Classificação dos códigos perfeitos bidimensionais na métrica de Lee

Claudio M. Qureshi[a] e Sueli I. R. Costa[a]

***Resumo*— Neste trabalho apresentamos uma descrição e a classificação completa de todos os códigos perfeitos (lineares e não lineares) em relação à métrica de Lee, demonstrando que num certo sentido os códigos apresentados por Golomb-Welch [4] são essencialmente os únicos para o caso bidimensional. Além disso, fazemos uma descrição explícita de todas as estruturas possíveis que podem ter os códigos lineares bidimensionais perfeitos exibindo uma "base". Alguns dos resultados e estratégias aqui apresentados podem ser generalizados para dimensões maiores e poderão ser usados para abordar a Conjectura de Golomb-Welch para códigos asociados a reticulados em outras dimensões.**

***Palavras-Chave*— Códigos perfeitos, métrica de Lee, Conjectura de Golomb Welch, classificação de grupos.**

***Abstract*— In this paper, we present a description and the complete classification of all (linear and non linear) two-dimensional Lee-perfect Codes. Our results prove that in dimension two the codes constructed by Golomb-Welch [4] are essentially the only ones. We also present a complete description of all possible structures of Lee-perfect two-dimensional codes. An explicit "basis" for such codes is provided. Some results and techniques can be generalized to higher dimensions and could be helpful to approach the Golomb-Welch Conjecture in other cases.**

***Keywords*— Lee-Perfect Codes, Lee metric, Golomb-Welch Conjecture, group classification.**

I. Introdução

A métrica de Lee para códigos n-dimensionais (de comprimento n) sobre $\mathbb{Z}_q$, a qual coincide com a métrica de Hamming para $q = 2, 3$, foi introduzida nos anos 1957-1958 em [1], [2] para transmissão de sinais sobre certos canais com ruído. Desde então diversos artigos tem abordado problemas a ela relacionados devido a várias aplicações [5], [6], [7], [8] tendo diversas destas surgido nesta última década. Códigos q-ários lineares estão associados a reticulados e vem sendo também utilizados na proposição de esquemas criptográficos,

Um dos problemas mais importantes relacionados a códigos na métrica de Lee é sobre a existência ou não existência de códigos perfeitos (Lee-perfeitos) o qual tem sido tratado em diversos artigos [9], [10], [11].

Inicialmente somente eram considerados com a métrica de Lee códigos de comprimento n sobre o alfabeto Z_p com p primo, e em 1970 esta abordagem foi generalizada por Golomb e Welch em [4] para $\mathbb{Z}_q$ para $q > 1$ qualquer. Nesse trabalho os autores apresentam sua famosa conjectura [4], a qual em termos de códigos sobre $\mathbb{Z}_q$ pode ser escrita como: Para $n = 1$ e $n = 2$ existem códigos perfeitos corrigindo e erros (e-perfeitos) para todo e, mas para $n > 2$ e $q > 2e$ só existem códigos e-perfeitos para $e = 1$. Foi também conjecturado [10] que para dimensão dois os códigos lineares perfeitos apresentados em [4] seriam essencialmente os únicos.

Neste trabalho, o resultado central é o Teorema 1 onde mostramos que esta última conjectura é verdadeira, e apresentamos uma classificação completa de todos os códigos q-arios bidimensionais perfeitos (lineares e não lineares). Apresentamos também todas as estruturas possíveis de grupos associadas a estes códigos.

a-Instituto de Matemática, Universidade de Campinas, Campinas - SP, Brasil, E-mails: cqureshi@gmail.com, sueli@ime.unicamp.br

Este trabalho teve o apoio da Fapesp 2012/10600-2 e do CNPq 309561/2009-4.

II. Preliminares

Consideramos o conjunto $\mathbb{Z}_q = \{0, 1, 2, \ldots, q-1\}$ com as operações módulo q e sobre ele definimos a métrica $d(x, y) = \min\{|x-y|, q-|x-y|\}$ à qual chamamos métrica de Lee. Se consideramos o grafo circular não dirigido que tem como arestas $(i, i+1)$ con $i \in \mathbb{Z}_q$, então a métrica de Lee coincide com a métrica do grafo. A métrica de Lee se estende ao conjunto $\mathbb{Z}_q^n$ como: $d(x, y) = \sum_{i=1}^{n} d(x_i, y_i)$ onde $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ são elementos de $\mathbb{Z}_q^n$. A métrica de Lee pode ser obtida também como a métrica induzida no quociente $\mathbb{Z}^n/q\mathbb{Z}^n$ quando consideramos $\mathbb{Z}^n$ com a métrica da soma. É usual denotar $\| x \|_{1,Lee} = d(x, 0)$ e $d(x, y) = \| x - y \|_{1,Lee}$.

Se d é a métrica de Lee em $\mathbb{Z}_q \times \mathbb{Z}_q$, definimos a bola de Lee de raio e com centro em $c \in \mathbb{Z}_q \times \mathbb{Z}_q$ como $B(c, e) = \{x \in \mathbb{Z}_q \times \mathbb{Z}_q : d(x, c) \leq e\}$. Se consideramos um quadriculado $q \times q$ podemos identificar um elemento de $\mathbb{Z}_q \times \mathbb{Z}_q$ ((i, j) com o quadradinho da coluna i e linha j). A bola de Lee será identificada com o poliomino formado por quadrados de lado um centrados nos pontos da bola (identificando os lados opostos do quadriculado $q \times q$). A Figura 2 ilustra duas bolas de Lee de raio $e = 2$ em $\mathbb{Z}_9 \times \mathbb{Z}_9$. Para $2e < q$, $B(c, e)$ contém $q_e = 2e^2 + 2e + 1$ pontos.

Diremos que duas bolas B_1 e B_2 são adjacentes se forem disjuntas e existirem $x_1 \in B_1$ e $x_2 \in B_2$ tais que $d(x_1, x_2) = 1$. Isto significa que os poliominos associados a estas bolas são disjuntos e se tocam em pelo menos uma aresta. Por exemplo as duas bolas adjacentes da Figura 2 tem duas arestas em comum.

Um código bidimensional q-ário C é um subconjunto qualquer de $\mathbb{Z}_q \times \mathbb{Z}_q$. Os elementos de C são chamados de palavras-código. A distância mínima de C é definida como a

menor distância (de Lee) entre duas palavras-código distintas e ela é denotada por $d_{min}(C)$. O código é dito e-corretor se as bolas $B(c,e)$ com $c \in C$ são disjuntas e existem $c_1, c_2 \in C$ tais que $B(c_1, e+1) \cap B(c_2, e+1) \neq \emptyset$. A relação entre e e $d_{min}(C)$ é dada por $e = [\frac{d_{min}(C)-1}{2}]$.

Um código $C \subseteq \mathbb{Z}_q \times \mathbb{Z}_q$ é dito e-perfeito (ou perfeito quando e é subentendido) se as bolas de raio e centradas nas palavras-código cobrem todo o espaço, ou seja $\biguplus_{c \in C} B(c,e) = \mathbb{Z}_q \times \mathbb{Z}_q$ (onde $\uplus$ denota união disjunta). Num código perfeito as bolas de Lee de raio e ladrilhan $\mathbb{Z}_q \times \mathbb{Z}_q$ (ver Figura 5). Uma condição necessária para que um código seja perfeito é que $d_{min} = 2e+1$. Além disto, se $2e+1 < q$ teremos necessariamente que o número, $\#C$, de palavras-código deverá satisfacer $q^2 = \#C \cdot q_e$ (onde $q_e = 2e^2 + 2e + 1$ é o número de pontos da bola de raio e) e portanto $q_e \mid q^2$.

Num código e-perfeito, para $c \in C$ consideremos as bolas $B(c_1, e), \ldots, B(c_\tau, e)$ centradas nas palavas do código que são adjacentes a $B(c,e)$. Definimos o "kissing number" relativo a c como $\tau = \tau(c)$ e dizemos que $c_1, \ldots, c_\tau$ são as palavras-código vizinhas de c. No caso em que todas as palavras tenham o mesmo "kissing number", definimos este número como o "kissing number" do código. Associado a C também temos uma função $f : \mathbb{Z}_q \times \mathbb{Z}_q \to C$ tais que $f(x) = c \Leftrightarrow x \in B(c,e)$ chamada função corretora de erro. O fato do código ser perfeito é essencial para que esta função esteja bem definida.

O conjunto formado por todos os códigos perfeitos e-corretores em $\mathbb{Z}_q \times \mathbb{Z}_q$ é denotado[1] por $PL(2,e,q)$. O conjunto $PL(2,e,q)$ é fechado em relaï¿½ï¿½o a translações e conjugação[2] ou seja, se $C \in PL(2,e,q)$ e $x \in \mathbb{Z}_q \times \mathbb{Z}_q$ então

- $x + C = \{x + c : c \in C\} \in PL(2,e,q)$.
- $\overline{C} = \{\overline{c} : c \in C\} \in PL(2,e,q)$.

Um código C é dito linear se ele é um subgrupo de $\mathbb{Z}_q \times \mathbb{Z}_q$. Códigos lineares são os mais usados na prática, já que a sua estrutura permite provar propriedades com mais facilidade. O Teorema de Estrutura para grupos abelianos [14], neste caso, implica que C vai ser isomorfo ou a $\mathbb{Z}_n$ para $n = \#C$ (e dizemos que C é cíclico), ou isomorfo a $\mathbb{Z}_t \times \mathbb{Z}_s$ com t múltiplo de s, $t > 1$ e $ts = \#C$. Achar uma base para C significa, no primeiro caso achar um gerador, e no segundo caso achar dois elementos $v_1, v_2 \in C$ tais que a função $\varphi : \mathbb{Z}_n \times \mathbb{Z}_m \to C$ dada por $\varphi(i,j) = iv_1 + jv_2$ seja um isomorfismo de grupos. Neste caso escrevemos $C = v_1\mathbb{Z} \oplus v_2\mathbb{Z}$. No caso em que $\{v_1, v_2\}$ seja um conjunto gerador qualquer (não necessariamente uma base) escrevemos $C = v_1\mathbb{Z} + v_2\mathbb{Z}$ (ou $C = v_1\mathbb{Z}_q + v_2\mathbb{Z}_q$ se quizermos enfatizar que estamos trabalhando em $\mathbb{Z}_q \times \mathbb{Z}_q$).

Denotaremos por $e_1 = (1,0)$ e $e_2 = (0,1)$ a base canônica de $\mathbb{Z}_q \times \mathbb{Z}_q$ e as retas horizontais e verticais por $h_i = \mathbb{Z}_q \times \{i\}$ e $v_j = \{j\} \times \mathbb{Z}_q$ respetivamente (para cada i e j em $\mathbb{Z}_q$ fixos). Um segmento horizontal é um subconjunto de uma reta horizontal da forma $s = s(p,\ell) = \{p + ke_1 : 0 \leq k < \ell\}$ onde $p \in \mathbb{Z}_q \times \mathbb{Z}_q$ e $\ell < q$ é o comprimento do segmento. Um segmento vertical é um subconjunto de uma reta vertical da forma $s = s(p,\ell) = \{p + ke_2 : 0 \leq k < \ell\}$ onde $p \in \mathbb{Z}_q \times \mathbb{Z}_q$ e $\ell < q$ é o comprimento do segmento. Também denotaremos por $\nu_1 = (e, e+1), \nu_2 = (-(e+1), e), \eta_1 = (1, -(2e+1)), \eta_2 = (0, q_e)$ (vetores de $\mathbb{Z}_q \times \mathbb{Z}_q$), $D_e = \nu_1\mathbb{Z} + \nu_2\mathbb{Z}$.

III. O Teorema de Classificação

O resultado principal deste trabalho é o seguinte teorema que será provado no final desta seção.

Teorema 1 (Classificação): Seja $PL(2,e,q)$ o conjunto dos códigos Lee-perfeitos (não necessáriamente lineares) e-corretores em $\mathbb{Z}_q \times \mathbb{Z}_q$. Sejam $q_e = 2e^2 + 2e + 1$ e $\nu_1 = (e, e+1), \nu_2 = (-(e+1), e), \eta_1 = (1, -(2e+1)), \eta_2 = (0, q_e)$ vetores de $\mathbb{Z}_q \times \mathbb{Z}_q$, $D_e = \nu_1\mathbb{Z} + \nu_2\mathbb{Z}$ e $\overline{v}$ o conjugado de v, então temos a seguinte caracterização:

1) (Existência) $PL(2,e,q) \neq \emptyset \Leftrightarrow q \equiv 0 \pmod{q_e}$ onde $q_e = 2e^2 + 2e + 1$.
2) (Caracterização) $C \in PL(2,e,q) \Leftrightarrow C = c + D_e$ ou $C = c + \overline{D_e}$ onde $c \in C$ qualquer (em particular $C - c$ é um grupo).
3) (Estrutura) Seja $C \in PL(2,e,q)$ e $G_C = C - c$, o grupo asociado a C (onde $c \in C$) então:
   i) G_C é cíclico se e somente se $q = q_e$. Neste caso $G_C \simeq \mathbb{Z}_q$ com gerador $\nu_1 = (e, e+1)$ se $G_C = D_e$ ou $\overline{\nu}_1$ se $G_C = \overline{D_e}$.
   ii) Se $q = hq_e$ com $h > 1$ então $G_C \simeq \mathbb{Z}_q \times \mathbb{Z}_h$. Mais explícitamente $G_C = \eta_1\mathbb{Z} \oplus \eta_2\mathbb{Z}$ ou $G_C = \overline{\eta_1}\mathbb{Z} \oplus \eta_2\mathbb{Z}$ dependendo se $G_C = D_e$ ou $G_C = \overline{D_e}$ respectivamente.

Os dois lemas geométricos a seguir são de simples verificação.

Lema 1 (Seções de bolas): Se uma reta horizontal r corta uma bola de Lee $B = B(c,e)$ então $\#(B \cap r) = 2\ell + 1$ com ℓ inteiro e $\ell \leq e$. Se $B \cap r = \{c' + (i,0) : -\ell \leq i \leq \ell\}$ então $c = c' + (e-\ell)e_2$ ou $c = c' - (e-\ell)e_2$. Em particular se $\ell = e$ temos que c é o ponto médio do segmento $B \cap r$.

Claramente um resultado análogo vale para retas verticais.

Definição 1: Se $x \in \mathbb{Z}_q \times \mathbb{Z}_q$ definimos o conjunto superior, inferior, direito e esquerdo de x como:

- $up(x) = x + \{(-1,1), (0,1), (1,1)\}$
- $down(x) = x + \{(-1,-1), (0,-1), (1,-1)\}$
- $right(x) = x + \{(1,-1), (1,0), (1,-1)\}$
- $left(x) = x + \{(-1,-1), (-1,0), (-1,1)\}$

respectivamente.

Lema 2 (Lema T): Seja B uma bola de raio e com $1 \leq e < \frac{q-1}{2}$.

[1] Na literatura é comum denotar por $PL(2,e,q)$ o conjunto dos códigos lineares e-corretores que são perfeitos na métrica de Lee, neste trabalho vamos a incluir também os não lineares.

[2] Se $v = (x,y) \in \mathbb{Z}_q \times \mathbb{Z}_q$ definimos seu conjugado como $\overline{v} = (-x, y)$.

i) Se $\#(h_{i+1} \cap B) > \#(h_i \cap B) \Rightarrow \forall x \in h_i \cap B : up(x) \subseteq B$.
ii) Se $\#(h_{i-1} \cap B) > \#(h_i \cap B) \Rightarrow \forall x \in h_i \cap B : down(x) \subseteq B$.
iii) Se $\#(h_i \cap B) > \max\{\#(h_{i+1} \cap B), \#(h_{i-1} \cap B)\} \Rightarrow \#(h_i \cap B) = 2e + 1$.

Por simetria, obtém-se a versão do Lema T, cortando a bola por retas verticais em lugar de horizontais.

Lema 3 (Lema do estilingue): Seja $C \in PL(2, e, q)$ e $f : \mathbb{Z}_q \times \mathbb{Z}_q \to C$ a função corretora de erro asociada. Seja $B = B(c, e)$ com $c \in C$ e $P \in B$:

1) Se $up(P) \not\subseteq B$ e $down(P) \not\subseteq B$ então:
   i) $f(P) \neq f(P - e_1) \Rightarrow f(P) = P + e \cdot e_1$.
   ii) $f(P) \neq f(P + e_1) \Rightarrow f(P) = P - e \cdot e_1$.
2) Se $right(P) \not\subseteq B$ e $left(P) \not\subseteq B$ então:
   i) $f(P) \neq f(P - e_2) \Rightarrow f(P) = P + e \cdot e_2$.
   ii) $f(P) \neq f(P + e_2) \Rightarrow f(P) = P - e \cdot e_2$.

Demonstração: Basta provar a parte i de 1) (as outras são análogas). Seja $i = x(P)$. Usando o Lema T obtemos que $\#(h_i \cap B) = 2e + 1$, logo, pelo Lema 1 $h_i \cap B = \{P + (j, 0) : -t \leq j \leq k\}$ com $t, k \geq 0$ e $t + k + 1 = 2e + 1$. Como $f(P) \in B$ (pois $P \in B$) e $f(P - e_1) \neq f(P)$ então $P - e_1 \notin B$. Em particular $P - e_1 \notin h_i \cap B$, logo $t = 0, k = 2e$ e $h_i \cap B = \{P, \ldots, P + (2e, 0)\}$ e pelo Lema 1 o centro da bola B é $f(P) = P + (e, 0)$ (ver a Figura 1 que justifica o nome do lema).

□

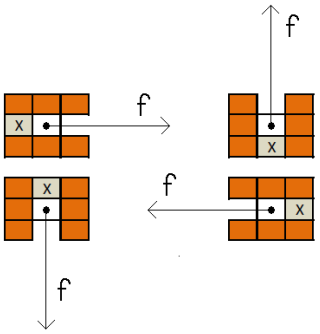

Fig. 1. Ilustração do Lema do estilingue.

Definição 2: Denotaremos por $\mathcal{C} \subseteq \mathbb{Z}_q \times \mathbb{Z}_q$ o conjunto dado por $\mathcal{C} = \{(-1, i) : -1 \leq i \leq 2\} \cup \{(0, -1), (0, 2)\}$.

Definição 3: Sejam B_1 e B_2 duas bolas de raio e adjacentes. Dizemos que estas estão bem encaixadas se $x + \mathcal{C} \subseteq B_1 \cup B_2 \Rightarrow x \in B_1 \cup B_2$ ou $x + e_2 \in B_1$. Caso contrário dizemos que estão mal encaixadas (ver Figura).

Lema 4 (Lema de encaixamento): Se $C \in PL(2, e, q)$ então no recobrimento $\biguplus_{c \in C} B(c, e) = \mathbb{Z}_q \times \mathbb{Z}_q$, duas bolas quaisquer são bem encaixadas.

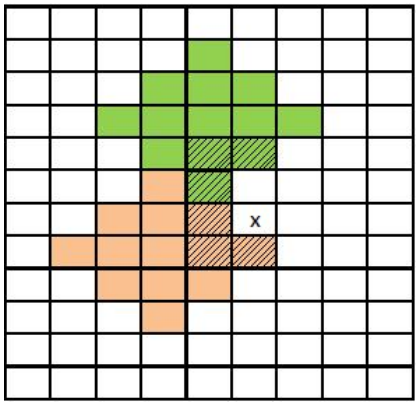

Fig. 2. Exemplo de bolas adjacentes mal encaixadas.

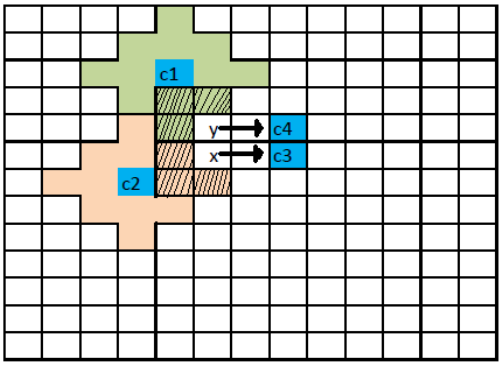

Fig. 3. Ilustração do lema de encaixamento (c_1, c_2, c_3, c_4, x e y como na prova do Lema).

Demonstração: Suponhamos por absurdo que existam duas bolas adjacentes $B_1 = B(c_1, e)$ e $B_2 = B(c_2, e)$ mal encaixadas e seja $x \in \mathbb{Z}_q \times \mathbb{Z}_q$ tais que $x + \mathcal{C} \subseteq B_1 \cup B_2$ mas $x \notin B_1 \cup B_2$ e $y = x + e_2 \notin B_1 \cup B_2$ (ver Figura). Se $f : \mathbb{Z}_q \times \mathbb{Z}_q \to C$ é a função corretora de erro asociada a C, podemos aplicar o Lema do estilingue a x e y obtendo duas palavras do código $c_3 = f(x) = x + e \cdot e_1$ e $c_4 = f(y) = y + e \cdot e_1$ com $d(c_3, c_4) = \| e_2 \|_{1,Lee} = 1 < 2e + 1 = d_{min}(C)$, o que é absurdo (ver Figura 3).

□

Lema 5 (Rigidez): Seja $C \in PL(2, e, q)$, $\biguplus_{c \in C} B(c, e) = \mathbb{Z}_q \times \mathbb{Z}_q$ e $f : \mathbb{Z}_q \times \mathbb{Z}_q \to C$ a função corretora de erro associada. Para todo $c \in C$ temos que $f(c + (e + 1)e_2) \neq f(c + ee_2)$.

Demonstração: Seja $c' = f(c + (e + 1)e_2)$ e r a reta vertical que passa por c. Como $c + (e+1)e_2 \in r \cap B(c', e) \Rightarrow \#(r \cap B(c', e)) = 2\ell + 1$ com $0 \leq \ell \leq e$. Observamos que $f(c + (e + 1)e_2) = f(c + (e + 2)e_2) \Leftrightarrow \ell = 0$. Vamos supor por absurdo que $\ell > 0$. Aplicando o Lema 1 resulta que $c' = x_0 \pm (e - \ell)e_1$ onde $r \cap B(c', e) = \{x_0 + ie_2 : -\ell \leq i \leq \ell\}$. Aplicando uma reflexão em relação a r se for necessário, podemos supor que $c' = x_0 - (e - \ell)e_1$. Não é dificil provar

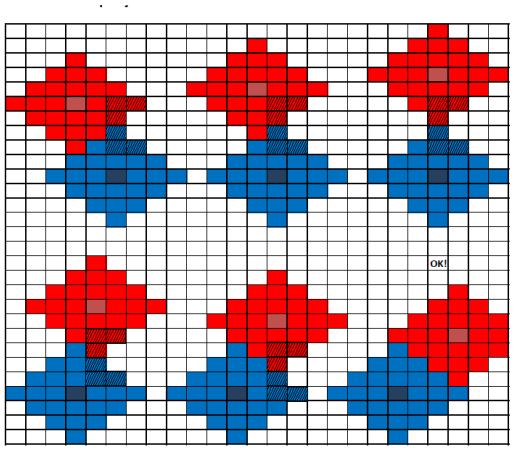

Fig. 4. Ilustração do Lema 5. A única posibilidade para encaixar a bola "por acima" a menos de simetrias.

que neste caso o ponto x verifica:

- $x = c + (1, e) \notin B(c, e) \cup B(c', e)$.
- $x + \mathcal{C} \subseteq B(c, e) \cup B(c', e)$.
- $x + (0, 1) \notin B(c, e) \cup B(c', e)$ (pois $\ell > 0$).

Mas então $B(c, e)$ e $B(c', e)$ seriam bolas adjacentes mal encaixadas o que contradiz o Lema de encaixamento (ver Figura 4).

□

Definição 4: Seja $C \in PL(2, e, q)$. Para cada $c \in C$ definimos o conjunto $\omega(c) = \{v_1, \ldots, v_\tau\}$ onde as bolas adjacentes a $B(c, e)$ são exatamente $B(c + v_i, e)$ para $1 \leq i \leq \tau$.

Lema 6 (Kissing Lema): Seja $C \in PL(2, e, q)$. O "kissing number" de C é $\tau = 4$ e o conjunto $\omega(c)$ não depende de c. Mais ainda, só temos duas possibilidades:

i) $\omega(c) = \{\pm\nu_1, \pm\nu_2\}$ (tipo 1).
ii) $\omega(c) = \{\pm\overline{\nu_1}, \pm\overline{\nu_2}\}$ (tipo 2).

Demonstração: Sejam $c \in C$, r a reta vertical passando por c e $c_1 = f(c+(e+1)e_2)$. A bola $B_1 = B(c_1, e)$ é vizinha de $B = B(c, e)$. Pelo Lema 5 $\#(r \cap B_1) = 1$, logo, usando o Lema 1 tem-se que $c_1 = c + \nu_1$ ou $c_1 = c + \overline{\nu_1}$. Vamos ver primeiro o caso em que $c_1 = c + \nu_1$. Aplicando o Lema do estilingue no ponto $P_1 = c + (-1, e)$ obtemos um novo ponto $c_2 = f(P) = c + \nu_2$ com $B_2 = B(c_2, e)$ adjacente a B. Aplicando o mesmo lema ao ponto $P_2 = c + (-e, -1)$ obtemos uma terceira bola $B_3 = B(c - \nu_1, e)$ adjacente a B e aplicando o "estilingue" a $P_3 = c + (1, -e)$ obtemos uma quarta bola $B(c - \nu_2, e)$ adjacente a B. Portanto[3] $\tau \geq 4$ e $\omega := \{\pm\nu_1, \pm\nu_2\} \subset \omega(c)$. Para provar a igualdade basta ver que $\{P \in \mathbb{Z}_q \times \mathbb{Z}_q : d(P, B) = 1\} - c = \bigcup_{i=1}^{4} \ell_i$ onde $\ell_1 = \{(x, e + 1 - x) : 0 \leq x \leq e\}, \ell_1 = \{(x, e + 1 - x) : 0 \leq x \leq e\}, \ell_2 = \{(y - (e + 1), y) : 0 \leq y \leq e\}, \ell_3 = \{(x, -x - (e + 1)) : 0 \leq x \leq e\}, \ell_4 = \{(y + (e + 1), y) : 0 \leq y \leq e\}$ e calculando as distâncias ao centro das bolas obtemos $c + \ell_i \subset B_i$ para $1 \leq i \leq 4$ o que prova $\tau = 4$ e $\omega(c) = \{\pm\nu_1, \pm\nu_2\}$. No caso em que $c_1 = c - \nu_1$, chegamos a que $\tau = 4$ e $\omega(c) = \overline{\omega} := \{\pm\overline{\nu_1}, \pm\overline{\nu_2}\}$. Para provar que $\omega(c)$ não depende de c basta provar que para $c, c' \in C$ vizinhos (ou seja, com bolas adjacentes) tem-se que $\omega(c) = \omega(c')$. Por serem vizinhos temos que $0 \in \omega(c) + \omega(c')$ mais se $\omega \neq \overline{\omega}$ então $0 \notin \omega + \overline{\omega} = \{\pm\nu_1 \pm \overline{\nu_1}, \pm\nu_2 \pm \overline{\nu_2}\}$ (pois $q > 2e$), logo $\omega(c) = \omega(c')$.

[3]Observar que as bolas são todas distintas já que $q > 2$.

□

Agora temos os elementos para provar o Teorema 1.

Demonstração do Teorema 1: Suponhamos $PL(2, e, q) \neq 0$ e sejam $C \in PL(2, e, q)$ e $c \in C$. Suponhamos que C seja tipo 1 $\Rightarrow$ C é fechado pelas translações $x \mapsto x + \nu_1$ e $x \mapsto x + \nu_2$ (Kissing Lema) $\Rightarrow c + \nu_1\mathbb{Z} + \nu_2\mathbb{Z} \subseteq C$. Se $c' \in C$ então existe uma sequência em C: $c_0 = c, c_1, \ldots, c_k = c'$ tais que $B(c_{i-1}, e)$ e $B(c_i, e)$ são adjacentes para $i = 1, \ldots, k \Rightarrow c_i - c_{i-1} \in \omega(c_{i-1}) \subset \nu_1\mathbb{Z} + \nu_2\mathbb{Z} \Rightarrow c' = c_0 + \sum_{i=1}^{k}(c_i - c_{i-1}) \in c + \nu_1\mathbb{Z} + \nu_2\mathbb{Z}$.

Como $mdc(e, e + 1) = 1 \Rightarrow |\nu_1\mathbb{Z}| = q$. Pelo Teorema de Lagrange [14] $q = |\nu_1\mathbb{Z}| \mid |\nu_1\mathbb{Z} + \nu_2\mathbb{Z}| = \#C \Rightarrow \#C = qh$ com $h \in \mathbb{Z}^+$. Pela condição de empacotamento $\#B(0, e) \cdot \#C = q^2 \Leftrightarrow q_e \cdot qh = q^2 \Leftrightarrow q = q_e h$ e portanto $q \equiv 0 \pmod{q_e}$.

Até aqui provamos que se $PL(2, e, q) \neq \emptyset \Rightarrow q \equiv 0 \pmod{q_e}$ e todo $C \in PL(2, e, q)$ e igual a D_e ou $\overline{D_e}$ a menos de translação. Reciprocamente, já sabemos que se $q = q_e h$ com $h \in \mathbb{Z}^+$ o código D_e é perfeito em $\mathbb{Z}_q \times \mathbb{Z}_q$ portanto $PL(2, e, q) \neq \emptyset$ o que prova a parte i). Como a perfeição e cardinalidade são preservadas por translação e conjugação temos que todos os códigos da forma $c + D_e$ ou $c + \overline{D_e}$ estão em $PL(2, e, q)$ e temos provada a parte ii.

Para provar a parte iii, podemos supor que C é linear e de tipo 1, ou seja $C = \nu_1\mathbb{Z} + \nu_2\mathbb{Z}$. Como $\begin{pmatrix} -1 & -1 \\ e+1 & e \end{pmatrix}\begin{pmatrix} \nu_1 \\ \nu_2 \end{pmatrix} = \begin{pmatrix} \eta_1 \\ \eta_2 \end{pmatrix}$ e $\det\begin{pmatrix} -1 & -1 \\ e+1 & e \end{pmatrix} = 1$ então $C = \eta_1\mathbb{Z} + \eta_2\mathbb{Z}$ onde $\eta_1 = (1, -(2e + 1))$ e $\eta_2 = (0, q_e)$ (em $\mathbb{Z}_q \times \mathbb{Z}_q$). Claramente $\eta_1\mathbb{Z} \cap \eta_2\mathbb{Z} = (0), |\eta_1\mathbb{Z}| = q$ e $|\eta_2\mathbb{Z}| = \frac{q}{q_e} = h$ onde comcluimos que $C = \eta_1\mathbb{Z} \oplus \eta_2\mathbb{Z} \simeq \mathbb{Z}_q \times \mathbb{Z}_h$. Como $h|q$ é claro que C cíclico se e somente se $h = 1$.

□

Corolário 1: Existem exatamente $2q_e = 4e^2 + 4e + 2$ códigos perfeitos em $PL(2, e, q)$ onde $q \equiv 0 \pmod{q_e}$, dois dos quais são lineares e os restantes são transladados destes dois códigos lineares. Os dois códigos lineares são conjugados. Portanto existe um único código Lee-perfeito em $PL(2, e, q)$ a menos de translação e conjugação.

Observação 1: No caso $q = q_e$ o código único do Corolário 1 é exatamente o código cíclico $D_e = \langle(e, e + 1)\rangle \subseteq \mathbb{Z}_q \times \mathbb{Z}_q$ introduzido por Golomb-Welch.

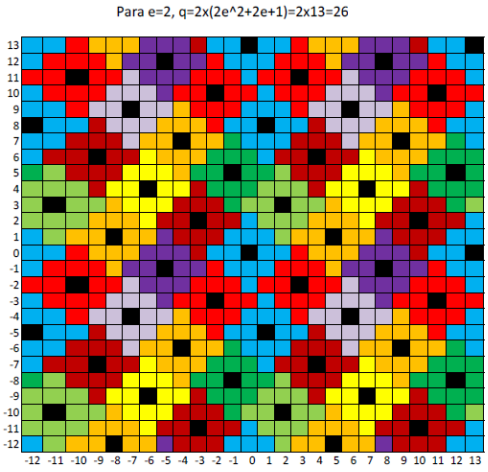

Fig. 5. Código Lee-perfeito em $\mathbb{Z}_{26} \times \mathbb{Z}_{26}$ não cíclico gerado pelos vetores $(1, 21)$ e $(0, 13)$ (os quadradinhos pretos representam as palavras-código).

Corolário 2: Existem códigos Lee-perfeitos não cíclicos (quando $q = hq_e$, $h > 1$).

Observação 2: O código em $\mathbb{Z}^2$ associado ao código único dado pelo Corolário 1 (imagem inversa da aplicação módulo q) para $q = hq_e$ com $h > 1$ é o mesmo que o código em $\mathbb{Z}^2$ associado ao código D_e ($q = 1$). Isto é equivalente a dizer que os reticulados em $\mathbb{Z}^2$ associados a qualquer código $C \in PL(2, q, e)$ é o mesmo que aquele obtido a partir de D_e via construção A [13]

Exemplo 1: Se $q = 26$ e $e = 2$ temos o código $C = (1, 21)\mathbb{Z}_{26} + (0, 13)\mathbb{Z}_{26}$ sobre $\mathbb{Z}_{26} \times \mathbb{Z}_{26}$ (ver figura 5).

Corolário 3: Para q fixo, a quantidade de códigos Lee-perfeitos em $\mathbb{Z}_q \times \mathbb{Z}_q$ coincide com a quantidades de divisores de q da forma $e^2 + (e + 1)^2$. Em particular, este número é a quantidade de divisores d de q da forma $d \equiv 1 \pmod{1 + i}$ nos enteros de Gauss (o que poderia dar indicio que tem uma estrutura de anél implícita que joga um papel importante).

Exemplo 2: Existem exatamente 5 códigos Lee-perfeitos em $\mathbb{Z}_{1105} \times \mathbb{Z}_{1105}$ a menos de translação e conjugação ($1105 = 5 \cdot 13 \cdot 17$), um dele é cíclico e os outros quatro são não cíclicos e vem dados por:

- $C_1 = (1, -3)\mathbb{Z}_{1105} \oplus (0, 5)\mathbb{Z}_{1105}$ ($e = 1$).
- $C_2 = (1, -5)\mathbb{Z}_{1105} \oplus (0, 13)\mathbb{Z}_{1105}$ ($e = 2$).
- $C_3 = (1, -13)\mathbb{Z}_{1105} \oplus (0, 85)\mathbb{Z}_{1105}$ ($e = 6$).
- $C_4 = (1, -21)\mathbb{Z}_{1105} \oplus (0, 221)\mathbb{Z}_{1105}$ ($e = 10$).
- $C_5 = (23, 24)\mathbb{Z}_{1105}$ ($e = 23$).

IV. Conclusão

Neste trabalho apresentamos uma classificação completa dos códigos q-ários bidimensionais que são perfeitos na métrica de Lee. Este resultado permite além de explicitar quais são os parâmetros possíveis (o que já era conhecido), determinar (Teorema 1, item 2) para cada q quais são todos os códigos perfeitos em $\mathbb{Z}_q \times \mathbb{Z}_q$, a menos de simetria, e determinar que estrutura tem esses códigos. A perspectiva é a de que alguns dos resultados aqui apresentados possam ser utilizados para abordar o problema da existência e possíveis aplicações de códigos (q-ários ou sobre grafos [12]) perfeitos ou densos em dimensões maiores.

Referências

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

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

[3] T. Etzion, A. Vardy, E. Yaakobi. Dense error-correcting codes in the Lee metric, Information Theory Workshop (ITW), 2010 IEEE.

[4] S. W. Golomb, L. R. Welch. Perfect Codes in the Lee metric and the packing of polynominoes, SIAM Journal Applied Math., vol. 18, pp. 302-317. 1970.

[5] R. M. Roth, P. H. Siegel. Lee-metric BCH codes and their application to constrained and partial-response channels, IEEE trans. Inform. Theory, vol. IT-40, pp. 1083-1096, July 1994.

[6] M. Blaum, J. Bruck, A. Vardy. Interleaving schemes for multidimensional cluster errors, IEEE trans. Inform. Theory, vol. IT-53, pp. 808-814, February 2007.

[7] K. U. Schmidt. Complementary sets, generalized Reed-Muller codes, and power control for OFDM, IEEE trans. Inform. Theory, vol. IT-53, pp. 808-814, February 2007.

[8] T. Etzion, E. Yaakobi. Error-Corretion of Multidimensional Burst, IEEE trans. Inform. Theory, vol. IT-55, pp. 961-976, 2009.

[9] J. Astola. On perfect Lee codes over small alphabets of odd cardinality, Discrete Applied Mathematics, vol. 4, pp. 369-380, 1975.

[10] P. Horak. On Perfect Lee Codes, Discrete Mathematics, vol. 309, pp. 5551-5561, 2009.

[11] B. AlBdaiwi, P. Horak, L. Milazzo. Enumerating and decoding perfect linear Lee codes, Des. Codes. Crypt., vol. 52, pp. 227-228, 1982.

[12] S. I. R. Costa, M. Muniz, E. Agustini, R. Palazzo. Graphs tessellations, and perfect codes on flat tori, IEEE trans. Onform. Theory, vol. IT-50, pp. 2363-2377, 2004.

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

[14] T. W. Hungerford.Algebra, Springer-Verlag, New York, 2003.