Limitantes para a distância da soma em reticulados obtidos via Construção D e suas variações

Eleonesio Strey e Sueli I. R. Costa

***Resumo*— Reticulados vem sendo utilizados na abordagem de vários problemas em Teoria de Códigos e Criptografia. Neste trabalho, abordamos as Construções D, D′ and $\overline{\text{D}}$, fornecemos cotas inferiores e superiores para a distância mínima em relação à métrica da soma do reticulado $\Lambda_{D'}$ em função das distâncias dos códigos lineares utilizados em sua construção. Também apresentamos, quando a cadeia de códigos usada é fechada sob a adição zero-um, expressões para as distâncias mínimas em relação à métrica da soma dos reticulados $\Lambda_{\overline{D}}$ e Λ_D em função das distâncias dos códigos utilizados em suas respectivas construções.**

***Palavras-Chave*— Reticulados, Códigos q-ários, Construção D, Métrica de Lee.**

I. Introdução

Um *código linear q-ário* C de comprimento n é um subgrupo aditivo de $\mathbb{Z}_q^n$, no qual $q \in \mathbb{N}$ e $\mathbb{Z}_q$ é o grupo dos inteiros módulo q. Se q é primo, então C pode ser visto como um subespaço vetorial de $\mathbb{Z}_q^n$ e, consequentemente, possui uma base com $m \leq n$ vetores. Caso contrário, podemos apenas garantir a existência de um conjunto minimal de geradores. Por exemplo, o código linear $C = \langle (2,4) \rangle = \{(0,0),(2,4),(4,2)\} \subseteq \mathbb{Z}_6^2$ não possui base, uma vez que todo subconjunto não vazio de C é linearmente dependente. Para cada par de vetores $\boldsymbol{x} = (x_1, ..., x_n)$ e $\boldsymbol{y} = (y_1, ..., y_n)$ em $\mathbb{Z}_q^n$, o *produto interno* de $\boldsymbol{x}$ e $\boldsymbol{y}$ é definido como $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = x_1y_1 + \cdots + x_ny_n$. $C^\perp = \{\boldsymbol{y} \in \mathbb{Z}_q^n;\ \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0, \forall \boldsymbol{x} \in C\}$ é um código linear q-ário, denominado o *código dual* de C. Se C_1 e C_2 são códigos lineares q-ários tais que $C_1 \supseteq C_2$, então $C_1^\perp \subseteq C_2^\perp$.

Um *reticulado* Λ é um subgrupo aditivo discreto de $\mathbb{R}^n$. Equivalentemente, $\Lambda \subseteq \mathbb{R}^n$ é um reticulado se e somente se existem vetores linearmente independentes $\boldsymbol{v}_1, ..., \boldsymbol{v}_m \in \mathbb{R}^n$ tais que Λ é o conjunto de todas as combinações lineares inteiras de $\boldsymbol{v}_i$, $i = 1, ..., m$, isto é,

$$\Lambda = \{\alpha_1 \boldsymbol{v}_1 + \cdots + \alpha_m \boldsymbol{v}_m;\ \alpha_1, ..., \alpha_m \in \mathbb{Z}\}.$$

Reticulados vem sendo utilizados na área de comunicações em códigos corretores de erros para a transmissão de dados (ver por exemplo [20], [21] e suas referências) e também na proposição de esquemas criptográficos [10], [11]. Na descrição acima, o conjunto $\{\boldsymbol{v}_1, ..., \boldsymbol{v}_m\}$ é dito uma *base* de Λ e o número m é denominado o *posto* de Λ. Se $m = n$ dizemos que Λ possui *posto completo*. A matriz M cujas linhas são os vetores $\boldsymbol{v}_1, ..., \boldsymbol{v}_m$ é dita uma *matriz geradora* de Λ. M_1 e M_2 são matrizes geradoras de um mesmo reticulado se, e somente se, existe uma matriz unimodular U (com entradas inteiras e $\det(U) = \pm 1$) tal que $M_2 = UM_1$. O *determinante* de Λ é definido como $\det \Lambda = \det(MM^t)$ e este é um invariante por mudança de base. O *volume* de Λ é definido como $\text{vol}(\Lambda) = \sqrt{\det \Lambda}$, este valor corresponde ao volume euclidiano do paralelotopo $P = \{\sum_{i=1}^n \alpha_i \boldsymbol{v}_i |\ 0 \leq \alpha_i < 1\}$, uma região fundamental de Λ.

Um *empacotamento reticulado* no $\mathbb{R}^n$ é uma coleção de esferas no $\mathbb{R}^n$, todas de mesmo raio de modo que o conjunto dos centros formam um reticulado e as esferas satisfazem a seguinte condição: quaisquer duas esferas ou não se interceptam ou se interceptam no bordo. O *raio de empacotamento* ρ de um reticulado Λ, em relação a uma métrica d, é o maior número real r tal que $\Lambda + B_d[\boldsymbol{0}, r]$ é um empacotamento reticulado, em que $B_d[\boldsymbol{0}, r]$ é a bola fechada de centro na origem e raio r na métrica d. Pode-se mostrar que $\rho = \lambda/2$, em que λ é o valor da distância mínima de Λ na métrica d, isto é,

$$\lambda = \min_{\boldsymbol{0} \neq \boldsymbol{x} \in \Lambda} d(\boldsymbol{x}, \boldsymbol{0}).$$

A *densidade de empacotamento* de um reticulado Λ de posto n em relação a uma métrica d é dada por

$$\Delta_d(\Lambda) = \frac{\text{vol}(B_d[\boldsymbol{0}, \rho])}{\text{vol}(\Lambda)} = \frac{\text{vol}(B_d[\boldsymbol{0}, 1])\rho^n}{\sqrt{\det \Lambda}},$$

em que $\text{vol}(B_d[\boldsymbol{0}, \rho])$ representa o volume euclidiano da bola $B_d[\boldsymbol{0}, \rho]$. A *densidade de centro* de um reticulado Λ de posto n em relação a métrica d é o número $\delta_d(\Lambda) = \rho^n/\text{vol}(\Lambda)$. Em cada dimensão, fixada uma métrica d, busca-se pelo reticulado com a maior densidade possível e são poucas as dimensões em que tais reticulados são conhecidos. Por exemplo, na métrica euclidiana são conhecidos os reticulados mais densos nas dimensões de 1 até 8 [4] e na dimensão 24 [3], e na métrica da soma são conhecidos apenas os reticulados mais densos nas dimensões $1, 2$ e 3 [6].

A *distância da soma* (também conhecida como *distância l_1* ou *distância de Manhattan*) entre dois elementos $\boldsymbol{x}$ e $\boldsymbol{y}$ de $\mathbb{R}^n$ é dada por

$$d^1(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\|_1 = \sum_{i=1}^n |x_i - y_i|.$$

Pode-se mostrar que se d é a distância da soma, então $\text{vol}(B_d[\boldsymbol{0}, 1]) = 2^n/n!$ [12]. Dados $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_q^n$, a *distância de Lee* entre $\boldsymbol{x}$ e $\boldsymbol{y}$ é definida como

$$d_{Lee}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^n \min\{\sigma(x_i - y_i), q - \sigma(x_i - y_i)\},$$

Departamento de Matemática Pura e Aplicada, UFES, Alegre-ES, Brasil (Eleonesio Strey) e Departamento de Matemática, IMECC-Unicamp, Campinas-SP, Brasil (Sueli I. R. Costa). E-mails: eleonesio.strey@ufes.br, sueli@ime.unicamp.br. Este trabalho foi parcialmente financiado por FAPESP 2013/25997-7 e CNPq 312926/2013-8.

sendo $\sigma : \mathbb{Z}_q \to \mathbb{Z}$ a inclusão natural. A *distância mínima de Lee* de um código linear não nulo $C \subseteq \mathbb{Z}_q^n$ é definida por

$$d_{Lee}(C) = \min_{\mathbf{0} \neq \boldsymbol{x} \in C} d_{Lee}(\boldsymbol{x}, \mathbf{0}).$$

A métrica de Lee foi introduzida em [9] e [18] na abordagem da transmissão de sinais em determinados canais com ruído. Recentes aplicações na área de comunicações podem ser encontradas, por exemplo, em [7] e suas referências.

Existem várias construções envolvendo códigos lineares q-ários e reticulados, como por exemplo a Construção A [4] e as Construções D, D$'$ e $\overline{\text{D}}$ [17]. Estas construções e a métrica da soma aparecem em trabalhos recentes tais como [1], [2], [5], [6], [7], [8], [13], [14], [15] e [19]. Neste artigo, estudamos as distâncias mínimas em relação à métrica da soma dos reticulados Λ_D, $\Lambda_{D'}$ e $\Lambda_{\overline{D}}$ obtidos a partir das Construções D, D$'$ e $\overline{\text{D}}$, respectivamente. Na seção II, apresentamos as construções citadas acima e também alguns resultados preliminares. Apresentamos os resultados obtidos sobre as distâncias mínimas dos reticulados Λ_D, $\Lambda_{D'}$ e $\Lambda_{\overline{D}}$ na seção III. Por fim, na seção IV apresentamos nossas observações finais.

II. Conceitos e resultados preliminares

Sejam $\sigma : \mathbb{Z}_q \to \mathbb{Z}$ a inclusão natural e $\overline{\sigma} : \mathbb{Z} \to \mathbb{Z}_q$ o homomorfismo módulo q. Definimos $\sigma : \mathbb{Z}_q^n \to \mathbb{Z}^n$ e $\overline{\sigma} : \mathbb{Z}^n \to \mathbb{Z}_q^n$ da seguinte forma: $\sigma(x_1, ..., x_n) = \big(\sigma(x_1), ..., \sigma(x_n)\big)$ e $\overline{\sigma}(x_1, ..., x_n) = \big(\overline{\sigma}(x_1), ..., \overline{\sigma}(x_n)\big)$. Por simplicidade, em alguns casos, escrevemos $\overline{x}$ ao invés de $\overline{\sigma}(x)$.

Definição 1: (Construção A) Dado um código linear $C \subseteq \mathbb{Z}_q^n$, definimos o conjunto $\Lambda_A(C)$ da seguinte forma

$$\Lambda_A(C) = q\mathbb{Z}^n + \sigma(C).$$

O conjunto $\Lambda_A(C)$ obtido via Construção A a partir de um código linear q-ário é sempre um reticulado de posto completo [20, p. 31].

Exemplo 1: Considere o código linear

$$C = \langle (1, 36, 3), (0, 37, 7) \rangle \subseteq \mathbb{Z}_{38}^3$$

e o reticulado $\Lambda_A(C) = 38\mathbb{Z}^3 + \sigma(C)$. É fácil ver que

$$\begin{bmatrix} 1 & 36 & 3 \\ 0 & -1 & 7 \\ 0 & 0 & 38 \end{bmatrix}$$

é uma matriz geradora para $\Lambda_A(C)$. Logo a matriz

$$M = \begin{bmatrix} 1 & 38 & -7 \\ -2 & -75 & 14 \\ 3 & 107 & -20 \end{bmatrix} \begin{bmatrix} 1 & 36 & 3 \\ 0 & -1 & 7 \\ 0 & 0 & 38 \end{bmatrix},$$

isto é,

$$M = \begin{bmatrix} 1 & -2 & 3 \\ -2 & 3 & 1 \\ 3 & 1 & -2 \end{bmatrix}$$

é também uma matriz geradora para $\Lambda_A(C)$, uma vez que

$$\begin{bmatrix} 1 & 38 & -7 \\ -2 & -75 & 14 \\ 3 & 107 & -20 \end{bmatrix}$$

é uma matriz unimodular. Em [12] foi mostrado que a densidade de $\Lambda(M)$ (e portanto de $\Lambda_A(C)$) em relação à métrica da soma é $18/19$ e que esta é a maior densidade possível em relação à métrica da soma no $\mathbb{R}^3$.

Dado um código linear não nulo $C \subseteq \mathbb{Z}_q^n$, temos que

$$d_{\min}^1\big(\Lambda_A(C)\big) = \min\big\{q, d_{Lee}(C)\big\} \tag{1}$$

é a distância mínima em relação à métrica da soma do reticulado $\Lambda_A(C)$ [16].

Definição 2: (Construção D) Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$, $q \in \mathbb{N}$, uma cadeia de códigos lineares. Dados números inteiros $k_1 \geq k_2 \geq \cdots \geq k_a \geq 0$ e vetores $\boldsymbol{b}_1, ..., \boldsymbol{b}_{k_1}$ em $\mathbb{Z}_q^n$ tais que $C_\ell = \langle \boldsymbol{b}_1, ..., \boldsymbol{b}_{k_\ell} \rangle$, para $\ell = 1, 2, ..., a$. O conjunto Λ_D consiste de todos os vetores da forma

$$q\boldsymbol{z} + \sum_{\ell=1}^{a} \sum_{j=1}^{k_\ell} \beta_j^{(\ell)} \frac{1}{q^{\ell-1}} \sigma(\boldsymbol{b}_j),$$

em que $\boldsymbol{z} \in \mathbb{Z}^n$ e $\beta_j^{(\ell)} \in \{0, 1, ..., q-1\}$.

Pode-se mostrar que Λ_D consiste de todos os vetores da forma

$$q\boldsymbol{z} + \sum_{i=1}^{a} \sum_{j=k_{i+1}+1}^{k_i} \alpha_j^{(i)} \frac{1}{q^{i-1}} \sigma(\boldsymbol{b}_j), \tag{2}$$

em que $\boldsymbol{z} \in \mathbb{Z}^n$ e $\alpha_j^{(i)} \in \{0, 1, ..., q^i - 1\}$. O conjunto Λ_D é um reticulado de posto completo [17]. Quando $a = 1$, temos que $\Lambda_D = \Lambda_A(C_1)$.

Definição 3: (Construção D$'$) Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ uma cadeia de códigos lineares q-ários. Dados números inteiros $r_1, r_2, ..., r_a$ satisfazendo $0 \leq r_1 \leq r_2 \leq \cdots \leq r_a$ e vetores $\boldsymbol{h}_1, ..., \boldsymbol{h}_{r_a}$ em $\mathbb{Z}_q^n$ tais que $C_\ell^\perp = \langle \boldsymbol{h}_1, ..., \boldsymbol{h}_{r_\ell} \rangle$ para $\ell = 1, 2, ..., a$, em que $C_\ell^\perp$ é o código dual de C_ℓ. O conjunto $\Lambda_{D'}$ consiste de todos os vetores $\boldsymbol{x} \in \mathbb{Z}^n$ tais que

$$\boldsymbol{x} \cdot \sigma(\boldsymbol{h}_j) \equiv 0 \mod q^{i+1}$$

para $0 \leq i < a$ e $r_{a-i-1} < j \leq r_{a-i}$, em que $r_0 = 0$.

O conjunto $\Lambda_{D'}$ sempre é um reticulado de posto completo [17]. Quando $a = 1$, temos que $\Lambda_{D'} = \Lambda_A(C_1)$.

Definição 4: (Construção $\overline{\text{D}}$) Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq \cdots \supseteq C_a$ uma cadeia de códigos lineares. O conjunto $\Gamma_{\overline{D}}$ é definido da seguinte forma

$$\Gamma_{\overline{D}} = q^a\mathbb{Z}^n + q^{a-1}\sigma(C_1) + \cdots + q^1\sigma(C_{a-1}) + \sigma(C_a).$$

Quando $a = 1$, temos que $\Gamma_{\overline{D}} = \Lambda_A(C_1)$ e, neste caso, $\Gamma_{\overline{D}}$ é um reticulado. Para $a \geq 2$, temos que $\Gamma_{\overline{D}}$ é um conjunto discreto, mas nem sempre é um reticulado. Dada uma cadeia de códigos lineares $\mathbb{Z}_q^n \supseteq C_1 \supseteq \cdots \supseteq C_a$, denotamos por $\Lambda_{\overline{D}}$ o menor reticulado que contém o conjunto $\Gamma_{\overline{D}}$ (Definição 4). Em outras palavras, $\Lambda_{\overline{D}}$ é o reticulado que contém $\Gamma_{\overline{D}}$ e satisfaz a seguinte propriedade: Se Λ é um reticulado em $\mathbb{R}^n$ que contém $\Gamma_{\overline{D}}$, então $\Lambda_{\overline{D}} \subseteq \Lambda$. Observe que quando $\Gamma_{\overline{D}}$ é um reticulado, temos $\Lambda_{\overline{D}} = \Gamma_{\overline{D}}$.

Para cada par de vetores $\boldsymbol{x} = (x_1, ..., x_n)$ e $\boldsymbol{y} = (y_1, ..., y_n)$ em $\mathbb{Z}_q^n$, a *adição zero-um* de $\boldsymbol{x}$ por $\boldsymbol{y}$ é dada por

$$\boldsymbol{x} * \boldsymbol{y} := (x_1 * y_1, ..., x_n * y_n) \in \mathbb{Z}_q^n,$$

sendo

$$x_i * y_i = \begin{cases} 0, & \text{se } \sigma(x_i)+\sigma(y_i) < q \\ 1, & \text{se } \sigma(x_i)+\sigma(y_i) \geq q. \end{cases}$$

Uma cadeia de códigos lineares $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ é dita *fechada sob a adição zero-um* quando a adição zero-um de dois elementos quaisquer de C_i sempre pertence a C_{i-1}, para $i = 2, ..., a$. Em [17], mostramos que $\Gamma_{\overline{D}}$ é um reticulado se, e somente se, a cadeia $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ é fechada sob a adição zero-um. Neste caso, $\Gamma_{\overline{D}} = q^{a-1}\Lambda_D$.

III. RESULTADOS

Nesta seção, apresentamos resultados que obtivemos sobre as distâncias mínimas (em relação à métrica da soma) dos reticulados $\Lambda_D, \Lambda_{D'}$ e $\Lambda_{\overline{D}}$.

Teorema 1: Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\mathbf{0}\}$ uma cadeia de códigos lineares fechada sob a adição zero-um e seja $\Lambda_{\overline{D}}$ o reticulado obtido via Construção $\overline{D}$ a partir desta cadeia. Se a distância de Lee mínima em C_ℓ é d_{Lee}^ℓ, para $\ell = 1, 2, ...a$, então

$$d^1_{\min}(\Lambda_{\overline{D}}) = \min\{q^a, q^{a-1}d^1_{Lee}, ..., d^a_{Lee}\}.$$

Demonstração: Para cada $k \in \{1, 2, ..., a\}$, seja o conjunto

$$\Lambda_k = q^k\mathbb{Z}^n + q^{k-1}\sigma(C_1) + \cdots + q^1\sigma(C_{k-1}) + \sigma(C_k).$$

Temos que Λ_k é um reticulado, pois a cadeia $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_k$ é fechada sob a adição zero-um. Vamos mostrar por indução sobre k que

$$d^1_{\min}(\Lambda_k) \leq \min\{q^k, q^{k-1}d^1_{Lee}, ..., d^k_{Lee}\}, \tag{3}$$

para $k = 1, 2, ..., a$. Com efeito, a desigualdade (3) é verdadeira para $k = 1$, uma vez que $\Lambda_1 = \Lambda_A(C_1)$ e

$$d^1_{\min}\big(\Lambda_A(C_1)\big) = \min\{q, d^1_{Lee}\}.$$

Suponha que $d^1_{\min}(\Lambda_k) \leq \min\{q^k, q^{k-1}d^1_{Lee}, ..., d^k_{Lee}\}$, para algum $1 \leq k < a$. Como $q\Lambda_k \subseteq \Lambda_{k+1}$, segue que

$$d^1_{\min}(\Lambda_{k+1}) \leq \min\{q^{k+1}, q^k d^1_{Lee}, ..., q d^k_{Lee}\}. \tag{4}$$

Agora, sejam $\overline{\boldsymbol{x}} \in C_{k+1}$ tal que $d_{Lee}(\overline{\boldsymbol{x}}, \overline{\mathbf{0}}) = d^{k+1}_{Lee}$ e o vetor $\boldsymbol{v} = \sigma(\overline{\boldsymbol{x}}) - q\sigma(\overline{\boldsymbol{z}})$, em que $\overline{\boldsymbol{z}} = (\overline{z}_1, ..., \overline{z}_n)$ e

$$\overline{z}_i = \begin{cases} \overline{0}, & \text{se } \sigma(\overline{x}_i) < q/2 \\ \overline{1}, & \text{se } \sigma(\overline{x}_i) \geq q/2. \end{cases}$$

Como $\overline{\boldsymbol{z}} = \overline{\boldsymbol{x}} * \overline{\boldsymbol{x}}$, $\overline{\boldsymbol{x}} \in C_{k+1}$ e a cadeia $C_k \supseteq C_{k+1}$ é fechada sob a adição zero-um, segue que $\overline{\boldsymbol{z}} \in C_k$. Logo $\boldsymbol{v} \in \Lambda_{k+1}$, uma vez que Λ_{k+1} é um reticulado e $\sigma(\overline{\boldsymbol{x}}), q\sigma(\overline{\boldsymbol{z}}) \in \Lambda_{k+1}$. Além disso,

$$\begin{aligned} \|\boldsymbol{v}\|_1 &= \sum_{i=1}^n |v_i| = \sum_{i=1}^n |\sigma(\overline{x}_i) - q\sigma(\overline{z}_i)| \\ &= \sum_{i=1}^n \min\{\sigma(\overline{x}_i), q - \sigma(\overline{x}_i)\} = d^{k+1}_{Lee} \end{aligned}$$

e consequentemente $d^1_{\min}(\Lambda_{k+1}) \leq d^{k+1}_{Lee}$. Usando a desigualdade (4), obtemos

$$d^1_{\min}(\Lambda_{k+1}) \leq \min\{q^{k+1}, q^k d^1_{Lee}, ..., q d^k_{Lee}, d^{k+1}_{Lee}\}.$$

Isto mostra que $d^1_{\min}(\Lambda_{\overline{D}}) \leq \min\{q^a, q^{a-1}d^1_{Lee}, ..., d^a_{Lee}\}$.

Dado $\mathbf{0} \neq \boldsymbol{y} \in \Lambda_{\overline{D}}$, podemos escrever $\boldsymbol{y} = q^\ell \boldsymbol{x}$ com $\boldsymbol{x} \in \mathbb{Z}^n$ e $\boldsymbol{x} \not\equiv \mathbf{0} \mod q$. Vamos dividir em dois casos: (i) Se $\ell \geq a$ então

$$d^1(\boldsymbol{y}, \mathbf{0}) = q^\ell d^1(\boldsymbol{x}, \mathbf{0}) \geq q^a, \text{ pois } \mathbf{0} \neq \boldsymbol{x} \in \mathbb{Z}^n.$$

(ii) Se $0 \leq \ell \leq a-1$, então existem $\boldsymbol{c}_i \in C_i$, $i = 1, ..., \ell$, e $\boldsymbol{z} \in \mathbb{Z}^n$ tais que $\boldsymbol{y} = q^a\boldsymbol{z} + q^{a-1}\sigma(\boldsymbol{c}_1) + \cdots + q^\ell\sigma(\boldsymbol{c}_{a-\ell})$ (pois $\Lambda_{\overline{D}} = \Gamma_{\overline{D}}$) e logo $\boldsymbol{x} = q^{a-\ell}\boldsymbol{z} + q^{a-1-\ell}\sigma(\boldsymbol{c}_1) + \cdots + q^0\sigma(\boldsymbol{c}_{a-\ell})$. Temos que $\overline{\mathbf{0}} \neq \overline{\boldsymbol{x}} \in C_{a-\ell}$ e consequentemente

$$d^1(\boldsymbol{x}, \mathbf{0}) = \sum_{i=1}^n |x_i| \geq \sum_{i=1}^n \min\{\sigma(\overline{x}_i), q - \sigma(\overline{x}_i)\} \geq d^{a-\ell}_{Lee},$$

pois $|x_i| \geq \min\{\sigma(\overline{x}_i), q - \sigma(\overline{x}_i)\}$, $i = 1, ..., n$. Logo

$$d^1(\boldsymbol{y}, \mathbf{0}) = q^\ell d^1(\boldsymbol{x}, \mathbf{0}) \geq q^\ell d^{a-\ell}_{Lee}.$$

Portanto $d^1_{\min}(\Lambda_{\overline{D}}) \geq \min\{q^a, q^{a-1}d^1_{Lee}, ..., d^a_{Lee}\}$. ■

Acreditamos que o Teorema 1 possa ser refinado, retirando-se a hipótese de que a cadeia $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ é fechada sob a adição zero-um. Propomos, portanto, a seguinte conjectura:

Conjectura 1: Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\mathbf{0}\}$ uma cadeia de códigos lineares e seja $\Lambda_{\overline{D}}$ o reticulado obtido via Construção $\overline{D}$ a partir desta cadeia. Se a distância de Lee mínima em C_ℓ é d_{Lee}^ℓ, para $\ell = 1, 2, ...a$, então

$$d^1_{\min}(\Lambda_{\overline{D}}) = \min\{q^a, q^{a-1}d^1_{Lee}, ..., d^a_{Lee}\}.$$

Corolário 1: Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\mathbf{0}\}$ uma cadeia de códigos lineares fechada sob a adição zero-um e seja Λ_D o reticulado obtido via Construção D a partir desta cadeia. Se a distância de Lee mínima em C_ℓ é d_{Lee}^ℓ, para $\ell = 1, 2, ...a$, então

$$d^1_{\min}(\Lambda_D) = \min_{1 \leq \ell \leq a} \left\{ q, \frac{1}{q^{\ell-1}} d^\ell_{Lee} \right\}.$$

Demonstração: Como a cadeia de códigos usada é fechada sob a adição zero-um, temos que $q^{a-1}\Lambda_D = \Lambda_{\overline{D}}$ e logo $d^1_{\min}(\Lambda_D) = (1/q^{a-1}) \min\{q^a, q^{a-1}d^1_{Lee}, ..., d^a_{Lee}\}$. ■

No exemplo a seguir mostramos que a condição de que a cadeia de códigos lineares utilizada na Construção D é fechada sob a adição zero-um não pode ser omitida no Corolário 1.

Exemplo 2: Seja $\mathbb{Z}_3^2 \supseteq C_1 \supseteq C_2$ a cadeia de códigos lineares, na qual $C_1 = C_2 = \langle(1, 2)\rangle$. Escolhendo os parâmetros $k_1 = 2, k_2 = 1$ e $\boldsymbol{b}_1 = (1, 2), \boldsymbol{b}_2 = (2, 1) \in \mathbb{Z}_3^2$, temos $0 \leq k_2 \leq k_1$, $C_1 = \langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle$, $C_2 = \langle \boldsymbol{b}_1 \rangle$ e, consequentemente, Λ_D consiste de todos os vetores da forma

$$z + \alpha_2^{(1)}(2, 1) + \alpha_1^{(2)}\frac{1}{3}(1, 2),$$

em que $z \in 3\mathbb{Z}^2, 0 \leq \alpha_2^{(1)} < 3$ e $0 \leq \alpha_1^{(2)} < 9$. Portanto,

$$\Lambda_D = \bigcup_{\boldsymbol{z} \in 3\mathbb{Z}^2} \big(\boldsymbol{z} + \Lambda_D \cap [0, 3)^2\big).$$

Os elementos de $\Lambda_D \cap [0, 3)^2$ estão representados na Figura 1. Neste exemplo, observamos que $d^1_{Lee} = d^2_{Lee} = 2$, $d^1_{\min}(\Lambda_D) = 1$,

$$\min_{1 \leq \ell \leq 2} \left\{ 3, \frac{1}{3^{\ell-1}} d^\ell_{Lee} \right\} = \frac{2}{3}$$

e que a cadeia $C_1 \supseteq C_2$ não é fechada sob a adição zero-um, uma vez que $(1,2) \in C_2$ e $(1,2) * (1,2) = (0,1) \notin C_1$.

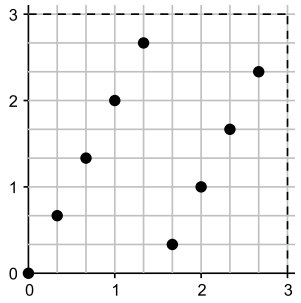

Fig. 1. Elementos de Λ_D na caixa $[0,3)^2$.

Observe que o Exemplo 2 não contradiz a Conjectura 1. De fato, temos que $\Gamma_{\overline{D}} = 3^2\mathbb{Z}^2 + 3^1\sigma(C_1) + 3^0\sigma(C_2)$ com $\sigma(C_1) = \sigma(C_2) = \{(0,0),(1,2),(2,1)\}$, isto é,

$$\Gamma_{\overline{D}} = 3^2\mathbb{Z}^2 + \Gamma_{\overline{D}} \cap [0,9)^2$$

e

$$\begin{aligned}\Gamma_{\overline{D}} \cap [0,9)^2 \quad &= \quad \{(0,0),(3,6),(6,3),(1,2),(4,8),\\ &\quad\ (7,5),(2,1),(5,7),(8,4)\}.\end{aligned}$$

Os elementos de $\Gamma_{\overline{D}} \cap [0,9)^2$ estão representados na Figura 2. Note que $\Gamma_{\overline{D}}$ não é um reticulado (evidentemente este resultado não poderia ser diferente, pois a cadeia utilizada nessa construção não é fechada sob a adição zero-um). Na Figura 3, temos o reticulado $\Lambda_{\overline{D}}$ (isto é, o menor reticulado que contém $\Gamma_{\overline{D}}$). Observe que $d^1_{\min}(\Lambda_{\overline{D}}) = 2$ (ver Figura 3) e $\min\{3^2, 3d^1_{Lee}, d^2_{Lee}\} = \min\{9,6,2\} = 2$. Isto mostra que o Exemplo 2 está de acordo com a Conjectura 1.

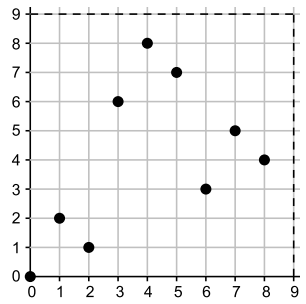

Fig. 2. Elementos de $\Gamma_{\overline{D}}$ na caixa $[0,9)^2$.

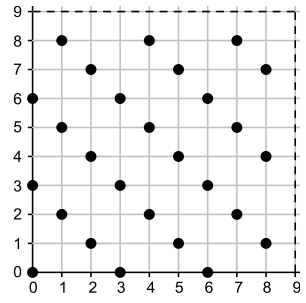

Fig. 3. Elementos de $\Lambda_{\overline{D}}$ na caixa $[0,9)^2$.

Corolário 2: Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\mathbf{0}\}$ uma cadeia de códigos lineares fechada sob a adição zero-um. Se a distância mínima d^ℓ_{Lee} de C_ℓ satisfaz $d^\ell_{Lee} \geq q^\ell$, $\ell = 1,2,...a$, então $d^1_{\min}(\Lambda_{\overline{D}}) = q^a$ e $d^1_{\min}(\Lambda_D) = q$.

Demonstração: Basta observar que $q^{a-\ell}d^\ell_{Lee} \geq q^a$ e $(1/q^{\ell-1})d^\ell_{Lee} \geq q$, para $\ell = 1,2,...,a$. Assim, aplicando o Teorema 1 e o Corolário 1, obtemos $d^1_{\min}(\Lambda_{\overline{D}}) = \min\{q^a, q^{a-1}d^1_{Lee}, ..., d^a_{Lee}\} = q^a$ e $d^1_{\min}(\Lambda_D) = q$. ■

Corolário 3: Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\mathbf{0}\}$ uma cadeia de códigos lineares fechada sob a adição zero-um. Suponhamos que os vetores $\boldsymbol{b}_1, ..., \boldsymbol{b}_{k_1} \in \mathbb{Z}_q^n$ usados na Construção D sejam não nulos e satisfaçam:

1) Alguma permutação das linhas da matriz $[\sigma(\boldsymbol{b}_1)\cdots\sigma(\boldsymbol{b}_{k_1})]^t$ forma uma matriz triangular superior (resp. inferior) na forma escalonada.
2) Para cada $j \in \{1,...,k_1\}$, a primeira (resp. última) componente não nula do vetor $\sigma(\boldsymbol{b}_j)$, denotada por α_j, divide q e todas as demais componentes do mesmo.

Para $\lambda = \min_{1\leq\ell\leq a}\{q, (1/q^{\ell-1})d^\ell_{Lee}\}$, em que d^ℓ_{Lee} é a distância de Lee mínima em C_ℓ, $\ell = 1,2,...a$, temos que a densidade de Λ_D na métrica da soma é dada por

$$\Delta_1(\Lambda_{\overline{D}}) = \Delta_1(\Lambda_D) = \frac{\lambda^n q^{\sum_{\ell=1}^a k_\ell - n}}{n!\prod_{i=1}^{k_1}\alpha_i} \tag{5}$$

e a densidade de centro

$$\delta_1(\Lambda_{\overline{D}}) = \delta_1(\Lambda_D) = \frac{\lambda^n q^{\sum_{\ell=1}^a k_\ell - n}}{2^n\prod_{i=1}^{k_1}\alpha_i}. \tag{6}$$

Além disso, temos que $d^\ell_{Lee} \geq q^\ell$ se e somente se

$$\Delta_1(\Lambda_D) = \frac{q^{\sum_{\ell=1}^a k_\ell}}{n!\prod_{i=1}^{k_1}\alpha_i} \quad \text{e} \quad \delta_1(\Lambda_D) = \frac{q^{\sum_{\ell=1}^a k_\ell}}{2^n\prod_{i=1}^{k_1}\alpha_i}. \tag{7}$$

Demonstração: Segue imediatamente do Teorema 1 e de [17, Teorema 6]. ■

No exemplo a seguir mostramos que a condição de que a cadeia de códigos lineares é fechada sob a adição zero-um não pode ser omitida no Corolário 3.

Exemplo 3: Seja $\mathbb{Z}_6^2 \supseteq C_1 \supseteq C_2$ a cadeia de códigos lineares com $C_1 = \langle(4,2),(3,0)\rangle$ e $C_2 = \langle(4,2)\rangle$. Escolhendo $k_1 = 2, k_2 = 1$ e $\boldsymbol{b}_1 = (4,2), \boldsymbol{b}_2 = (3,0) \in \mathbb{Z}_6^2$, temos $0 \leq k_2 \leq k_1$, $C_1 = \langle\boldsymbol{b}_1, \boldsymbol{b}_2\rangle$, $C_2 = \langle\boldsymbol{b}_1\rangle$ e, consequentemente, Λ_D consiste de todos os vetores da forma

$$\boldsymbol{z} + \alpha_2^{(1)}(3,0) + \alpha_1^{(2)}\frac{1}{6}(4,2),$$

em que $\boldsymbol{z} \in 6\mathbb{Z}^2, 0 \leq \alpha_2^{(1)} < 6$ e $0 \leq \alpha_1^{(2)} < 36$. Observe que $d^1_{Lee} = 3$, $d^2_{Lee} = 4$ e os vetores $\boldsymbol{b}_1$ e $\boldsymbol{b}_2$ são não nulos e satisfazem as hipóteses 1 e 2 do Corolário 3. Considere também o conjunto

$$\Gamma_{\overline{D}} = 36\mathbb{Z}^2 + 6\sigma(C_1) + \sigma(C_2)$$

e o reticulado $\Lambda_{\overline{D}}$ (menor reticulado que contém $\Gamma_{\overline{D}}$). Pode-se mostrar que $\Delta_1(\Lambda_{\overline{D}}) = 2/3$ e $\Delta_1(\Lambda_D) = 1/2$. Logo neste exemplo não vale a igualdade (5), caso contrário teríamos $\Delta_1(\Lambda_{\overline{D}}) = \Delta_1(\Lambda_D) = 2/9$. Evidentemente isto não contradiz o Corolário 3, pois a cadeia de códigos utilizada neste exemplo não é fechada sob a adição zero-um.

De forma análoga, e com as adaptações necessárias, ao que foi desenvolvido no Teorema 1, podemos mostrar o seguinte resultado.

Teorema 2: Sejam $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a \neq \{\mathbf{0}\}$ uma cadeia de códigos lineares, $0 \leq r_1 \leq r_2 \leq \cdots \leq r_a$ e $\boldsymbol{h}_1, ..., \boldsymbol{h}_{r_a} \in \mathbb{Z}_q^n$ tais que $C_\ell^\perp = \langle \boldsymbol{h}_1, ..., \boldsymbol{h}_{r_\ell} \rangle$ para $\ell = 1, 2, ..., a$. Se $\Lambda_{D'}$ é o reticulado obtido via Construção D$'$ usando os parâmetros descritos acima, então

$$\min\{q^a, q^{a-1}d_{Lee}^1, ..., d_{Lee}^a\} \leq d_{\min}^1(\Lambda_{D'}) \leq q^a,$$

em que d_{Lee}^ℓ é a distância de Lee mínima em C_ℓ, para $\ell = 1, 2, ...a$.

Exemplo 4: Seja $\mathbb{Z}_3^2 \supseteq C_1 \supseteq C_2$ a cadeia de códigos lineares, na qual $C_1 = C_2 = \langle (1,1) \rangle$. Temos que $C_1^\perp = C_2^\perp = \{(x,y) \in \mathbb{Z}_3^2; x + y = 0\} = \{(0,0), (1,2), (2,1)\} = \langle (1,2) \rangle$. Assim, para $r_1 = 1$, $r_2 = 2$ e $\boldsymbol{h}_1 = (1,2), \boldsymbol{h}_2 = (1,2) \in \mathbb{Z}_3^2$, temos que $0 \leq r_1 \leq r_2$, $C_1^\perp = \langle \boldsymbol{h}_1 \rangle$, $C_2^\perp = \langle \boldsymbol{h}_1, \boldsymbol{h}_2 \rangle$ e, consequentemente,

$$\Lambda_{D'} = \big\{(x,y) \in \mathbb{Z}^2 \big| \ x + 2y \equiv 0 \mod 9\big\}.$$

Portanto

$$\Lambda_{D'} = \bigcup_{\boldsymbol{z} \in 9\mathbb{Z}^2} \big(\boldsymbol{z} + \Lambda_{D'} \cap [0,9)^2\big),$$

e os elementos de $\Lambda_{D'} \cap [0,9)^2$ estão representados na Figura 4. Neste exemplo, observamos que $d_{Lee}^1 = d_{Lee}^2 = 2$ e portanto $\min\{d_{Lee}^2, 3d_{Lee}^1, 3^2\} = 2 < 3 = d_{\min}^1(\Lambda_D) < 3^2$.

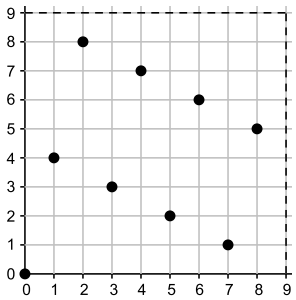

Fig. 4. Elementos de $\Lambda_{D'}$ na caixa $[0,9)^2$.

IV. Conclusões

Neste trabalho, estudamos as distâncias mínimas em relação à métrica da soma dos reticulados Λ_D, $\Lambda_{D'}$ e $\Lambda_{\overline{D}}$ obtidos a partir das Construções D, D$'$ e $\overline{\text{D}}$, respectivamente. Fornecemos cotas inferiores e superiores para a distância mínima do reticulado $\Lambda_{D'}$ em função das distâncias mínimas de Lee dos códigos lineares utilizados em sua construção (Teorema 2). Também apresentamos, no caso em que a cadeia de códigos utilizada é fechada sob a adição zero-um, expressões para as distâncias mínimas dos reticulados $\Lambda_{\overline{D}}$ e Λ_D em função das distâncias mínimas de Lee dos códigos utilizados em suas respectivas construções (Teorema 1 e Corolário 1). Conjecturamos que a conclusão do Teorema 1 também vale quando a cadeia de códigos utilizada não é fechada sob a adição zero-um (Conjectura 1).

Agradecimentos

Os autores agradecem aos revisores pelos comentários e sugestões muito pertinentes.

Referências

[1] A. Campello, G. C. Jorge e S. R. I. Costa, Reticulados q-ários na norma l_p e uma generalização da métrica de Lee, *XXX Simpósio Brasileiro de Telecomunicações (SBrT)*, Brasilia - DF, 2012.

[2] A. Campello, G. C. Jorge, J. E. Strapasson and S. R. I. Costa, Perfect codes in the l_p metric, *European Journal of Combinatorics*, vol. 53, pp. 72-85, 2016.

[3] H. Cohn and A. Kumar, Optimality and uniqueness of the Leech lattice among lattices, *Annals of Mathematics*, Princeton, vol. 170, pp. 1003-1050, 2009.

[4] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 3rd Ed. 1998.

[5] S. I. R. Costa, A. Campello, G. C. Jorge, J. E. Strapasson and C. Qureshi, Codes and lattices in the l_p metric, *IEEE Information Theory and Applications Workshop*, pages 1-4, 2014.

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

[7] T. Etzion, A. Vardy and E. Yaakobi, Coding for the lee and manhattan metrics with weighing matrices, *IEEE Transactions on Information Theory*, vol. 59, No. 10, pp. 6712-6723, 2013.

[8] G. C. Jorge, A. C. Campello, S. I. R Costa, q-ary lattices in the l_p norm and a generalization of the Lee metric, *International Workshop on Coding and Cryptography*, Bergen, Norway, 2013.

[9] C. Y. Lee, Some properties of nonbinary error-correcting code, *IRE Trans. on Inform. Theory*, vol. IT-4, pp. 72-82, 1958.

[10] S. Liu, Y. Hong and E. Viterbo. Unshared Secret Key Cryptography, *IEEE Transactions on Wireless Communications*, 13(12): 6670-6683, 2014.

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

[12] H. Minkowski, Dichteste gitterformige lagerung kongruenter korper, *Nachrichten Ges. Wiss. Gottingen*, pp. 311-355, 1904.

[13] M.-R. Sadeghi, A. H. Banihashemi and D. Panario, Low-density parity-check lattices: construction and decoding analysis, *IEEE Trans. Inf. Theory* 52(10), pp. 4481-4495, 2006.

[14] A. Sakzad, M.-R. Sadeghi and D. Panario, Turbo Lattices: Construction and Error Decoding Performance, *Submitted to IEEE Trans. on Inform. Theory*, available on arXiv:1108.1873v3, September 2012.

[15] P. R. B. da Silva and D. Silva, Design of Lattice Network Codes Based on Construction D, *International Telecommunications Symposium*, 2014.

[16] 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.

[17] E. Strey and S. I. R. Costa, Lattices from codes over $\mathbb{Z}_n$: Generalization of Constructions D, D$'$ and $\overline{\text{D}}$, available on http://arxiv.org/abs/1512.05841, 2015.

[18] W. Ulrich, Non-binary error correction codes, *Bell Sys. Journal*, vol. 36, pp. 1341-1387, 1957.

[19] I. Woungang, S. Misra and S. Chandra Misra, Selected Topics in Information and Coding Theory, *Series on Coding Theory and Cryptology*, volume 7, chapter 2, pages 41-76, 2010. ISBN: 978-981-283-716-5.

[20] R. Zamir, Lattice Coding of Signals and Networks: A Structured Coding Approach to Quantization, Modulation and Multi-user Information Theory. *Cambridge University Press*, 2014.

[21] R. Zamir, Lattices are everywhere, *Information Theory and Applications Workshop*, San Diego-CA, pp. 392-421, 2009.