Construção B para códigos q-ários

Grasiele C. Jorge[1] & Sueli I. R. Costa[2]

[1]Instituto de Ciência e Tecnologia - UNIFESP

[2]Instituto de Matemática, Estatística e Computação Científica - UNICAMP

grasiele.jorge@unifesp.br, sueli@ime.unicamp.br

Códigos e reticulados q-ários

Definição 1. *Seja $q \geq 2$ um número natural. Um* **código linear q-ário** *$C \subseteq \mathbb{Z}_q^n$ é um $\mathbb{Z}_q$-submódulo de $\mathbb{Z}_q^n$.*

Definição 2. *Seja $\{v_1, \ldots, v_m\}$, $m \leq n$, um conjunto de vetores linearmente independentes em $\mathbb{R}^n$. O conjunto*

$$\Lambda = \left\{ \sum_{i=1}^{m} \lambda_i v_i,\ \lambda_i \in \mathbb{Z} \text{ para todo } i = 1, \ldots, m \right\}$$

é chamado de **reticulado**.

Proposição 1. *[1] Considere a aplicação sobrejetora*

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

Temos que $C \subseteq \mathbb{Z}_q^n$ é um código linear q-ário se, e somente se, $\phi^{-1}(C) = \Lambda_A(C) \subseteq \mathbb{Z}^n$ é um reticulado. Além disso, temos que $q\mathbb{Z}^n \subseteq \Lambda_A(C)$ e $\Lambda_A(C)/q\mathbb{Z}^n \simeq C$.

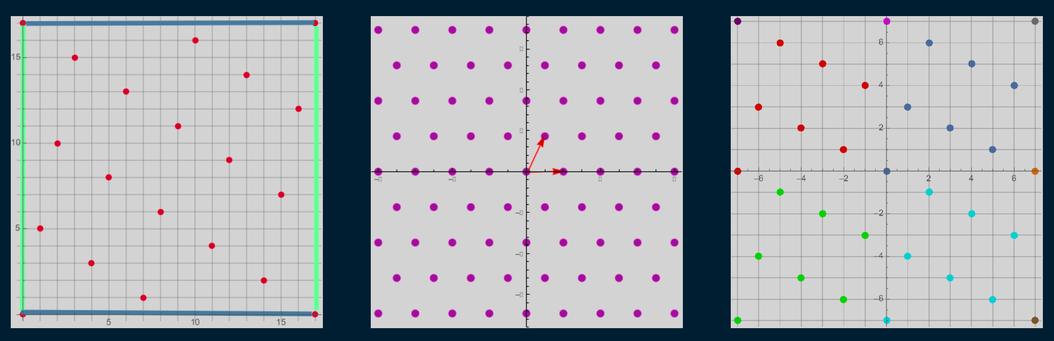

Figura 1: Código 17-ário gerado por $(\overline{1}, \overline{5})$ em $\mathbb{Z}_{17}^2$, reticulado gerado por $\{(1, 0), (1/2, \sqrt{3}/2)\}$ e reticulado 7-ário associado ao código gerado por $(\overline{1}, \overline{3})$ em $\mathbb{Z}_7^2$.

Construção B estendida

Definição 3. *Sejam $q = 2^r b$, onde $b \in \mathbb{N}$ é ímpar e $C \subseteq \mathbb{Z}_q^n$ é um código linear q-ário tal que 2^r divide $\sum_{i=1}^{n} c_i$ para todo $\overline{c} = (\overline{c_1}, \ldots, \overline{c_n}) \in C$. Definimos*

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

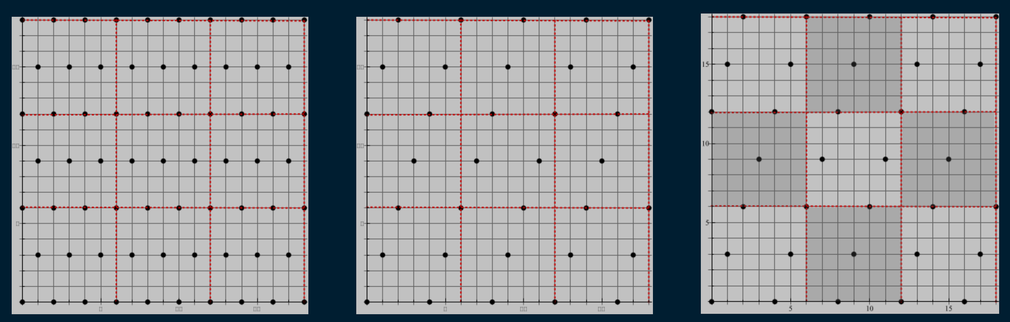

Figura 2: $\Lambda_B(C)$ para $C = \langle(\overline{1}, \overline{3})\rangle \subseteq \mathbb{Z}_6^2$.

Proposição 2. *[2] $\Lambda_B(C)$ é um reticulado, $\Lambda_B(C) \subseteq \Lambda_A(C)$ e $|\Lambda_A(C)/\Lambda_B(C)| = 2$.*

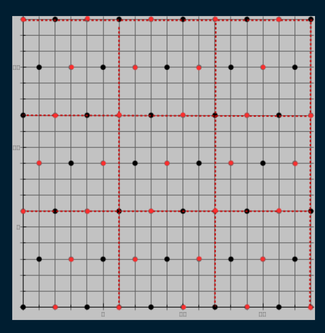

Figura 3: Os pontos coloridos com preto são pontos de $\Lambda_B(C)$ para $C = \langle(\overline{1}, \overline{3})\rangle \subseteq \mathbb{Z}_6^2$ e os pontos coloridos com preto e vermelho são pontos de $\Lambda_A(C)$.

Exemplo 1. *[1] O reticulado E_8 é definido por*

$$\{(x_1, \ldots, x_8);\ \text{ou } x_i \in \mathbb{Z}\ \forall i \text{ ou } x_i \in \mathbb{Z}+1/2\ \forall i,\ \text{e } \sum_{i=1}^{8} x_i \text{ é par}\}.$$

Uma versão escalonada $2E_8$ é obtida via Construção B do código binário $C = \{(\overline{0}, \ldots, \overline{0}), (\overline{1}, \ldots, \overline{1})\} \subseteq \mathbb{Z}_2^8$.

Consideremos o reticulado D_n, definido por:

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

Proposição 3. *[2] Sejam $C \subseteq \mathbb{Z}_q^n$ um código q-ário. Temos que $qD_n \subseteq \Lambda_B(C)$ e $|\Lambda_B(C)/qD_n| = |C|$.*

Exemplo 2. *Para o reticulado $2E_8$ do* **Exemplo 1** *temos que $|\Lambda_B(C)/2D_8| = |C| = 2$. Desta forma, podemos particionar o reticulado $2E_8$ como duas cópias do reticulado $2D_8$ e utilizando a decodificação do reticulado D_8, podemos decodificar E_8.*

Sejam q um número primo e $[I_{k\times k} \mid B_{k\times n-k}]$ uma matriz geradora para $C \subseteq \mathbb{Z}_q^n$ na forma sistemática, onde $B = (b_{i,j})$.

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

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

Proposição 4. *[2] Seja q um número primo. Uma matriz geradora para $\Lambda_B(C)$ é dada por*

$$N = \begin{pmatrix} I_{k\times k} & {B^*}_{n\times(n-k)} \\ 0_{(n-k)\times k} & q\, D^*_{(n-k)\times(n-k)} \end{pmatrix}, \quad \text{onde}$$

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

Observação 1. *Um reticulado obtido pela Construção B de um código q-ário nunca é q-ário pois $qe_i \notin \Lambda_B(C)$ para todo $i = 1, \cdots, n$.*

Proposição 5. *[2] Se $C_1 \subseteq \mathbb{Z}_q^n$ é um código q-ário, então $\Lambda_B(C_1) = \Lambda_A(C_2)$, onde $C_2 \subseteq \mathbb{Z}_{2q}^n$ é o código $2q$-ário associado ao quociente $\Lambda_B(C_1)/2q\mathbb{Z}^n$. Mais ainda, C_2 é gerado pelas linhas de uma matriz geradora de $\Lambda_B(C_1)$ reduzindo as entradas módulo $2q$.*

Referências

[1] J. H. Conway e N. J. A. Sloane. *Sphere packings, lattices and groups*. Springer-Verlag, New York, NY, USA, 1998.

[2] G. C. Jorge. Reticulados q-ários e algébricos. *Tese de Doutorado, Universidade Estadual de Campinas*, 2012.

Agradecimentos