On Construction D and Related Constructions of Lattices from Linear Codes

Wittawat Kositwattanarerk and Frédérique Oggier

Division of Mathematical Sciences
Nanyang Technological University, Singapore

April 18, 2013

Notation

$\mathbb{F}_2 = \{0, 1\}$ is the binary field.
$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ is the set of integers.
$\mathbb{R}$ is the set of real numbers.

Notation

$\mathbb{F}_2 = \{0, 1\}$ is the binary field.
$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ is the set of integers.
$\mathbb{R}$ is the set of real numbers.

A **binary linear code** C of length n is a subspace of $\mathbb{F}_2^n$. Elements of C are called codewords.

A **lattice** Λ of dimension n is a discrete additive subgroup of $\mathbb{R}^n$.

Notation

$\mathbb{F}_2 = \{0, 1\}$ is the binary field.
$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ is the set of integers.
$\mathbb{R}$ is the set of real numbers.

A **binary linear code** C of length n is a subspace of $\mathbb{F}_2^n$. Elements of C are called codewords.

A **lattice** Λ of dimension n is a discrete additive subgroup of $\mathbb{R}^n$.

Let ψ be the natural embedding of $\mathbb{F}_2^n$ into $\mathbb{Z}^n$.

Construction A simply "lifts" the code.

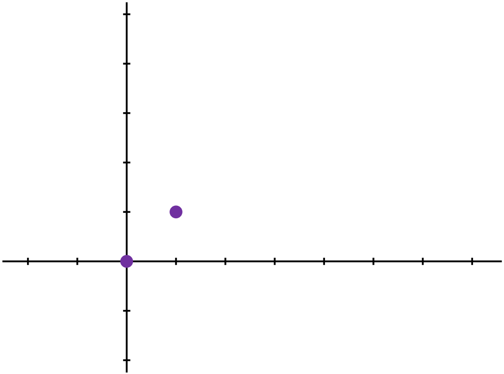
Definition of Construction A

Let C be a binary linear code of length n, then

$$\Lambda_A = \psi(C) \oplus 2\mathbb{Z}^n$$

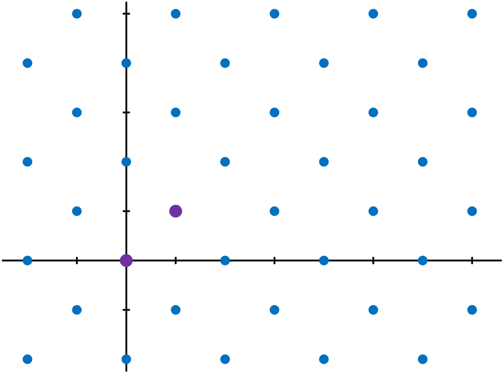
is a lattice of dimension n.

Construction A simply "lifts" the code.



Consider a code $C = \{(0,0),(1,1)\} \in \mathbb{F}_2^2$.

Construction A simply "lifts" the code.

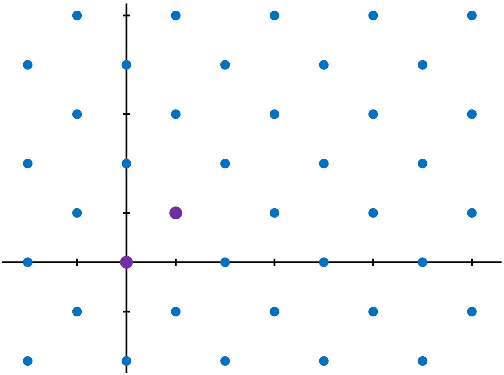


Consider a code $C = \{(0,0),(1,1)\} \in \mathbb{F}_2^2$.
Construction A,

$$\Lambda_A = \psi(C) \oplus 2\mathbb{Z}^n$$

gives the checkerboard lattice D_2.

Construction A simply "lifts" the code.



Consider a code $C = \{(0,0),(1,1)\} \in \mathbb{F}_2^2$.
Construction A,

$$\Lambda_A = \psi(C) \oplus 2\mathbb{Z}^n$$

gives the checkerboard lattice D_2.

Construction D's use nested codes.

Definition of Construction $\overline{\text{D}}$ (Forney 1988)

Let

$$C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$$

be a family of nested binary linear codes. Let

$$\Gamma_{\overline{D}} = \psi(C_0) \oplus 2\psi(C_1) \oplus \ldots \oplus 2^{a-1}\psi(C_{a-1}) \oplus 2^a\mathbb{Z}^n.$$

Construction D's use nested codes.

Definition of Construction $\overline{\mathrm{D}}$ (Forney 1988)

Let

$$C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$$

be a family of nested binary linear codes. Let

$$\Gamma_{\overline{D}} = \psi(C_0) \oplus 2\psi(C_1) \oplus \ldots \oplus 2^{a-1}\psi(C_{a-1}) \oplus 2^a\mathbb{Z}^n.$$

Let $R(r, m)$ be the Reed-Muller code of length $n = 2^m$ and order r. From the chain $R(0, m) \subset R(1, m) \subset \ldots \subset R(m, m)$, Construction $\overline{\mathrm{D}}$ yields the Barnes-Wall lattices.

Construction D's use nested codes.

Definition of Construction D (Barnes and Sloane 1983)

Let

$$C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$$

be a family of nested binary linear codes. Let $k_i = \dim(C_i)$ and let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{F}_2^n$ such that $\mathbf{b}_1, \ldots, \mathbf{b}_{k_i}$ span C_i. The lattice Λ_D consists of all vectors of the form

$$\sum_{\substack{\mathbf{b}_{j_0} \text{ among} \\ \text{generators} \\ \text{for } C_0}} \psi(\mathbf{b}_{j_0}) + 2 \sum_{\substack{\mathbf{b}_{j_1} \text{ among} \\ \text{generators} \\ \text{for } C_1}} \psi(\mathbf{b}_{j_1}) + \ldots + 2^{a-1} \sum_{\substack{\mathbf{b}_{j_1} \text{ among} \\ \text{generators} \\ \text{for } C_{a-1}}} \psi(\mathbf{b}_{j_{a-1}}) + 2^a \mathbf{l}$$

where $\alpha_j \in \{0, 1\}$ and $\mathbf{l} \in \mathbb{Z}^n$.

Construction D's use nested codes.

Definition of Construction D (Barnes and Sloane 1983)

Let

$$C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$$

be a family of nested binary linear codes. Let $k_i = \dim(C_i)$ and let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{F}_2^n$ such that $\mathbf{b}_1, \ldots, \mathbf{b}_{k_i}$ span C_i. The lattice Λ_D consists of all vectors of the form

$$\sum_{\substack{\mathbf{b}_{j_0} \text{ among} \\ \text{generators} \\ \text{for } C_0}} \psi(\mathbf{b}_{j_0}) + 2 \sum_{\substack{\mathbf{b}_{j_1} \text{ among} \\ \text{generators} \\ \text{for } C_1}} \psi(\mathbf{b}_{j_1}) + \ldots + 2^{a-1} \sum_{\substack{\mathbf{b}_{j_1} \text{ among} \\ \text{generators} \\ \text{for } C_{a-1}}} \psi(\mathbf{b}_{j_{a-1}}) + 2^a \mathbf{l}$$

where $\alpha_j \in \{0, 1\}$ and $\mathbf{l} \in \mathbb{Z}^n$.

Let $R(r, m)$ be the Reed-Muller code of length $n = 2^m$ and order r. From the chain $R(0, m) \subset R(1, m) \subset \ldots \subset R(m, m)$, Construction D yields the Barnes-Wall lattices.

Construction D's use nested codes.

Definition of Construction $\overline{\text{D}}$

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. Let

$$\Gamma_{\overline{D}} = \psi(C_0) \oplus 2\psi(C_1) \oplus \ldots \oplus 2^{a-1}\psi(C_{a-1}) \oplus 2^a\mathbb{Z}^n.$$

Definition of Construction D

Let $k_i = \dim(C_i)$ and let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{F}_2^n$ such that $\mathbf{b}_1, \ldots, \mathbf{b}_{k_i}$ span C_i. The lattice Λ_D consists of all vectors of the form

$$\sum_{\substack{\mathbf{b}_{j_0} \text{ among} \\ \text{generators} \\ \text{for } C_0}} \psi(\mathbf{b}_{j_0}) + 2 \sum_{\substack{\mathbf{b}_{j_1} \text{ among} \\ \text{generators} \\ \text{for } C_1}} \psi(\mathbf{b}_{j_1}) + \ldots + 2^{a-1} \sum_{\substack{\mathbf{b}_{j_1} \text{ among} \\ \text{generators} \\ \text{for } C_{a-1}}} \psi(\mathbf{b}_{j_{a-1}}) + 2^a\mathbf{l}$$

where $\alpha_j \in \{0, 1\}$ and $\mathbf{l} \in \mathbb{Z}^n$.

Construction $\overline{\text{D}}$ can fail.

Definition of Construction $\overline{\text{D}}$

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. Let

$$\Gamma_{\overline{D}} = \psi(C_0) \oplus 2\psi(C_1) \oplus \ldots \oplus 2^{a-1}\psi(C_{a-1}) \oplus 2^a\mathbb{Z}^n.$$

Let $\mathbf{c}_1, \mathbf{c}_2 \in C_i$, and let $\mathbf{c}_3$ be the sum of $\mathbf{c}_1$ and $\mathbf{c}_2$ over $\mathbb{F}_2$. Then,

$$\psi(\mathbf{c}_1) + \psi(\mathbf{c}_2) - \psi(\mathbf{c}_3)$$

may or may not be in $\Gamma_{\overline{D}}$.

Construction $\overline{\text{D}}$ can fail.

Definition of Construction $\overline{\text{D}}$

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. Let

$$\Gamma_{\overline{D}} = \psi(C_0) \oplus 2\psi(C_1) \oplus \ldots \oplus 2^{a-1}\psi(C_{a-1}) \oplus 2^a\mathbb{Z}^n.$$

Let $\mathbf{c}_1, \mathbf{c}_2 \in C_i$, and let $\mathbf{c}_3$ be the sum of $\mathbf{c}_1$ and $\mathbf{c}_2$ over $\mathbb{F}_2$. Then,

$$\psi(\mathbf{c}_1) + \psi(\mathbf{c}_2) - \psi(\mathbf{c}_3)$$

may or may not be in $\Gamma_{\overline{D}}$.

So, $\Gamma_{\overline{D}}$ may or may not be a lattice whereas Λ_D is always a lattice.

Construction $\overline{\text{D}}$ can fail.

Definition of Construction $\overline{\text{D}}$

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. Let

$$\Gamma_{\overline{D}} = \psi(C_0) \oplus 2\psi(C_1) \oplus \ldots \oplus 2^{a-1}\psi(C_{a-1}) \oplus 2^a\mathbb{Z}^n.$$

Let $\Lambda_{\overline{D}}$ be the smallest lattice that contains $\Gamma_{\overline{D}}$.

Let $\mathbf{c}_1, \mathbf{c}_2 \in C_i$, and let $\mathbf{c}_3$ be the sum of $\mathbf{c}_1$ and $\mathbf{c}_2$ over $\mathbb{F}_2$. Then,

$$\psi(\mathbf{c}_1) + \psi(\mathbf{c}_2) - \psi(\mathbf{c}_3)$$

may or may not be in $\Gamma_{\overline{D}}$.

So, $\Gamma_{\overline{D}}$ may or may not be a lattice whereas Λ_D is always a lattice.

Construction $\overline{\text{D}}$ can fail.

Definition of Construction $\overline{\text{D}}$

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. Let

$$\Gamma_{\overline{D}} = \psi(C_0) \oplus 2\psi(C_1) \oplus \ldots \oplus 2^{a-1}\psi(C_{a-1}) \oplus 2^a\mathbb{Z}^n.$$

Let $\Lambda_{\overline{D}}$ be the smallest lattice that contains $\Gamma_{\overline{D}}$.

Let $\mathbf{c}_1, \mathbf{c}_2 \in C_i$, and let $\mathbf{c}_3$ be the sum of $\mathbf{c}_1$ and $\mathbf{c}_2$ over $\mathbb{F}_2$. Then,

$$\psi(\mathbf{c}_1) + \psi(\mathbf{c}_2) - \psi(\mathbf{c}_3)$$

may or may not be in $\Gamma_{\overline{D}}$.

So, $\Gamma_{\overline{D}}$ may or may not be a lattice whereas Λ_D is always a lattice.

Question: Is $\Lambda_{\overline{D}} = \Lambda_D$? What make Construction $\overline{\text{D}}$ works for Reed-Muller code?

Construction $\overline{\mathrm{D}}$ can fail.

Definition of Construction $\overline{\mathrm{D}}$

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. Let

$$\Gamma_{\overline{D}} = \psi(C_0) \oplus 2\psi(C_1) \oplus \ldots \oplus 2^{a-1}\psi(C_{a-1}) \oplus 2^a\mathbb{Z}^n.$$

Let $\Lambda_{\overline{D}}$ be the smallest lattice that contains $\Gamma_{\overline{D}}$.

Let $\mathbf{c}_1, \mathbf{c}_2 \in C_i$, and let $\mathbf{c}_3$ be the sum of $\mathbf{c}_1$ and $\mathbf{c}_2$ over $\mathbb{F}_2$. Then,

$$\psi(\mathbf{c}_1) + \psi(\mathbf{c}_2) - \psi(\mathbf{c}_3)$$

may or may not be in $\Gamma_{\overline{D}}$.

So, $\Gamma_{\overline{D}}$ may or may not be a lattice whereas Λ_D is always a lattice.

Question: Is $\Lambda_{\overline{D}} = \Lambda_D$? What make Construction $\overline{\mathrm{D}}$ works for Reed-Muller code?

Let $*$ denote componentwise multiplication (known also as the Schur product or Hadamard product). If $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$, then

$$\mathbf{x} * \mathbf{y} := (x_1 y_1, \ldots, x_n y_n) \in \mathbb{F}_2^n.$$

Let $*$ denote componentwise multiplication (known also as the Schur product or Hadamard product). If $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$, then

$$\mathbf{x} * \mathbf{y} := (x_1 y_1, \ldots, x_n y_n) \in \mathbb{F}_2^n.$$

Now, if $\mathbf{z}$ is the binary sum of $\mathbf{x}$ and $\mathbf{y}$, then

$$\psi(\mathbf{x}) + \psi(\mathbf{y}) - \psi(\mathbf{z}) = 2\psi(\mathbf{x} * \mathbf{y}).$$

Let $*$ denote componentwise multiplication (known also as the Schur product or Hadamard product). If $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$, then

$$\mathbf{x} * \mathbf{y} := (x_1 y_1, \ldots, x_n y_n) \in \mathbb{F}_2^n.$$

Now, if $\mathbf{z}$ is the binary sum of $\mathbf{x}$ and $\mathbf{y}$, then

$$\psi(\mathbf{x}) + \psi(\mathbf{y}) - \psi(\mathbf{z}) = 2\psi(\mathbf{x} * \mathbf{y}).$$

Given a chain $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ of binary linear codes, if the Schur product of any two codewords of C_i is contained in C_{i+1} for all i, then we say that the chain is **closed under Schur product**.

Theorem (K. and O.)

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. The following statements are equivalent.

1. $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ is closed under Schur product.
2. $\Gamma_{\overline{D}}$ is a lattice.
3. $\Gamma_{\overline{D}} = \Lambda_D$.

Theorem (K. and O.)

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. The following statements are equivalent.

1. $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ is closed under Schur product.
2. $\Gamma_{\overline{D}}$ is a lattice.
3. $\Gamma_{\overline{D}} = \Lambda_D$.

Proof (3. $\Rightarrow$ 2.): Trivial.

Theorem (K. and O.)

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. The following statements are equivalent.

1. $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ is closed under Schur product.
2. $\Gamma_{\overline{D}}$ is a lattice.
3. $\Gamma_{\overline{D}} = \Lambda_D$.

Proof (2. $\Rightarrow$ 1.): Pick $\mathbf{c}_1, \mathbf{c}_2 \in C_i$ such that $\mathbf{c}_1 * \mathbf{c}_2 \notin C_{i+1}$ and consider

$$\psi(\mathbf{c}_1) + \psi(\mathbf{c}_2) - \psi(\mathbf{c}_3)$$

where $\mathbf{c}_3$ is the binary sum of $\mathbf{c}_1$ and $\mathbf{c}_2$.

Theorem (K. and O.)

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. The following statements are equivalent.

1. $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ is closed under Schur product.
2. $\Gamma_{\overline{D}}$ is a lattice.
3. $\Gamma_{\overline{D}} = \Lambda_D$.

Proof (1. $\Rightarrow$ 3.): We do induction on a. When $a = 1$, $\Gamma_{\overline{D}} = \Lambda_D = \Lambda_A$ from Construction A using C_0.

Theorem (K. and O.)

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. The following statements are equivalent.

1. $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ is closed under Schur product.
2. $\Gamma_{\overline{D}}$ is a lattice.
3. $\Gamma_{\overline{D}} = \Lambda_D$.

Proof (1. $\Rightarrow$ 3.): We do induction on a. When $a = 1$, $\Gamma_{\overline{D}} = \Lambda_D = \Lambda_A$ from Construction A using C_0.

For inductive step, use standard set arguments to show that $\Gamma_{\overline{D}} = \Lambda_D$.

Theorem (K. and O.)

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. The following statements are equivalent.

1. $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ is closed under Schur product.
2. $\Gamma_{\overline{D}}$ is a lattice.
3. $\Gamma_{\overline{D}} = \Lambda_D$.

- Since a family of Reed-Muller codes is closed under Schur product, Construction $\overline{\text{D}}$ yields the lattice same lattice as Construction D.
- Lattices from Construction D is independent of the basis of Reed-Muller codes.
- In general, the sum of all lattices constructible from Construction D yields the lattice from Construction $\overline{\text{D}}$ using the same nested codes.

$\mathcal{U}_a := \mathbb{F}_2[u]/u^a$, a polynomial quotient ring where u is a variable.

A **linear code over $\mathcal{U}_a$** of length n is a submodule of $\mathcal{U}_a^n$.

$\mathcal{U}_a := \mathbb{F}_2[u]/u^a$, a polynomial quotient ring where u is a variable.

A **linear code over $\mathcal{U}_a$** of length n is a submodule of $\mathcal{U}_a^n$.

Φ is the embedding given by

$$\begin{array}{rccc} \Phi : & \mathcal{U}_a & \to & \mathbb{R} \\ & \sum_{j=0}^{a-1} b_j u^j & \mapsto & \sum_{j=0}^{a-1} \psi(b_j) 2^j. \end{array}$$

We will also use Φ as a bit-wise embedding from $\mathcal{U}_a^n$ into $\mathbb{R}^n$.

$\mathcal{U}_a := \mathbb{F}_2[u]/u^a$, a polynomial quotient ring where u is a variable.

A **linear code over $\mathcal{U}_a$** of length n is a submodule of $\mathcal{U}_a^n$.

Φ is the embedding given by

$$\begin{array}{rccc} \Phi : & \mathcal{U}_a & \rightarrow & \mathbb{R} \\ & \sum_{j=0}^{a-1} b_j u^j & \mapsto & \sum_{j=0}^{a-1} \psi(b_j) 2^j. \end{array}$$

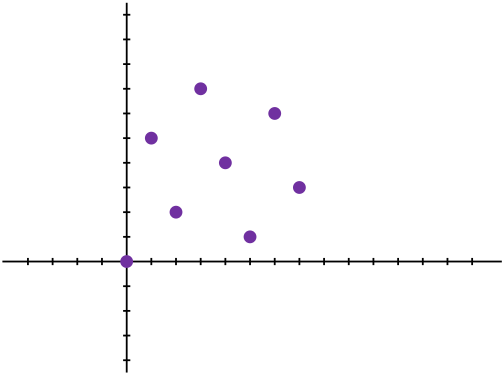
We will also use Φ as a bit-wise embedding from $\mathcal{U}_a^n$ into $\mathbb{R}^n$.

Definition of Construction A′ (Harshan, Viterbo, Belfiore 2012)

Let C be a linear code over $\mathcal{U}_a$ of length n, then

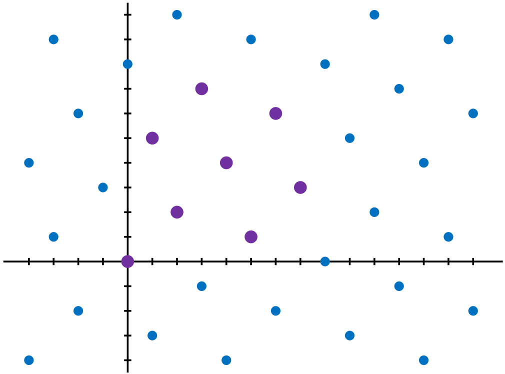
$$\Gamma_{A'} = \Phi(C) \oplus 2^a \mathbb{Z}^n.$$

Consider a code C of length 2 over $\mathcal{U}_3$ generated by $\begin{bmatrix} 1+u & 1+u+u^2 \end{bmatrix}$.



Consider a code C of length 2 over $\mathcal{U}_3$ generated by $[\ 1+u \quad 1+u+u^2\ ]$. Then, we have

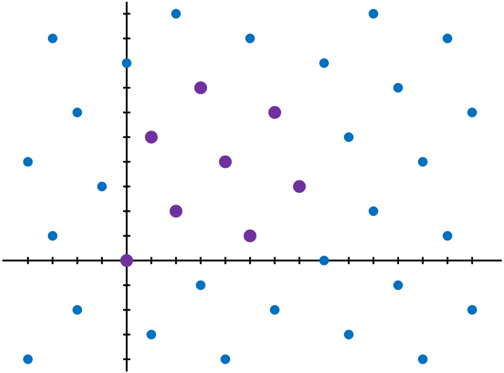
$$C = \{(0,0),(u,u),(u^2,u^2),(u+u^2,u+u^2),(1,1+u^2),\\ (1+u^2,1),(1+u,1+u+u^2),(1+u+u^2,1+u)\}$$



Consider a code C of length 2 over $\mathcal{U}_3$ generated by $\begin{bmatrix} 1+u & 1+u+u^2 \end{bmatrix}$. Then, we have

$$C = \{(0,0),(u,u),(u^2,u^2),(u+u^2,u+u^2),(1,1+u^2),\\ (1+u^2,1),(1+u,1+u+u^2),(1+u+u^2,1+u)\}$$

and $\Gamma_{A'} = \Phi(C) \oplus 8\mathbb{Z}^2$.



Let C be the code generated by the generator matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & u \end{bmatrix}^{\otimes m},$$

then Construction A′ yields the Barnes-Walls lattices.

Φ is the embedding given by

$$\begin{array}{cccc} \Phi : & \mathcal{U}_a & \rightarrow & \mathbb{R} \\ & \sum_{j=0}^{a-1} b_j u^j & \mapsto & \sum_{j=0}^{a-1} \psi(b_j) 2^j . \end{array}$$

Definition of Construction A′

Let C be a linear code over $\mathcal{U}_a$ of length n, then

$$\Gamma_{A'} = \Phi(C) \oplus 2^a \mathbb{Z}^n .$$

Let C be the code generated by the generator matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & u \end{bmatrix}^{\otimes m},$$

then Construction A′ yields the Barnes-Walls lattices.

Φ is the embedding given by

$$\begin{array}{rccc} \Phi: & \mathcal{U}_a & \to & \mathbb{R} \\ & \displaystyle\sum_{j=0}^{a-1} b_j u^j & \mapsto & \displaystyle\sum_{j=0}^{a-1} \psi(b_j) 2^j. \end{array}$$

Definition of Construction A′

Let C be a linear code over $\mathcal{U}_a$ of length n, then

$$\Gamma_{A'} = \Phi(C) \oplus 2^a \mathbb{Z}^n.$$

Definition of Construction $\overline{\text{D}}$

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes. Let

$$\Gamma_{\overline{D}} = \psi(C_0) \oplus 2\psi(C_1) \oplus \ldots \oplus 2^{a-1}\psi(C_{a-1}) \oplus 2^a \mathbb{Z}^n.$$

Proposition (K. and O.)

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a chain of binary linear codes. Then,

$$C = C_0 \oplus uC_1 \oplus \ldots \oplus u^{a-1} C_{a-1}$$

is a code over $\mathcal{U}_a$, and

$$\Gamma_{\overline{D}} = \Gamma_{A'}.$$

Proposition (K. and O.)

Let $C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{a-1} \subseteq C_a = \mathbb{F}_2^n$ be a chain of binary linear codes. Then,

$$C = C_0 \oplus uC_1 \oplus \ldots \oplus u^{a-1}C_{a-1}$$

is a code over $\mathcal{U}_a$, and

$$\Gamma_{\overline{D}} = \Gamma_{A'}.$$

Corollary

- $\Gamma_{A'}$ from Construction A′ may not be a lattice.
- Any lattice constructible using Construction $\overline{\text{D}}$ is also constructible using Construction A′ (converse not true from the previous example).

References

- E. S. Barnes and N. J. A. Sloane, New Lattice Packings of Spheres, Can. J. Math. **35** (1983), no. 1, 117–130.
- J. H. Conway, and N. J. A. Sloane, Sphere Packings, Lattices, and Groups, Third Edition, 1998, Springer-Verlag, New York.
- G. D. Forney, Coset Codes–Part II: Binary Lattices and Related Codes, IEEE Trans. Inform. Theory **34** (1988), no. 5, 1152–1187.
- J. Harshan, E. Viterbo, and J.-C. Belfiore, Construction of Barnes-Wall Lattices from Linear Codes over Rings, Proc. IEEE Int. Symp. Inform. Theory, Cambridge, MA, pp. 3110-3114, July 1-6, 2012.
- J. Harshan, E. Viterbo, and J.-C. Belfiore, Practical Encoders and Decoders for Euclidean Codes from Barnes-Wall Lattices, available on `arXiv:1203.3282v2` [cs.IT], March 2012.
- W. Kositwattanarerk and Frédérique Oggier, On Construction D and Related Constructions of Lattices from Linear Codes, to appear.