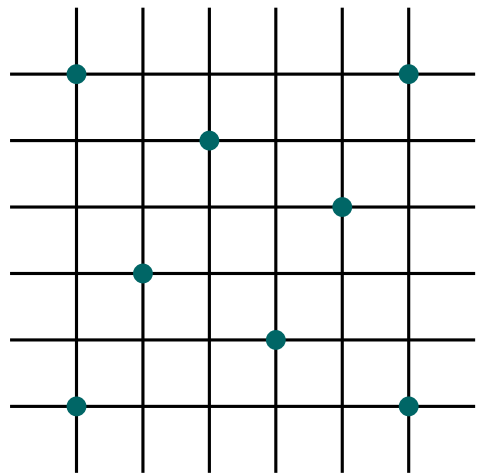
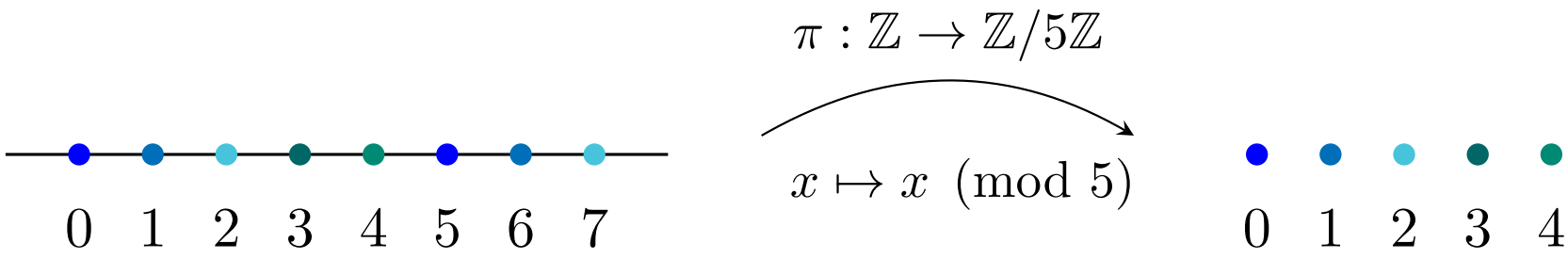
(A Quadratic Form Approach to) Construction A of Lattices

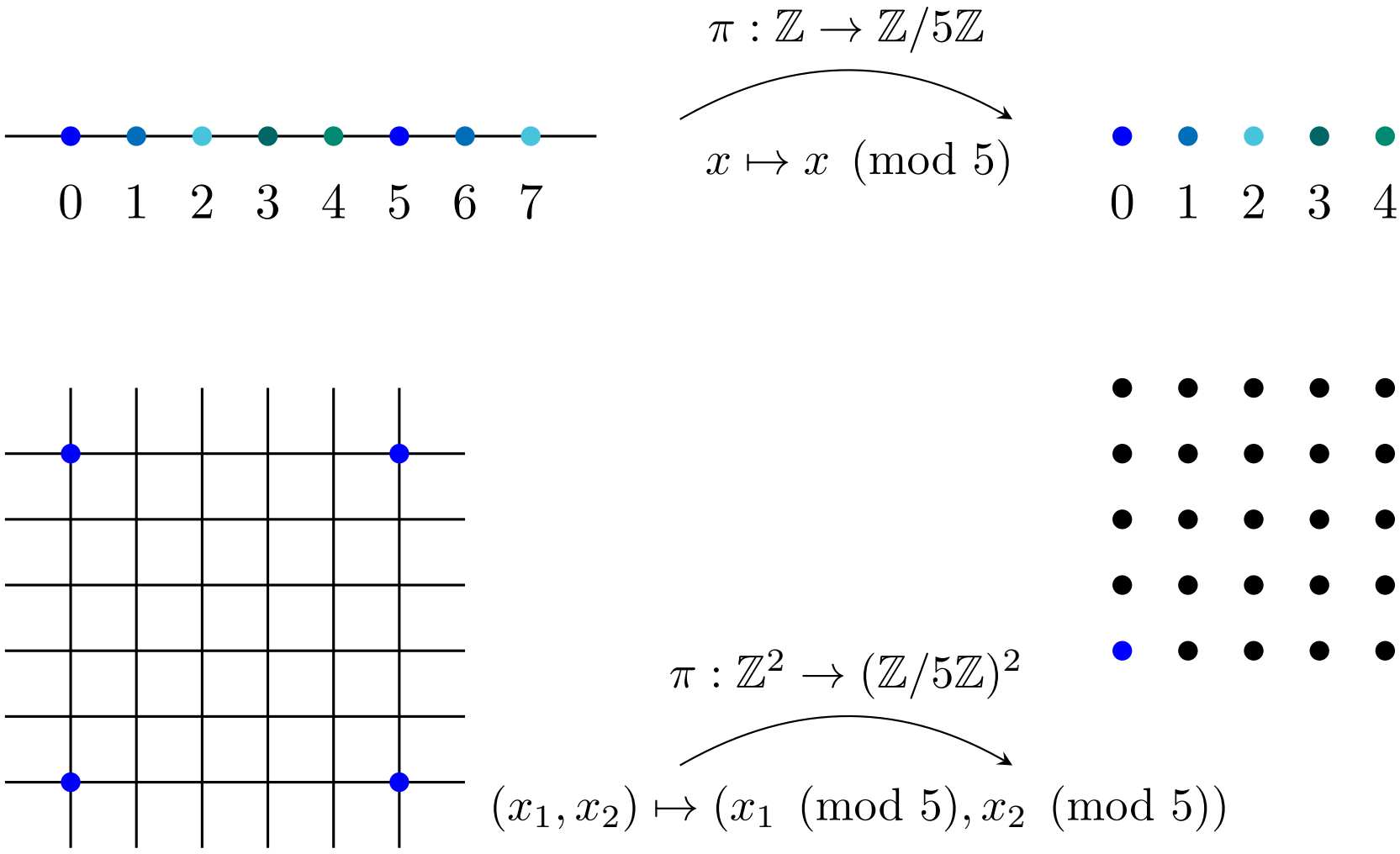
F. Oggier

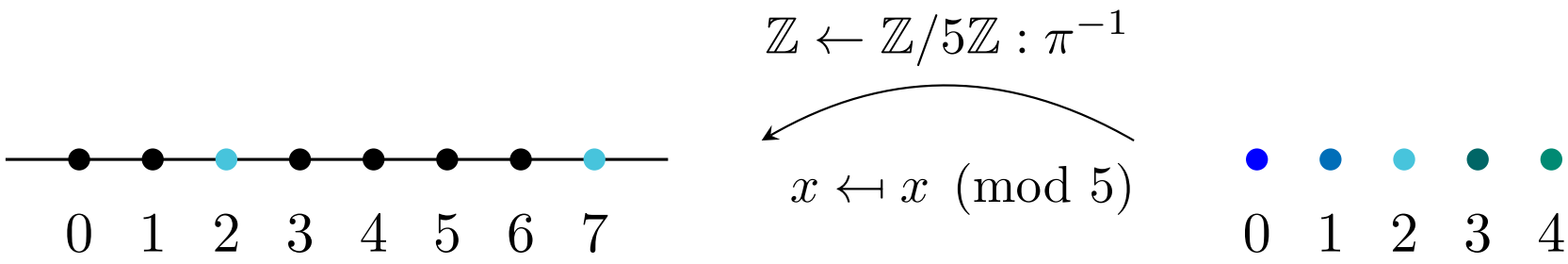
Warm-up

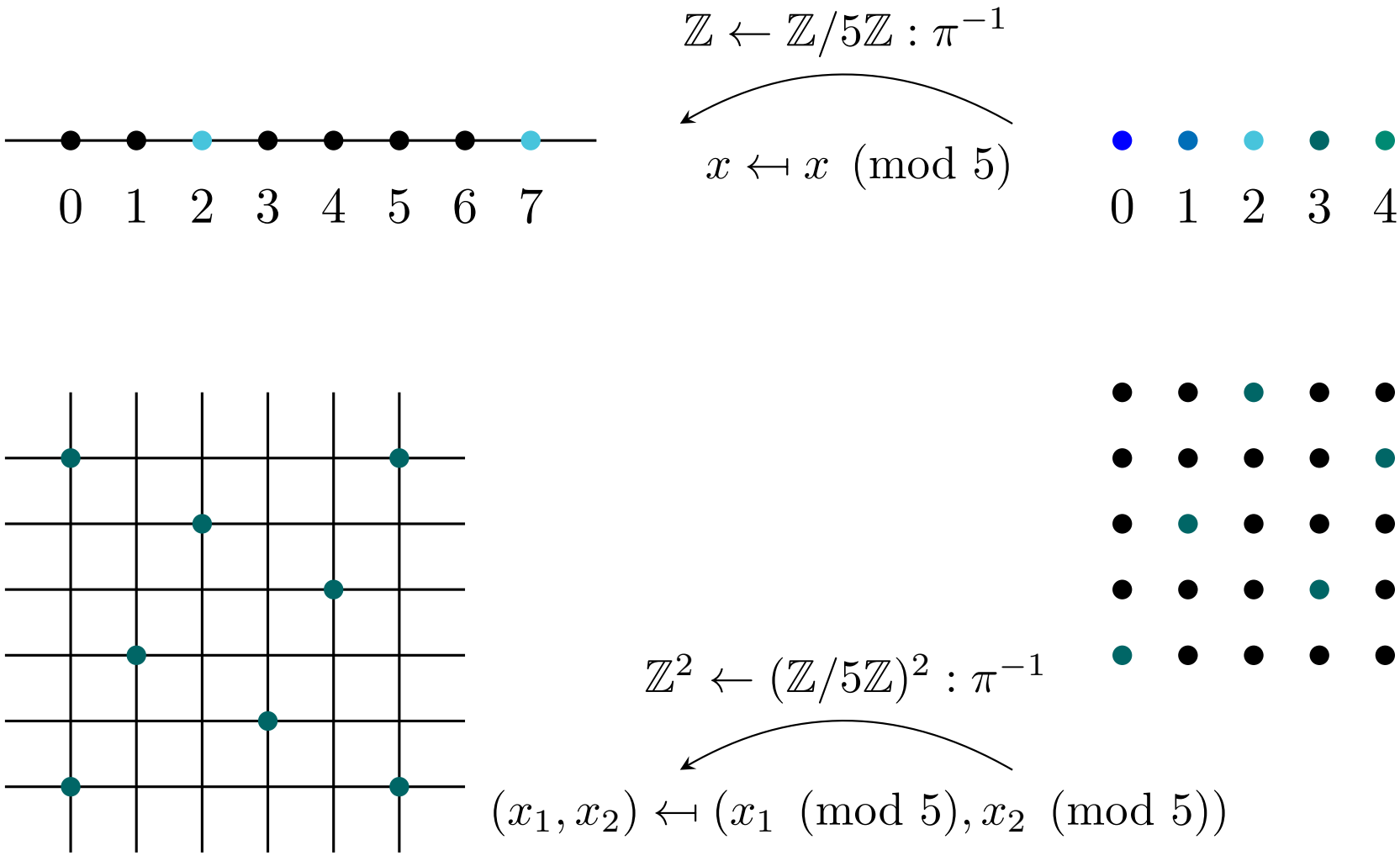
- ✓ Construction A
- ✓ Gram matrix and quadratic form




$\pi : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$
$x \mapsto x \pmod 5$
0 1 2 3 4 5 6 7
0 1 2 3 4


$\pi : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$
$x \mapsto x \pmod 5$
0 1 2 3 4 5 6 7
0 1 2 3 4
$\pi : \mathbb{Z}^2 \to (\mathbb{Z}/5\mathbb{Z})^2$
$(x_1, x_2) \mapsto (x_1 \pmod 5, x_2 \pmod 5)$


$\mathbb{Z} \leftarrow \mathbb{Z}/5\mathbb{Z} : \pi^{-1}$
$x \leftarrow\!\shortmid x \pmod 5$
0 1 2 3 4 5 6 7
0 1 2 3 4

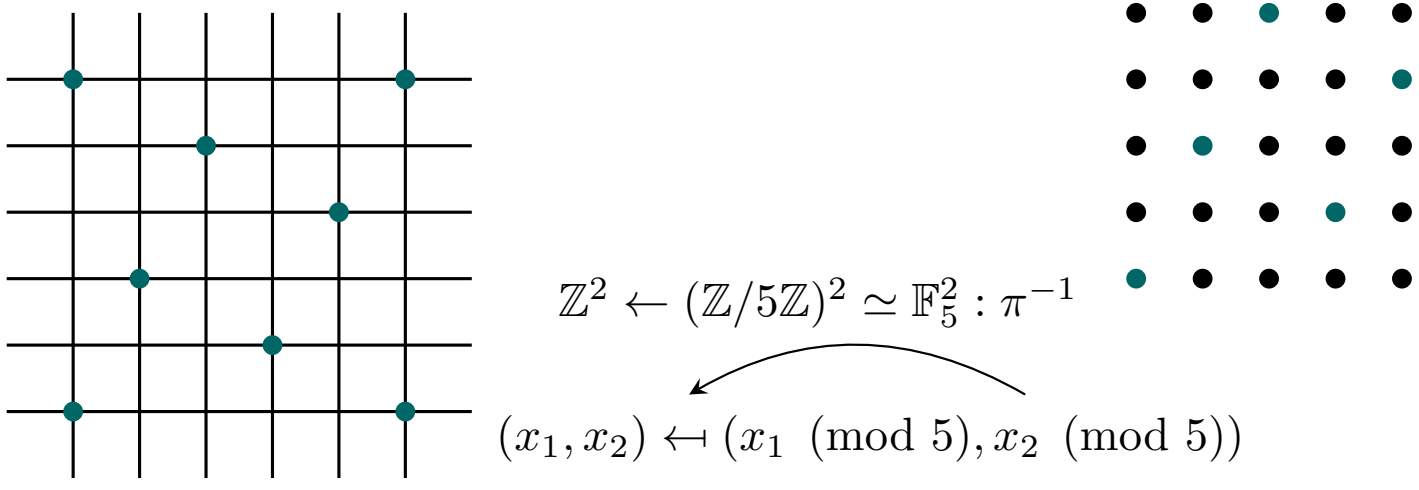

$\mathbb{Z} \leftarrow \mathbb{Z}/5\mathbb{Z} : \pi^{-1}$
$x \leftarrow\!\shortmid x \pmod 5$
0 1 2 3 4 5 6 7
0 1 2 3 4
$\mathbb{Z}^2 \leftarrow (\mathbb{Z}/5\mathbb{Z})^2 : \pi^{-1}$
$(x_1, x_2) \leftarrow\!\shortmid (x_1 \pmod 5, x_2 \pmod 5)$

First observation

Given a subset $\mathcal{C} \subset \mathbb{F}_p^n$, then $\pi^{-1}(\mathcal{C})$ is a lattice in $\mathbb{R}^n$ if and only if $\mathcal{C}$ is a linear code (a linear subspace) in $\mathbb{F}_p^n$.

- Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be linearly independent vectors in $\mathbb{R}^n$. A lattice Λ with basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is defined as

$$\Lambda = \{u_1\mathbf{b}_1 + \ldots + u_n\mathbf{b}_n,\ u_1, \ldots, u_m \in \mathbb{Z}\}.$$



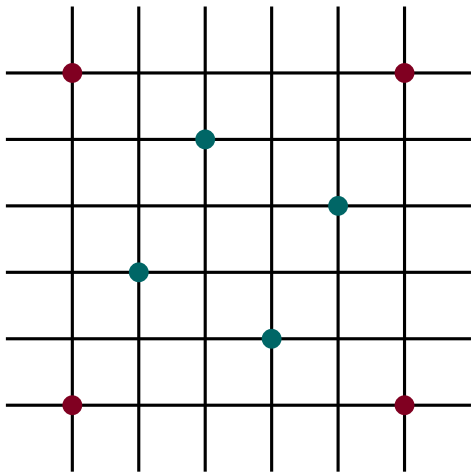
$$\pi^{-1}(\mathcal{C}) = \{u_1(1,2) + u_2(3,1),\ u_1, u_2 \in \mathbb{Z}\},\ \mathcal{C} = \{a(1,2),\ a \in \mathbb{F}_5\}$$

Construction A

Let $\mathcal{C}$ be a linear code in $\mathbb{F}_p^n$ and π be the reduction modulo p componentwise on $\mathbb{Z}^n$. The lattice $\Lambda_C = \pi^{-1}(\mathcal{C})$ is said to have been obtained via Construction A.

Construction A

Let $\mathcal{C}$ be a linear code in $\mathbb{F}_p^n$ and π be the reduction modulo p componentwise on $\mathbb{Z}^n$. The lattice $\Lambda_C = \pi^{-1}(\mathcal{C})$ is said to have been obtained via Construction A.



Since $\mathbf{0} \in \mathcal{C}$, $p\mathbf{e}_i \in \Lambda_C$ for all canonical vectors $\mathbf{e}_i$, and hence $p\mathbb{Z}^n$ is a sublattice of Λ_C (this makes Λ a *p-ary lattice*).

Since $\Lambda = \{u_1\mathbf{b}_1 + \ldots + u_n\mathbf{b}_n,\ u_1, \ldots, u_m \in \mathbb{Z}\}$, we may write

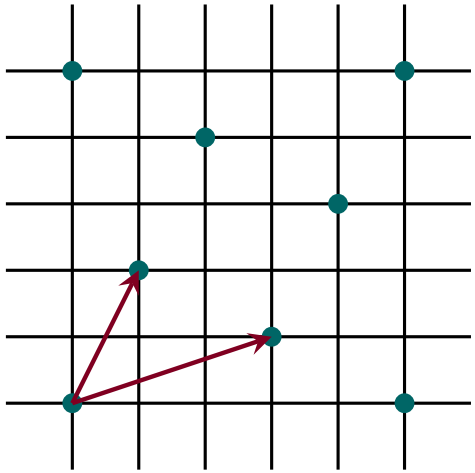
$$\Lambda = \left\{ x \in \mathbb{R}^n,\ x = (u_1, \ldots, u_n) \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_n \end{pmatrix},\quad u_1, \ldots, u_m \in \mathbb{Z} \right\}$$

Since $\Lambda = \{u_1\mathbf{b}_1 + \ldots + u_n\mathbf{b}_n,\ u_1, \ldots, u_m \in \mathbb{Z}\}$, we may write

$$\Lambda = \left\{ x \in \mathbb{R}^n,\ x = (u_1, \ldots, u_n) \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_n \end{pmatrix},\quad u_1, \ldots, u_m \in \mathbb{Z} \right\}$$

Then for $x, y \in \Lambda$

$$\begin{aligned} x \cdot y &= \sum_{i=1}^{n} x_i y_i = (u_1, \ldots, u_n) \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_n \end{pmatrix} \begin{pmatrix} \mathbf{b}_1^T & \ldots & \mathbf{b}_n^T \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \\ &= (u_1, \ldots, u_n) \underbrace{\begin{pmatrix} \mathbf{b}_1 \cdot \mathbf{b}_1 & \ldots & \mathbf{b}_1 \cdot \mathbf{b}_n \\ \vdots & & \\ \mathbf{b}_n \cdot \mathbf{b}_1 & \ldots & \mathbf{b}_n \cdot \mathbf{b}_n \end{pmatrix}}_{\text{Gram matrix}} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \end{aligned}$$



A Gram matrix is

$$\begin{pmatrix} 5 & 5 \\ 5 & 10 \end{pmatrix} = 5 \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

$\pi^{-1}(\mathcal{C}) = \{u_1(1,2)+u_2(3,1),\ u_1, u_2 \in \mathbb{Z}\}$

We say "a" Gram matrix since it is not unique.

The Euclidean scalar product $x \cdot y = \sum_{i=1}^{n} x_i y_i$ is a symmetric bilinear form, that is of the form $b : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, such that

1. $b(x, y) = b(y, x)$ for all $x, y \in \mathbb{R}^n$
2. $b(x + y, z) = b(x, z) + b(y, z)$ for all $x, y, z \in \mathbb{R}^n$
3. $b(\lambda x, y) = \lambda b(x, y)$ for all $\lambda \in \mathbb{R}$, for all $x, y \in \mathbb{R}^n$.

The Euclidean scalar product $x \cdot y = \sum_{i=1}^{n} x_i y_i$ is a symmetric bilinear form, that is of the form $b : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, such that

1. $b(x, y) = b(y, x)$ for all $x, y \in \mathbb{R}^n$
2. $b(x + y, z) = b(x, z) + b(y, z)$ for all $x, y, z \in \mathbb{R}^n$
3. $b(\lambda x, y) = \lambda b(x, y)$ for all $\lambda \in \mathbb{R}$, for all $x, y \in \mathbb{R}^n$.

It is furthermore *positive definite*, namely: $b(x, x) > 0$ for all $x \in \mathbb{R}^n$, $x \neq 0$.

The Euclidean scalar product $x \cdot y = \sum_{i=1}^{n} x_i y_i$ is a symmetric bilinear form, that is of the form $b : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, such that

1. $b(x, y) = b(y, x)$ for all $x, y \in \mathbb{R}^n$
2. $b(x + y, z) = b(x, z) + b(y, z)$ for all $x, y, z \in \mathbb{R}^n$
3. $b(\lambda x, y) = \lambda b(x, y)$ for all $\lambda \in \mathbb{R}$, for all $x, y \in \mathbb{R}^n$.

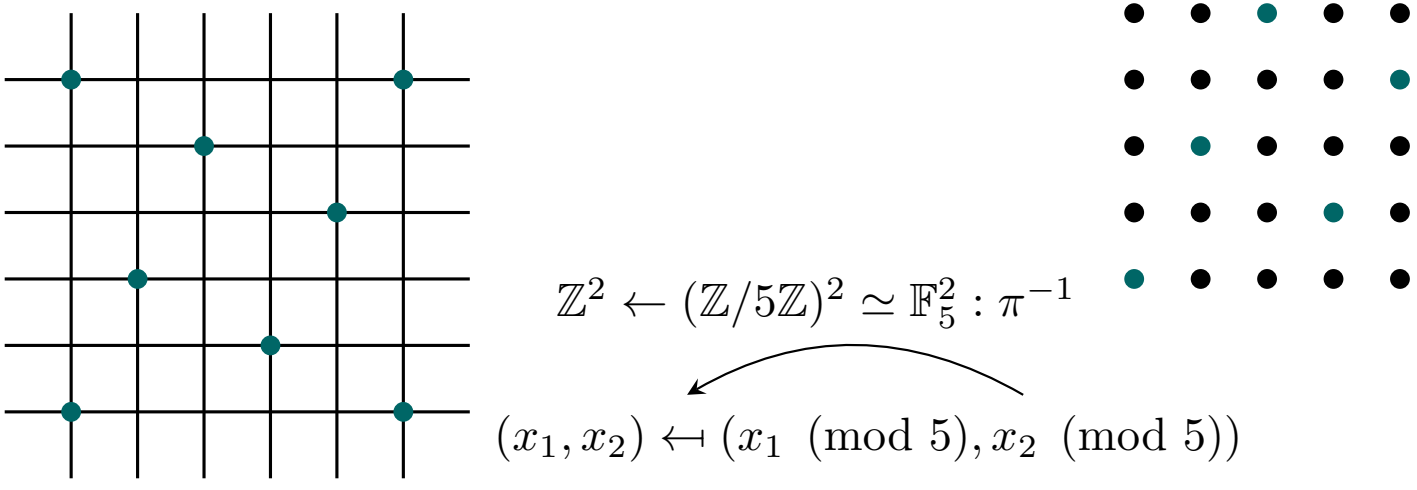
It is furthermore *positive definite*, namely: $b(x, x) > 0$ for all $x \in \mathbb{R}^n$, $x \neq 0$.
This allows us to say

> “An integral lattice Λ is a free $\mathbb{Z}$-module of finite rank n endowed with a positive definite symmetric bilinear form $b : \Lambda \times \Lambda \to \mathbb{Z}$.”

Summary

Given a linear code $\mathcal{C} \subset \mathbb{F}_p^n$ and π the componentwise reduction modulo p on $\mathbb{Z}^n$, $\pi^{-1}(\mathcal{C}) \subset \mathbb{R}^n$ is a lattice, obtained by Construction A. It is equipped with a positive definite symmetric bilinear form b given by the inner product.

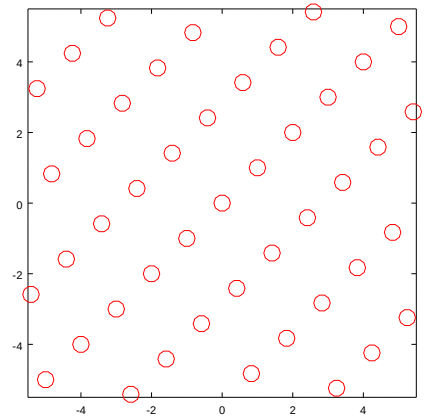
$$\begin{pmatrix} b(\mathbf{b}_1, \mathbf{b}_1) & b(\mathbf{b}_1, \mathbf{b}_2) \\ b(\mathbf{b}_2, \mathbf{b}_1) & b(\mathbf{b}_1, \mathbf{b}_1) \end{pmatrix} = \begin{pmatrix} 5 & 5 \\ 5 & 10 \end{pmatrix}.$$



$$\pi^{-1}(\mathcal{C}) = \{u_1(1,2) + u_2(3,1),\ u_1, u_2 \in \mathbb{Z}\},\ \mathcal{C} = \{a(1,2),\ a \in \mathbb{F}_5\}$$

Lattices from Number Fields

- ✓ Algebraic lattices
- ✓ Construction A
- ✓ Properties

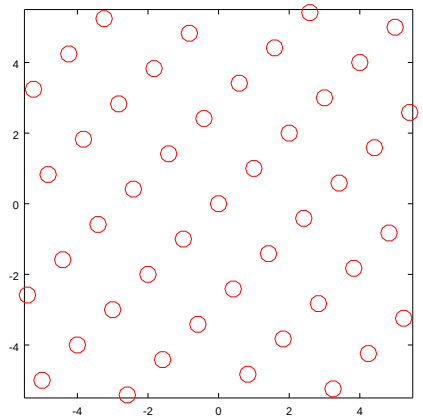


Consider the sets

$$\begin{aligned}\mathbb{Q}(\sqrt{2}) &= \{a+b\sqrt{2},\ a,b\in\mathbb{Q}\}\\ \mathbb{Z}[\sqrt{2}] &= \{a+b\sqrt{2},\ a,b\in\mathbb{Z}\}\end{aligned}$$

and the maps

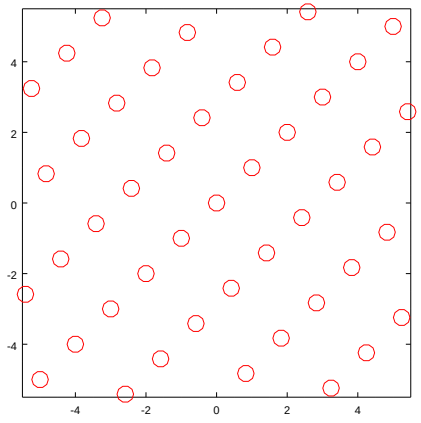
$$\begin{aligned}\sigma_1:&\quad a+b\sqrt{2}\mapsto a+b\sqrt{2}\\ \sigma_2:&\quad a+b\sqrt{2}\mapsto a-b\sqrt{2}.\end{aligned}$$



Create the lattice $\sigma(\mathbb{Z}[\sqrt{2}])$ with $\mathbb{Z}$-basis $(1,1),(\sqrt{2},-\sqrt{2})$ and Gram matrix

$$\begin{bmatrix}\sigma_1(1) & \sigma_2(1)\\ \sigma_1(\sqrt{2}) & \sigma_2(\sqrt{2})\end{bmatrix}\begin{bmatrix}\sigma_1(1) & \sigma_1(\sqrt{2})\\ \sigma_2(1) & \sigma_2(\sqrt{2})\end{bmatrix}=\begin{bmatrix}2 & 0\\ 0 & 4\end{bmatrix}.$$

The set $\mathbb{Z}[\sqrt{2}]$ is a free $\mathbb{Z}$-module of rank 2 endowed with a positive definite symmetric bilinear form given by $(x, y) \mapsto \mathrm{Tr}(xy)$:



$$\begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{2}) \\ \mathrm{Tr}(\sqrt{2}) & \mathrm{Tr}(2) \end{bmatrix}$$

$$= \begin{bmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{2}) & \sigma_2(\sqrt{2}) \end{bmatrix} \begin{bmatrix} \sigma_1(1) & \sigma_1(\sqrt{2}) \\ \sigma_2(1) & \sigma_2(\sqrt{2}) \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}$$

where $\mathrm{Tr}(x) = \sigma_1(x) + \sigma_2(x) \in \mathbb{Z}$ for $x \in \mathbb{Z}[\sqrt{2}]$.

Set $\zeta = \exp(2\pi i/p)$. Consider the sets

$$\begin{aligned} \mathbb{Q}(\zeta_p) &= \{a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2},\ a_i \in \mathbb{Q} \text{ for all } i\} \\ \mathbb{Z}[\zeta_p] &= \{a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2},\ a_i \in \mathbb{Z} \text{ for all } i\} \end{aligned}$$

and the maps

$$\sigma_r : \zeta \mapsto \zeta^r,\ r = 1, \ldots, p-1.$$

Let $\mathrm{Tr}(\alpha) = \sum_{i=1}^{p-1} \sigma_i(\alpha),\ \alpha \in \mathbb{Q}(\zeta_p)$.

Set $\zeta = \exp(2\pi i/p)$. Consider the sets

$$\begin{aligned} \mathbb{Q}(\zeta_p) &= \{a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2},\ a_i \in \mathbb{Q} \text{ for all } i\} \\ \mathbb{Z}[\zeta_p] &= \{a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2},\ a_i \in \mathbb{Z} \text{ for all } i\} \end{aligned}$$

and the maps

$$\sigma_r : \zeta \mapsto \zeta^r,\ r = 1, \ldots, p-1.$$

Let $\mathrm{Tr}(\alpha) = \sum_{i=1}^{p-1} \sigma_i(\alpha),\ \alpha \in \mathbb{Q}(\zeta_p)$. Let $\overline{x}$ denote the complex conjugate of x for $x \in \mathbb{Z}(\zeta_p)$. Then $(x, y) \mapsto \mathrm{Tr}(x\overline{y})$ is a positive definite symmetric bilinear form:

$$\mathrm{Tr}(x\overline{x}) = \sum_{i=1}^{p-1} \sigma_i(x)\overline{\sigma_i(x)} > 0,\ x \neq 0.$$

Set $\mathfrak{P} = (1-\zeta)\mathbb{Z}[\zeta_p] = \{(1-\zeta)(a_0 + a_1\zeta + \ldots + a_{p-1}\zeta^{p-2}),\ a_i \in \mathbb{Z} \text{ for all } i\}$.

Claim. $\mathfrak{P}$ equipped with $(x, y) \mapsto \mathrm{Tr}(x\overline{y}/p)$ is an integral lattice.

Set $\mathfrak{P} = (1-\zeta)\mathbb{Z}[\zeta_p] = \{(1-\zeta)(a_0 + a_1\zeta + \ldots + a_{p-1}\zeta^{p-2}),\ a_i \in \mathbb{Z} \text{ for all } i\}$.

Claim. $\mathfrak{P}$ equipped with $(x, y) \mapsto \mathrm{Tr}(x\overline{y}/p)$ is an integral lattice.

- $\mathrm{Tr}(x) \in \mathbb{Z}$ for $x \in \mathbb{Z}[\zeta]$.
- $\mathrm{Tr}(x\overline{y}) \in p\mathbb{Z}$

Set $\mathfrak{P} = (1-\zeta)\mathbb{Z}[\zeta_p] = \{(1-\zeta)(a_0 + a_1\zeta + \ldots + a_{p-1}\zeta^{p-2}),\ a_i \in \mathbb{Z} \text{ for all } i\}$.

Claim. $\mathfrak{P}$ equipped with $(x, y) \mapsto \mathrm{Tr}(x\overline{y}/p)$ is an integral lattice.

- $\mathrm{Tr}(x) \in \mathbb{Z}$ for $x \in \mathbb{Z}[\zeta]$.
- $\mathrm{Tr}(x\overline{y}) \in p\mathbb{Z}$

For $p = 3$, we have $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$, $\mathfrak{P}$ has $\mathbb{Z}$-basis $(1-\zeta_3), (1-\zeta_3)\zeta_3 = 2\zeta_3 + 1$. Then $\sigma(\mathfrak{P}) = \{u_0(1-\zeta_3) + u_1(1+2\zeta_3),\ u_0, u_1 \in \mathbb{Z}\}$ and

Set $\mathfrak{P} = (1-\zeta)\mathbb{Z}[\zeta_p] = \{(1-\zeta)(a_0 + a_1\zeta + \ldots + a_{p-1}\zeta^{p-2}),\ a_i \in \mathbb{Z} \text{ for all } i\}$.

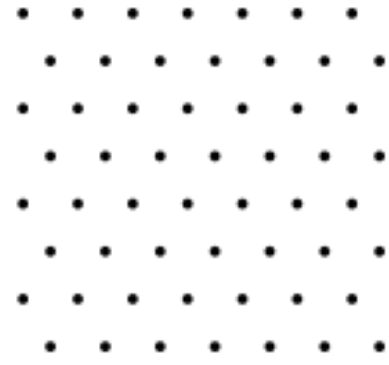
Claim. $\mathfrak{P}$ equipped with $(x, y) \mapsto \mathrm{Tr}(x\overline{y}/p)$ is an integral lattice.

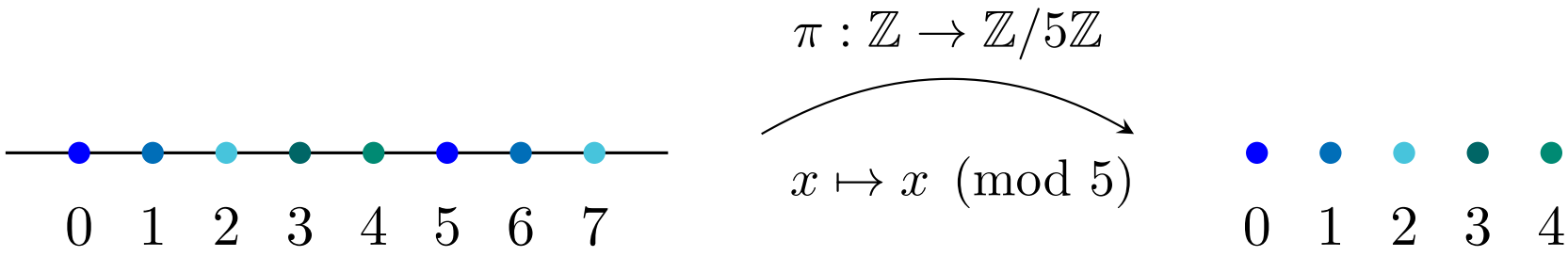
- $\mathrm{Tr}(x) \in \mathbb{Z}$ for $x \in \mathbb{Z}[\zeta]$.
- $\mathrm{Tr}(x\overline{y}) \in p\mathbb{Z}$

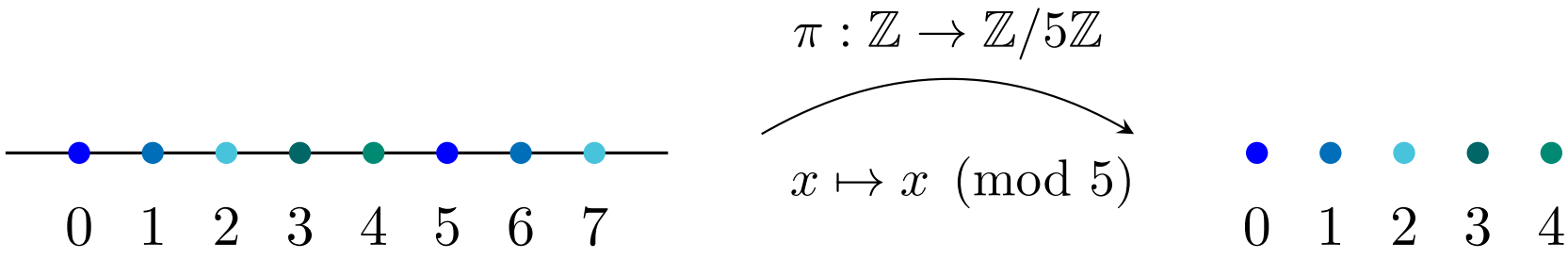
For $p = 3$, we have $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$, $\mathfrak{P}$ has $\mathbb{Z}$-basis $(1-\zeta_3), (1-\zeta_3)\zeta_3 = 2\zeta_3 + 1$. Then $\sigma(\mathfrak{P}) = \{u_0(1-\zeta_3) + u_1(1+2\zeta_3),\ u_0, u_1 \in \mathbb{Z}\}$ and

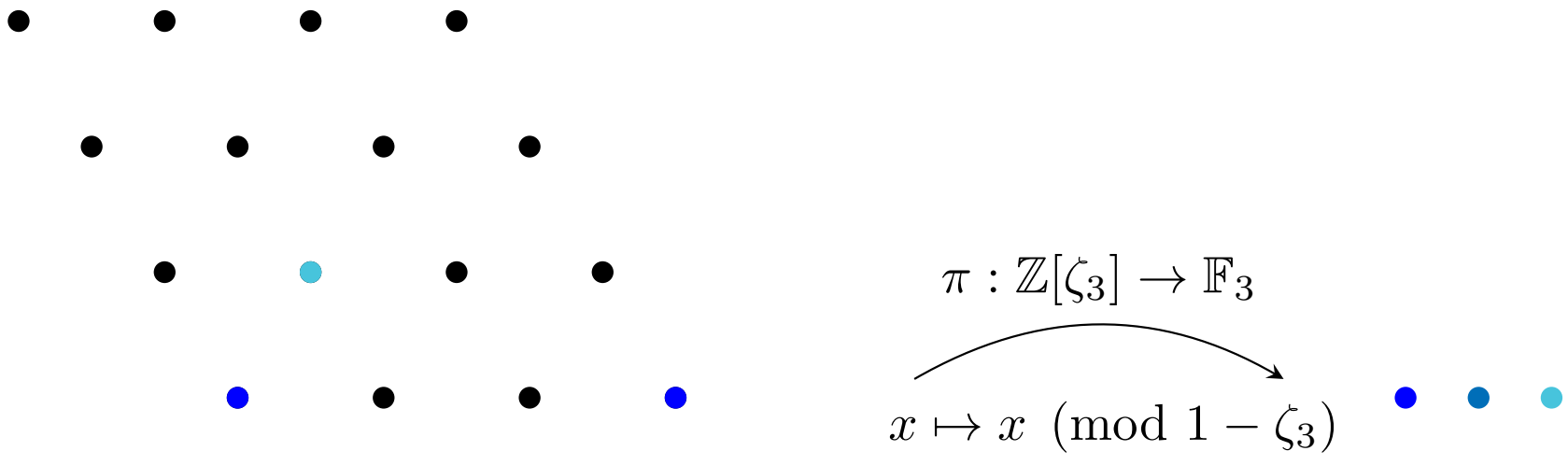
$$\frac{1}{3}\begin{pmatrix} 6 & -3 \\ -3 & 6 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}.$$

This is A_2, the hexagonal lattice.



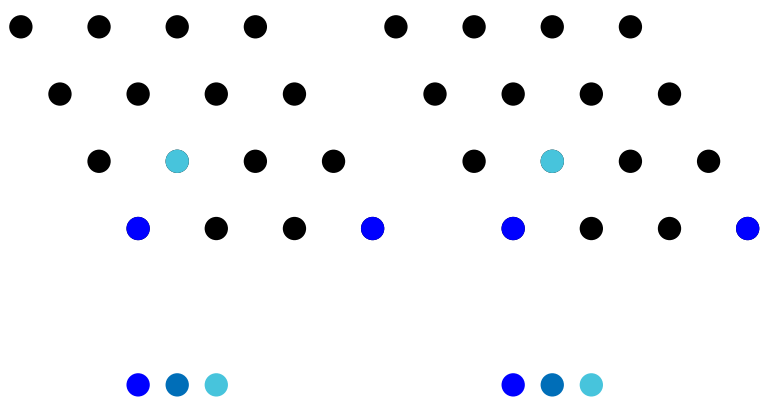

$\pi : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$
$x \mapsto x \pmod 5$
0 1 2 3 4 5 6 7
0 1 2 3 4


$\pi : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$
$x \mapsto x \pmod 5$
0 1 2 3 4 5 6 7
0 1 2 3 4


$\pi : \mathbb{Z}[\zeta_3] \to \mathbb{F}_3$
$x \mapsto x \pmod{1-\zeta_3}$

Given a linear code $\mathcal{C} \subset \mathbb{F}_p^n$ and π the componentwise reduction modulo $1-\zeta$ on $\mathbb{Z}[\zeta]^n$, $\pi^{-1}(\mathcal{C}) \subset \mathbb{R}^n$ equipped with $(x, y) \mapsto \mathrm{Tr}(x\overline{y}/p)$ is an integral lattice obtained by Construction A.

Given a linear code $\mathcal{C} \subset \mathbb{F}_p^n$ and π the componentwise reduction modulo $1-\zeta$ on $\mathbb{Z}[\zeta]^n$, $\pi^{-1}(\mathcal{C}) \subset \mathbb{R}^n$ equipped with $(x, y) \mapsto \mathrm{Tr}(x\overline{y}/p)$ is an integral lattice obtained by Construction A.



The volume $\mathrm{vol}(\Lambda)$ of a lattice Λ is

$$\mathrm{vol}(\Lambda) = \sqrt{(b(\mathbf{b}_i, \mathbf{b}_j))_{i,j}}.$$

- For $\mathcal{C}$ a linear code of dimension m

$$\mathrm{vol}(\Lambda_C) = \sqrt{p^{n-2m}}$$

$(\Delta_{\mathbb{Q}(\zeta)} = (-1)^{(p-1)/2} p^{p-2})$.

The dual lattice Λ^* of a lattice Λ is

$$\Lambda^* = \{x \in \mathbb{R}^n \mid x \cdot y \ \ (b(x,y)) \in \mathbb{Z} \text{ for all } y \in \Lambda\}.$$

If $\Lambda = \Lambda^*$, the lattice is called unimodular.

The dual lattice Λ^* of a lattice Λ is

$$\Lambda^* = \{x \in \mathbb{R}^n \mid x \cdot y \ \ (b(x,y)) \in \mathbb{Z} \text{ for all } y \in \Lambda\}.$$

If $\Lambda = \Lambda^*$, the lattice is called unimodular.

The dual code $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ is

$$\mathcal{C}^\perp = \{y \in \mathbb{F}_p^n \mid x \cdot y = 0 \text{ for all } x \in \mathcal{C}\}.$$

If $\mathcal{C} = \mathcal{C}^\perp$, the lattice is called self-dual.

The dual lattice Λ^* of a lattice Λ is

$$\Lambda^* = \{x \in \mathbb{R}^n \mid x \cdot y \ \ (b(x,y)) \in \mathbb{Z} \text{ for all } y \in \Lambda\}.$$

If $\Lambda = \Lambda^*$, the lattice is called unimodular.

The dual code $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ is

$$\mathcal{C}^\perp = \{y \in \mathbb{F}_p^n \mid x \cdot y = 0 \text{ for all } x \in \mathcal{C}\}.$$

If $\mathcal{C} = \mathcal{C}^\perp$, the lattice is called self-dual.

Let $\mathcal{C} \subset \mathbb{F}_p^n$ be a linear code of dimension m with $\mathcal{C} \subset \mathcal{C}^\perp$. Then

$$\Lambda_{\mathcal{C}}^* = \Lambda_{\mathcal{C}^\perp}.$$

If $\mathcal{C}$ is self-dual, then $\Lambda_{\mathcal{C}}$ is unimodular. ($\Gamma_{\mathcal{C}^\perp} \subseteq \Gamma_{\mathcal{C}}^*$ + volume argument).

Summary

Given a linear code $\mathcal{C} \subset \mathbb{F}_p^n$ of dimension m and π the componentwise reduction modulo $1-\zeta$ on $\mathbb{Z}[\zeta]^n$, $\Lambda_C = \pi^{-1}(\mathcal{C}) \subset \mathbb{R}^n$ equipped with $(x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)) \mapsto \sum_{i=1}^n \mathrm{Tr}(x_i \overline{y_i}/p)$ is an integral lattice obtained by Construction A. It has rank $n(p-1)$, volume $\sqrt{p^{n-2m}}$. If $\mathcal{C}$ is self-dual, then $\Lambda_{\mathcal{C}}$ is unimodular.

Summary

Given a linear code $\mathcal{C} \subset \mathbb{F}_p^n$ of dimension m and π the componentwise reduction modulo $1-\zeta$ on $\mathbb{Z}[\zeta]^n$, $\Lambda_C = \pi^{-1}(\mathcal{C}) \subset \mathbb{R}^n$ equipped with $(x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)) \mapsto \sum_{i=1}^n \mathrm{Tr}(x_i \overline{y_i}/p)$ is an integral lattice obtained by Construction A. It has rank $n(p-1)$, volume $\sqrt{p^{n-2m}}$. If $\mathcal{C}$ is self-dual, then $\Lambda_{\mathcal{C}}$ is unimodular.

- May want normalization or not. If $p = 2$, $\zeta_p = -1$.

Summary

Given a linear code $\mathcal{C} \subset \mathbb{F}_p^n$ of dimension m and π the componentwise reduction modulo $1-\zeta$ on $\mathbb{Z}[\zeta]^n$, $\Lambda_C = \pi^{-1}(\mathcal{C}) \subset \mathbb{R}^n$ equipped with $(x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)) \mapsto \sum_{i=1}^n \mathrm{Tr}(x_i \overline{y_i}/p)$ is an integral lattice obtained by Construction A. It has rank $n(p-1)$, volume $\sqrt{p^{n-2m}}$. If $\mathcal{C}$ is self-dual, then $\Lambda_{\mathcal{C}}$ is unimodular.

- May want normalization or not. If $p = 2$, $\zeta_p = -1$.
- Applications to (not exhaustive): (1) encoder design (labelling), (2) constructions of "interesting" (extremal, dense) lattices, (3) physical network coding.

A Quadratic Form Approach to Construction A of Lattices over Cyclic Algebras

(joint work with G. Berhuy)

- ✓ Number fields (ideas)
- ✓ Cyclic algebras ("ideas")

Question: is it possible to add a multiplicative structure to Construction A?

Question: is it possible to add a multiplicative structure to Construction A?

- Lattices are inherently additive.
- Algebras and number fields (not copies of them) also come with a multiplication.
- Would like to retain "dual" properties.

First idea

Λ: $b(x,y)$	$\mathcal{C}$: $x \cdot y$
Λ^*: $b(x,y) \in \mathbb{Z}$	$\mathcal{C}^\perp$: $x \cdot y$

Let M be an integral lattice, and let N be a sublattice of M such that $pM \subset N \subset M$. Assume also that $b(x,y) \in p\mathbb{Z}$ for all $x \in M$ and $y \in N$. Then b induces on M a symmetric $\mathbb{Z}$-bilinear form $b : M \times M \to \mathbb{Z}$, which in turn induces a symmetric $\mathbb{F}_p$-bilinear form

$$\overline{b}: \begin{array}{c} M/N \times M/N \longrightarrow \mathbb{F}_p \\ ([x]_N, [y]_N) \longmapsto [b(x,y)]_p. \end{array}$$

First idea

Λ: $b(x,y)$	$\mathcal{C}$: $x \cdot y$
Λ^*: $b(x,y) \in \mathbb{Z}$	$\mathcal{C}^\perp$: $x \cdot y$

Let M be an integral lattice, and let N be a sublattice of M such that $pM \subset N \subset M$. Assume also that $b(x,y) \in p\mathbb{Z}$ for all $x \in M$ and $y \in N$. Then b induces on M a symmetric $\mathbb{Z}$-bilinear form $b : M \times M \to \mathbb{Z}$, which in turn induces a symmetric $\mathbb{F}_p$-bilinear form

$$\overline{b}: \begin{array}{c} M/N \times M/N \longrightarrow \mathbb{F}_p \\ ([x]_N, [y]_N) \longmapsto [b(x,y)]_p. \end{array}$$

Furthermore $\overline{b}$ is nondegenerate ($\overline{b}([x]_N, [y]_N) = 0$ for all $[y]_N$ implies $[x]_N = 0$) if and only if $pM^* \cap M = N$.

Number fields: ingredients

a number field L • complex conjugation * induces an automorphism of L • a prime number p • an ideal I of $\mathcal{O}_L$ containing p such that $I^* = I$ • a $\mathbb{Z}$-linear map $s : \mathcal{O}_L \to \mathbb{Z}$.

(H_1) The linear map s induces on $\mathcal{O}_L/I$ a well-defined nondegenerate symmetric $\mathbb{F}_p$-bilinear map

$$\varphi : \begin{array}{c} \mathcal{O}_L/I \times \mathcal{O}_L/I \longrightarrow \mathbb{F}_p \\ ([x]_I, [y]_I) \longmapsto [s(x^* y)]_p. \end{array}$$

(H_2) There exists a nonzero monic polynomial $\overline{\mu} \in \mathbb{F}_p[X]$ such that we have an isomorphism of $\mathbb{F}_p$-algebras

$$\mathbb{F}_p[X]/(\overline{\mu}) \simeq \mathcal{O}_L/I.$$

Number fields: ingredients

a number field L • complex conjugation * induces an automorphism of L • a prime number p • an ideal I of $\mathcal{O}_L$ containing p such that $I^* = I$ • a $\mathbb{Z}$-linear map $s : \mathcal{O}_L \to \mathbb{Z}$.

(H_1) The linear map s induces on $\mathcal{O}_L/I$ a well-defined nondegenerate symmetric $\mathbb{F}_p$-bilinear map

$$\varphi : \begin{array}{c} \mathcal{O}_L/I \times \mathcal{O}_L/I \longrightarrow \mathbb{F}_p \\ ([x]_I, [y]_I) \longmapsto [s(x^*y)]_p. \end{array}$$

(H_2) There exists a nonzero monic polynomial $\overline{\mu} \in \mathbb{F}_p[X]$ such that we have an isomorphism of $\mathbb{F}_p$-algebras

$$\mathbb{F}_p[X]/(\overline{\mu}) \simeq \mathcal{O}_L/I.$$

(H_1) becomes finding the "right" trace form, (H_2) is about finding number fields with "right" rings of integers.

Number fields: polynomial codes

(H_2):$\mathbb{F}_p[X]/(\overline{\mu}) \simeq \mathcal{O}_L/I$.

Ideals of $\mathcal{O}_L/I \iff$ ideals of $\mathbb{F}_p[X]$ containing $\overline{\mu} \iff$ monic divisors of $\overline{\mu} \iff$ generator polynomials of polynomial codes.

Number fields: polynomial codes

(H_2):$\mathbb{F}_p[X]/(\overline{\mu}) \simeq \mathcal{O}_L/I$.

Ideals of $\mathcal{O}_L/I \iff$ ideals of $\mathbb{F}_p[X]$ containing $\overline{\mu} \iff$ monic divisors of $\overline{\mu} \iff$ generator polynomials of polynomial codes.

Complex conjugation is an automorphism of $L \Rightarrow$ it induces an automorphism of $\mathcal{O}_L \Rightarrow$ which induces an automorphism of $\mathcal{O}_L/I$, since $I^* = I$, still denoted by $^* \Rightarrow$ complex conjugation induces a correspondence between ideals, hence between monic divisors of $\overline{\mu}$. If $\overline{g}$ is such a monic divisor, $\overline{g}_*$ is the corresponding monic divisor of $\overline{\mu}$.

Theorem. If the ideal I'/I corresponds to the ideal generated by $\overline{g}$, then I'/I is self-orthogonal if and only if $\overline{\mu} \mid \overline{g}_*\overline{g}$, and self-dual if and only if $\overline{g}_*\overline{g} = \overline{\mu}$.

Number fields: An Example

$L = \mathbb{Q}(\zeta_{8p}) = K_1K_2$ • $K_1 = \mathbb{Q}(\zeta_8), K_2 = \mathbb{Q}(\zeta_p)$, $p = 3, 5, 11, 13, 19$.

Number fields: An Example

$L = \mathbb{Q}(\zeta_{8p}) = K_1K_2$ • $K_1 = \mathbb{Q}(\zeta_8), K_2 = \mathbb{Q}(\zeta_p)$, $p = 3$, 5, 11, 13, 19. We will build polynomial codes over $\mathbb{F}_p[X]/(\bar{\mu}_{\alpha_1,\mathbb{Q}})$ for $\alpha_1 = \zeta_8$:

$$\mathcal{O}_L/\mathfrak{p}_2\mathcal{O}_L \simeq \mathcal{O}_{K_1}/p\mathcal{O}_{K_1} \simeq \mathbb{F}_p[X]/(\overline{\mu}_{\alpha_1,\mathbb{Q}})$$

We have $\overline{\mu}_{\alpha_1,\mathbb{Q}} = X^4 + 1$. Take $\overline{g}$ to be $X^2 + X + \overline{2} \pmod 3$, $X^2 + \overline{2} \pmod 5$, $X^2 + \overline{3}X + \overline{10} \pmod{11}$, $X^2 + \overline{5} \pmod{13}$, respectively $X^2 + \overline{6}X + \overline{18} \pmod{19}$. For these cases, $\overline{g}_*\overline{g} = \overline{\mu}_{\alpha_1,\mathbb{Q}}$ and it follows from the theorem that $\mathcal{C}^\perp = \mathcal{C}$.
The volume of the lattice under the trace form of $(H1)$ is controlled by the introduction of a twisting element $\lambda_1 = \dfrac{1}{4}$ in the trace form.
The degree of L is $4(p-1)$ So for $p = 3$ we get a unimodular lattice in dimension 8 which is even, namely E_8.

Cyclic Algebras

L/k a cyclic Galois number field extension of group $G = \langle \sigma \rangle$ and degree n • $L/\mathbb{Q}$ is totally real or CM • complex conjugation induces a ring automorphism on k (possibly trivial).

Cyclic Algebras

L/k a cyclic Galois number field extension of group $G = \langle \sigma \rangle$ and degree n • $L/\mathbb{Q}$ is totally real or CM • complex conjugation induces a ring automorphism on k (possibly trivial).
$\gamma \in k^\times$ such that $\gamma\gamma^* = 1$ • the cyclic algebra $B = (\gamma, L/k, \sigma)$:

$$B = L \oplus eL \oplus \cdots \oplus e^{n-1}L = \bigoplus_{j=0}^{n-1} e^j L$$

where $e^n = \gamma$ and $ae = ea^\sigma$ for all $a \in L$. Note that $e \in B^\times$, and that $e^{-1} = e^{n-1}\gamma^{-1}$.

Cyclic Algebras

L/k a cyclic Galois number field extension of group $G = \langle \sigma \rangle$ and degree n • $L/\mathbb{Q}$ is totally real or CM • complex conjugation induces a ring automorphism on k (possibly trivial).
$\gamma \in k^\times$ such that $\gamma\gamma^* = 1$ • the cyclic algebra $B = (\gamma, L/k, \sigma)$:

$$B = L \oplus eL \oplus \cdots \oplus e^{n-1}L = \bigoplus_{j=0}^{n-1} e^j L$$

where $e^n = \gamma$ and $ae = ea^\sigma$ for all $a \in L$. Note that $e \in B^\times$, and that $e^{-1} = e^{n-1}\gamma^{-1}$.
An involution on B: $\tau : B \to B$, such that for all $x_j \in L$

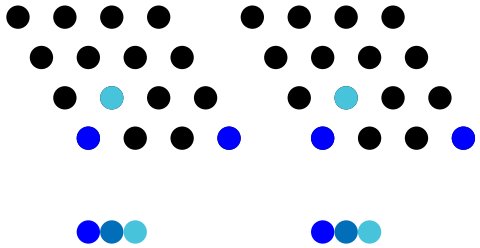
$$\tau(\sum_{j=0}^{n-1} e^j x_j) = \sum_{j=0}^{n-1} x_j^* e^{-j}.$$

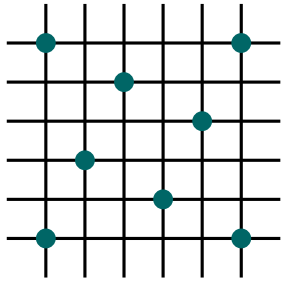
The order $\bigoplus_{j=0}^{n-1} e^j \mathcal{O}_L$.

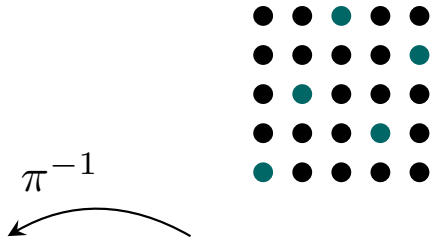
1. Define a suitable trace form.
2. Consider the quotient $\bigoplus_{j=0}^{n-1} e^j \mathcal{O}_L/\mathcal{P}$ ($\mathcal{P}$ two-sided).
3. Set $\mathbb{F}_q = \mathcal{O}_L/\mathfrak{P}$. Identify this quotient with $\mathbb{F}_q[X;\overline{\sigma}]/(X^n - [\gamma]_{\mathfrak{P}})$ which leads to consider skew-polynomial codes.
4. Define conditions on skew-polynomial codes for getting self-dual codes (with respect with the trace form induced by that of the algebra).
5. Use an argument of volume (and a possible twisting element) to deduce unimodularity of the lattice.

Summary

$\mathbb{Z}^n$	$\mathbb{Z}[\zeta]^n$	$\mathcal{O}_L$	$\bigoplus_{j=0}^{n-1} e^j \mathcal{O}_L$
$\mathbb{Z}/p\mathbb{Z}$	$\mathbb{Z}[\zeta]/(1-\zeta)$	$\mathcal{O}_L/I$	$\bigoplus_{j=0}^{n-1} e^j \mathcal{O}_L/\mathcal{P}$
$\mathbb{F}_p^n$	$\mathbb{F}_p^n$	$\mathcal{O}_L/I \simeq \mathbb{F}_p[X]/(\overline{\mu})$	$\mathbb{F}_q[X;\overline{\sigma}]/(X^n - [\gamma]_{\mathfrak{P}})$
$\mathcal{C}$	$\mathcal{C}$	$\overline{g}\|\overline{\mu}$	$\overline{g}\|X^n - [\gamma]_{\mathfrak{P}}$
		polynomial codes	skew-polynomial codes
$x \cdot y$	$\sum_i \mathrm{Tr}(x_i \overline{y}_i)$	$\mathrm{Tr}_{L/\mathbb{Q}}(\lambda x^* y)$	$\mathrm{Tr}_{k/\mathbb{Q}}(\mathrm{Trd}_B(\lambda \tau(x) y))$







https://arxiv.org/abs/2004.01641
Ebeling, “Lattices and Codes”