Trabalho apresentado no CNMAC, Gramado - RS, 2016.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Reticulados a partir de Códigos sobre Anéis Finitos: Conexões entre as Construções D, D' e $\overline{D}$

Eleonesio Strey[1]
Departamento de Matemática Pura e Aplicada, UFES, Alegre, ES
Sueli I. R. Costa[2]
Departamento de Matemática, IMECC-UNICAMP, Campinas, SP

Resumo. Neste trabalho, mostramos que o reticulado $\Lambda_{D'}$ obtido via Construção D' a partir de uma cadeia de códigos lineares q-ários é igual ao reticulado $q\Lambda^*_{D^\perp}$, onde $\Lambda_{D^\perp}$ é o reticulado obtido via Construção D a partir da cadeia de códigos lineares duais associada e $\Lambda^*_{D^\perp}$ é o reticulado dual de $\Lambda_{D^\perp}$. Além disso, a cadeia de códigos lineares duais associada é fechada sob a adição zero-um se e somente se $\Gamma_{\overline{D}^\perp}$ é um reticulado e $\Lambda_{D'} = q^a\Gamma^*_{\overline{D}^\perp}$, onde $\Gamma_{\overline{D}^\perp}$ é obtido via Construção $\overline{D}$ a partir da cadeia de códigos lineares duais associada. Finalmente, sob certas condições, fornecemos uma base para o reticulado $\Lambda_{D'}$ em função dos parâmetros utilizados em sua construção.

Palavras-chave. Reticulados, Códigos sobre Anéis, Construção D

1 Introdução

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 (veja [10] e suas referências) e na proposição de esquemas criptográficos [6, 7]. 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. O *determinante* de Λ é definido como $\det\Lambda = \det(MM^t)$ e este é um invariante por mudança de base. Denotamos por $\text{span}(M) = \{\boldsymbol{u}M;\ \boldsymbol{u} \in \mathbb{R}^n\}$ o espaço vetorial gerado pelas linhas da matriz M. O *reticulado dual* de $\Lambda = \Lambda(M)$, denotado por $\Lambda^* = \Lambda^*(M)$, é definido como

$$\Lambda^* = \{\boldsymbol{w} \in \text{span}(M);\ \langle \boldsymbol{v}, \boldsymbol{w}\rangle \in \mathbb{Z}, \forall \boldsymbol{v} \in \Lambda\},$$

[0]Este trabalho foi parcialmente financiado por FAPESP 2013/25997-7 e CNPq 312926/2013-8.
[1]eleonesio.strey@ufes.br
[2]sueli@ime.unicamp.br

onde $\langle , \rangle$ representa o produto interno canônico em $\mathbb{R}^n$. Pode-se mostrar que M é uma matriz geradora para Λ se e somente se $(MM^t)^{-1}M$ (a pseudo-inversa de M^t) é uma matriz geradora para Λ^*. O dual de $k\Lambda$ é $(1/k)\Lambda^*$, para todo $0 \neq k \in \mathbb{R}$. Além disso, para qualquer reticulado Λ, tem-se $(\Lambda^*)^* = \Lambda$.

Um *código linear q-ário* C é um subgrupo aditivo de $\mathbb{Z}_q^n$, $q \in \mathbb{N}$. 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 $C = \langle(\overline{2}, \overline{4})\rangle = \{(\overline{0}, \overline{0}), (\overline{2}, \overline{4}), (\overline{4}, \overline{2})\} \subseteq \mathbb{Z}_6^2$ 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 $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = x_1y_1 + \cdots + x_ny_n$. Pode-se mostrar que $C^\perp = \{\boldsymbol{y} \in \mathbb{Z}_q^n;\ \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0, \forall \boldsymbol{x} \in C\}$ é um código linear q-ário, $C^\perp$ é denominado o *código dual* de C. Se C_1 e C_2 são códigos q-ários tais que $C_1 \supseteq C_2$, então $C_1^\perp \subseteq C_2^\perp$.

Existem várias construções que fornecem reticulados a partir de códigos lineares q-ários. Neste trabalho estudamos as Construções D e D' que foram introduzidas por Barnes e Sloane em [1] e a Construção $\overline{D}$ que foi introduzida por Forney em [3,4]. Inicialmente estas construções eram feitas apenas a partir de cadeias de códigos binários e depois a partir de códigos sobre $\mathbb{Z}_p$, p primo. Em [8] estas construções foram estendidas para cadeias de códigos q-ários, $q \in \mathbb{N}$. Na próxima seção apresentamos estas construções e também alguns resultados preliminares.

2 Conceitos e resultados preliminares

Sejam $\overline{\sigma} : \mathbb{Z} \to \mathbb{Z}_q$ o homomorfismo módulo q e $\sigma : \mathbb{Z}_q \to \mathbb{Z}$ a "inclusão" natural tal que $\overline{\sigma}\big(\sigma(x)\big) = x$ para todo $x \in \mathbb{Z}_q$. A aplicação σ é estendida naturalmente da seguinte forma: $\sigma : \mathbb{Z}_q^n \to \mathbb{Z}^n$ dada por $\sigma(x_1, ..., x_n) = \big(\sigma(x_1), ..., \sigma(x_n)\big)$.

Definição 2.1. (*Construção D*) *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$, $q \in \mathbb{N}$, uma família de códigos lineares q-ários. 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*

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

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

Teorema 2.1. [8] *O conjunto Λ_D pode ser representado da seguinte forma:*

$$\Lambda_D = \left\{ q\boldsymbol{z} + \sum_{i=1}^{a} \sum_{j=k_{i+1}+1}^{k_i} \alpha_j^{(i)} \frac{1}{q^{i-1}} \sigma(\boldsymbol{b}_j) \,\middle|\, \boldsymbol{z} \in \mathbb{Z}^n \text{ e } \alpha_j^{(i)} \in \{0, 1, ..., q^i - 1\} \right\}.$$

Definição 2.2. (*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 $0 \leq r_1 \leq r_2 \leq \cdots \leq r_a$*

DOI: 10.5540/03.2017.005.01.0228

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* $\ell = 1, 2, ..., a$, *onde* $C_\ell^\perp$ *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 todo par (i, j) *satisfazendo* $0 \leq i < a$ *e* $r_{a-i-1} < j \leq r_{a-i}$, *onde* $r_0 := 0$.

Definição 2.3. (*Construção* $\overline{D}$) *Seja* $\mathbb{Z}_q^n \supseteq C_1 \supseteq \cdots \supseteq C_a$ *uma cadeia de códigos lineares q-ários. Definimos o conjunto* $\Gamma_{\overline{D}} \subseteq \mathbb{Z}^n$ *da seguinte forma*

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

As Construções D e D' sempre geram reticulados de posto completo [8]. O conjunto $\Gamma_{\overline{D}} \subseteq \mathbb{Z}^n$ obtido via Construção $\overline{D}$ nem sempre é um reticulado (Exemplo 2.1). No Teorema 3.1 fornecemos uma condição necessária e suficiente para que $\Gamma_{\overline{D}}$ seja um reticulado.

Definição 2.4. *Dizemos que o menor reticulado que contém* $\Gamma_{\overline{D}}$, *o qual será denotado por* $\Lambda_{\overline{D}}$, *é o reticulado obtido via Construção* $\overline{D}$.

Exemplo 2.1. *Seja* $\mathbb{Z}_3^2 \supseteq C_1 \supseteq C_2$ *a cadeia de códigos lineares, onde* $C_1 = C_2 = \langle (1, 2) \rangle$. *Temos que* $C_1^\perp = C_2^\perp = \{(x, y) \in \mathbb{Z}_3^2; x + 2y = 0\} = \{(0, 0), (1, 1), (2, 2)\} = \langle (1, 1) \rangle$. *Assim, escolhendo os parâmetros* $k_1 = 2, k_2 = 1$, $r_1 = 1$, $r_2 = 2$ *e* $\boldsymbol{b}_1 = (1, 2), \boldsymbol{b}_2 = (2, 1), \boldsymbol{h}_1 = (1, 1), \boldsymbol{h}_2 = (2, 2) \in \mathbb{Z}_3^2$, *temos* $0 \leq k_2 \leq k_1$, $0 \leq r_1 \leq r_2$, $C_1 = \langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle$, $C_2 = \langle \boldsymbol{b}_1 \rangle$, $C_1^\perp = \langle \boldsymbol{h}_1 \rangle$, $C_2^\perp = \langle \boldsymbol{h}_1, \boldsymbol{h}_2 \rangle$ *e, consequentemente,*

$$\Lambda_D = \left\{ z + \alpha_2^{(1)}(2, 1) + \alpha_1^{(2)}\frac{1}{3}(1, 2) \,\middle|\, z \in 3\mathbb{Z}^2, 0 \leq \alpha_2^{(1)} < 3 \text{ e } 0 \leq \alpha_1^{(2)} < 9 \right\}$$

e

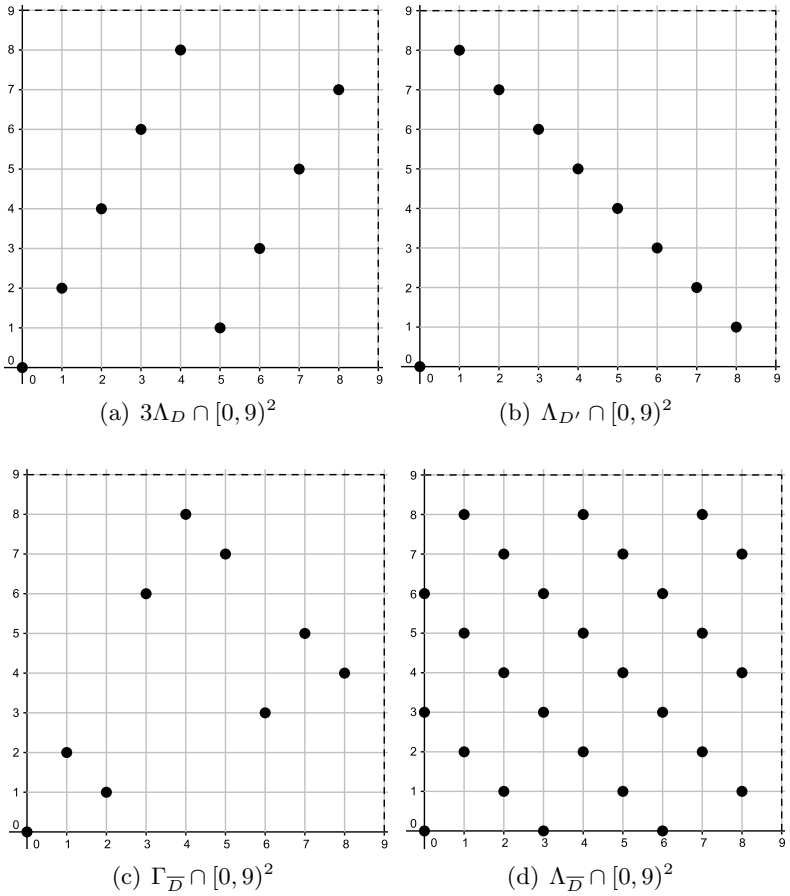
$$\Lambda_{D'} = \left\{ (x, y) \in \mathbb{Z}^2 \,\middle|\, x + y \equiv 0 \mod 9 \quad e \quad 2x + 2y \equiv 0 \mod 3 \right\}.$$

Além disso, $\Gamma_{\overline{D}} = 3^2\mathbb{Z}^2 + 3^1\sigma(C_1) + 3^0\sigma(C_2)$, *onde* $\sigma(C_1) = \sigma(C_2) = \{(0, 0), (1, 2), (2, 1)\}$. *Portanto,*

$$\begin{aligned}
3\Lambda_D &= \bigcup_{\boldsymbol{z} \in 9\mathbb{Z}^2} \left(\boldsymbol{z} + (3\Lambda_D) \cap [0, 9)^2\right), \\
\Lambda_{D'} &= \bigcup_{\boldsymbol{z} \in 9\mathbb{Z}^2} \left(\boldsymbol{z} + \Lambda_{D'} \cap [0, 9)^2\right), \\
\Gamma_{\overline{D}} &= \bigcup_{\boldsymbol{z} \in 9\mathbb{Z}^2} \left(\boldsymbol{z} + \Gamma_{\overline{D}} \cap [0, 9)^2\right) \text{ e} \\
\Lambda_{\overline{D}} &= \bigcup_{\boldsymbol{z} \in 9\mathbb{Z}^2} \left(\boldsymbol{z} + \Lambda_{\overline{D}} \cap [0, 9)^2\right),
\end{aligned}$$

onde os elementos de $3\Lambda_D \cap [0, 9)^2$, $\Lambda_{D'} \cap [0, 9)^2$, $\Gamma_{\overline{D}} \cap [0, 9)^2$ *e* $\Lambda_{D'} \cap [0, 9)^2$ *estão representados na Figura* 1. *Neste exemplo, observamos que* (*i*) $\Gamma_{\overline{D}} \subsetneqq \Lambda_{\overline{D}}$ (*isto é,* $\Gamma_{\overline{D}}$ *não é um reticulado*), (*ii*) $3\Lambda_D \subsetneqq \Lambda_{\overline{D}}$, (*iii*) $3\Lambda_D \not\subset \Lambda_{D'}$, (*iv*) $\Lambda_{D'} \not\subset 3\Lambda_D$ *e* (*v*) $\Lambda_{D'} \subsetneqq \Lambda_{\overline{D}}$.

DOI: 10.5540/03.2017.005.01.0228



(a) $3\Lambda_D \cap [0,9)^2$ (b) $\Lambda_{D'} \cap [0,9)^2$

(c) $\Gamma_{\overline{D}} \cap [0,9)^2$ (d) $\Lambda_{\overline{D}} \cap [0,9)^2$

Figura 1: Elementos de $3\Lambda_D$, $\Lambda_{D'}$, $\Gamma_{\overline{D}}$ e $\Lambda_{\overline{D}}$ em $[0,9)^2$

3 Conexões entre as Construções D, D' e $\overline{D}$

Definimos uma operação em $\mathbb{Z}_q^n$, chamada *adição zero-um*, da seguinte forma: Para cada par de vetores $\boldsymbol{x} = (x_1, ..., x_n), \boldsymbol{y} = (y_1, ..., y_n) \in \mathbb{Z}_q^n$, a adição zero-um de $\boldsymbol{x}$ por $\boldsymbol{y}$ é dada por

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

onde

$$x_i * y_i = \begin{cases} 0, \text{ se } \sigma(x_i) + \sigma(y_i) < q \\ 1, \text{ se } q \leq \sigma(x_i) + \sigma(y_i) \leq 2(q-1). \end{cases}$$

Uma família de códigos lineares q-ários $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ 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 $i = 2, ..., a$. Por exemplo, a cadeia $\mathbb{Z}_3^2 \supseteq C_1 \supseteq C_2$ usada no Exemplo 2.1 não é fechada sob a adição zero-um, pois $(1,2) \in C_2$ e $(1,2) * (1,2) = (0,1) \notin C_1$.

Teorema 3.1. [8] *$\Gamma_{\overline{D}}$ 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 o adição zero-um. Neste caso, $\Gamma_{\overline{D}} = q^{a-1}\Lambda_D$.*

DOI: 10.5540/03.2017.005.01.0228

Os próximos dois lemas estendem para códigos q-ários resultados conhecidos anteriormente para Construções D e D' a partir de códigos binários [9].

Lema 3.1. *Se H é a matriz $k_1 \times n$, cujas linhas são*

$$\sigma(\boldsymbol{b}_1), ..., \sigma(\boldsymbol{b}_{k_a}), q\sigma(\boldsymbol{b}_{k_a+1}), ..., q\sigma(\boldsymbol{b}_{k_{a-1}}), ..., q^{a-1}\sigma(\boldsymbol{b}_{k_2+1}), ..., q^{a-1}\sigma(\boldsymbol{b}_{k_1}),$$

então $\boldsymbol{x} \in \Lambda_D^*$ se e somente se $q\boldsymbol{x} \in \mathbb{Z}^n$ e $H\boldsymbol{x}^t \equiv 0 \mod q^{a-1}$.

Demonstração. Por definição, $\Lambda_D^* = \{\boldsymbol{x} \in \mathbb{R}^n; \langle \boldsymbol{x}, \boldsymbol{y}\rangle \in \mathbb{Z}, \forall \boldsymbol{y} \in \Lambda_D\}$. Usando o Teorema 2.1, obtemos que $\boldsymbol{x} \in \Lambda_D^*$ se e somente se $\langle \boldsymbol{x}, q\boldsymbol{z}\rangle \in \mathbb{Z}$ e $\left\langle \boldsymbol{x}, (1/q^{i-1})\sigma(b_j)\right\rangle \in \mathbb{Z}$ para $1 \leq i \leq a$, $k_{i+1} < j \leq k_i$ e para todo $\boldsymbol{z} \in \mathbb{Z}^n$. Logo

$$\boldsymbol{x} \in \Lambda_D^* \quad \text{se e somente se} \quad q^{a-i}\langle \boldsymbol{x}, \sigma(\boldsymbol{b}_j)\rangle \equiv q^a \langle \boldsymbol{x}, \boldsymbol{e}_t\rangle \equiv 0 \mod q^{a-1}$$

para $1 \leq i \leq a$, $k_{i+1} < j \leq k_i$ e $1 \leq t \leq n$, onde $\{\boldsymbol{e}_1, ..., \boldsymbol{e}_n\}$ é a base canônica do $\mathbb{R}^n$. Portanto $\boldsymbol{x} \in \Lambda_D^*$ se e somente se $q\boldsymbol{x} \in \mathbb{Z}^n$ e $H\boldsymbol{x}^t \equiv 0 \mod q^{a-1}$. □

Lema 3.2. *Seja H a matriz $r_a \times n$, cujas linhas são*

$$\sigma(\boldsymbol{h}_1), ..., \sigma(\boldsymbol{h}_{r_1}), q\sigma(\boldsymbol{h}_{r_1+1}), ..., q\sigma(\boldsymbol{h}_{r_2}), ..., q^{a-1}\sigma(\boldsymbol{h}_{r_{a-1}+1}), ..., q^{a-1}\sigma(\boldsymbol{h}_{r_a}).$$

Temos que $\boldsymbol{x} \in \Lambda_{D'}$ se e somente se $\boldsymbol{x} \in \mathbb{Z}^n$ e $H\boldsymbol{x}^t \equiv 0 \mod q^a$.

Demonstração. Basta observar que $\boldsymbol{x} \in \Lambda_{D'}$ se e somente se $\boldsymbol{x} \in \mathbb{Z}^n$ e $q^{a-i}\boldsymbol{x} \cdot \sigma(\boldsymbol{h}_j) \equiv 0 \mod q^a$ para $0 < i \leq a$ e $r_{a-i} < j \leq r_{a-i+1}$. Logo $\boldsymbol{x} \in \Lambda_{D'}$ se e somente se $\boldsymbol{x} \in \mathbb{Z}^n$ e $H\boldsymbol{x}^t \equiv 0 \mod q^a$. □

Dada uma cadeia $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ de códigos lineares q-ários e parâmetros $0 \leq r_1 \leq r_2 \leq \cdots \leq r_a$ e $\boldsymbol{h}_1, ..., \boldsymbol{h}_{r_a} \in \mathbb{Z}_q^n$ tais que $C_i^\perp = \langle \boldsymbol{h}_1, ..., \boldsymbol{h}_{r_i}\rangle$ para $i = 1, 2, ..., a$, seja $\Lambda_{D^\perp}$ o reticulado obtido via Construção D a partir da cadeia $C_1^\perp \subseteq C_2^\perp \subseteq \cdots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$ (usando os parâmetros $r_1, r_2, ..., r_a, \boldsymbol{h}_1, ..., \boldsymbol{h}_{r_a}$), isto é,

$$\Lambda_{D^\perp} = \left\{ q\boldsymbol{z} + \sum_{i=1}^{a} \sum_{j=r_{a-i}+1}^{r_{a-i+1}} \alpha_j^{(i)} \frac{1}{q^{i-1}} \sigma(\boldsymbol{h}_j) \,\middle|\, \boldsymbol{z} \in \mathbb{Z}^n \text{ e } \alpha_j^{(i)} \in \{0, 1, ..., q^i - 1\} \right\}.$$

Seja $\Lambda_{D'}$ o reticulado obtido via Construção D' a partir da cadeia $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ (usando os parâmetros $r_1, r_2, ..., r_a, \boldsymbol{h}_1, ..., \boldsymbol{h}_{r_a}$). Nessas condições obtemos os seguintes resultados:

Teorema 3.2. *Seja $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ uma cadeia de códigos lineares. Temos que $q\Lambda_{D^\perp}^* = \Lambda_{D'}$. Além disso, M é uma matriz geradora de $\Lambda_{D^\perp}$ se e somente se $q(M^t)^{-1}$ é uma matriz geradora de $\Lambda_{D'}$.*

Demonstração. Seja H a matriz, cujas linhas são

$$\sigma(\boldsymbol{h}_1), ..., \sigma(\boldsymbol{h}_{r_1}), q\sigma(\boldsymbol{h}_{r_1+1}), ..., q\sigma(\boldsymbol{h}_{r_2}), ..., q^{a-1}\sigma(\boldsymbol{h}_{r_{a-1}+1}), ..., q^{a-1}\sigma(\boldsymbol{h}_{r_a}).$$

Temos que

$$\begin{aligned} \boldsymbol{y} \in q\Lambda^*_{D^\perp} &\overset{\text{Lema 3.1}}{\iff} \boldsymbol{y} = q\boldsymbol{x}, q\boldsymbol{x} \in \mathbb{Z}^n \text{ e } H\boldsymbol{x}^t \equiv 0 \mod q^{a-1} \\ &\iff \boldsymbol{y} \in \mathbb{Z}^n \text{ e } H\boldsymbol{y}^t \equiv 0 \mod q^a \\ &\overset{\text{Lema 3.2}}{\iff} \boldsymbol{y} \in \Lambda_{D'}. \end{aligned}$$

Logo $q\Lambda^*_{D^\perp} = \Lambda_{D'}$. Observamos que M é uma matriz geradora de $\Lambda_{D^\perp}$ se e somente se $(M^t)^{-1}$ é uma matriz geradora de $\Lambda^*_{D^\perp}$. Portanto M é uma matriz geradora de $\Lambda_{D^\perp}$ se e somente se $q(M^t)^{-1}$ é uma matriz geradora de $\Lambda_{D'}$, pois $\Lambda_{D'} = q\Lambda^*_{D^\perp}$. □

Corolário 3.1. *A cadeia $C_1^\perp \subseteq C_2^\perp \subseteq \cdots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$ é fechada sob a adição zero-um se e somente se $\Lambda_{D'} = q^a\Gamma^*_{\overline{D}^\perp} = q^a\Lambda^*_{\overline{D}^\perp}$, onde $\Gamma_{\overline{D}^\perp}$ e $\Lambda_{\overline{D}^\perp}$ são obtidos via Contrução $\overline{D}$ a partir da cadeia $C_1^\perp \subseteq C_2^\perp \subseteq \cdots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$.*

Demonstração. O Teorema 3.1 garante que a cadeia $C_1^\perp \subseteq C_2^\perp \subseteq \cdots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$ é fechada sob a adição zero-um se e somente se $\Lambda_{\overline{D}^\perp} = \Gamma_{\overline{D}^\perp} = q^{a-1}\Lambda_{D^\perp}$. Por outro lado, $\Lambda_{\overline{D}^\perp} = \Gamma_{\overline{D}^\perp} = q^{a-1}\Lambda_{D^\perp}$ se e somente se $\Gamma^*_{\overline{D}^\perp} = \Lambda^*_{\overline{D}^\perp} = (q^{a-1}\Lambda_{D^\perp})^* = (1/q^{a-1})\Lambda^*_{D^\perp} = (1/q^a)\Lambda_{D'}$. Logo a cadeia $C_1^\perp \subseteq C_2^\perp \subseteq \cdots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$ é fechada sob a adição zero-um se e somente se $\Lambda_{D'} = q^a\Gamma^*_{\overline{D}^\perp} = q^a\Lambda^*_{\overline{D}^\perp}$. □

Teorema 3.3. [8] *Sejam $\boldsymbol{h}_1, ..., \boldsymbol{h}_{r_a} \in \mathbb{Z}_q^n$ vetores não nulos tais que*

1. *$C_\ell^\perp = \langle \boldsymbol{h}_1, ..., \boldsymbol{h}_{r_\ell} \rangle$ para $\ell = 0, 1, ..., a$.*
2. *Alguma permutação das linhas da matriz, cujas linhas são $\sigma(\boldsymbol{h}_1), ..., \sigma(\boldsymbol{h}_{r_a})$, forma uma matriz "triangular superior" (resp. inferior) na forma escalonada.*
3. *Para cada $j \in \{1, ..., r_a\}$, a primeira (resp. última) componente não nula do vetor $\sigma(\boldsymbol{h}_j)$, denotada por α_j, divide q e todas as demais componentes do mesmo.*

Então existe uma base para o reticulado $\Lambda_{\overline{D}}^\perp$ formada pelos r_a vetores $(1/q^{i-1})\sigma(\boldsymbol{h}_j)$, onde $1 \leq i \leq a$ e $r_{a-i} < j \leq r_{a-i+1}$, mais $n - r_a$ vetores do tipo $(0, ..., 0, q, 0, ..., 0)$ de modo que alguma permutação das linhas da matriz, cujas linhas são os elementos desta base, forma uma matriz M triangular superior (resp. inferior). Em particular, M é uma matriz geradora de $\Lambda_{\overline{D}}^\perp$ e

$$\det \Lambda_{\overline{D}}^\perp = \det(MM^t) = \left(\prod_{j=1}^{r_a} \alpha_j\right)^2 \left(q^2\right)^{n - \sum_{\ell=1}^{a} r_\ell}.$$

Corolário 3.2. *Nas condições do Teorema 3.3, temos que*

$$\det \Lambda_{D'} = \left(\prod_{j=1}^{r_a} \alpha_j\right)^{-2} \left(q^2\right)^{\sum_{\ell=1}^{a} r_\ell}.$$

Em particular, quando $q = 2$ temos $\det \Lambda_{D'} = 4^{\sum_{\ell=1}^{a} r_\ell}$.

DOI: 10.5540/03.2017.005.01.0228

Demonstração. Pelo Teorema 3.2, $q(M^t)^{-1}$ é uma matriz geradora de $\Lambda_{D'}$. Logo

$$\det \Lambda_{D'} = \det\left[q(M^t)^{-1}(q(M^t)^{-1})^t\right] = (q^2)^n \det\left(MM^t\right)^{-1} = (q^2)^n (\det \Lambda_{D^\perp})^{-1}.$$

Para concluir a prova, basta aplicar o Teorema 3.3. □

Exemplo 3.1. *Seja a cadeia de códigos lineares* $\mathbb{Z}_6^2 \supseteq C_1 \supseteq C_2$, *onde* $C_1 = \langle(1,2)\rangle$ *e* $C_2 = \langle(2,4)\rangle$. *Temos que* $C_1^\perp = \{(x,y) \in \mathbb{Z}_6^2; x + 2y = 0\} = \langle(4,1)\rangle$ *e* $C_2^\perp = \{(x,y) \in \mathbb{Z}_6^2; 2x + 4y = 0\} = \langle(4,1),(3,0)\rangle$. *Seja* $\Lambda_{D^\perp}$ *o reticulado obtido via Construção D a partir desta cadeia usando os parâmetros* $r_1 = 1, r_2 = 2, \boldsymbol{h}_1 = (4,1)$ *e* $\boldsymbol{h}_2 = (3,0)$. *Estes parâmetros satisfazem as condições* 1, 2 *e* 3 *do Teorema* 3.3, *logo*

$$\det \Lambda_{D'} = \left(3 \cdot 1\right)^{-2}\left(6^2\right)^{1+2} = (6^3/3)^2 = 72^2$$

e matrizes geradoras para $\Lambda_{D^\perp}$ *e* $\Lambda_{D'}$ *são dadas respectivamente por*

$$M = \begin{bmatrix} \sigma(\boldsymbol{h}_2) \\ (1/6)\sigma(\boldsymbol{h}_1) \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 4/6 & 1/6 \end{bmatrix} \quad e \quad 6(M^t)^{-1} = \begin{bmatrix} 2 & -8 \\ 0 & 36 \end{bmatrix}.$$

Referências

[1] E. S. Barnes and N. J. A. Sloane. New lattice packings of spheres, *Canad. J. Math.*, 35:117–130, 1983.

[2] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups, 3rd edn.* Springer, New York, 1998.

[3] G. D. Forney. Coset Codes-Part I: Introduction and Geometrical Classification, *IEEE Trans. Inform. Theory*, 34(5):1123–1151, 1988.

[4] G. D. Forney. Coset Codes-Part II: Binary Lattices and Related Codes, *IEEE Trans. Inform. Theory*, 34(5):1152–1187, 1988.

[5] G. C. Jorge, Reticulados q-ários e Algébricos, Tese de Doutorado, Unicamp, 2012.

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

[7] D. Micciancio and O. Regev: Lattice-Based Cryptography in Post Quantum Cryptography, chapter 4, pages 147-191, 2009.

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

[9] 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.

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

