Reticulados q-ários na norma l_p e uma generalização da métrica de Lee

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

***Resumo*— Reticulados q-ários são obtidos através da Construção A de códigos lineares q-ários. Neste trabalho, mostramos que no estudo de tais reticulados munidos da métrica l_p, surge naturalmente uma nova métrica no conjunto $\mathbb{Z}_q^n$, a qual chamamos métrica p-Lee. Para $p = 1$, esta métrica é a chamada métrica de Lee, largamente estudada na literatura. Para $1 < p \leq \infty$, generalizamos um resultado sobre decodificação de reticulados na métrica de Lee e discutimos brevemente sobre a existência de códigos perfeitos em tais métricas, estabelecendo uma caracterização de todos os códigos perfeitos quando $p = \infty$ e algumas propriedades para o caso geral.**

***Palavras-Chave*— Reticulados, Códigos Corretores de Erros, Métrica de Lee**

I. Introdução

De todas as construções envolvendo códigos corretores de erros e reticulados, uma das mais utilizadas é a Construção A, que relaciona um código corretor de erro no módulo $\mathbb{Z}_q^n$ e um reticulado no espaço $\mathbb{Z}^n$. Tais reticulados são chamados q-ários e possuem diversas aplicações em Teoria da Informação e Criptografia. De fato, uma grande parte dos esquemas criptográficos baseados em reticulados são construídos a partir de reticulados q-ários pois, apesar da sua aparente estrutura mais simples, preservam a dificuldade computacional de diversos problemas envolvendo reticulados [7]. Do ponto de vista de Teoria de Informação, a Construção A é utilizada para construir bons códigos reticulados para o canal gaussiano e para uma boa gama de canais com informação lateral [12].

Neste artigo, abordamos problemas de reticulados q-ários na métrica l_p. Em geral, não há uma literatura extensa sobre reticulados nestas métricas para $p \neq 2$. Peikert estuda em [8] a complexidade de importantes problemas computacionais de reticulados (como o CVP e SVP) para $2 < p \leq \infty$ e interessantemente não consegue o obter nenhum resultado para o caso $1 \leq p < 2$. Em [4], Grell et al. mostram algoritmos ótimos para a busca pelo ponto mais próximo na norma l_p para algumas famílias famosas de reticulados, como $\mathbb{Z}^n$, D_n, A_n, E_6, E_7 e E_8, entretanto não abordam o problema de reticulados q-ários de maneira geral. Ao lidarmos com tais reticulados na norma l_p, na tentativa de generalizar um recente resultado sobre a busca pelo ponto mais próximo na métrica de Lee [1], uma nova métrica é naturalmente induzida no espaço $\mathbb{Z}_q^n$ (que também pode ser vista como uma métrica no quociente $\mathbb{Z}^n/q\mathbb{Z}^n$), a qual chamamos p-Lee. Mostramos que dado um ponto no $\mathbb{Z}^n$, encontrar o ponto de um reticulado q-ário Λ que minimize a distância ate $\boldsymbol{y}$ na norma l_p é equivalente a encontrar o ponto do código associado a Λ mais próximo de um dado ponto na métrica p-Lee.

Este trabalho está organizado conforme descrito a seguir. Na Seção II exibimos alguns resultados preliminares e notações utilizadas. Na Seção III descrevemos a métrica p-Lee e mostramos que ela de fato satisfaz as propriedades de métrica para $1 \leq p \leq \infty$, e definimos os parâmetros de um código nesta métrica. Na Seção IV, discutimos a existência de códigos perfeitos para alguns valores de p e apresentamos algumas conjecturas. Por fim, na Seção V apresentamos nossas conclusões.

II. Preliminares

Nesta seção, descreveremos alguns resultados iniciais e estabeleceremos a notação utilizada ao longo do trabalho.

A. Códigos e reticulados

Dado $q \in \mathbb{N}$, um *código linear* q-ário C é um $\mathbb{Z}_q$-submódulo de $\mathbb{Z}_q^n$. Um ponto $\overline{\boldsymbol{x}} \in C$ é usualmente chamado de *palavra-código* ou simplesmente palavra. Se q é um número primo, então C é um subespaço vetorial de $\mathbb{Z}_q^n$ e portanto possui uma base constituída por $k \leq n$ vetores. Caso contrário, podemos apenas garantir a existência de um conjunto minimal de geradores, não necessariamente linearmente independentes. A matriz A cujas colunas são os vetores de tal conjunto minimal é dita *matriz geradora* de C. Para q primo, sempre existe uma matriz geradora A para C na *forma sistemática* i.e,

$$A_{n\times k} = \begin{bmatrix} I_{k\times k} \\ B_{k\times n-k} \end{bmatrix}. \tag{1}$$

Um reticulado Λ é um subgrupo aditivo discreto do $\mathbb{R}^n$. Equivalentemente, $\Lambda \subset \mathbb{R}^n$ é um reticulado se, e somente se, existe um conjunto de vetores linearmente independentes $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbb{R}^n$, $m \leq n$, tal que Λ é o conjunto de todas combinações lineares $y = \sum_{i=1}^{m} \alpha_i \boldsymbol{v}_i$, onde $\alpha_i \in \mathbb{Z}$. Uma matriz M cujas colunas são os vetores de tal conjunto é dita uma *matriz geradora* para Λ, enquanto $G = M^t M$ é a matriz de Gram associada. O *determinante* de Λ é definido como $\det \Lambda = \sqrt{\det G} = \det M$. O valor $\det \Lambda$ corresponde também ao volume euclidiano do paralelotopo $P = \{\sum_{i=1}^{m} \alpha_i \boldsymbol{v}_i,\ 0 \leq \alpha_i < 1\}$, uma região fundamental de Λ. O reticulado cúbico $\mathbb{Z}^n$ é o conjunto de todos os vetores com coordenadas inteiras no plano. Um reticulado Λ é dito

Departamento de Matemática Aplicada (Antonio Campelo e Grasiele Jorge), Departamento de Matemática (Sueli Costa), IMECC-Unicamp, Campinas-SP, Brasil. E-mails: campello@ime.unicamp.br, grajorge@ime.unicamp.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)

inteiro se $\Lambda \subseteq \mathbb{Z}^n$. Dado um reticulado Λ munido da métrica l_p, a distância mínima μ de Λ é dada por

$$\min_{\mathbf{0}\neq \boldsymbol{x}\in\Lambda} d_p(\boldsymbol{x}, \mathbf{0}).$$

Seja Λ um reticulado. Dada uma métrica d em $\mathbb{R}^n$ e um ponto $\boldsymbol{r} \in \mathbb{R}^n$, um importante problema que possui diversas aplicações em codificação e criptografia é o de encontrar o ponto de Λ mais próximo de $\boldsymbol{r}$. Um processo para encontrar a solução $\boldsymbol{x} \in \Lambda$ deste problema (isto é, o ponto que do reticulado que minimiza a distância até $\boldsymbol{r}$) é chamado de decodificação no reticulado Λ. Se d é a distância euclidiana, então a decodificação tem aplicações no envio de informação sobre um canal Gaussiano com ruído branco e é um problema largamente estudado. A versão geral deste problema em reticulados inteiros é computacionalmente difícil e é classificado na Teoria de Complexidade como NP-hard [7].

B. Construção A

A chamada Construção A estendida para códigos q-ários [2] associa um código $C \subseteq \mathbb{Z}_q^n$ a um reticulado inteiro e pode ser descrita conforme mostrado a seguir. Seja ϕ a aplicação sobrejetiva

$$\begin{aligned} \phi : \mathbb{Z}^n &\longrightarrow \mathbb{Z}_q^n \\ (x_1, \ldots, x_n)^t &\longmapsto (\overline{x_1}, \ldots, \overline{x_n})^t, \end{aligned} \tag{2}$$

onde $\overline{x_i} = x_i \pmod{\text{q}}$ para $i = 1, \ldots, n$. Dado um código $C \in \mathbb{Z}_q^n$, definimos $\Lambda_A(C)$ como a imagem inversa de C por ϕ, isto é $\Lambda_A(C) = \phi^{-1}(C)$. É fácil ver que $\Lambda_A(C)$ é um reticulado se, e somente se C é um código linear. Neste caso, dizemos que $\Lambda_A(C)$ é o reticulado q-ário associado a C. Todos os reticulados q-ários contêm $(q\mathbb{Z})^n = \{q\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^n\}$ como sub-reticulado e esta propriedade pode ser usada como uma alternativa para a definição de reticulados q-ários, como em [7]. Com efeito, se $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$, então o quociente $\Lambda/q\mathbb{Z}^n$ é sempre isomorfo a um código linear $C \in \mathbb{Z}_q^n$. As palavras de C podem ser vistas como os representantes do quociente $\Lambda/q\mathbb{Z}^n$ dentro do hipercubo $[0, q)^n$ e $\Lambda_A(C)$ será então obtido como copias destes pontos transladados de direções múltiplas de q, isto é, de $q\boldsymbol{w}$, onde $\boldsymbol{w} \in \mathbb{Z}^n$. Algumas propriedades da construção A utilizadas neste trabalho são dadas na seguinte proposição:

Proposição 1: Seja $\Lambda_A(C)$ o reticulado q-ário associado a um código $C \in \mathbb{Z}_q^n$. Valem as seguintes propriedades:

1) O número de palavras de C é dado por
$$|C| = \left|\frac{\Lambda_A(C)}{q\mathbb{Z}^n}\right| = \frac{q^n}{\det(\Lambda_A(C))}.$$
2) Se C é gerado pela matriz $\begin{bmatrix} I_{k\times k} \\ B_{k\times n-k} \end{bmatrix}$, então:
$$M = \begin{bmatrix} I_{k\times k} & 0_{k\times(n-k)} \\ B_{(n-k)\times k} & qI_{(n-k)\times(n-k)} \end{bmatrix} \tag{3}$$
é uma matriz geradora para $\Lambda_A(C)$.
3) Todo reticulado $\Lambda \subseteq \mathbb{Z}^n$ é q-ário.

Demonstração: O isomorfismo entre C e $\Lambda_A(C)/q\mathbb{Z}^n$ é direto e o número de representantes neste quociente é dado pela segunda igualdade [2], mostrando 1). A demonstração de 2) segue pelos fatos de que $\overline{(M\boldsymbol{x})} \in C$ para qualquer $\boldsymbol{x} \in \mathbb{Z}^n$ e qualquer ponto de $\Lambda_A(C)$ pode ser escrito como $\boldsymbol{x} + q\boldsymbol{w}$, onde $\boldsymbol{w} \in \mathbb{Z}^n$ e $\boldsymbol{x} \in C$. A terceira propriedade vem do fato de que, se Λ é inteiro, então possui matriz geradora M inteira, e portanto $\det\Lambda$ também é inteiro. Assim, tomando $q = \det\Lambda$, o sistema linear $M\boldsymbol{x} = q\boldsymbol{z}$ sempre tem solução para $\boldsymbol{z} \in \mathbb{Z}^n$ um vetor fixo, mostrando que $\mathbb{Z}_q^n \subseteq \Lambda$ e portanto Λ é um reticulado q-ário. ■

A última propriedade nos mostra que, tratando de reticulados q-ários estamos, de um ponto de vista teórico, lidando com qualquer reticulado inteiro.

III. A MÉTRICA p-LEE

Ao invés da usual métrica de Hamming para códigos e euclidiana para reticulados, consideramos aqui a distância l_p em $\Lambda_A(C) \subset \mathbb{Z}^n$ e a métrica induzida que denotamos por p-Lee para códigos. Mostramos mais adiante (Seção IV) como esta métrica surge naturalmente do estudo de reticulados na norma l_p e como poderemos relacionar a busca pelo ponto mais próximo em $\Lambda_A(C)$ como um problema de decodificação em C.

Sejam $1 \leq p < \infty$ e $\boldsymbol{x} = (x_1, \ldots, x_n)^t, \boldsymbol{y} = (y_1, \ldots, y_n)^t \in \mathbb{R}^n$,. A distância d_p entre estes vetores é definida como

$$d_p(\boldsymbol{x}, \boldsymbol{y}) := \left(\sum_{i=1}^{n} |x_i - y_i|^p\right)^{1/p}.$$

Se $p = \infty$, então definimos

$$d_\infty(\boldsymbol{x}, \boldsymbol{y}) := \max\{|x_i - y_i|;\ i = 1, \ldots, n\}.$$

A métrica de Lee, introduzida em [6], pode ser vista como a distância no quociente $\mathbb{Z}^n/q\mathbb{Z}^n$ induzida pela métrica l_1 no reticulado. Para dois elementos $\overline{x}, \overline{y} \in \mathbb{Z}_q$ ela é definida como

$$d_{Lee}(\overline{x}, \overline{y}) = \min\left\{(\overline{x} - \overline{y}) \pmod{\text{q}}, (\overline{y} - \overline{x}) \pmod{\text{q}}\right\}, \tag{4}$$

enquanto para dois vetores $\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}} \in \mathbb{Z}_q^n$, temos

$$d_{Lee_1}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) = \sum_{i=1}^{n} \min\left\{(\overline{x}_i - \overline{y}_i) \pmod{\text{q}}, (\overline{y}_i - \overline{x}_i) \pmod{\text{q}}\right\}, \tag{5}$$

Como demonstrado em [6], as distâncias satisfazem as propriedades de simetria, positividade e desigualdade triangular, definindo assim uma métrica nos seus respectivos espaços. A generalização da métrica de Lee aqui proposta é dada pela Proposição 2 abaixo.

Proposição 2: Sejam $1 \leq p < \infty$ e $\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}} \in \mathbb{Z}_q^n$. A aplicação $d_{Lee,p} : \mathbb{Z}_q^n \times \mathbb{Z}_q^n \to \mathbb{R}$ dada por

$$d_{Lee,p}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) = \left(\sum_{i=1}^{n} (d_{Lee}(\overline{x}_i, \overline{y}_i))^p\right)^{1/p},$$

onde $d_{Lee}(\overline{x}, \overline{y})$ é dada pela Equação 4, define uma métrica em $\mathbb{Z}_q^n$, a qual denotamos por métrica p-Lee.

Demonstração: As condições de simetria e positividade são imediatas. Para a desigualdade triangular, sejam

$\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}, \overline{\boldsymbol{z}} \in \mathbb{Z}_q^n$. Como a métrica de Lee 4 satisfaz a desigualdade triangular, temos

$$d_{Lee}(\overline{x}_i, \overline{y}_i)^p \leq \left(d_{Lee}(\overline{x}_i, \overline{z}_i) + d_{Lee}(\overline{z}_i, \overline{y}_i)\right)^p .$$

Consequentemente

$$\begin{aligned} d_{Lee,p}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) &= \left(\sum_{i=1}^{n} (d_{Lee}(\overline{x}_i, \overline{y}_i))^p\right)^{1/p} \\ &\leq \left(\sum_{i=1}^{n} (d_{Lee,1}(\overline{x}_i, \overline{z}_i) + d_{Lee,p}(\overline{z}_i, \overline{y}_i))^p\right)^{1/p} . \end{aligned}$$

Pela Desigualdade de Minkowski, temos

$$\begin{aligned} &d_{Lee,p}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) = \left(\sum_{i=1}^{n} (d_{Lee}(\overline{x}_i, \overline{y}_i))^p\right)^{1/p} \\ &\leq \left(\sum_{i=1}^{n} (d_{Lee}(\overline{x}_i, \overline{z}_i))^p\right)^{1/p} + \left(\sum_{i=1}^{n} (d_{Lee}(\overline{z}_i, \overline{y}_i))^p\right)^{1/p} \\ &d_{Lee,p}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{z}}) + d_{Lee,p}(\overline{\boldsymbol{z}}, \overline{\boldsymbol{y}}) \end{aligned}$$

■

Para $p = \infty$ definimos analogamente:

$$d_\infty(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) := \max\{|\overline{x}_i - \overline{y}_i|;\ i = 1, \ldots, n\},$$

e também valerão as propriedades da Proposição (2) acima.

Assim como em qualquer métrica, a distância mínima $d_{Lee,p}(C)$ de um código $C \in \mathbb{Z}_q^n$ é definida como a menor distância entre duas palavras distintas de C. Uma bola na métrica p-Lee é definida analogamente da maneira usual, como:

$$B_{Lee,p}(\overline{\boldsymbol{x}}, R) = \left\{\overline{\boldsymbol{y}} \in \mathbb{Z}_q^n : d_{Lee,p}(\overline{\boldsymbol{x}}, \overline{\boldsymbol{y}}) \leq R.\right\} \qquad (6)$$

O conceito de capacidade de correção de erro de um código C é estendido como o maior t para o qual as bolas na métrica de raio $B_{Lee,p}(R, \overline{\boldsymbol{x}})$ centradas em pontos distintos do código são disjuntas. Na métrica de Lee (isto é, para $p = 1$), a capacidade de correção de erros de um código é dada pela formula clássica $t = \lfloor (d_{Lee}(C) - 1)/2 \rfloor$. Para $p > 1$, este fato não é verdade. Para verificarmos isto, tome por exemplo o código 13-ário

$$C = \langle (1, 5) \rangle = \{j(1, 5) \pmod{13} : j = 0, \ldots, 12\} . \qquad (7)$$

Para $p = 2$, temos $\lfloor (d_{Lee,2}(C) - 1)/2 \rfloor = 1$, mas as esferas de raio 2 centradas em palavra-código não se intersectam, e portanto a capacidade de correção de erros é estritamente maior do que $\lfloor (d_{Lee,2}(C) - 1)/2 \rfloor$. Este exemplo pode ser estendido para qualquer $p > 1$.

Se C é um código q-ário, a distância mínima μ de $\Lambda_A(C)$ na métrica l_p está relacionada à distância mínima do código C na métrica $d_{Lee,p}(C)$ conforme a equação [10]

$$\mu = \min\{q, d_{Lee,p}(C)\}. \qquad (8)$$

IV. Decodificação de reticulados via Construção A

Para reticulados construídos a partir de códigos q-ários, mostramos em [1] que decodificar (ou seja, encontrar a palavra-código mais próxima de um ponto recebido) um código q-ário $C \subseteq \mathbb{Z}_q^n$ na métrica de Lee corresponde a decodificar o respectivo reticulado q-ário $\Lambda_A(C) \subseteq \mathbb{R}^n$ na métrica da soma (ou métrica l_1). Nesta seção, obtemos o mesmo tipo de relação para códigos na métrica p-Lee e reticulados na métrica l_p.

A fim de melhorar a notação, quando nos referirmos a um vetor $\overline{\boldsymbol{x}}$, estamos considerando-o como um ponto do código q-ário C, mas quando nos referirmos a $\boldsymbol{x}$, estamos considerando-o como um ponto do reticulado q-ário $\Lambda_A(C)$. Devido ao isomorfismo $\Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n \simeq C$, não faremos distinção entre os elementos de C e $\Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n$. Denotamos por $[a]$ o arredondamento ao inteiro mais próximo de a.

Proposição 3: Sejam $\Lambda_A(C)$ um reticulado q-ário e $\boldsymbol{r} = (r_1, \cdots, r_n) \in \mathbb{R}^n$ um vetor. Dado um elemento $\overline{\boldsymbol{x}} \in \Lambda_A(C)/q\mathbb{Z}^n$ com $\boldsymbol{x} = (x_1, \cdots, x_n)$, o representante $\overline{\boldsymbol{z}}$ da classe $\overline{\boldsymbol{x}}$ que está mais próximo de $\boldsymbol{r}$ em $\Lambda_A(C)$, considerando a métrica d_p, é dado por $\boldsymbol{z} = (z_1, \cdots, z_n)$, onde $z_i = x_i + qw_i$ e $w_i = \left[\dfrac{r_i - x_i}{q}\right]$ para cada $i = 1, \cdots, n$.

Demonstração: Cada representante da classe de $\boldsymbol{x}$ é dado por $\boldsymbol{z} = \boldsymbol{x} + q\boldsymbol{w}$, onde $\boldsymbol{w} \in \mathbb{Z}^n$. Na métrica da soma, $d_p(\boldsymbol{r}, \boldsymbol{z}) = \left(\sum_{i=1}^{n} (r_i - x_i - qw_i)^p\right)^{1/p}$ é mínima quando cada parcela do somatório é mínima, isto é, $w_i = \left[\frac{r_i - x_i}{q}\right]$. ■

Definição 1: Sejam $\Lambda_A(C)$ um reticulado q-ário e $\boldsymbol{r} \in \mathbb{R}^n$ um vetor. Chamaremos de $\boldsymbol{r}$ (mod q) o vetor obtido de $\boldsymbol{r}$ por reduções módulo q em cada entrada de $\boldsymbol{r}$. Essas reduções são feitas tomando o resto da divisão de cada entrada de $\boldsymbol{r}$ por q com coeficientes inteiros.

A próxima proposição relaciona a decodificação no reticulado q-ário $\Lambda_A(C)$ na métrica d_p com a decodificação no código q-ário C na métrica $d_{Lee,p}$.

Proposição 4: Sejam $\Lambda_A(C)$ um reticulado q-ário e $\boldsymbol{r} = (r_1, \cdots, r_n) \in \mathbb{R}^n$ um vetor. Se $\overline{\boldsymbol{x}} \in C$ é o elemento do código C mais próximo de $\boldsymbol{r}$ (mod q) considerando a métrica $d_{Lee,p}$, então $\boldsymbol{z} \in \Lambda_A(C)$ dado pela Proposição 3 tal que $\overline{\boldsymbol{z}} = \overline{\boldsymbol{x}}$ em $\Lambda_A(\boldsymbol{C})/q\mathbb{Z}^n$, é um elemento de $\Lambda_A(C)$ mais próximo de $\boldsymbol{r}$ na métrica d_p.

Demonstração: Seja $\boldsymbol{r}$ (mod q) $= \boldsymbol{r}^*$, isto é, $\boldsymbol{r} = (r_1, \cdots, r_n) = (r_1{}^*, \cdots, r_n{}^*) + q(t_1, \cdots, t_n)$, onde $0 \leq r_i{}^* < q$ e $t_i \in \mathbb{Z}$ para $i = 1, \cdots, n$. Seja $\overline{\boldsymbol{x}} \in \boldsymbol{C}$ com $\boldsymbol{x} = (x_1, \cdots, x_n)$, $0 \leq x_i \leq q - 1$ para $i = 1, \cdots, n$, o ponto mais próximo de $\boldsymbol{r}$ (mod q) considerando a métrica de Lee. Mostramos que o ponto mais próximo de $\boldsymbol{r}$ em $\Lambda_A(C)$ está na mesma classe que $\boldsymbol{x}$ em $\Lambda_A(C)/q\mathbb{Z}^n$. Para cada classe $\overline{\boldsymbol{a}} \in C$ com $\boldsymbol{a} = (a_1, \cdots, a_n)$, pela Proposição 3 encontramos o representante $\boldsymbol{a}^*$ mais próximo de $\boldsymbol{r}$ considerando a métrica de Lee. Mostramos que $d_p(\boldsymbol{r}, \boldsymbol{a}^*) = d_{Lee,p}(\boldsymbol{r} \pmod{\text{q}}, \overline{\boldsymbol{a}})$. Para a métrica d_p temos que

$$d_p(\boldsymbol{r}, \boldsymbol{a}^*) = \left(\sum_{i=1}^{n} (r_i{}^* - a_i - \alpha_i q)^p\right)^{1/p} ,$$

onde $\alpha_i = \left(\left[\frac{r_i{}^* - a_i}{q} + t_i\right] - t_i\right)$. Então, $-1 \leq \frac{r_i{}^* - a_i}{q} \leq 1$ pois $|r_i{}^* - x_i| \leq q$, $\alpha_i \in \{-1, 0, 1\}$. Assim, podemos observar que:

- Se $\alpha_i = 0$ para algum i, então $-q/2 \leq r_i{}^* - a_i \leq q/2$ e isto implica que
$$\min\{|r_i^* - a_i|, q - |r_i^* - a_i|\} = |r_i^* - a_i|.$$
- Se $\alpha_i = 1$ para algum i, então $q/2 < r_i{}^* - a_i \leq q$ e portanto
$$\min\{|r_i^* - a_i|, q - |r_i^* - a_i|\} = q - |r_i^* - a_i|$$
$$\text{e } |r_i^* - a_i| = r_i^* - a_i.$$
- Se $\alpha_i = -1$ para algum i, então $-q \leq r_i{}^* - a_i < -q/2$ e então
$$\min\{|r_i^* - a_i|, q - |r_i^* - a_i|\} = q - |r_i^* - a_i|$$
$$\text{e } |r_i^* - a_i| = -(r_i^* - a_i).$$

Deste modo: que

$$\begin{aligned} d_p(\boldsymbol{r}, \boldsymbol{a}^*) &= \left(\sum_{i=1}^{n} |r_i{}^* - a_i - \alpha_i q|^p\right)^{1/p} \\ &= \left(\sum_{i=1}^{n} \min\{|r_i{}^* - a_i|, q - |r_i{}^* - a_i|\}^p\right)^{1/p} \\ &= d_{Lee,p}(\overline{\boldsymbol{r}}, \overline{\boldsymbol{a}}). \end{aligned}$$

Como $\overline{\boldsymbol{x}}$ satisfaz $d_{Lee,p}(\overline{\boldsymbol{r}}, \overline{\boldsymbol{x}}) = \min\{d_{Lee,p}(\overline{\boldsymbol{r}}, \overline{\boldsymbol{a}}), \overline{\boldsymbol{a}} \in C\}$ então $\boldsymbol{z}$ satisfaz $d_p(\boldsymbol{r}, \boldsymbol{z}) = \min\{d_p(\boldsymbol{r}, \boldsymbol{y}), \boldsymbol{y} \in \Lambda_A(C)\}$. ■

V. Códigos perfeitos na métrica p-Lee

Seja $C \subseteq \mathbb{Z}_q^n$ um código. Denotamos por $\mu_p(n, R)$ a quantidade de pontos em $\mathbb{Z}_q^n$ dentro de uma bola de raio R centradas em uma palavra de C na distância $d_{Lee,p}$. Temos a seguinte proposição:

Teorema 1 ([3]): Se a distância mínima de um código $C \subseteq \mathbb{Z}_q^n$ é $2R + 1$, então $|C|\,\mu_p(n, R) \leq q^n$.

Este limitante, válido para para qualquer métrica em $\mathbb{Z}_q^n$ é conhecido como limitante do empacotamento esférico. Códigos para os quais vale a igualdade no teorema acima são conhecidos como *códigos perfeitos*. Os códigos perfeitos triviais são constituídos por todo o $\mathbb{Z}_q^n$ e pelo conjunto contendo apenas uma palavra-código.

Para $p = 1$ [9] e $p = \infty$, o valor de $\mu_p(n, R)$, onde $(2R + 1 \leq q)$ é conhecido explicitamente e dado pelas equações abaixo:

$$\mu_1(n, R) = \sum_{i=0}^{\min\{n,R\}} 2^i \binom{n}{i}\binom{R}{i} \tag{9}$$

e

$$\mu_\infty(n, R) = (2R + 1)^n. \tag{10}$$

Considerando a métrica de Lee ($p = 1$), é fácil exibir exemplos para $n = 2$ e qualquer R, mas a conhecida conjectura de Golomb-Welch propõe que para $n > 2$ só existem códigos perfeitos para $R = 1$ [5]. Abaixo, mostramos que proposições acerca da existência de códigos perfeitos para a métrica p-Lee, $p \neq 1$.

Proposição 5: Para $1 \leq p < \infty$, existem códigos perfeitos não triviais na métrica p-Lee para $n = 2$.

Demonstração: Exibimos, a seguir, um código perfeito não trivial na métrica p-Lee. Considere o código gerado pelos múltiplos do vetor $(1, 5)$, $C = \langle(1, 5)\rangle \subseteq \mathbb{Z}_{13}^2$. Este código é perfeito na métrica p-Lee para $1 \leq p < \infty$. De fato, para $1 \leq p < \infty$ as esferas $B_{Lee,p}(\overline{\boldsymbol{x}}, 2)$ centradas em uma palavra estão contidas na esfera $B_{Lee,\infty}(\overline{\boldsymbol{x}}, 2)$ de raio 2 centrada na mesma palavra. As esferas $B_{Lee,p}(\overline{\boldsymbol{x}}, 2)$ intersectam $B_{Lee,\infty}(\overline{\boldsymbol{x}}, 2)$ em exatos 4 pontos, correspondendo aos vértices do losango inscrito em $B_{Lee,p}$, como ilustrado na Figura 1. Como $\mu_\infty(2, 2) = 25$ e 16 destes pontos estão no bordo do quadrado de lado 4, então $\mu_p(2, 2) = 25 - 16 + 4 = 13$. Assim, $|C|\mu_p(2, 2) = 13^2$ e a igualdade é atingida no Teorema (1), para $\mathbb{Z}_{13}^2$. ■

Proposição 6: Para $1 \leq p < \infty$, existem códigos perfeitos n-dimensionais na métrica p-Lee para $q = 2n + 1$ e $R = 1$.

Demonstração: Para $p = 1$, este é um resultado clássico e sua demonstração pode ser encontrada em [5]. Considere agora, o vetor nulo $\overline{\mathbf{0}}$. Para $1 \leq p < \infty$, as equações $|x_1|^p + \ldots + |x_n|^p \leq 1$ possuem exatamente $2n + 1$ soluções inteiras e portanto $\mu_1(n, 1) = \mu_p(n, 1) = 2n + 1$. Como existe um código perfeito na métrica de Lee, então existe $C \subseteq \mathbb{Z}_q^n$ satisfazendo $|C|\mu_1(n, 1) = q^n$, donde segue que $|C|\mu_p(n, 1) = q^n$. ■

Tendo em vista isto, apresentamos abaixo a seguinte conjectura, que é uma extensão da famosa Conjectura de Golomb-Welch.

Conjectura 1: Não existem códigos perfeitos na métrica p-Lee, $p \leq \infty$, para $n > 2$ e $R > 1$.

Proposição 7: Existem códigos perfeitos $C \subset \mathbb{Z}_q^n$ não-triviais na métrica ∞-Lee se, e somente se $q = bm$ com $b > 1$ um inteiro ímpar e $m > 1$.

Demonstração: Um código $C \subseteq \mathbb{Z}_q^n$ com distância mínima $2R + 1$ é perfeito com respeito à distância $d_{Lee,\infty}$ se e somente se

$$|C|(2R + 1)^n = q^n. \tag{11}$$

- Condição necessária: Pela condição acima (Equação (11)), se existe um código perfeito C, então
$$|C| = \left(\frac{q}{2R + 1}\right)^n.$$
E assim temos que $2R + 1$ deve dividir q. Excluindo o código trivial no qual $R = 0$, q deve possuir um fator ímpar maior que 1, mostrando que $q = 2^a$ é impossível. Caso q seja primo, como $2R + 1$ divide q, segue que $2R + 1 = q$ (caso trivial em que C possui apenas uma palavra). Mostramos assim que não é possível termos um código perfeito com q primo, nem potência de 2. Deste modo, a condição necessária é a de que q seja fatorável como $q = mb$, para b um inteiro ímpar maior que 1 e $m > 1$.
- Condição suficiente: Seja $q = mb$ com $b > 1$ um inteiro ímpar e $m > 1$. Tomando o código $C = \langle(b, 0, \ldots, 0), \ldots, (0, \ldots, 0, b)\rangle \subseteq \mathbb{Z}_q^n$ temos claramente que $|C| = m^n$ e $R = (b - 1)/2$, ou seja, sua distância mínima é igual a b. Deste modo, $|C|\mu_{\infty(n,R)} = m^n b^n =$

q^n, $1 < |C| < q^n$ e portanto este código é perfeito e não-trivial, mostrando que a condição é suficiente. ■

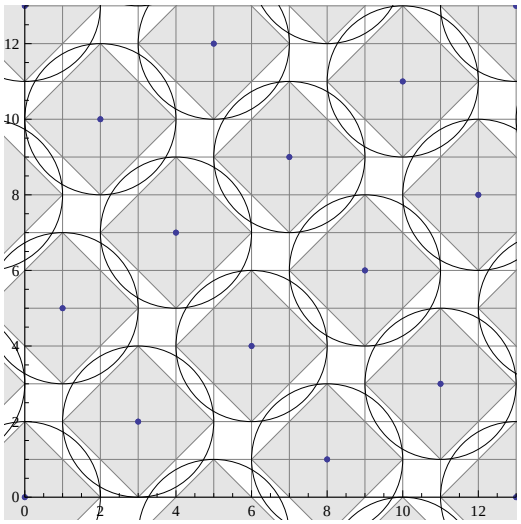

Fig. 1. Ilustração da Proposição 5 para o código $C = \langle(1, 5)\rangle$. As bolas na métrica p-Lee, $p = 1, 2$ são os pontos inteiros contidos no losango em azul e no disco, respectivamente

VI. Conclusões

Neste trabalho, apresentamos uma proposta de generalização da métrica de Lee no conjunto $\mathbb{Z}_q^n$ e mostramos que o problema de decodificar em reticulados q-ários na métrica l_p é equivalente ao de decodificar em um código na metrica p-Lee. Em seguida, discutimos alguns aspectos sobre a existência ou não de códigos perfeitos em tais métricas. Para $p = \infty$ caracterizamos todos os casos em que existem códigos perfeitos e para $1 < p < \infty$ conjecturamos que os únicos códigos perfeitos com $n > 2$ são os dados pela Proposição 3, ou seja, com $R = 1$. Essa conjectura está de acordo com a famosa conjectura de Golomb-Welch [5] para códigos perfeitos na métrica de Lee.

Referências

[1] A. Campello, G. C. Jorge and S. I. R. Costa, Decoding q-ary lattices in the Lee Metric, *Proceedings of IEEE Information Theory Workshop*, Paraty-RJ, pp. 220-224, 2011.

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

[3] T. Etzion, Product Constructions for Perfect Lee Codes, *IEEE Transactions on Information Theory*, vol. IT 57, pg. 7473-7481, 2011.

[4] E. Grell, T. Eriksson, A. Vardy and K. Zeger, Closest point search in lattices *IEEE Transactions on Information Theory*, Vol. 48, pp. 2201-2214, 2002.

[5] S. W. Golomb and L. R. Welch, Perfect Codes in the Lee Metric and the Packing of Polyominoes. *SIAM Journal on Applied Mathematics*, Vol. 18, No. 2, pp. 302-317, 1970.

[6] C. Y. Lee, Some properties of nonbinary error-correcting code, *IRE Transactions on Information Theory*, vol.4, pp.72-82, 1958.

[7] 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.

[8] C. Peikert, Limits on the Hardness of Lattice Problems in l_p norms, *Journal of Computational Complexity*, Vol. 17, 2008

[9] J. Serra-Sagristà and J. Borrell, Lattice points enumeration for image coding. *Proceedings of the IEEE International Conference of Information Intelligence and Systems*, Bethesda-MD, pp.482-489, 1999.

[10] 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.

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

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