q-ary lattices in the l_p norm and a generalization of the Lee metric

Grasiele C. Jorge

Antonio Campello

Sueli I. R. Costa

University of Campinas - UNICAMP - Brazil

WCC 2013

International Workshop on Coding and Cryptography

Topics

- Introduction of the induced p-Lee metric in $\mathbb{R}^n/q\mathbb{Z}^n$ by the l_p metric in $\mathbb{R}^n$;

Topics

- Introduction of the induced p-Lee metric in $\mathbb{R}^n/q\mathbb{Z}^n$ by the l_p metric in $\mathbb{R}^n$;
- A relation between the decoding processes of a q-ary lattice in the l_p norm and its associated code in the p-Lee metric;

Topics

- Introduction of the induced p-Lee metric in $\mathbb{R}^n/q\mathbb{Z}^n$ by the l_p metric in $\mathbb{R}^n$;
- A relation between the decoding processes of a q-ary lattice in the l_p norm and its associated code in the p-Lee metric;
- Perfect codes in $\mathbb{Z}_q^n$ considering these p-Lee metrics.

Lattices in $\mathbb{R}^n$

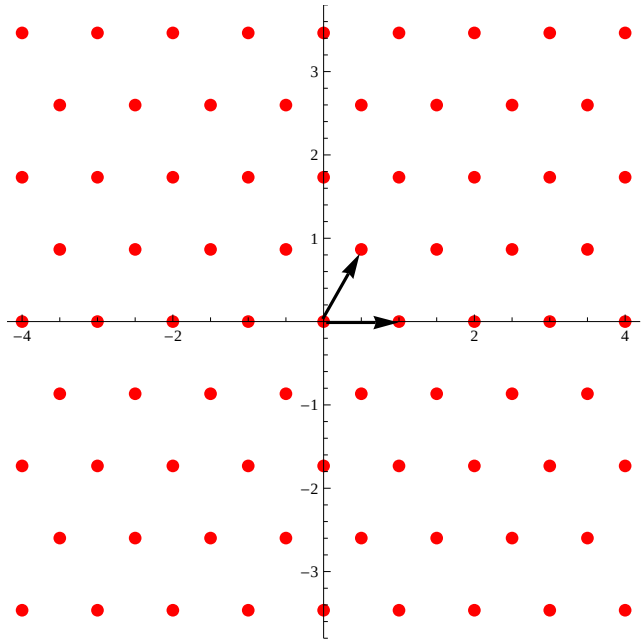
- Let $\{v_1, \cdots, v_m\}$, $m \leq n$, be a set of linearly independent vectors in $\mathbb{R}^n$. The set

$$\Lambda = \left\{ \sum_{i=1}^{m} a_i v_i, \text{ where } a_i \in \mathbb{Z}, \ i = 1, \cdots, m \right\}$$

  is called **lattice**.

- The set $\{v_1, \cdots, v_m\}$ is called a **basis** of Λ and the matrix M whose rows are these vectors is said to be a **generator matrix** for Λ. The **determinant** of a full rank lattice Λ, $(m = n)$, can be defined as $\det \Lambda = |\det M|$.

Lattices



- [Conway, Sloane, 1999]
- [Zamir, 2009]

q-ary codes

Definition

Given $q \in \mathbb{N}$, a linear **q-ary code** C is an additive subgroup of $\mathbb{Z}_q^n$.

$$C = \langle(\overline{2}, \overline{6})\rangle = \{(\overline{2}, \overline{6}), (\overline{4}, \overline{0}), (\overline{6}, \overline{6}), (\overline{8}, \overline{0}), (\overline{10}, \overline{6}), (\overline{0}, \overline{0})\} \subseteq \mathbb{Z}_{12}^2$$

Construction A

Let ϕ be the surjective map

$$\phi : \mathbb{Z}^n \longrightarrow \mathbb{Z}_q^n$$

$$(x_1, \cdots, x_n) \longmapsto (\overline{x_1}, \cdots, \overline{x_n}).$$

$C \subseteq \mathbb{Z}_q^n$ is a q-ary code iff $\phi^{-1}(C)$ is a lattice in $\mathbb{R}^n$.

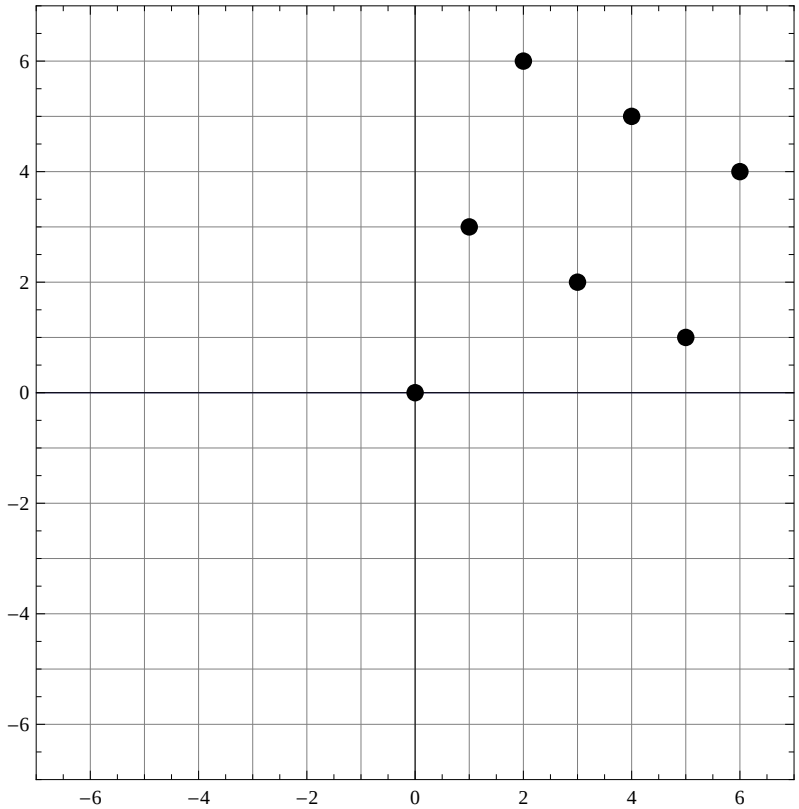
Definition

The lattice $\Lambda_A(C) = \phi^{-1}(C)$ is said to be the q-ary lattice associated to C.

- [Micciancio, Regev, 2009]

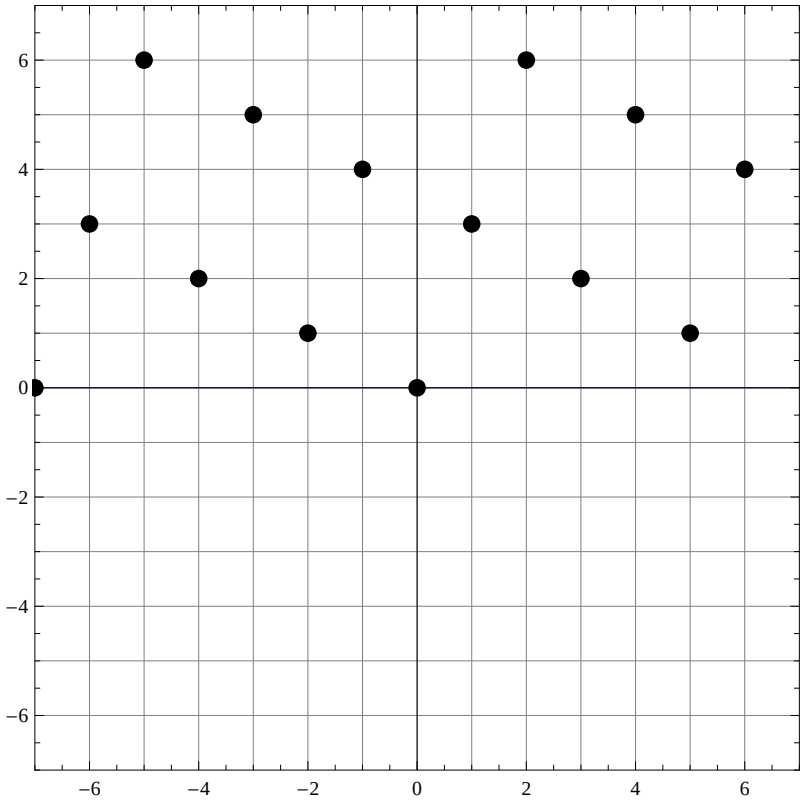
Example

$$C = \langle(\overline{1}, \overline{3})\rangle = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{3}), (\overline{2}, \overline{6}), (\overline{3}, \overline{2}), (\overline{4}, \overline{5}), (\overline{5}, \overline{2}), (\overline{6}, \overline{4})\} \subseteq \mathbb{Z}_7^2$$



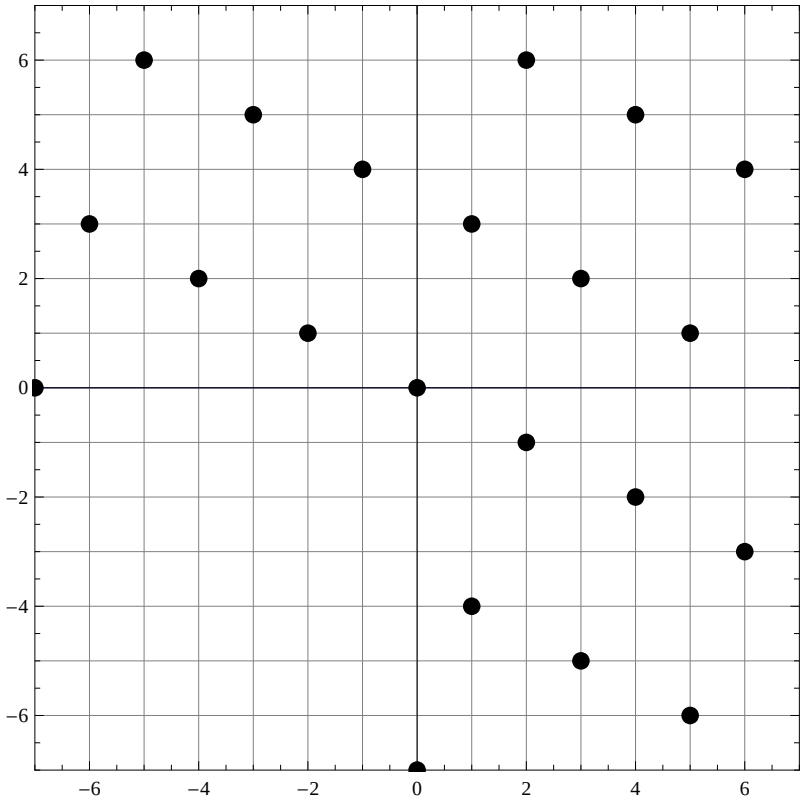
Example

$$C = \langle(\overline{1},\overline{3})\rangle = \{(\overline{0},\overline{0}),(\overline{1},\overline{3}),(\overline{2},\overline{6}),(\overline{3},\overline{2}),(\overline{4},\overline{5}),(\overline{5},\overline{2}),(\overline{6},\overline{4})\} \subseteq \mathbb{Z}_7^2$$



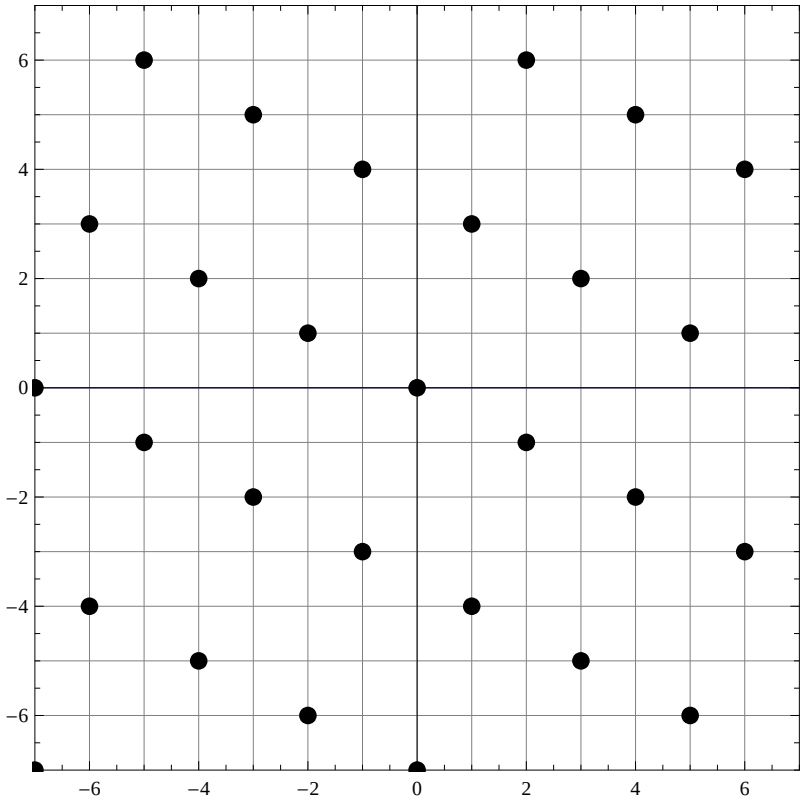
Example

$$C = \langle(\overline{1}, \overline{3})\rangle = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{3}), (\overline{2}, \overline{6}), (\overline{3}, \overline{2}), (\overline{4}, \overline{5}), (\overline{5}, \overline{2}), (\overline{6}, \overline{4})\} \subseteq \mathbb{Z}_7^2$$



Example

$$C = \langle(\overline{1}, \overline{3})\rangle = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{3}), (\overline{2}, \overline{6}), (\overline{3}, \overline{2}), (\overline{4}, \overline{5}), (\overline{5}, \overline{2}), (\overline{6}, \overline{4})\} \subseteq \mathbb{Z}_7^2$$



q-ary lattice

Let $C \subset \mathbb{Z}_q^n$ be a q-ary code. We have that:

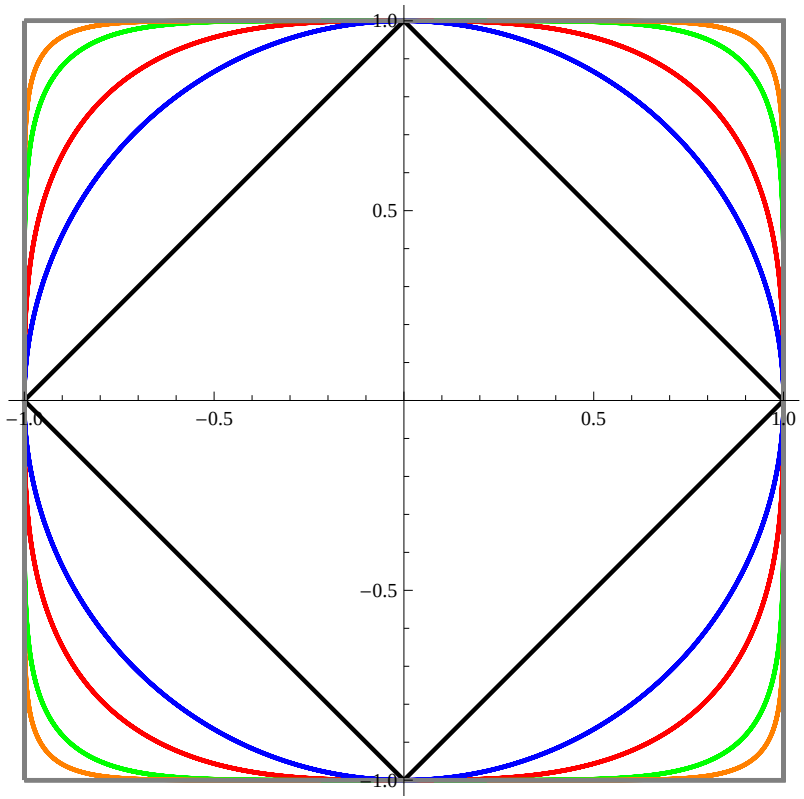
- $q\mathbb{Z}^n \subseteq \Lambda_A(C)$ and $\frac{\Lambda_A(C)}{q\mathbb{Z}^n} \simeq C.$
- $\left|\frac{\Lambda_A(C)}{q\mathbb{Z}^n}\right| = \frac{q^n}{\det \Lambda_A(C)} = |C|$
- Any full rank integer lattice $\Lambda \subseteq \mathbb{Z}^n$ is q-ary for $q = \det(\Lambda)$.

d_p metric in $\mathbb{R}^n$

Let $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{R}^n$.

$$d_p(\boldsymbol{x}, \boldsymbol{y}) := \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{1/p} \quad \text{if } 1 \leq p < \infty \text{ and}$$

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



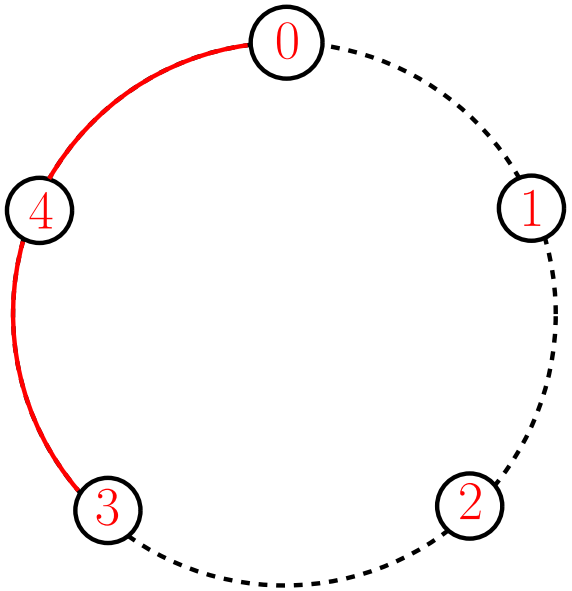
$$B_1(1,0) \subseteq B_2(1,0) \subseteq B_3(1,0) \subseteq \cdots \subseteq B_6(1,0) \subseteq \cdots \subseteq B_{10}(1,0) \subseteq \cdots \subseteq B_\infty(1,0)$$

Lee Metric

Definition

For $\overline{a}, \overline{b} \in \mathbb{Z}_q$ (or $\mathbb{R}/q\mathbb{Z}$) we define

$$d_{Lee}(\overline{a}, \overline{b}) = min\{|a-b|, q-|a-b|\}.$$



Definition

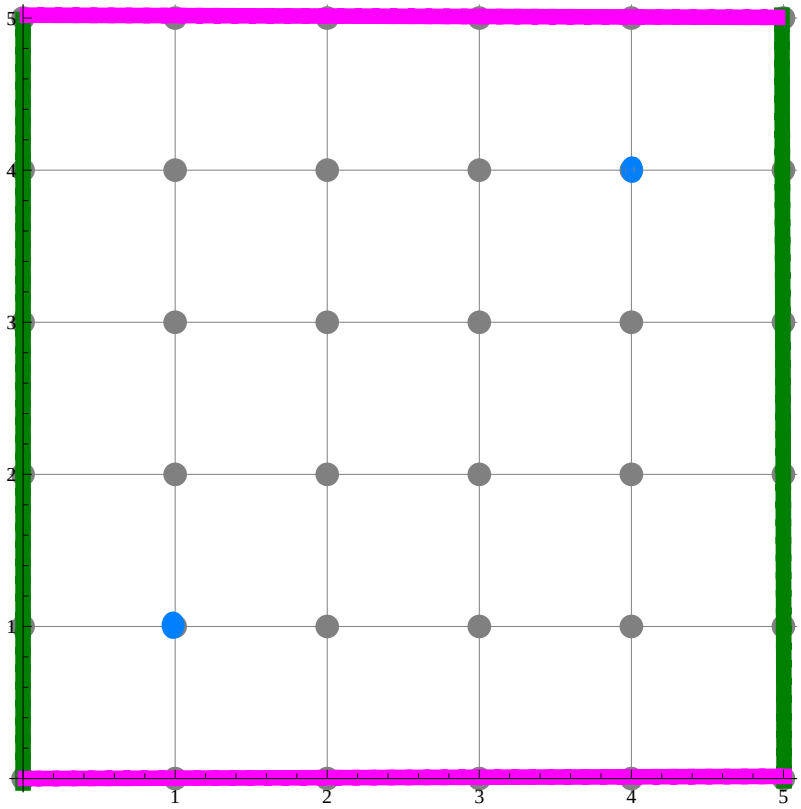
For $a = (\overline{a_1}, \cdots, \overline{a_n}), b = (\overline{b_1}, \cdots, \overline{b_n}) \in \mathbb{Z}_q^n \simeq \mathbb{Z}^n/q\mathbb{Z}^n$ or $\mathbb{R}^n/q\mathbb{Z}^n$ the Lee distance is defined as

$$d_{Lee}(a, b) = \sum_{i=1}^{n} d_{Lee}(\overline{a_i}, \overline{b_i}).$$

Example

Let $a = (\overline{1}, \overline{1}), b = (\overline{4}, \overline{4}) \in \mathbb{Z}_5^2$

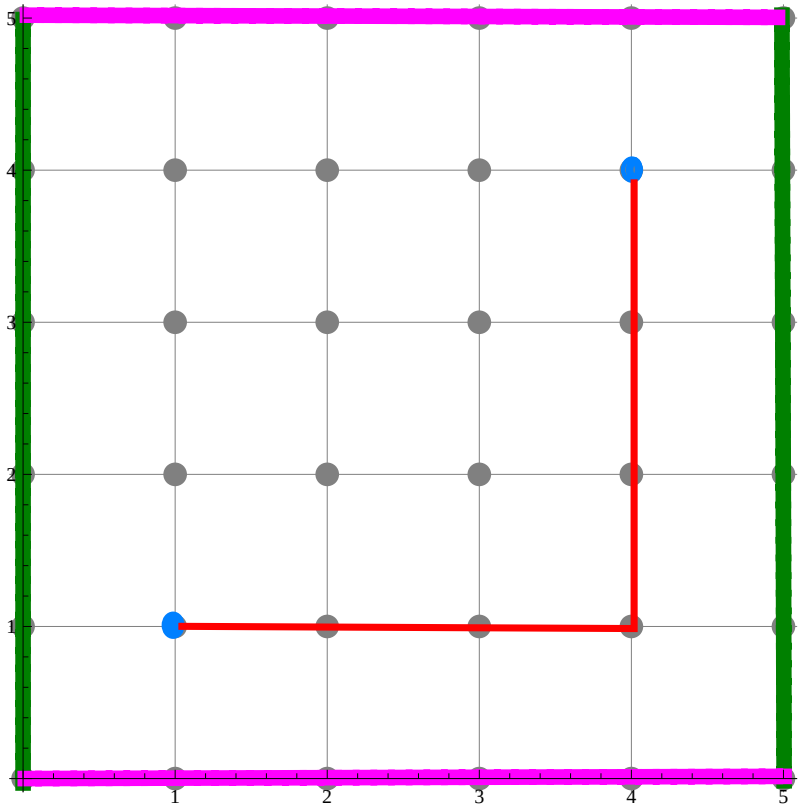
$$d_{Lee}(a, b) = min\{|1 - 4|, 5 - |1 - 4|\} + min\{|1 - 4|, 5 - |1 - 4|\} = 4.$$



Example

Let $a = (\overline{1}, \overline{1}), b = (\overline{4}, \overline{4}) \in \mathbb{Z}_5^2$

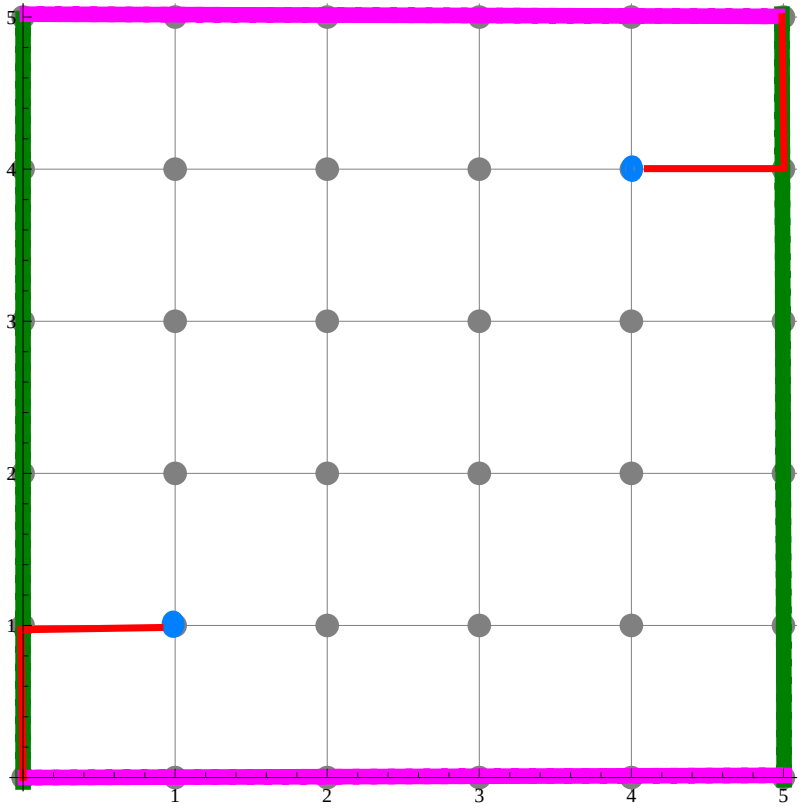
$$d_{Lee}(a, b) = min\{|1 - 4|, 5 - |1 - 4|\} + min\{|1 - 4|, 5 - |1 - 4|\} = 4.$$



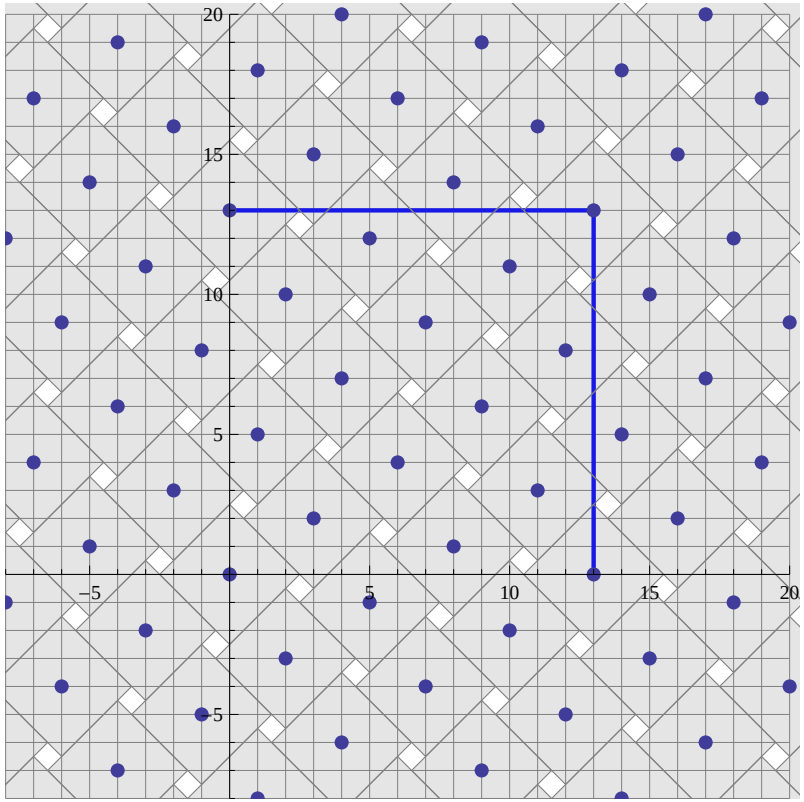
Example

Let $a = (\overline{1}, \overline{1}), b = (\overline{4}, \overline{4}) \in \mathbb{Z}_5^2$

$$d_{Lee}(a, b) = min\{|1 - 4|, 5 - |1 - 4|\} + min\{|1 - 4|, 5 - |1 - 4|\} = 4.$$



The Lee metric can be viewed as the distance in $\mathbb{R}^n/q\mathbb{Z}^n$ induced by the d_1-metric (or sum metric) in $\mathbb{R}^n$



Induced Metric

What is the induced metric in $\mathbb{R}^n/q\mathbb{Z}^n$ by d_p, $1 < p \leq \infty$?

Proposition

Let $\overline{\boldsymbol{x}} = (\overline{x_1}, \cdots, \overline{x_n}), \overline{\boldsymbol{y}} = (\overline{y_1}, \cdots, \overline{y_n}) \in \mathbb{R}^n/q\mathbb{Z}^n$, $0 \leq x_i, y_i < q$. The induced metric in $\mathbb{Z}_q^n$ by the metric d_p is given by

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

and

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

where $d_{Lee}(\overline{x}, \overline{y})$ is the Lee metric between $\overline{x}$ and $\overline{y}$.

Error Capacity Correction

- In the Lee metric the error capacity correction is

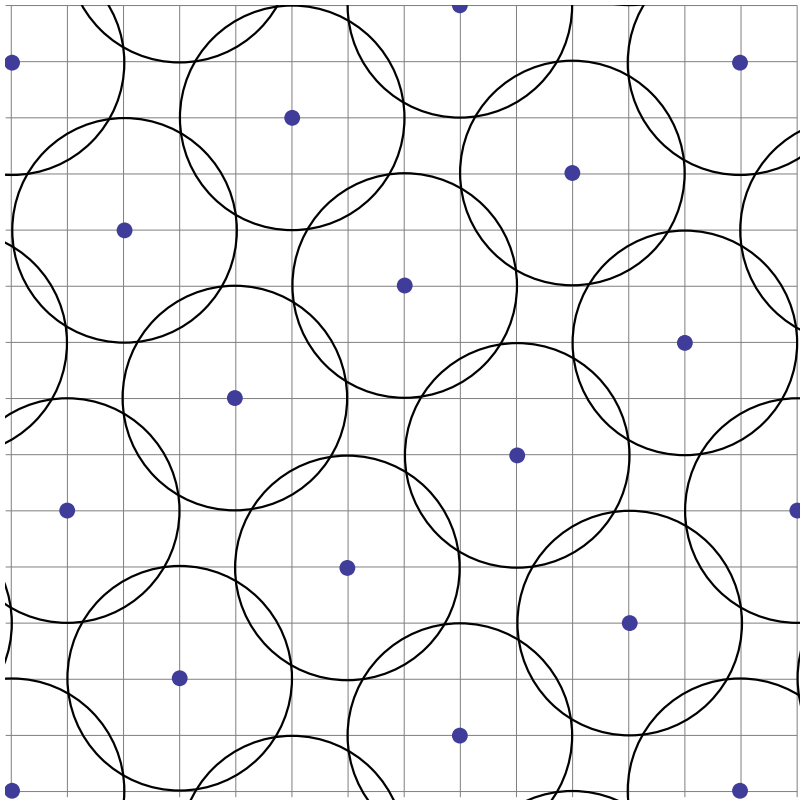
  $$t_1 = \lfloor (d_{1,Lee}(C) - 1)/2 \rfloor .$$

- For p>1 the error capacity correction can be greater than

  $$t_p = \lfloor (d_{p,Lee}(C) - 1)/2 \rfloor .$$

Error Capacity Correction

$C =< (\overline{1}, \overline{5}) > \subseteq \mathbb{Z}_{13}^2$, $t_2 = \lfloor (d_{2,Lee}(C) - 1)/2 \rfloor = 1$ and $R = 2$



The Decoding Process

For Codes

Let d be a metric in $\mathbb{R}^n/q\mathbb{Z}^n$ (or $\mathbb{Z}_q^n$). Given a code C and a vector $\boldsymbol{r} \in \mathbb{Z}_q^n$, what is the closest vector to $\boldsymbol{r}$ in C?

For Lattices

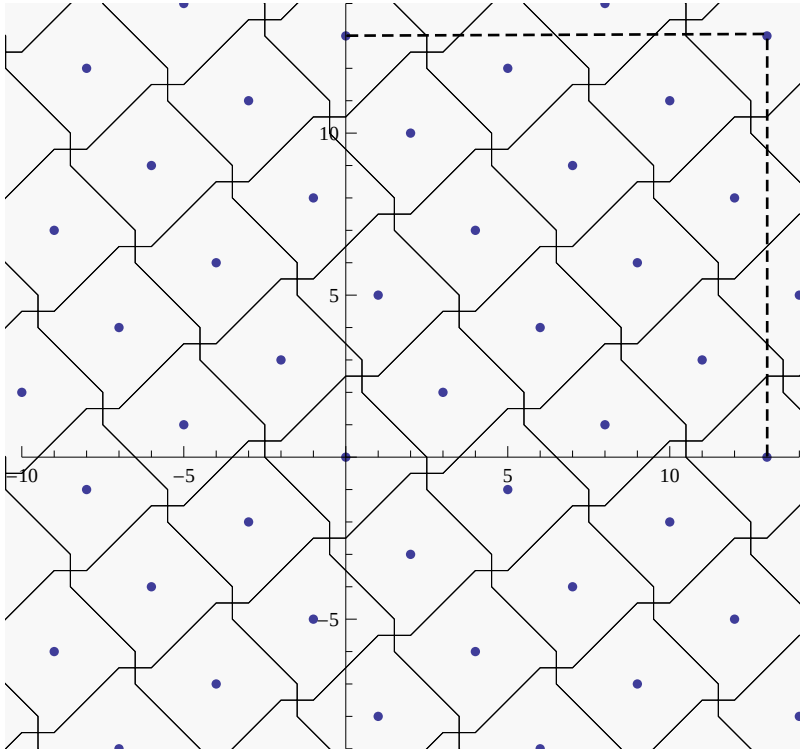
Let d be a metric in $\mathbb{R}^n$ (or $\mathbb{Z}_n$). Given a lattice Λ and a vector $\boldsymbol{r} \in \mathbb{R}^n$, what is the closest vector to $\boldsymbol{r}$ in Λ?

- E. Grell, T. Eriksson, A. Vardy and K. Zeger, Closest point search in lattices, 2002
- C. Peikert, Limits on the Hardness of Lattice Problems in l_p norms, 2008
- K. Takizawa, H. Yagi, T. Kawabata, Closest Point Algorithms with l_p Norm for Root Lattices, 2010
- A. Campello, G. C. Jorge and S. I. R. Costa, Decoding q-ary lattices in the Lee Metric, 2011

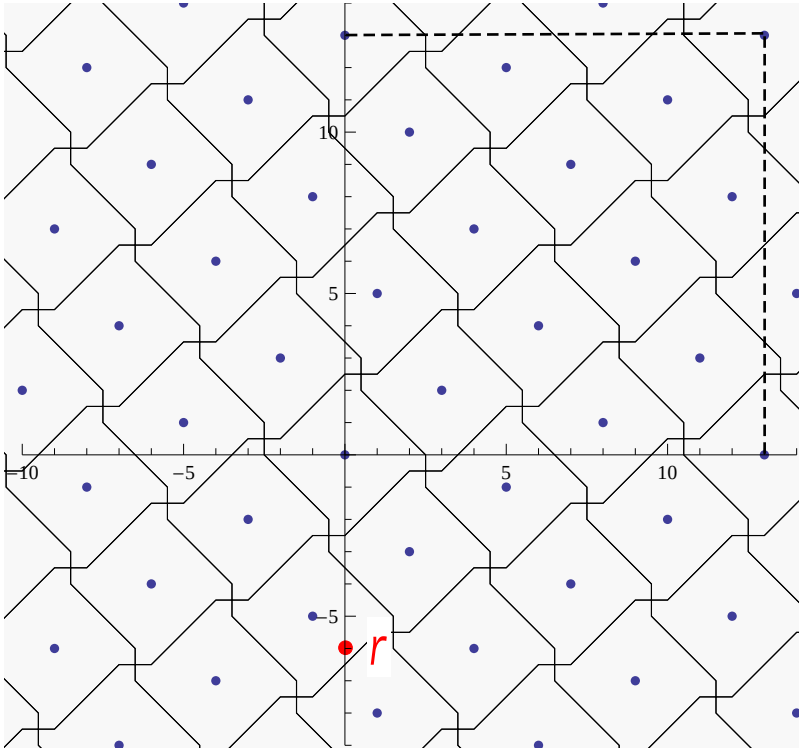
Relating the decoding processes

A relation between the decoding process of a q-ary lattice $\Lambda_A(C)$ in the d_p metric and its associated code C in the induced p-Lee metric.

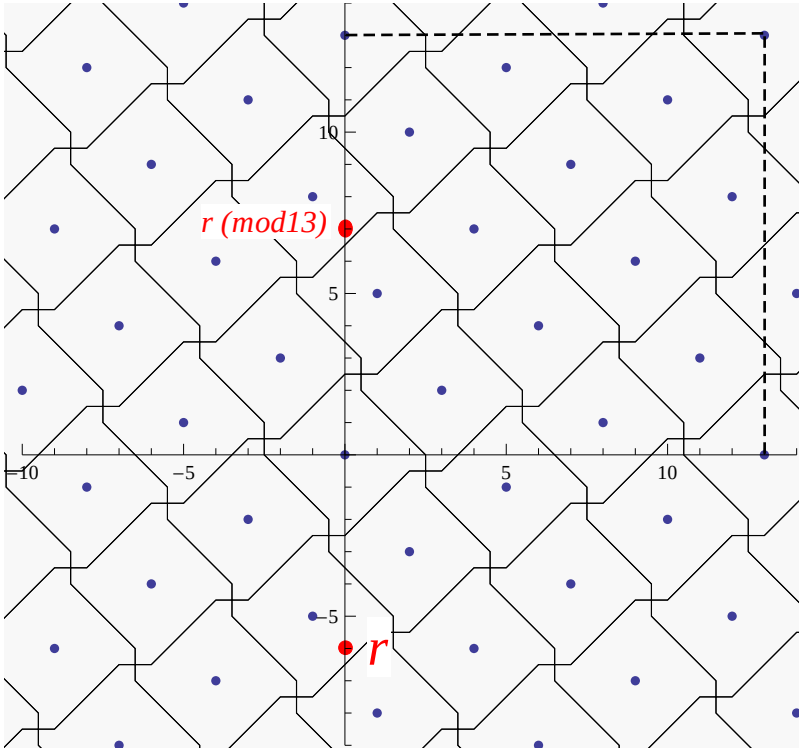
$C =< (\overline{1}, \overline{5}) > \subseteq \mathbb{Z}_{13}^2$



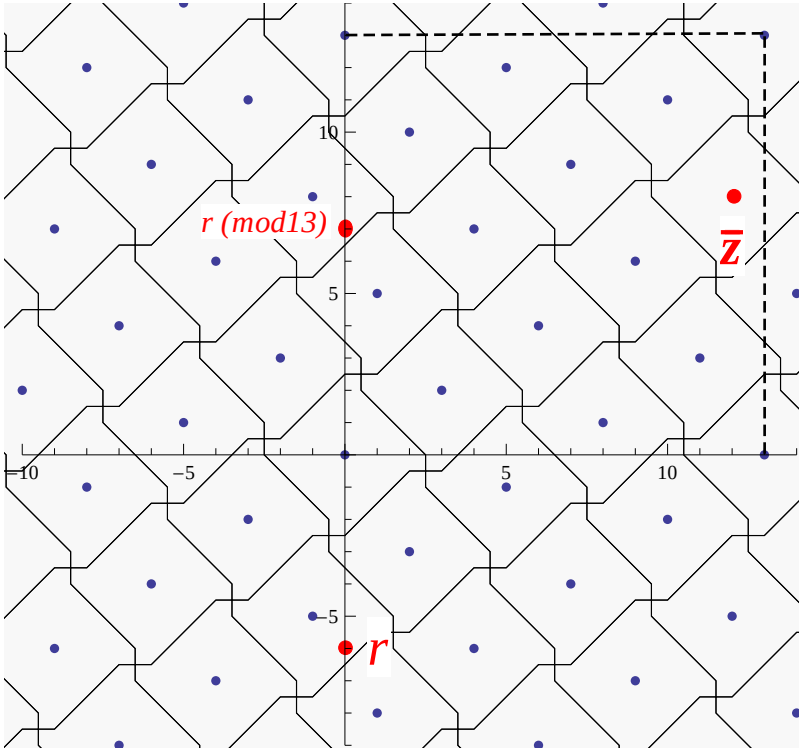
$r = (0, -6)$



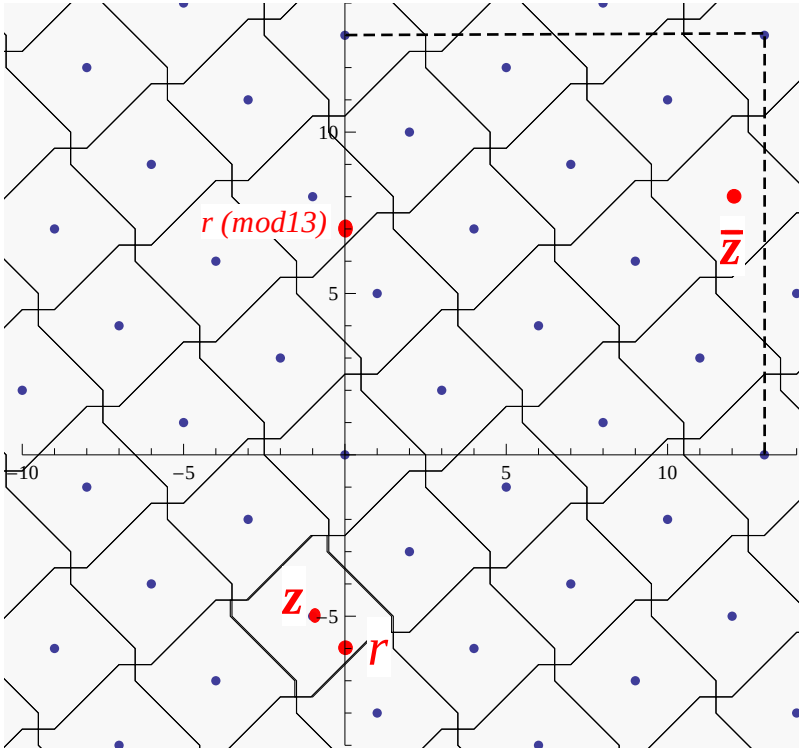
$\boldsymbol{r} \pmod{13} = (0, 7)$



$\overline{z} = (12, 8)$



$z = (-1, -5)$



Proposition

- $\Lambda_A(C)$ a q-ary lattice
- $\boldsymbol{r} = (r_1, \ldots, r_n) \in \mathbb{R}^n$ a received vector

If $\overline{\boldsymbol{x}} \in C$ is an element of C closest to $\boldsymbol{r}$ (mod q) considering the p-Lee metric,then

$$z \in \Lambda_A(C);\ \overline{z} = \overline{x}$$

given by

$$z_i = x_i + qw_i \text{ where } w_i = \left\lceil \frac{r_i - x_i}{q} \right\rfloor, \text{ for each } i = 1, \ldots, n.$$

is the closest lattice point to $\boldsymbol{r}$ considering the d_p metric.

On perfect codes in the p-Lee metric in $\mathbb{Z}_q^n$ for $1 \leq p \leq \infty$.

- [Golomb, Welch, 1970]
- [Etzion, 2011]

Perfect Codes

- Given a metric d, a code $C \subseteq \mathbb{Z}_q^n$ is called *perfect* (or R-perfect) if for any $\overline{x} \in \mathbb{Z}_q^n$ there is only one codeword $\overline{c} \in C$ such that $d(\overline{c}, \overline{x}) \leq R$.
- Let $\mu_p(n, R)$ be the number of points in $\mathbb{Z}_q^n$ inside a ball in the p-Lee metric of radius R centered at the origin. A code C is R-perfect iff

$$|C|\mu_p(n, R) = q^n.$$

- For $p = 1$ and $2R + 1 \leq q$

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

- For $p = \infty$

$$\mu_\infty(n, R) = (2R + 1)^n$$

Perfect codes in the ∞-Lee metric

Proposition

There are non-trivial perfect codes $C \subset \mathbb{Z}_q^n$ in the ∞-Lee metric iff $q = bm$ with $b > 1$ an odd integer and $m > 1$ an integer.

Necessary condition: If there exists a perfect code C,

$$|C| = \left(\frac{q}{2R+1}\right)^n.$$

- $2R+1$ must divide q.
- $q = 2^a$ is impossible.
- If q is prime, then $2R+1 = q$, which gives a trivial perfect code.

Sufficient condition: Let $q = bm$ with $b > 1$ an odd integer and $m > 1$ an integer.

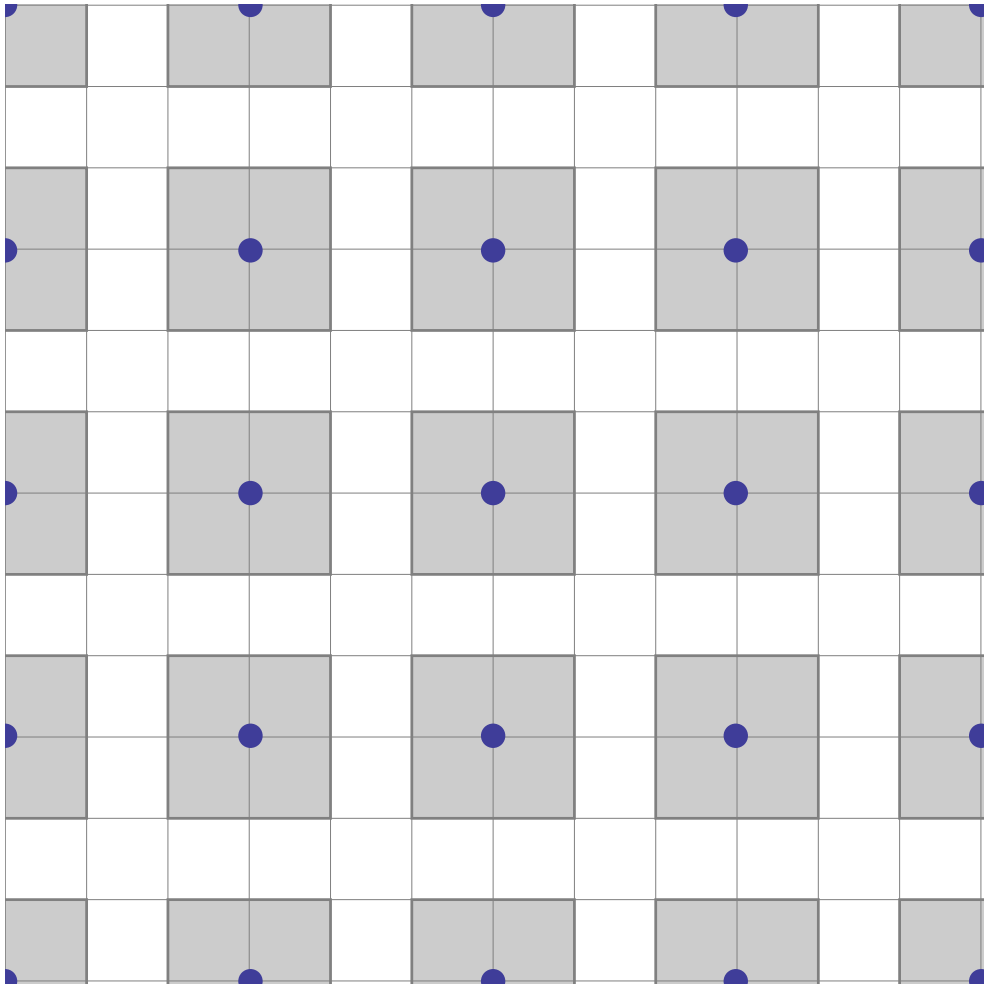
- Let C be the code generated by the vectors

$$\{(\overline{b}, \overline{0}, \ldots, \overline{0}), (\overline{0}, \overline{b}, \ldots, \overline{0}) \ldots, (\overline{0}, \ldots, \overline{0}, \overline{b})\} \subseteq \mathbb{Z}_q^n$$

- $|C| = m^n$.
- $\mu = \min\{d_{\infty,Lee}(\overline{x}, \overline{y});\ \overline{x}, \overline{y} \in C,\ \overline{x} \neq \overline{y}\} = b$.
- $R = (b-1)/2$.
- Since $\mu_\infty(n, R) = (2R+1)^n = b^n$, it follows that $|C|\mu_\infty(n, R) = m^n b^n = q^n$, $1 < |C| < q^n$ and this code is perfect and non-trivial.

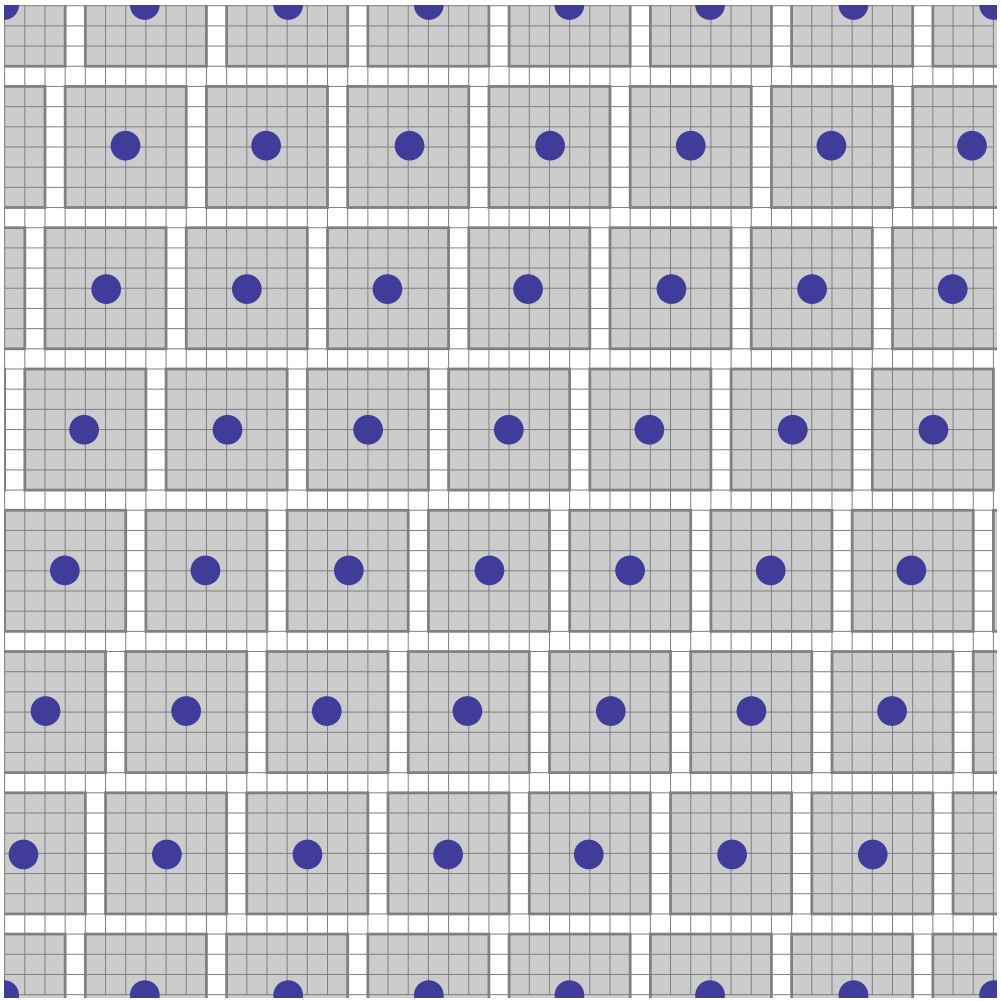
Example

Let $C = \langle(\overline{3}, \overline{0}), (\overline{0}, \overline{3})\rangle \subseteq \mathbb{Z}_{12}^2$



Example

Let $C = \langle(\overline{1}, \overline{7})\rangle \subseteq \mathbb{Z}_{49}^2$



Perfect codes in the p-Lee metric

Proposition

For $1 \leq p < \infty$, there are perfect codes in $\mathbb{Z}_q^n$ in the p-Lee metric for

$R = 1$ and $q = 2n + 1$.

- The case $p = 1$ was proved in S. W. Golomb and L. R. Welch, Perfect Codes in the Lee Metric and the Packing of Polyminoes, 1970
- For $1 < p < \infty$ the equation $|x_1|^p + \ldots + |x_n|^p \leq 1$ has exactly $2n + 1$ integer solutions and then

$$\mu_p(n, 1) = 2n + 1 = \mu_1(n, 1).$$

Perfect codes in the p-Lee metric

- Since there is a perfect code $C \subseteq \mathbb{Z}_q^n$ in the 1-Lee metric satisfying the conditions of the proposition, it follows that this code is also a perfect code in the p-Lee metric for any $1 < p < \infty$ since

$$|C|\mu_p(n,1) = |C|\mu_1(n,1) = q^n.$$

Extending the Golomb-Welch Conjecture (1970)

Conjecture

For $R > 1$, $n > 2$, $q > 3$, there are no perfect codes $C \subseteq \mathbb{Z}_q^n$ in the p-Lee metric $(1 \leq p < \infty)$

Thank You!


UNICAMP


CNPq
Conselho Nacional de Desenvolvimento
Científico e Tecnológico


FAPESP