} w_{1i}$, $\sum_{i=1}^{n} w_{2i}$ têm a mesma paridade, donde $\boldsymbol{w}_1 - \boldsymbol{w}_2 \in D_n$ e $\overline{\boldsymbol{x}_1} = \overline{\boldsymbol{x}_2}$ em $\Lambda_B(\boldsymbol{C})/qD_n$. Agora, se $\boldsymbol{x}_1 = \boldsymbol{c}_1 + q\boldsymbol{w}_1$, $\boldsymbol{x}_2 = \boldsymbol{c}_2 + q\boldsymbol{w}_2 \in \Lambda_B(\boldsymbol{C})$ com $\boldsymbol{c}_1 \neq \boldsymbol{c}_2$ então $\overline{\boldsymbol{x}_1} \not\equiv \overline{\boldsymbol{x}_2}$ em $\Lambda_B(\boldsymbol{C})/qD_n$. De fato, suponhamos $\boldsymbol{x}_1 - \boldsymbol{x}_2 \in qD_n$. Temos que $\boldsymbol{c}_1 - \boldsymbol{c}_2 = \boldsymbol{c} + q\boldsymbol{k}$ para algum $\boldsymbol{k} \in \mathbb{Z}^n$ e $\boldsymbol{c} \in [0, q)^n$ com $\boldsymbol{c} \neq \boldsymbol{0}$. Então $\boldsymbol{x}_1 - \boldsymbol{x}_2 = \boldsymbol{c} + q(\boldsymbol{k} + \boldsymbol{w}_1 - \boldsymbol{w}_2) \in qD_n$ implica $\boldsymbol{c} = q(\boldsymbol{t} - \boldsymbol{k} - \boldsymbol{w}_1 + \boldsymbol{w}_2)$ para algum $\boldsymbol{t} \in D_n$. Como $\boldsymbol{c} \notin q\mathbb{Z}^n$, segue que $\boldsymbol{x}_1 - \boldsymbol{x}_2 \notin qD_n$. □

Observação 3: Em [13], é apresentado um algoritmo para encontrar o ponto mais próximo no reticulado D_n na métrica l_p, $(p \geq 1)$. Usando a decodificação por classes de [3], pela Proposição 5 é possível decodificar o reticulado $\Lambda_B(\boldsymbol{C})$ na métrica l_p, decompondo-o como soma de $|\boldsymbol{C}|$ classes distintas em $\Lambda_B(\boldsymbol{C})/qD_n$.

Exemplo 5: Para o reticulado $2E_8$ do Exemplo 2 temos que $|\Lambda_B(\boldsymbol{C})/2D_8| = |\boldsymbol{C}| = 2$. Desta forma, podemos particionar o reticulado $2E_8$ como duas cópias do reticulado $2D_8$ e utilizando a decodificação do reticulado D_8, podemos decodificar E_8.

Para $q \in \mathbb{N}$ um número primo, vamos encontrar uma matriz geradora para o reticulado $\Lambda_B(\boldsymbol{C})$ em função de uma matriz para o código $\boldsymbol{C}$.

Sejam $q \in \mathbb{N}$ um número primo e $[\boldsymbol{I}_{k\times k} \mid \boldsymbol{B}_{k\times n-k}]$ uma matriz geradora para o código q-ário $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ na forma sistemática [7], onde $\boldsymbol{B} = (b_{i,j})$ e

$$\boldsymbol{D}^* = \begin{pmatrix} 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ 0 & 0 & q & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \\ 0 & 0 & 0 & \cdots & & 2 \end{pmatrix}. \tag{5}$$

Definimos a matriz $\boldsymbol{B}^* = (b_{i,j}^*)$ da seguinte forma: as primeiras $n - k - 1$ colunas de $\boldsymbol{B}$ e $\boldsymbol{B}^*$ são iguais. Para a última coluna consideramos:

$$b_{n-k,j}^* = \begin{cases} b_{n-k,j} & \text{se } \sum_{i=1}^{n-k} b_{i,j} \text{ é ímpar;} \\ b_{n-k,j} + q & \text{se } \sum_{i=1}^{n-k} b_{i,j} \text{ é par.} \end{cases}$$

Proposição 6: Seja q um número primo. Uma matriz geradora para $\Lambda_B(\boldsymbol{C})$ é dada por

$$\boldsymbol{N} = \begin{pmatrix} \boldsymbol{I}_{k\times k} & \boldsymbol{B}^*{}_{n\times(n-k)} \\ \boldsymbol{0}_{(n-k)\times k} & q\,\boldsymbol{D}^*_{(n-k)\times(n-k)} \end{pmatrix}, \tag{6}$$

onde $\boldsymbol{B}^*$ e $\boldsymbol{D}^*$ são definidas como acima.

Demonstração: Seja $\boldsymbol{x} = \boldsymbol{c} + q\boldsymbol{w} \in \Lambda_B(\boldsymbol{C})$, $\overline{\boldsymbol{c}} \in \boldsymbol{C}$ e $\boldsymbol{w} \in \mathbb{Z}^n$. Como $\overline{\boldsymbol{c}} = \sum_{i=1}^{k} \overline{a}_i \overline{\boldsymbol{c}_i}$, onde $\overline{\boldsymbol{c}_i}$ são as linhas de $[\boldsymbol{I}_{k\times k} \mid \boldsymbol{B}_{k\times n-k}]$ e $\overline{a}_i \in \mathbb{Z}_q$, segue que $\boldsymbol{c} = \sum_{i=1}^{k} a_i \boldsymbol{c}_i + q\boldsymbol{s}$ para algum $\boldsymbol{s} \in \mathbb{Z}^n$. Cada $\boldsymbol{c}_i$ pode ser gerado como $\boldsymbol{c}_i = \boldsymbol{c}_i^* + q\boldsymbol{t}_i$, onde $\boldsymbol{c}_i^*$ é uma linha de $\boldsymbol{B}^*$ e ou $\boldsymbol{t}_i$ é $\boldsymbol{0}$ ou $(0, 0, \cdots, 0, -1)$. Então $\boldsymbol{x} = \sum_{i=1}^{k} a_i \boldsymbol{c}_i^* + q\left(\boldsymbol{s} + \boldsymbol{w} + \sum_{i=1}^{k} \boldsymbol{t}_i\right)$. Como $\sum_{i=1}^{n} a_i c_i^*$ é par, segue que $\left(\boldsymbol{s} + \boldsymbol{w} + \sum_{i=1}^{k} \boldsymbol{t}_i\right) \in D_n$. Notemos que a matriz

$$\boldsymbol{D}^{**} = \begin{pmatrix} q\boldsymbol{I}_{k\times k} & q\boldsymbol{B}^*_{k\times(n-k)} \\ \boldsymbol{0}_{(n-k)\times k} & \boldsymbol{D}^*_{(n-k)\times(n-k)} \end{pmatrix}$$

é uma matriz geradora para o reticulado qD_n. De fato, seja Λ o reticulado gerador por $\boldsymbol{D}^{**}$. É fácil ver que $\Lambda \subseteq qD_n$. Como $2q^n = \det(\Lambda) = q^n \det(D_n)$, segue que $\Lambda = qD_n$. Logo, $\boldsymbol{x}$ pode ser escrito como $\boldsymbol{x} = \boldsymbol{k}_1[\boldsymbol{I}_{k\times k} \mid \boldsymbol{B}^*_{k\times n-k}] + (\boldsymbol{k}_2{}^{(1)}, \boldsymbol{k}_2{}^{(2)})\boldsymbol{D}^* = (\boldsymbol{k}_1 + q\boldsymbol{k}_2^{(1)}, \boldsymbol{0} + \boldsymbol{k}_2^{(2)})\boldsymbol{N}$. □

Exemplo 6: Uma matriz geradora para o reticulado $2E_8$ do Exemplo 2 é dada por

$$\boldsymbol{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}. \quad (7)$$

Um reticulado obtido pela Construção B de um código q-ário nunca é q-ário pois $q\boldsymbol{e}_i \notin \Lambda_B(\boldsymbol{C})$ para todo $i = 1, \cdots, n$. A proposição seguinte mostra que tal reticulado é $2q$-ário pois pode ser visto como a Construção A de um código $2q$-ário.

Proposição 7: Se $\boldsymbol{C}_1 \subseteq \mathbb{Z}_q^n$ é um código q-ário, então $\Lambda_B(\boldsymbol{C}_1) = \Lambda_A(\boldsymbol{C}_2)$, onde $\boldsymbol{C}_2 \subseteq \mathbb{Z}_{2q}^n$ é o código $2q$-ário associado ao quociente $\Lambda_B(\boldsymbol{C}_1)/2q\mathbb{Z}^n$. Mais ainda, $\boldsymbol{C}_2$ é gerado pelas linhas de uma matriz geradora de $\Lambda_B(\boldsymbol{C}_1)$ reduzindo as entradas módulo $2q$.

Demonstração: Temos que $2q\mathbb{Z}^n \subseteq \Lambda_B(\boldsymbol{C}_1)$. Note que $\Lambda_B(\boldsymbol{C}_1)/2q\mathbb{Z}^n$ é um grupo e um conjunto de seus representantes de classe é dado pelos pontos de $\Lambda_B(\boldsymbol{C}_1)$ dentro do hipercubo $[0, 2q)^n$. Este conjunto pode ser identificado com um código $\boldsymbol{C}_2 \subseteq \mathbb{Z}_{2q}^n$. Então $\Lambda_A(\boldsymbol{C}_2) = \Lambda_B(\boldsymbol{C}_1)$. Agora, se $\{\boldsymbol{y}_i,\ i = 1, \cdots, n\}$ é uma base para $\Lambda_B(\boldsymbol{C}_1)$, então um conjunto de geradores para $\Lambda_B(\boldsymbol{C}_1)/2q\mathbb{Z}^n$ é dado por $\{\overline{\boldsymbol{y}}_{\boldsymbol{i}},\ i = 1, \cdots, n\}$, onde $\overline{\boldsymbol{y}}_{\boldsymbol{i}}$ é obtido de $\boldsymbol{y}_i$ por reduções módulo $2q$ em cada entrada. □

Exemplo 7: O reticulado $2E_8$ do Exemplo 2 pode ser visto como $\Lambda_A(\boldsymbol{C}_2)$ onde $\boldsymbol{C}_2 \subseteq \mathbb{Z}_4^8$ é o código gerado pelas linhas da matriz $\boldsymbol{G}$ de (7) com as entradas reduzidas módulo 4. Temos que $|\boldsymbol{C}| = \det(4\mathbb{Z}^8)^{1/2}/\det(\Lambda_B(\boldsymbol{C}))^{1/2} = 2^8$.

III. Decodificação em reticulados obtidos via Construção B

Nesta seção, apresentamos uma adaptação do algoritmo Sphere Decoding [6], [14] quando q é um número primo. A idéia do algoritmo "Sphere decoding" é a partir de um vetor $\boldsymbol{y} \in \mathbb{R}^n$ e um raio $\boldsymbol{R}$ encontrar os pontos do reticulado Λ que estão dentro da esfera centrada em $\boldsymbol{y}$ com raio $\boldsymbol{R}$. Após enumerar todos estes pontos do reticulado, encontramos o ponto mais próximo de $\boldsymbol{y}$.

Quando q é um número primo, pela Equação (6), temos que uma matriz geradora de um reticulado q-ário $\Lambda_B(\boldsymbol{C})$ é dada por $\boldsymbol{N}$.

Cada ponto $\boldsymbol{x} \in \Lambda_B(\boldsymbol{C})$ pode ser escrito como $\boldsymbol{x} = \boldsymbol{sN}$ para algum $\boldsymbol{s} \in \mathbb{Z}^n$. Fazendo $\boldsymbol{s} = (\boldsymbol{s}_1, \boldsymbol{s}_2) \in \mathbb{Z}^k \times \mathbb{Z}^{n-k}$, temos que

$$\boldsymbol{sN} = (\boldsymbol{s}_1, \boldsymbol{s}_1\boldsymbol{B}^* + q\boldsymbol{s}_2\boldsymbol{D}),$$

onde

$$\boldsymbol{D} = \begin{pmatrix} 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \\ 0 & 0 & 0 & \cdots & & 2 \end{pmatrix}$$

é uma matriz geradora do reticulado D_{n-k} (4).

Dado $\boldsymbol{y} \in \mathbb{R}^n$, note que

$$\|\boldsymbol{sN} - \boldsymbol{y}\|_1 = \|\boldsymbol{s}_1 - \boldsymbol{y}_1\|_1 + \|\boldsymbol{s}_1\boldsymbol{B}^* + q\boldsymbol{s}_2\boldsymbol{D} - \boldsymbol{y}_2\|_1. \quad (8)$$

Fixado $\boldsymbol{s}_1 \in \mathbb{Z}^k$, para encontrar $\boldsymbol{s}_2 \in \mathbb{Z}^{n-k}$ que minimiza (8), devemos decodificar o vetor $\frac{1}{q}(-\boldsymbol{s}_1\boldsymbol{B}^* + \boldsymbol{y}_2)$ em D_{n-k}. Essa é a idéia geral do algoritmo: primeiro, vamos encontrar $\boldsymbol{s}_1$ e a partir de $\boldsymbol{s}_1$ encontrarmos $\boldsymbol{s}_2$. Essa maneira de resolver o problema só é possível pela forma especial da matriz $\boldsymbol{N}$.

Dado um raio $\boldsymbol{R}$, vamos encontrar todos os vetores inteiros $\boldsymbol{s} \in \mathbb{Z}^n$ satisfazendo $||\boldsymbol{sN} - \boldsymbol{y}||_1 \leq \boldsymbol{R}$, isto é,

$$\begin{aligned} &\sum_{i=1}^{k} |s_i - y_i| + \left| \sum_{i=1}^{k} b_{i,k+1}^* s_i + s_{k+1}q - y_{k+1} \right| + \\ &\left| \sum_{i=1}^{k} b_{i,k+2}^* s_i - s_{k+1}q + s_{k+2}q - y_{k+2} \right| + \cdots + \\ &\left| \sum_{i=1}^{k} b_{i,n}^* s_i - s_{n-1}q + s_n 2q - y_n \right| \leq \boldsymbol{R}. \end{aligned} \quad (9)$$

Para as k primeiras parcelas da soma em (9), procederemos da seguinte forma: Para $k = 1$, temos a seguinte variação:

$$\lceil -\boldsymbol{R} + y_1 \rceil \leq s_1 \leq \lfloor \boldsymbol{R} + y_1 \rfloor.$$

Para $2 \leq j \leq k$, fixados valores para $s_1, \cdots, s_{j-1}$, e fazendo $R_j = R_{j-1} - |s_{j-1} - y_{j-1}|$, temos a seguinte variação:

$$\lceil -R_j + y_j \rceil \leq s_j \leq \lfloor R_j + y_j \rfloor.$$

Para $j > k$, não precisamos calcular todas as possibilidades de valores para $\boldsymbol{s}_2 = (s_{k+1}, \cdots, s_n)$ em $\mathbb{Z}^{n-k}$, sendo esse fato que introduz simplificações no algoritmo.

Para cada vetor $\boldsymbol{s}_1$ listado acima, temos que o vetor $\boldsymbol{s}_2$ que minimiza (8) é o vetor de D_{n-k} mais próximo de $\frac{1}{q}(-\boldsymbol{s}_1\boldsymbol{B}^* + \boldsymbol{y}_2)$. Para calcular tal vetor devemos proceder como na decodificação em D_n [3], que é feita da seguinte forma: primeiro decodificamos o vetor $\boldsymbol{s}_2$ em $\mathbb{Z}^{n-k}$ tomando

$$s_j = \left\lceil \frac{-\sum_{i=1}^{k} r_{i,j}s_i + y_j}{q} \right\rfloor,\ j = k+1, \cdots, n.$$

Se $\sum_{j=k+1}^{n} s_j$ for par, então $\boldsymbol{s}_2 \in D_{n-k}$. Caso contrário, calculamos os erros

$$e_j = \frac{-\sum_{i=1}^{k} r_{i,j}s_i + y_j}{q} - \left\lceil \frac{-\sum_{i=1}^{k} r_{i,j}s_i + y_j}{q} \right\rfloor$$

para $j = k+1, \cdots, n$ e encontramos o índice i tal que $|e_i| \geq |e_j|$ para todo j. A seguir, substituímos s_i por $s_i + 1$ se $e_i \geq 0$ ou por $s_i - 1$ se $e_i < 0$. O novo vetor $\boldsymbol{s}_2$ está em D_{n-k}.

Nem todo ponto $\boldsymbol{x} = \boldsymbol{sN}$ gerado pelo algoritmo satisfaz $\|\boldsymbol{sN} - \boldsymbol{y}\|_1 \leq \boldsymbol{R}$. Após gerarmos $\boldsymbol{s}_1$ para cada coordenada s_j de $\boldsymbol{s}_2$, gerada podemos testar se

$$t_j = \|(\boldsymbol{s}_1, s_{k+1}, \cdots, s_j)\boldsymbol{N}_{j\times n} - (y_1, \cdots, y_j)\|_1 \leq \boldsymbol{R}.$$

Se a desigualdade não for satisfeita com este valor de s_j, não será satisfeita com nenhum outro valor, pois este é o inteiro que minimiza o valor da parcela em que s_j aparece. Portanto, se a desigualdade for satisfeita continuamos testando os outros coeficientes.

Após gerar todos os caminhos da árvore, calculamos qual o ponto mais próximo de $\boldsymbol{y}$ entre as possibilidades encontradas. O cálculo das distâncias pode ser feito em conjunto com a geração da árvore a fim de economizar passos.

Observação 4: O algoritmo proposto nesta seção pode ser utilizado para códigos lineares $\boldsymbol{C} \subseteq \mathbb{Z}_q^n$ com q não necessariamente primo, desde que uma matriz geradora do código tenha forma similar à matriz $\boldsymbol{N}$ da Equação (6). Nesta seção, utilizamos q primo, pois neste caso o código sempre possui uma matriz geradora na forma requerida. No Exemplo 8 utilizamos o algoritmo para $q = 9$.

Exemplo 8: Seja $\boldsymbol{C}$ o código BCH 9-ário com matriz verificação de paridade

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 2 & 0 & 7 & 8 & 0 \\ 8 & 2 & 0 & 7 & 1 & 7 & 0 & 1 \\ 8 & 0 & 1 & 0 & 8 & 0 & 1 & 0 \\ 0 & 8 & 0 & 1 & 0 & 8 & 0 & 1 \\ 0 & 2 & 1 & 2 & 0 & 7 & 8 & 7 \\ 1 & 7 & 0 & 2 & 8 & 2 & 0 & 7 \end{pmatrix}$$

dado em [1]. Este código corrige todos os erros de Lee de peso até 3 [1]. Seja $\boldsymbol{y} = (1, 0, 0, 0, 5, 1, 1, 3)$ um vetor recebido e $R = 1$. A Figura 3 representa a árvore de pontos gerados pelo algoritmo para decodificar em $\Lambda_B(\boldsymbol{C})$ na métrica da soma.

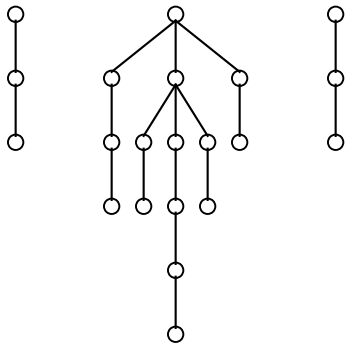

Fig. 3. Árvore representando o algoritmo Lee sphere decoding para o reticulado $\Lambda_B(\boldsymbol{C})$, $R = 1$ e $\boldsymbol{y} = (1, 0, 0, 0, 5, 1, 1, 3)$

REFERÊNCIAS

[1] A.A. Andrade, *Uma contribuição a construção e decodificação de codigos de bloco lineares sobre aneis finitos,* Tese de Doutorado, FEEC-UNICAMP, 1996.

[2] A.C. Campello, G.C. Jorge, S.I.R. Costa, *Decoding q-ary lattices in the Lee metric*, Proceedings of 2011 IEEE Information Theory Workshop, ISBN 978-4577.0436-9, disponível em IEEE-Xplore, Paraty, Brasil, 2011.

[3] J. H. Conway and N. J. A. Sloane *S*phere packings, lattices and groups. Springer-Verlag, New York, 3rd Ed. 1998.

[4] T. Etzion, A. Vardy and E. Yaakobi. Dense Error-Correcting Codes in the Lee Metric, *Proceedings of IEEE Information Theory Workshop* Dublin, Ireland, 2010.

[5] D. Guo, S. Shamai and S. Verdú, Additive Non-Gaussian Noise Channels: Mutual Information and Condition Mean Estimation, *IEEE International Symposium on Information Theory*, 2005.

[6] B. Hassibi, H. Vikalo, On the Sphere Decoding Algorithm I. Expected Complexity, *IEEE Transactions on Signal Processing*, vol.53, no.8, August, 2005.

[7] A. Hefes, M.L.T. Villela, "Códigos Corretores de Erros," IMPA, Rio De Janeiro, 2002.

[8] G.C. Jorge, "Reticulados q-ários e algébricos", Tese de Doutorado, IMECC-UNICAMP, 2012.

[9] D. Micciancio and O. Regev, Lattice-Based Cryptography in *P*ost Quantum Cryptography, Bernstein D.J., Buchmann J., Dahmen E. (eds), pp. 147-191, Springer, 2009.

[10] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems; A Cryptographic Perspective*, The Kluwer International Series in Engineering and Computer Science, vol. 671. Kluwer Academic Publishers, 2002.

[11] J. A. Rush and N.J.A. Sloane An improvement to the Minkowski-Hlawka bound for packing superballs, *Mathematika*, vol. 34, pp. 8-18, 1987.

[12] I.N. Stewart, D.O. Tall, *Algebraic Number Theory*, London: Chapman & Hall, 1987.

[13] K. Takizawa, H. Yagi, T. Kawabata, Closest Point Algorithms with l_p Norm for Root Lattices, *Proceedigns of IEEE International Symposium on Information Theory*,Austin, Texas, pp. 1042-1046, 2010

[14] E. Viterbo and J. Boutros, A universal lattice code decoder for fading channels, *IEEE Transactions on Information Theory*, vol.45, no.5, July 1999.

[15] R. Zamir, "Lattices are everywhere", in Proceedings of the 4th Annual Workshop on Information Theory and its Applications (ITA 2009), (La Jolla, CA), February 2009.