

\mathbb{Z}_4 -Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets

Hajime Tanaka

Graduate School of Information Sciences
Tohoku University

Designs and Codes
June 23, 2009

- ▶ $m \in \mathbb{N}$ will **always** denote an **odd** integer.

A. R. Calderbank, P. J. Cameron, W. M. Kantor & J. J. Seidel, \mathbb{Z}_4 -Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets, Proc. London Math. Soc. (3) 75 (1997) 436–480.

- ▶ contains many important results & viewpoints
- ▶ cited in 34 papers (according to MathSciNet)
- ▶ not very easy to read

Topic 1: Orthogonal and symplectic spreads

- ▶ an **orthogonal spread** Σ : a set of $2^m + 1$ maximal isotropic subspaces of an $\Omega^+(2m + 2, 2)$ -space with pairwise trivial intersection
- ▶ a **symplectic spread** Σ' : a set of $2^m + 1$ maximal isotropic subspaces of an $\text{Sp}(2m, 2)$ -space with pairwise trivial intersection
- ▶ Σ' : used to construct an affine plane

Topic 2: MUBs (mutually unbiased bases)

- ▶ $\mathcal{C}_i = \{\mathbf{x}_j^{(i)}\}_{j=1}^N$ ($i = 1, 2, \dots, s$) : orthonormal bases for \mathbb{C}^N
- ▶ $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_s$: **mutually unbiased**

$$\stackrel{\text{def}}{\Leftrightarrow} \quad |(\mathbf{x}_j^{(i)} | \mathbf{x}_\ell^{(k)})| = \frac{1}{\sqrt{N}} \quad \text{whenever } i \neq k$$

Remark

MUBs play an important role in quantum information theory:

- ▶ introduced by Wootters & Fields (1989)
- ▶ but studied earlier (e.g., Schwinger (1960))
- ▶ also studied in different contexts (e.g., Cameron & Seidel (1973); Delsarte, Goethals & Seidel (1975))

Topic 3: Kerdock and Preparata codes

- ▶ a **Kerdock code** $\mathcal{K}(m+1)$: binary, of length 2^{m+1}
- ▶ a **Preparata code** $\mathcal{P}(m+1)$: binary, of length 2^{m+1}
- ▶ $\mathcal{K}(m+1), \mathcal{P}(m+1)$: non-linear, but formally dual
- ▶ Hammons et al. (1994) introduced a **\mathbb{Z}_4 -Kerdock code** $\mathcal{K}_4(m)$ and a **\mathbb{Z}_4 -Preparata code** $\mathcal{P}_4(m)$.
- ▶ $\mathcal{K}_4(m), \mathcal{P}_4(m)$: \mathbb{Z}_4 -linear, dual, and moreover:

$$\begin{array}{ccc} \mathcal{K}(m+1) & \xleftarrow{\text{Gray map } \phi} & \mathcal{K}_4(m) \\ & & \updownarrow \text{dual} \\ \text{'}\mathcal{P}(m+1)\text{' } & \xleftarrow{\text{Gray map } \phi} & \mathcal{P}_4(m) \end{array}$$

where

$$\phi(0) = 00, \quad \phi(1) = 01, \quad \phi(2) = 11, \quad \phi(3) = 10.$$

We shall deepen our understanding of the following relations:

- 1 Orthogonal spreads \longleftrightarrow Symplectic spreads
- 2 Kerdock codes $\xleftarrow{\text{Gray map}} \mathbb{Z}_4\text{-Kerdock codes}$
- 3 (some) real MUBs \longrightarrow (some) complex MUBs

The key is the following inclusion:

$$\blacktriangleright O^+(2m + 2, 2) \supseteq 2 \cdot \text{Sp}(2m, 2)$$

We shall “realize” the above inclusion in:

$$\blacktriangleright O(\mathbb{R}^{2^{m+1}})/\langle -I \rangle \supseteq U(\mathbb{C}^{2^m})/\langle -I \rangle$$

$O^+(2m+2, 2) \supseteq 2 \cdot \text{Sp}(2m, 2)$

- ▶ $Q : \mathbb{Z}_2^{2m+2} \rightarrow \mathbb{Z}_2$: a quadratic form with associated alternating form (\mid) :

$$Q(\mathbf{u} + \mathbf{v}) = Q(\mathbf{u}) + Q(\mathbf{v}) + (\mathbf{u}|\mathbf{v})$$

- ▶ Suppose Q is non-degenerate and has Witt index $m+1$.

- ▶ Q : **non-degenerate** $\stackrel{\text{def}}{\Leftrightarrow} (\mid)$: non-degenerate

- ▶ **Witt index** : the dimension of maximal isotropic subspaces

- ▶ \mathbb{Z}_2^{2m+2} : an “ **$\Omega^+(2m+2, 2)$ -space**” (or “[$D_{m+1}(2)$]-space”)

$$O^+(2m+2, 2) \supseteq 2 \cdot \text{Sp}(2m, 2)$$

Example

- ▶ $V := \mathbb{Z}_2^{m+1}$
- ▶ View \mathbb{Z}_2^{2m+2} as $V \oplus V$.
- ▶ Up to equivalence,

$$Q(\mathbf{u}) = a \cdot b,$$

$$(\mathbf{u}|\mathbf{v}) = a \cdot b' + a' \cdot b,$$

where we write $\mathbf{u} = (a, b)$ and $\mathbf{v} = (a', b')$.

- ▶ Note $(a + a') \cdot (b + b') = a \cdot b + a' \cdot b' + (a \cdot b' + a' \cdot b)$.

$$O^+(2m+2, 2) \supseteq 2 \cdot \text{Sp}(2m, 2)$$

- ▶ $\mathbf{w} \in \mathbb{Z}_2^{2m+2}$: non-isotropic
- ▶ $\dim \langle \mathbf{w} \rangle^\perp = 2m+1$
- ▶ $Q|_{\langle \mathbf{w} \rangle^\perp}$: non-degenerate (with Witt index m)
- ▶ $O(2m+2, 2)_{\mathbf{w}} = 2 \cdot O(2m+1, 2)$
- ▶ $\langle \mathbf{w} \rangle^\perp$: an “ $\Omega(2m+1, 2)$ -space” (or “[$B_m(2)$]-space”)

Example

- ▶ v_1, v_2, \dots, v_{m+1} : the standard basis of $V = \mathbb{Z}_2^{m+1}$
- ▶ $\mathbf{w} = (v_{m+1}, v_{m+1})$ (Note $Q(\mathbf{w}) = v_{m+1} \cdot v_{m+1} = 1$.)
- ▶ $\langle \mathbf{w} \rangle^\perp = \langle (v_i, 0), (0, v_i) \mid i = 1, 2, \dots, m \rangle + \langle \mathbf{w} \rangle$

$$O^+(2m+2, 2) \supseteq 2 \cdot \text{Sp}(2m, 2)$$

- ▶ $(\bar{u}|\bar{v}) := (u|v)$: an alternating form on $\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle$, where $\bar{u} = u + \langle \mathbf{w} \rangle$ and $\bar{v} = v + \langle \mathbf{w} \rangle$
- ▶ $\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle$: an “ $\text{Sp}(2m, 2)$ -space” (or “ $[C_m(2)]$ -space”)

Example

- ▶ $\mathbf{w} = (v_{m+1}, v_{m+1})$
- ▶ $\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle = \langle \overline{(v_i, 0)}, \overline{(0, v_i)} \mid i = 1, 2, \dots, m \rangle$

$$O^+(2m+2, 2) \supseteq 2 \cdot \text{Sp}(2m, 2)$$

- ▶ $\mathbb{Z}_2^{2m+2} = V \oplus V$: an $\Omega^+(2m+2, 2)$ -space
- ▶ Λ : the set of maximal isotropic subspaces of \mathbb{Z}_2^{2m+2}

Example

- ▶ $\langle (v_i, 0) \mid i = 1, 2, \dots, m+1 \rangle \in \Lambda$
- ▶ $\langle (0, v_i) \mid i = 1, 2, \dots, m+1 \rangle \in \Lambda$

- ▶ $\Sigma \subseteq \Lambda$: an **orthogonal spread**

def
 \Leftrightarrow

1 $|\Sigma| = 2^m + 1$

2 $A \cap B = 0$ for distinct $A, B \in \Sigma$

$$O^+(2m+2, 2) \supseteq 2 \cdot \text{Sp}(2m, 2)$$

▶ $\Sigma \subseteq \Lambda$: an orthogonal spread

$$\Leftrightarrow \begin{array}{l} \textcircled{1} |\Sigma| = 2^m + 1 \\ \textcircled{2} A \cap B = 0 \text{ for distinct } A, B \in \Sigma \end{array}$$

Remark

▶ Recall $Q((a, b)) = a \cdot b$.

▶ Ξ : the set of isotropic (projective) points of \mathbb{Z}_2^{2m+2}

$$\text{▶ } |\Xi| = \underbrace{1 \cdot (2^{m+1} - 1)}_{a=0} + \underbrace{(2^{m+1} - 1) \cdot 2^m}_{a \neq 0} = (2^m + 1)(2^{m+1} - 1)$$

▶ $\Xi = \bigcup_{A \in \Sigma} (A \setminus \{0\})$: a **partition** of Ξ

$$O^+(2m+2, 2) \supseteq 2 \cdot \text{Sp}(2m, 2)$$

- ▶ $\mathbf{w} \in \mathbb{Z}_2^{2m+2} = V \oplus V$: non-isotropic
- ▶ $\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle$: an $\text{Sp}(2m, 2)$ -space
- ▶ Λ' : the set of maximal isotropic subspaces of $\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle$

Example

- ▶ $\langle \overline{(v_i, 0)} \mid i = 1, 2, \dots, m \rangle \in \Lambda'$
 - ▶ $\langle \overline{(0, v_i)} \mid i = 1, 2, \dots, m \rangle \in \Lambda'$
- ▶ $\Sigma' \subseteq \Lambda'$: a **symplectic spread**

def
 \Leftrightarrow

- 1 $|\Sigma'| = 2^m + 1$
- 2 $A' \cap B' = \bar{0}$ for distinct $A', B' \in \Sigma'$

$$O^+(2m+2, 2) \supseteq 2 \cdot \text{Sp}(2m, 2)$$

▶ $\Sigma' \subseteq \Lambda'$: a symplectic spread

\Leftrightarrow

① $|\Sigma'| = 2^m + 1$

② $A' \cap B' = \bar{0}$ for distinct $A', B' \in \Sigma'$

Remark

▶ $|(\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle) \setminus \{\bar{0}\}| = 2^{2m} - 1 = (2^m + 1)(2^m - 1)$

▶ $(\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle) \setminus \{\bar{0}\} = \bigcup_{A' \in \Sigma'} (A' \setminus \{\bar{0}\})$: a **partition** of $\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle$

$$O^+(2m+2, 2) \supseteq 2 \cdot \text{Sp}(2m, 2)$$

- ▶ Λ : the set of maximal isotropic subspaces of \mathbb{Z}_2^{2m+2}
- ▶ $O^+(2m+2, 2)$ acts transitively on each of the following:

$$R_i = \{(A, B) \mid A, B \in \Lambda, \dim A \cap B = m+1-i\} \quad (i = 0, 1, \dots, m+1)$$

Remark*

- ▶ (Λ, R_1) : the **dual-polar graph** on $[D_{m+1}(2)]$ (bipartite)
- ▶ (Λ, R_i) : the distance- i graph of (Λ, R_1) ($i = 0, 1, \dots, m+1$)
- ▶ Σ : a maximal clique of (Λ, R_{m+1})

$O^+(2m+2, 2) \supseteq 2 \cdot \text{Sp}(2m, 2)$

- ▶ $\mathbf{w} \in \mathbb{Z}_2^{2m+2}$: non-isotropic
- ▶ $\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle$: an $\text{Sp}(2m, 2)$ -space
- ▶ Λ' : the set of maximal isotropic subspaces of $\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle$
- ▶ $\text{Sp}(2m, 2)$ acts transitively on each of the following:

$$R'_i = \{(A', B') \mid A', B' \in \Lambda', \dim A' \cap B' = m-i\} \quad (i = 0, 1, \dots, m)$$

Remark*

- ▶ (Λ', R'_1) : the **dual-polar graph** on $[C_m(2)]$
- ▶ (Λ', R'_i) : the distance- i graph of (Λ', R'_1) ($i = 0, 1, \dots, m$)
- ▶ Σ' : a maximal clique of (Λ', R'_m)

$$O^+(2m+2, 2) \supseteq 2 \cdot \text{Sp}(2m, 2)$$

Example

- ▶ Consider $2^m + 1$ lines in $\text{GF}(2^m)^2$:

$$x = 0, \quad y = \alpha x \quad (\alpha \in \text{GF}(2^m))$$

- ▶ isotropic w.r.t. $((a_1, b_1) \mid (a_2, b_2))_m := a_1 b_2 - a_2 b_1$
- ▶ isotropic w.r.t. $(\mid)_1 := \text{Tr}(\mid)_m$, where $\text{Tr} : \text{GF}(2^m) \rightarrow \mathbb{Z}_2$ is the trace map:

$$\text{Tr}(\alpha) = \alpha + \alpha^2 + \alpha^4 + \cdots + \alpha^{2^{m-1}} \quad (\alpha \in \text{GF}(2^m))$$

- ▶ forms a symplectic spread in an $\text{Sp}(2m, 2)$ -space
 $\text{GF}(2^m)^2 \cong \langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle$

$$\Sigma \xrightarrow{2:1} \Sigma'$$

Any symplectic spread Σ' lifts to an orthogonal spread Σ .

- ▶ $\langle \mathbf{w} \rangle^\perp$: an $\Omega(2m + 1, 2)$ -space (equipped with $Q|_{\langle \mathbf{w} \rangle^\perp}$)
 - ▶ $\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle$: an $\text{Sp}(2m, 2)$ -space (equipped with (\mid))
 - ▶ $\forall A \in \Lambda$ (i.e., maximal isotropic in \mathbb{Z}_2^{2m+2})
 - ▶ $A \cap \langle \mathbf{w} \rangle^\perp$: maximal isotropic in $\langle \mathbf{w} \rangle^\perp$ (of dimension m)
 - ▶ $A' := \overline{A \cap \langle \mathbf{w} \rangle^\perp} \in \Lambda'$ (i.e., maximal isotropic in $\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle$)
-
- ▶ $A \mapsto A \cap \langle \mathbf{w} \rangle^\perp \mapsto A' := \overline{A \cap \langle \mathbf{w} \rangle^\perp}$
 - ▶ $\Sigma \mapsto \Sigma' := \{A' \mid A \in \Sigma\}$

$$\Sigma \xrightarrow{2:1} \Sigma'$$

Example

- ▶ v_1, v_2, \dots, v_{m+1} : the standard basis of $V = \mathbb{Z}_2^{m+1}$
- ▶ $\mathbf{w} = (v_{m+1}, v_{m+1})$
- ▶ $A := \langle (v_i, 0) \mid i = 1, 2, \dots, m+1 \rangle \in \Lambda$
- ▶ $A \cap \langle \mathbf{w} \rangle^\perp = \langle (v_i, 0) \mid i = 1, 2, \dots, m \rangle$ ($\because ((v_{m+1}, 0) | \mathbf{w}) = 1$)
- ▶ $A' = \langle \overline{(v_i, 0)} \mid i = 1, 2, \dots, m \rangle \in \Lambda'$

- ▶ $\forall A' \in \Lambda'$
- ▶ $A'\uparrow := \{\mathbf{u} \in \langle \mathbf{w} \rangle^\perp \mid \bar{\mathbf{u}} \in A', Q(\mathbf{u}) = 0\}$: maximal isotropic in $\langle \mathbf{w} \rangle^\perp$
 - ▶ $\mathbf{u} \in \langle \mathbf{w} \rangle^\perp \Rightarrow \{Q(\mathbf{u}), Q(\mathbf{u} + \mathbf{w})(= Q(\mathbf{u}) + 1)\} = \mathbb{Z}_2$
 - ▶ $|A'\uparrow| = 2^m$
- ▶ $\exists^2 A \in \Lambda$ s.t. $A \cap \langle \mathbf{w} \rangle^\perp = A'\uparrow$
- ▶ $\overline{A \cap \langle \mathbf{w} \rangle^\perp} = \overline{A'\uparrow} = A'$
- ▶ $\exists^2 \Sigma$ s.t. $\Sigma \mapsto \Sigma'$ ($\because (\Lambda, R_1)$: bipartite, of diameter $m + 1$)

Example

- ▶ $A' := \langle \overline{(v_i, 0)} \mid i = 1, 2, \dots, m \rangle \in \Lambda'$
- ▶ $A'\uparrow = \langle (v_i, 0) \mid i = 1, 2, \dots, m \rangle \subseteq \langle \mathbf{w} \rangle^\perp$
- ▶ $A = \begin{cases} \langle (v_i, 0) \mid i = 1, 2, \dots, m+1 \rangle \\ \langle (v_i, 0) \mid i = 1, 2, \dots, m \rangle + \langle (0, v_{m+1}) \rangle \end{cases} \in \Lambda$

Remark*

Concerning dual polar graphs:

- ▶ $[D_{m+1}(2)] \cong$ the extended bipartite double of $[C_m(2)]$
- ▶ $\frac{1}{2}[D_{m+1}(2)] \cong$ distance-1 or -2 graph of $[C_m(2)]$

$$\Sigma \xrightarrow{2:1} \Sigma'$$

We may view the correspondence $\Sigma \mapsto \Sigma'$ in terms of matrices.

- ▶ Λ : the set of maximal isotropic subspaces of \mathbb{Z}_2^{2m+2}
- ▶ $O^+(2m+2, 2)$ acts transitively on:

$$R_{m+1} = \{(A, B) \mid A, B \in \Lambda, \dim A \cap B = 0\}$$

- ▶ $\Sigma \subseteq \Lambda$: an orthogonal spread
- ▶ **We shall always assume $X, Z \in \Sigma$, where**

$$X := \langle (v_i, 0) \mid i = 1, 2, \dots, m+1 \rangle \in \Lambda$$

$$Z := \langle (0, v_i) \mid i = 1, 2, \dots, m+1 \rangle \in \Lambda$$

$$\Sigma \xrightarrow{2:1} \Sigma'$$

▶ Observe $K^b := \begin{pmatrix} K & O \\ O & K^{-T} \end{pmatrix} \in O^+(2m+2, 2)$ ($K \in \text{GL}(V)$)

$$\text{▶ } Q((a, b)K^b) = Q((aK, bK^{-T})) = (aK) \cdot (bK^{-T}) = a \cdot b$$

▶ $\forall A \in \Sigma \setminus \{Z\} \quad \exists g \in O^+(2m+2, 2)$ s.t. $(X, Z)g = (A, Z)$

▶ $\exists^1 M_A : (m+1) \times (m+1)$ alternating s.t. $X \begin{pmatrix} I & M_A \\ O & I \end{pmatrix} = A$

▶ The above g is of the form $\begin{pmatrix} K & M \\ O & K^{-T} \end{pmatrix}$.

▶ Replace g by $K^{b-1}g$.

$$\text{▶ } \underbrace{Q\left(\left(a, b\right) \begin{pmatrix} I & M_A \\ O & I \end{pmatrix}\right)}_{=Q((a,b))=a \cdot b} = Q((a, aM_A + b)) = a \cdot (aM_A) + a \cdot b$$

▶ $\text{rank}(M_A - M_B) = m+1$ ($\forall A, B \in \Sigma \setminus \{Z\}, A \neq B$)

▶ $A = \text{row space of } (I \ M_A); \quad B = \text{row space of } (I \ M_B)$

▶ $a(I \ M_A) = b(I \ M_B) \Leftrightarrow a = b, \quad a(M_A - M_B) = 0$

$$\Sigma \xrightarrow{2:1} \Sigma'$$

- ▶ $\Sigma(\ni X, Z) \xleftrightarrow{1:1} \{M_A \mid A \in \Sigma \setminus \{Z\}\}$
- ▶ $\{M_A \mid A \in \Sigma \setminus \{Z\}\}$: a **Kerdock set**, i.e.,

- 1 $|\Sigma \setminus \{Z\}| = 2^m$
- 2 M_A : alternating ($A \in \Sigma \setminus \{Z\}$)
- 3 $\text{rank}(M_A - M_B) = m + 1$ for distinct $A, B \in \Sigma \setminus \{Z\}$

Remark*

The above arguments show how to embed the alternating forms graph $\text{Alt}_{m+1}(2)$ into the dual polar graph on $[D_{m+1}(2)]$.

- ▶ Λ' : the set of maximal isotropic subspaces of $\langle \mathbf{w} \rangle^\perp / \langle \mathbf{w} \rangle$
- ▶ $\text{Sp}(2m, 2)$ acts transitively on:

$$R'_m = \{(A', B') \mid A', B' \in \Lambda', \dim A' \cap B' = \bar{0}\}$$

- ▶ $\Sigma' \subseteq \Lambda'$: a symplectic spread
- ▶ **We shall always assume $X', Z' \in \Sigma'$, where**

$$X' := \langle \overline{(v_i, 0)} \mid i = 1, 2, \dots, m \rangle \in \Lambda'$$

$$Z' := \langle \overline{(0, v_i)} \mid i = 1, 2, \dots, m \rangle \in \Lambda'$$

$$\Sigma \xrightarrow{2:1} \Sigma'$$

- ▶ $\forall A' \in \Sigma \setminus \{Z'\} \exists! P_{A'} : m \times m$ symmetric s.t. $X' \begin{pmatrix} I & P_{A'} \\ O & I \end{pmatrix} = A'$
- ▶ $\text{rank}(P_{A'} - P_{B'}) = m \quad (\forall A', B' \in \Sigma' \setminus \{Z'\}, A' \neq B')$
- ▶ $\Sigma'(\ni X', Z') \xleftrightarrow{1:1} \{P_{A'} \mid A' \in \Sigma' \setminus \{Z'\}\}$

Remark*

The symmetric bilinear forms graph $\text{Sym}_m(2)$ can be embedded into the dual polar graph on $[C_m(2)]$.

- ▶ $A (\in \Sigma \setminus \{Z\}) \mapsto A \cap \langle \mathbf{w} \rangle^\perp \mapsto A' := \overline{A \cap \langle \mathbf{w} \rangle^\perp} (\in \Sigma \setminus \{Z'\})$
- ▶ $\mathbf{w} = (v_{m+1}, v_{m+1}) = (0, 0, \dots, 0, 1, 0, 0, \dots, 0, 1)$
- ▶ $A = \text{row space of } (I M_A) = \langle (v_i, v_i M_A) \mid i = 1, 2, \dots, m+1 \rangle$
- ▶ $A \cap \langle \mathbf{w} \rangle^\perp$: given by

$$\langle (v_i, v_i M_A) - (M_A)_{i,m+1} \cdot (v_{m+1}, v_{m+1} M_A) \mid i = 1, \dots, m \rangle$$

- ▶ $((v_{m+1}, v_{m+1} M_A) \mid \mathbf{w}) = 1$
- ▶ $((v_i, v_i M_A) \mid \mathbf{w}) = (M_A)_{i,m+1} \quad (i = 1, 2, \dots, m)$

We conclude:

- ▶ $P_{A'} = ((M_A)_{ij} - (M_A)_{i,m+1} (M_A)_{j,m+1})_{i,j=1}^m$

$$\mathbb{Z}_2^{2m+2} \subseteq O(\mathbb{R}^{2^{m+1}}) / \langle -I \rangle$$

- ▶ $V = \mathbb{Z}_2^{m+1}$
- ▶ $\mathbb{R}^{2^{m+1}}$: with standard basis $\{e_v \mid v \in V\}$
- ▶ $(\mid)_{\mathbb{R}}$: usual inner product on $\mathbb{R}^{2^{m+1}}$
- ▶ $X(b), Z(b) \in O(\mathbb{R}^{2^m})$ ($b \in V$):

$$X(b) : e_v \mapsto e_{v+b}, \quad Z(b) := \text{diag}[(-1)^{b \cdot v}]_{v \in V}$$

- ▶ $X(V) := \{X(b) \mid b \in V\}$
- ▶ $Z(V) := \{Z(b) \mid b \in V\}$
- ▶ $X(V), Z(V) \cong V$

$$\mathbb{Z}_2^{2m+2} \subseteq \mathcal{O}(\mathbb{R}^{2^{m+1}}) / \langle -I \rangle$$

Example

- ▶ Suppose $m = 0$ (contrary to our convention).
- ▶ $X(1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z(1) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$: **Pauli matrices**
- ▶ In general, for $b = (b_1, b_2, \dots, b_{m+1}) \in V$,

$$X(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{b_1} \otimes \cdots \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{b_{m+1}},$$

$$Z(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{b_1} \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{b_{m+1}}.$$

Remark*

- ▶ $\mathbb{R}X(V)$: the group (or Bose–Mesner) algebra of $V = \mathbb{Z}_2^{m+1}$
- ▶ $\mathbb{R}Z(V)$: the dual Bose–Mesner algebra of V

$$\mathbb{Z}_2^{2m+2} \subseteq \mathcal{O}(\mathbb{R}^{2^{m+1}}) / \langle -I \rangle$$

▶ $E = E_{m+1} := \langle X(V), Z(V) \rangle$

Remark*

▶ $\mathbb{R}E$: the Terwilliger algebra of $V = \mathbb{Z}_2^{m+1}$

▶ $X(a)Z(b)X(a)Z(b) = (-1)^{a \cdot b} I$

$$\begin{aligned} e_v X(a)Z(b)X(a)Z(b) &= [(-1)^{b \cdot (v+a)} e_{v+a}] X(a)Z(b) \\ &= (-1)^{b \cdot (v+a)} (-1)^{b \cdot v} e_v \end{aligned}$$

▶ $(X(a)Z(b))(X(a')Z(b')) = (-1)^{a' \cdot b} X(a + a')Z(b + b')$

▶ $E = X(V)Z(V)\langle -I \rangle$: extraspecial of order $2^{1+(2m+2)}$

$$\mathbb{Z}_2^{2m+2} \subseteq \mathcal{O}(\mathbb{R}^{2^{m+1}})/\langle -I \rangle$$

- ▶ $E = X(V)Z(V)\langle -I \rangle$: extraspecial of order $2^{1+(2m+2)}$
- ▶ $e^2 \in \langle -I \rangle$ ($e \in E$)
- ▶ $X(a)Z(b)X(a)Z(b) = (-1)^{a \cdot b} I$
- ▶ $\tilde{E} := E/\langle -I \rangle \cong \mathbb{Z}_2^{2m+2}$: a vector space over \mathbb{Z}_2
- ▶ $\tilde{e} := e\langle -I \rangle$ for $e \in E$
- ▶ $\tilde{E} = \tilde{X}(V)\tilde{Z}(V) \cong V \oplus V$
- ▶ $Q : \tilde{E} \rightarrow \mathbb{Z}_2$ ($\tilde{X}(a)\tilde{Z}(b) \mapsto a \cdot b$) : a quadratic form on \tilde{E}
- ▶ $e^2 = (-I)^{Q(\tilde{e})}$ ($e \in E$)

$$\mathbb{Z}_2^{2m+2} \subseteq \mathcal{O}(\mathbb{R}^{2^{m+1}}) / \langle -I \rangle$$

▶ $\mathbf{e}^2 = (-I)^{Q(\tilde{\mathbf{e}})} \quad (\mathbf{e} \in E)$

▶ $(\mid)_{\tilde{E}}$: the associated alternating form of Q :

$$(\tilde{X}(a)\tilde{Z}(b) \mid \tilde{X}(a')\tilde{Z}(b'))_{\tilde{E}} = a \cdot b' + a' \cdot b$$

▶ $[\mathbf{e}_1, \mathbf{e}_2] = (-I)^{(\tilde{\mathbf{e}}_1 \mid \tilde{\mathbf{e}}_2)_{\tilde{E}}} \quad (\mathbf{e}_1, \mathbf{e}_2 \in E)$

▶ $(\mathbf{e}_1\mathbf{e}_2)(\mathbf{e}_1\mathbf{e}_2) = (-I)^{Q(\tilde{\mathbf{e}}_1+\tilde{\mathbf{e}}_2)} = (-I)^{Q(\tilde{\mathbf{e}}_1)+Q(\tilde{\mathbf{e}}_2)+(\tilde{\mathbf{e}}_1 \mid \tilde{\mathbf{e}}_2)_{\tilde{E}}}$

▶ $\mathbf{e}_1^2\mathbf{e}_2^2 = (-I)^{Q(\tilde{\mathbf{e}}_1)+Q(\tilde{\mathbf{e}}_2)}$

$$\mathbb{Z}_2^{2m+2} \subseteq O(\mathbb{R}^{2^{m+1}}) / \langle -I \rangle$$

- ▶ $\mathbf{e}^2 = (-I)^{Q(\tilde{\mathbf{e}})}$ ($\mathbf{e} \in E$)
- ▶ $[\mathbf{e}_1, \mathbf{e}_2] = (-I)^{(\tilde{\mathbf{e}}_1 | \tilde{\mathbf{e}}_2)_{\tilde{E}}}$ ($\mathbf{e}_1, \mathbf{e}_2 \in E$)
- ▶ $Q(\mathbf{g}^{-1}\tilde{\mathbf{e}}\mathbf{g}) = Q(\tilde{\mathbf{e}})$ ($\mathbf{g} \in N_{O(\mathbb{R}^{2^{m+1}})}(E), \mathbf{e} \in E$)

$$\text{▶ } (\mathbf{g}^{-1}\mathbf{e}\mathbf{g})^2 = \mathbf{g}^{-1}(-I)^{Q(\tilde{\mathbf{e}})}\mathbf{g} = (-I)^{Q(\tilde{\mathbf{e}})}$$

Proposition

$$N_{O(\mathbb{R}^{2^{m+1}})}(E) \twoheadrightarrow O^+(2m+2, 2) \text{ (surjective)}$$

$$\mathbb{Z}_2^{2m+2} \subseteq O(\mathbb{R}^{2^{m+1}})/\langle -I \rangle$$

Example

- ▶ $M : (m + 1) \times (m + 1)$ alternating
- ▶ Recall $\begin{pmatrix} I & M \\ O & I \end{pmatrix} \in O^+(2m + 2, 2)$.
- ▶ $Q_M : V \rightarrow \mathbb{Z}_2$: a quadratic form with associated alternating form uMv^T
- ▶ $d_M := \text{diag}[(-1)^{Q_M(v)}]_{v \in V}$
- ▶ $d_M^{-1}(\tilde{X}(a)\tilde{Z}(b))d_M = \tilde{X}(a)\tilde{Z}(aM)\tilde{Z}(b) = \tilde{X}(a)\tilde{Z}(b) \begin{pmatrix} I & M \\ O & I \end{pmatrix}$

- ▶ $d_M^{-1}Z(b)d_M = Z(b)$
- ▶ $e_v d_M^{-1}X(a)d_M X(a) = (-1)^{Q_M(v)} e_{v+a} d_M X(a)$

$$= (-1)^{Q_M(v)+Q_M(v+a)} e_v$$

$$= (-1)^{Q_M(a)} (-1)^{aM \cdot v} e_v$$
- ▶ $d_M^{-1}X(a)d_M = (-1)^{Q_M(a)} Z(aM)X(a)$

$$\langle \tilde{\mathbf{w}} \rangle^\perp / \langle \tilde{\mathbf{w}} \rangle \subseteq U(\mathbb{C}^{2^m}) / \langle \sqrt{-1} I \rangle$$

The basic idea is the identification $\mathbb{C} = \mathbb{R}^2$ by $x+y\sqrt{-1} \leftrightarrow (x, -y)$.

- ▶ v_1, v_2, \dots, v_{m+1} : the standard basis of $V = \mathbb{Z}_2^{m+1}$
- ▶ $\mathbf{w} := X(v_{m+1})Z(v_{m+1}) \in E$ (Note $Q(\tilde{\mathbf{w}}) = v_{m+1} \cdot v_{m+1} = 1$.)
- ▶ $\mathbf{w}^2 = -I$
- ▶ $\mathbb{R}I + \mathbb{R}\mathbf{w} \cong \mathbb{C}$
- ▶ $\mathbb{R}^{2^{m+1}} = \mathbb{C}^{2^m}$
- ▶ Write $V' := \langle v_1, v_2, \dots, v_m \rangle$.
- ▶ For $v' \in V'$,

$$\sqrt{-1} e_{v'} = e_{v'} \mathbf{w} = (-1)^{(v'+v_{m+1}) \cdot v_{m+1}} e_{v'+v_{m+1}} = -e_{v'+v_{m+1}}$$

- ▶ $\{e_{v'} \mid v' \in V'\}$: the standard basis for \mathbb{C}^{2^m}
- ▶ $(\mid)_{\mathbb{C}}$: usual inner product on \mathbb{C}^{2^m}

$$\langle \tilde{\mathbf{w}} \rangle^\perp / \langle \tilde{\mathbf{w}} \rangle \subseteq U(\mathbb{C}^{2^m}) / \langle \sqrt{-1} I \rangle$$

Example

▶ Suppose $m = 1$; $V = \mathbb{Z}_2^2 = \langle 10, 01 \rangle$, $V' = \langle 10 \rangle$

$$\text{▶ } \mathbf{w} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} 00 \\ 10 \\ 01 \\ 11 \end{matrix}$$

▶ $e_{00} = (1, 0, 0, 0)$; $\sqrt{-1} e_{00} = e_{00}\mathbf{w} = -e_{01} = (0, 0, -1, 0)$

▶ $e_{10} = (0, 1, 0, 0)$; $\sqrt{-1} e_{10} = e_{10}\mathbf{w} = -e_{11} = (0, 0, 0, -1)$

▶ $\alpha e_{00} + \beta e_{10} = (\operatorname{Re}\alpha, \operatorname{Re}\beta, -\operatorname{Im}\alpha, -\operatorname{Im}\beta)$ ($\alpha, \beta \in \mathbb{C}$)

▶ $(\mathbf{u}|\mathbf{v})_{\mathbb{C}} = (\mathbf{u}|\mathbf{v})_{\mathbb{R}} + (\mathbf{u}|\mathbf{v}\mathbf{w})_{\mathbb{R}}\sqrt{-1}$

$$\begin{aligned} \text{▶ } & (x_1 + y_1\sqrt{-1} \mid x_2 + y_2\sqrt{-1})_{\mathbb{C}} \\ &= (x_1x_2 + y_1y_2) + (x_2y_1 - x_1y_2)\sqrt{-1} \\ &= ((x_1, -y_1) \mid (x_2, -y_2))_{\mathbb{R}} + ((x_1, -y_1) \mid (-y_2, -x_2))_{\mathbb{R}}\sqrt{-1} \end{aligned}$$

$$\langle \tilde{\mathbf{w}} \rangle^\perp / \langle \tilde{\mathbf{w}} \rangle \subseteq U(\mathbb{C}^{2^m}) / \langle \sqrt{-1} I \rangle$$

- ▶ $(\mathbf{u} | \mathbf{v})_{\mathbb{C}} = (\mathbf{u} | \mathbf{v})_{\mathbb{R}} + (\mathbf{u} | \mathbf{v} \mathbf{w})_{\mathbb{R}} \sqrt{-1}$
- ▶ $U(\mathbb{C}^{2^m}) = C_{O(\mathbb{R}^{2^{m+1}})}(\mathbf{w})$
- ▶ $\mathbf{e} \in E \cap U(\mathbb{C}^{2^m}) \Leftrightarrow I = [\mathbf{e}, \mathbf{w}] = (-I)^{(\tilde{\mathbf{e}} | \tilde{\mathbf{w}})_{\tilde{E}}} \Leftrightarrow \tilde{\mathbf{e}} \in \langle \tilde{\mathbf{w}} \rangle^\perp$
- ▶ $\langle \tilde{\mathbf{w}} \rangle^\perp / \langle \tilde{\mathbf{w}} \rangle = (E \cap U(\mathbb{C}^{2^m})) / \langle \sqrt{-1} I \rangle$ (Recall $\sqrt{-1} I = \mathbf{w}$.)
- ▶ $X(V') := \{X(b) \mid b \in V'\} = X(V) \cap U(\mathbb{C}^{2^m})$
- ▶ $Z(V') := \{Z(b) \mid b \in V'\} = Z(V) \cap U(\mathbb{C}^{2^m})$
- ▶ $X(V'), Z(V') \cong V'$
- ▶ $\bar{\mathbf{e}} := \mathbf{e} \langle \sqrt{-1} I \rangle$ for $\mathbf{e} \in E \cap U(\mathbb{C}^{2^m})$
- ▶ $\langle \tilde{\mathbf{w}} \rangle^\perp / \langle \tilde{\mathbf{w}} \rangle = \bar{X}(V') \bar{Z}(V') \cong V' \oplus V'$

$$\langle \tilde{\mathbf{w}} \rangle^\perp / \langle \tilde{\mathbf{w}} \rangle \subseteq U(\mathbb{C}^{2^m}) / \langle \sqrt{-1} I \rangle$$

- ▶ You may now guess how real and complex MUBs, and orthogonal and symplectic spreads can be related with each other.
- ▶ Concerning Kerdock and \mathbb{Z}_4 -Kerdock codes, the Gray map

$$\phi(0) = 00, \quad \phi(1) = 01, \quad \phi(2) = 11, \quad \phi(3) = 10$$

will arise in this context as follows:

$$\begin{array}{ccc}
 \mathbb{Z}_4 & \xrightarrow{z \mapsto (\sqrt{-1})^z} & \{\pm 1, \pm\sqrt{-1}\} \\
 \downarrow \phi & & \downarrow \begin{array}{l} \times(1 - \sqrt{-1}) \\ \mathbb{C} \cong \mathbb{R}^2 \end{array} \\
 \mathbb{Z}_2^2 & \xrightarrow{(x,y) \mapsto ((-1)^x, (-1)^y)} & \{(\pm 1, \pm 1)\}
 \end{array}$$

$$\langle \tilde{\mathbf{w}} \rangle^\perp / \langle \tilde{\mathbf{w}} \rangle \subseteq U(\mathbb{C}^{2^m}) / \langle \sqrt{-1} I \rangle$$

Proposition

$$N_{U(\mathbb{C}^{2^m})}(\langle \tilde{\mathbf{w}} \rangle^\perp / \langle \tilde{\mathbf{w}} \rangle) \twoheadrightarrow \mathrm{Sp}(2m, 2) \quad (\text{surjective})$$

$$\blacktriangleright N_{O(\mathbb{R}^{2m+1})}(E) \twoheadrightarrow O^+(2m+2, 2) \quad (\text{surjective})$$

$$\blacktriangleright O^+(2m+2, 2)_{\mathbf{w}} = 2 \cdot O(2m+1, 2) \cong 2 \cdot \mathrm{Sp}(2m, 2)$$

- $\blacktriangleright \hat{\cdot} : \mathbb{Z}_2 = \{0, 1\} \hookrightarrow \mathbb{Z}_4 = \{0, 1, 2, 3\} : \text{inclusion (as a set)}$
- $\blacktriangleright \text{extended naturally to binary vectors, matrices, etc.}$
- $\blacktriangleright P : m \times m \text{ binary symmetric}$
- $\blacktriangleright T : V' \rightarrow \mathbb{Z}_4 : \text{a } \mathbb{Z}_4\text{-valued quadratic form associated with } P$

$$\stackrel{\text{def}}{\Leftrightarrow} T(u+v) = T(u) + T(v) + 2 \hat{u} \hat{P} \hat{v}^T \quad (u, v \in V')$$

$$\langle \widehat{\mathbf{w}} \rangle^\perp / \langle \widehat{\mathbf{w}} \rangle \subseteq U(\mathbb{C}^{2^m}) / \langle \sqrt{-1} I \rangle$$

$$\blacktriangleright T(u + v) = T(u) + T(v) + 2 \hat{u} \hat{P} \hat{v}^T \quad (u, v \in V')$$

Example

- $\blacktriangleright T_P(u) := \hat{u} \hat{P} \hat{u}^T \quad (u \in V') : \text{associated with } P$
- $\blacktriangleright \text{Recall } \begin{pmatrix} I & P \\ 0 & I \end{pmatrix} \in \text{Sp}(2m, 2).$
- $\blacktriangleright d'_P := \text{diag}[(\sqrt{-1})^{T_P(v)}]_{v \in V'} \in U(\mathbb{C}^{2^m})$
- $\blacktriangleright d'_P{}^{-1}(\bar{X}(a)\bar{Z}(b))d'_P = \bar{X}(a)\bar{Z}(aP)\bar{Z}(b) = \bar{X}(a)\bar{Z}(b) \begin{pmatrix} I & P \\ 0 & I \end{pmatrix}$

- $\blacktriangleright d'_P{}^{-1}Z(b)d'_P = Z(b)$
- $\blacktriangleright e_v d'_P{}^{-1}X(a)d'_P X(a) = (\sqrt{-1})^{-T'_P(v)} e_{v+a} d'_P X(a)$
 $= (\sqrt{-1})^{-T'_P(v) + T'_P(v+a)} e_v$
 $= (\sqrt{-1})^{T'_P(a)} (-1)^{aP \cdot v} e_v$
- $\blacktriangleright d'_P{}^{-1}X(a)d'_P = (\sqrt{-1})^{T'_P(a)} Z(aP)X(a)$

$$\langle \tilde{\mathbf{w}} \rangle^\perp / \langle \tilde{\mathbf{w}} \rangle \subseteq U(\mathbb{C}^{2^m}) / \langle \sqrt{-1} I \rangle$$

Remark

- ▶ $T_1, T_2 : V' \rightarrow \mathbb{Z}_4$: \mathbb{Z}_4 -valued quadratic forms associated with P
 - ▶ $T_1 - T_2 : V' \rightarrow 2\mathbb{Z}_4 \cong \mathbb{Z}_2$: a linear functional on V'
-
- ▶ $T_1(u + v) - T_2(u + v) = T_1(u) + T_1(v) - T_2(u) - T_2(v)$
 - ▶ $T_1 - T_2$: additive

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

First we consider **real** line-sets in $\mathbb{R}^{2^{m+1}}$.

- ▶ $V = \mathbb{Z}_2^{m+1}$
- ▶ $X(V) = \{X(a) \mid a \in V\}$
- ▶ $Z(V) = \{Z(b) \mid b \in V\}$
- ▶ $\tilde{E} = \tilde{X}(V)\tilde{Z}(V)$: an $\Omega^+(2m+2, 2)$ -space
- ▶ Recall $N_{O(\mathbb{R}^{2^{m+1}})}(E) \rightarrow O^+(2m+2, 2)$.

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

- ▶ $e_v X(b) = e_{v+b}$
- ▶ $e_v Z(b) = (-1)^{b \cdot v} e_v$
- ▶ $\langle e_v \rangle_{\mathbb{R}} \ (v \in V)$: the irreducible submodules for $Z(V)$ in $\mathbb{R}^{2^{m+1}}$
- ▶ $e_u^* := \frac{1}{\sqrt{2^{m+1}}} \sum_{v \in V} (-1)^{u \cdot v} e_v \ (u \in V)$
- ▶ $e_u^* Z(b) = e_{u+b}^*$
- ▶ $e_u^* X(b) = \frac{1}{\sqrt{2^{m+1}}} \sum_{v \in V} (-1)^{u \cdot v} e_{v+b} = (-1)^{u \cdot b} e_u^*$
- ▶ $\langle e_u^* \rangle_{\mathbb{R}} \ (u \in V)$: the irreducible submodules for $X(V)$ in $\mathbb{R}^{2^{m+1}}$
- ▶ $|(e_v | e_u^*)_{\mathbb{R}}| = \frac{1}{\sqrt{2^{m+1}}} \ (u, v \in V)$; i.e.,
- ▶ $\{e_v \mid v \in V\}, \{e_u^* \mid u \in V\}$: **mutually unbiased**

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

- ▶ Σ : an orthogonal spread of \tilde{E}
- ▶ We shall always assume $\tilde{X}(V), \tilde{Z}(V) \in \Sigma$.
- ▶ A : a subgroup of E s.t. $\tilde{A} \in \Sigma \setminus \{\tilde{Z}(V)\}$
(Note that $\langle A, -I \rangle$ is the preimage of \tilde{A} .)
- ▶ $\mathcal{F}_{\mathbb{R}}(A)$: the set of A -irreducible submodules of $\mathbb{R}^{2^{m+1}}$
- ▶ $\exists \mathbf{g} \in N_{O(\mathbb{R}^{2^{m+1}})}(E)$ s.t. $\mathbf{g}^{-1}\tilde{X}(V)\mathbf{g} = \tilde{A}$
- ▶ $\mathcal{F}_{\mathbb{R}}(A) = \{\langle e_u^* \rangle_{\mathbb{R}\mathbf{g}} \mid u \in V\}$: an orthogonal frame

Remark

Since $\langle A, -I \rangle \trianglelefteq E$, we have $\mathcal{F}_{\mathbb{R}}(A)E = \mathcal{F}_{\mathbb{R}}(A)$.

- ▶ $\mathcal{F}_{\mathbb{R}}(\Sigma) := \bigcup_{\tilde{A} \in \Sigma} \mathcal{F}_{\mathbb{R}}(A)$

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

Example

- ▶ Suppose $m = 1$ so that $V = \mathbb{Z}_2^2$ and $\tilde{E} \cong V \oplus V$.
- ▶ $\Sigma := \{\tilde{X}(V), \tilde{Z}(V), \tilde{A}\}$, where $\tilde{A} := \tilde{X}(V) \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
- ▶ $\tilde{A} = d_{M_A}^{-1} \tilde{X}(V) d_{M_A}$ where $d_{M_A} := \text{diag}[(1, 1, 1, -1)]$
- ▶ $\mathcal{F}_{\mathbb{R}}(X(V)) = \left\{ \begin{array}{l} \langle (1, 1, 1, 1) \rangle_{\mathbb{R}}, \langle (1, -1, 1, -1) \rangle_{\mathbb{R}}, \\ \langle (1, 1, -1, -1) \rangle_{\mathbb{R}}, \langle (1, -1, -1, 1) \rangle_{\mathbb{R}} \end{array} \right\}$
- ▶ $\mathcal{F}_{\mathbb{R}}(Z(V)) = \left\{ \begin{array}{l} \langle (1, 0, 0, 0) \rangle_{\mathbb{R}}, \langle (0, 1, 0, 0) \rangle_{\mathbb{R}}, \\ \langle (0, 0, 1, 0) \rangle_{\mathbb{R}}, \langle (0, 0, 0, 1) \rangle_{\mathbb{R}} \end{array} \right\}$
- ▶ $\mathcal{F}_{\mathbb{R}}(A) = \mathcal{F}_{\mathbb{R}}(X(V)) d_{M_A}$

$$= \left\{ \begin{array}{l} \langle (1, 1, 1, -1) \rangle_{\mathbb{R}}, \langle (1, -1, 1, 1) \rangle_{\mathbb{R}}, \\ \langle (1, 1, -1, 1) \rangle_{\mathbb{R}}, \langle (1, -1, -1, -1) \rangle_{\mathbb{R}} \end{array} \right\}$$

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

- ▶ $\tilde{A} \in \Sigma$; $\mathcal{F}_{\mathbb{R}}(A) = \{\ell_1^{(A)}, \ell_2^{(A)}, \dots, \ell_{2^{m+1}}^{(A)}\}$
 - ▶ Pick a unit vector $\mathbf{x}_i^{(A)} \in \ell_i^{(A)}$ ($i = 1, 2, \dots, 2^{m+1}$).
 - ▶ $\mathcal{C}_A := \{\mathbf{x}_i^{(A)}\}_{i=1}^{2^{m+1}}$: an orthonormal basis for $\mathbb{R}^{2^{m+1}}$
 - ▶ $\{\mathcal{C}_A \mid \tilde{A} \in \Sigma\}$: $(2^m + 1)$ **real** MUBs
- ▶ Pick distinct $\tilde{A}, \tilde{B} \in \Sigma$.
 - ▶ $\exists \mathbf{g} \in N_{O(\mathbb{R}^{2^{m+1}})}(E)$ s.t. $\mathbf{g}^{-1}\tilde{X}(V)\mathbf{g} = \tilde{A}$, $\mathbf{g}^{-1}\tilde{Z}(V)\mathbf{g} = \tilde{B}$
 - ▶ $\mathcal{F}_{\mathbb{R}}(A) = \{\langle e_u^* \rangle_{\mathbb{R}\mathbf{g}} \mid u \in V\}$, $\mathcal{F}_{\mathbb{R}}(B) = \{\langle e_v \rangle_{\mathbb{R}\mathbf{g}} \mid v \in V\}$

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

Remark*

- ▶ $\bigcup_{A \in \Sigma} (\mathcal{C}_A \cup (-\mathcal{C}_A))$ forms a Q -bipartite Q -antipodal cometric association scheme with 4 classes and $2 \cdot 2^{m+1} \cdot (2^m + 1)$ vertices. Conversely, any such cometric scheme is obtained in this way. (LeCompte, Martin & Owens (2008))
- ▶ Suda (2009) showed that these schemes are quadruply regular.

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

Lemma

Let $\mathbf{g} \in O(\mathbb{R}^{2^{m+1}})$. Then

$$\mathbf{g} \in N_{O(\mathbb{R}^{2^{m+1}})}(E) \text{ if } \begin{array}{l} \textcircled{1} \mathcal{F}_{\mathbb{R}}(X(V))\mathbf{g} = \mathcal{F}_{\mathbb{R}}(X(V)) \\ \textcircled{2} \mathcal{F}_{\mathbb{R}}(Z(V))\mathbf{g} = \mathcal{F}_{\mathbb{R}}(Z(V)) \end{array}$$

Proposition

Let Σ_1, Σ_2 be orthogonal spreads of \tilde{E} , and let $\mathbf{g} \in O(\mathbb{R}^{2^{m+1}})$. Then

$$\mathcal{F}_{\mathbb{R}}(\Sigma_1)\mathbf{g} = \mathcal{F}_{\mathbb{R}}(\Sigma_2) \Leftrightarrow \begin{array}{l} \textcircled{1} \mathbf{g} \in N_{O(\mathbb{R}^{2^{m+1}})}(E) \\ \textcircled{2} \mathbf{g}^{-1}\Sigma_1\mathbf{g} = \Sigma_2 \end{array}$$

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

Proof.

- ▶ We show (\Rightarrow) .
- ▶ Recall $\tilde{X}(V), \tilde{Z}(V) \in \Sigma_1$.
- ▶ $\exists \tilde{A}, \tilde{B} \in \Sigma_2$ ($\tilde{A} \neq \tilde{B}$) s.t.
 - 1 $\mathcal{F}_{\mathbb{R}}(X(V))\mathbf{g} = \mathcal{F}_{\mathbb{R}}(\tilde{A})$
 - 2 $\mathcal{F}_{\mathbb{R}}(Z(V))\mathbf{g} = \mathcal{F}_{\mathbb{R}}(\tilde{B})$
- ▶ $\exists \mathbf{h} \in N_{O(\mathbb{R}^{2m+1})}(E)$ s.t.
 - 1 $\mathcal{F}_{\mathbb{R}}(X(V))\mathbf{gh} = \mathcal{F}_{\mathbb{R}}(X(V))$
 - 2 $\mathcal{F}_{\mathbb{R}}(Z(V))\mathbf{gh} = \mathcal{F}_{\mathbb{R}}(Z(V))$
- ▶ By the lemma, $\mathbf{gh} \in N_{O(\mathbb{R}^{2m+1})}(E)$, so $\mathbf{g} \in N_{O(\mathbb{R}^{2m+1})}(E)$. □

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

Next we consider **complex** line-sets in \mathbb{C}^{2^m} .

- ▶ $V' = \langle v_1, v_2, \dots, v_m \rangle$
- ▶ $X(V') = \{X(b) \mid b \in V'\}$
- ▶ $Z(V') = \{Z(b) \mid b \in V'\}$
- ▶ $\langle \tilde{\mathbf{w}} \rangle^\perp / \langle \tilde{\mathbf{w}} \rangle = \bar{X}(V')\bar{Z}(V') : \text{an } \text{Sp}(2m, 2)\text{-space}$

It is possible to proceed as in the real case, but we take a different approach.

- ▶ $(\mathbf{u}|\mathbf{v})_{\mathbb{C}} = (\mathbf{u}|\mathbf{v})_{\mathbb{R}} + (\mathbf{u}|\mathbf{vw})_{\mathbb{R}}\sqrt{-1}$
 - ▶ $(\mathbf{u}|\mathbf{uw})_{\mathbb{R}} = 0$
- ▶ $(\mathbf{u}|\mathbf{uw})_{\mathbb{R}} = (\mathbf{uw}|\mathbf{uw}^2)_{\mathbb{R}} = -(\mathbf{uw}|\mathbf{u})_{\mathbb{R}}$

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

- ▶ $(\mathbf{u}|\mathbf{v})_{\mathbb{C}} = (\mathbf{u}|\mathbf{v})_{\mathbb{R}} + (\mathbf{u}|\mathbf{v}\mathbf{w})_{\mathbb{R}}\sqrt{-1}$
- ▶ $(\mathbf{u}|\mathbf{u}\mathbf{w})_{\mathbb{R}} = 0$
- ▶ Σ : an orthogonal spread of \tilde{E}
- ▶ Recall $\Sigma' = \left\{ \overline{\tilde{A} \cap \langle \tilde{\mathbf{w}} \rangle^{\perp}} \mid \tilde{A} \in \Sigma \right\}$.
- ▶ $\tilde{A} \in \Sigma$
- ▶ $\mathcal{F}_{\mathbb{R}}(A)\mathbf{w} = \mathcal{F}_{\mathbb{R}}(A)$
- ▶ $l \neq l\mathbf{w}$ ($\forall l \in \mathcal{F}_{\mathbb{R}}(A)$) ($\because (l|l\mathbf{w})_{\mathbb{R}} = 0$)
- ▶ A' : a subgroup of $E \cap U(\mathbb{C}^{2^m})$ s.t. $\overline{A'} = \overline{\tilde{A} \cap \langle \tilde{\mathbf{w}} \rangle^{\perp}}$
- ▶ $\mathcal{F}_{\mathbb{C}}(A') := \{\mathbb{C}l = l + l\mathbf{w} \mid l \in \mathcal{F}_{\mathbb{R}}(A)\}$: the set of A' -irreducible submodules of \mathbb{C}^{2^m} ; an orthogonal frame
- ▶ $\mathcal{F}_{\mathbb{C}}(\Sigma') := \bigcup_{\overline{A'} \in \Sigma'} \mathcal{F}_{\mathbb{C}}(A') = \{\mathbb{C}l = l + l\mathbf{w} \mid l \in \mathcal{F}_{\mathbb{R}}(\Sigma)\}$

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

- ▶ $\tilde{A}, \tilde{B} \in \Sigma$ ($\tilde{A} \neq \tilde{B}$)
- ▶ $\ell^{(A)} \in \mathcal{F}_{\mathbb{R}}(A)$, $\ell^{(B)} \in \mathcal{F}_{\mathbb{R}}(B)$
- ▶ $\mathbf{x}^{(A)} \in \ell^{(A)}$, $\mathbf{x}^{(B)} \in \ell^{(B)}$: unit vectors
- ▶
$$\begin{aligned} \left| (\mathbf{x}^{(A)} | \mathbf{x}^{(B)})_{\mathbb{C}} \right| &= \left| (\mathbf{x}^{(A)} | \mathbf{x}^{(B)})_{\mathbb{R}} + (\mathbf{x}^{(A)} | \mathbf{x}^{(B)} \mathbf{w})_{\mathbb{R}} \sqrt{-1} \right| \\ &= \sqrt{\left(\frac{1}{\sqrt{2^{m+1}}} \right)^2 + \left(\frac{1}{\sqrt{2^{m+1}}} \right)^2} \\ &= \frac{1}{\sqrt{2^m}} \end{aligned}$$
- ▶ $\overline{A'} \in \Sigma'$; $\mathcal{F}_{\mathbb{C}}(A') = \{\ell_1^{(A')}, \ell_2^{(A')}, \dots, \ell_{2^m}^{(A')}\}$
- ▶ Pick a unit vector $\mathbf{z}_i^{(A')} \in \ell_i^{(A')}$ ($i = 1, 2, \dots, 2^m$).
- ▶ $\mathcal{C}'_{A'} := \{\mathbf{z}_i^{(A')}\}_{i=1}^{2^m}$: an orthonormal bases for \mathbb{C}^{2^m}
- ▶ $\{\mathcal{C}'_{A'} \mid \overline{A'} \in \Sigma'\}$: $(2^m + 1)$ **complex** MUBs

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

Example

- ▶ Suppose $m = 1$, and recall $\mathbf{w} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$.
- ▶ $l_1 := \langle (1, 0, 0, 0) \rangle_{\mathbb{R}} \in \mathcal{F}_{\mathbb{R}}(Z(V))$
- ▶ $l_1 \mathbf{w} = \langle (0, 0, -1, 0) \rangle_{\mathbb{R}} \in \mathcal{F}_{\mathbb{R}}(Z(V))$
- ▶ $\mathbb{C}l_1 = \langle (1, 0) \rangle_{\mathbb{C}}$
- ▶ $l_2 := \langle (1, 1, 1, 1) \rangle_{\mathbb{R}} \in \mathcal{F}_{\mathbb{R}}(X(V))$
- ▶ $l_2 \mathbf{w} = \langle (1, 1, -1, -1) \rangle_{\mathbb{R}} \in \mathcal{F}_{\mathbb{R}}(X(V))$
- ▶ $\mathbb{C}l_2 = \langle (1 - \sqrt{-1}, 1 - \sqrt{-1}) \rangle_{\mathbb{C}} = \langle (1, 1) \rangle_{\mathbb{C}}$
- ▶ $(1, 0) \in \mathbb{C}l_1, \frac{1}{\sqrt{2}}(1, 1) \in \mathbb{C}l_2$: unit vectors
- ▶ $\left| \langle (1, 0) | \frac{1}{\sqrt{2}}(1, 1) \rangle_{\mathbb{C}} \right| = \frac{1}{\sqrt{2}}$

$$\mathcal{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$$

Remark

- ▶ The number of bases in a set of MUBs for \mathbb{C}^N is at most $N + 1$.
- ▶ The construction using symplectic spreads works as well for $N = p^r$ with p being an odd prime.
- ▶ All **known** maximal sets of (complex) MUBs are obtained in this way. (Godsil & Roy (2009))
- ▶ There is a generalization of this construction which is valid for all $N \in \mathbb{N}$ (“nice unitary bases”). But when N is not a prime power, this does **not** attain the bound $N + 1$. (Aschbacher, Childs & Wocjan (2007))

$$\mathcal{K}_4(\Sigma') \xrightarrow{\phi} \mathcal{K}(\Sigma)$$

We relate “ $\mathcal{K}_4(\Sigma') \xrightarrow{\phi} \mathcal{K}(\Sigma)$ ” with “ $\mathcal{F}_{\mathbb{R}}(\Sigma) \mapsto \mathcal{F}_{\mathbb{C}}(\Sigma')$ ”.

- ▶ $\tilde{A} \in \Sigma \setminus \{\tilde{Z}(V)\}$
- ▶ $\exists! M_A : (m+1) \times (m+1)$ alternating s.t. $\tilde{X}(V) \begin{pmatrix} I & M_A \\ 0 & I \end{pmatrix} = \tilde{A}$
- ▶ $Q_{M_A} : V \rightarrow \mathbb{Z}_2$: a quadratic form with associated alternating form $uM_A v^T$
- ▶ $\mathcal{K}(\Sigma) := \left\{ (Q_{M_A}(v) + s \cdot v + \epsilon)_{v \in V} \mid \begin{array}{l} \tilde{A} \in \Sigma \setminus \{\tilde{Z}(V)\}, \\ s \in V, \epsilon \in \mathbb{Z}_2 \end{array} \right\} \subseteq \mathbb{Z}_2^{2^{m+1}}$
: a **Kerdock code**

Remark

The maps $v \mapsto Q_{M_A}(v) + s \cdot v$ ($s \in V$) are **the** quadratic forms with associated alternating form $uM_A v^T$.

$$\mathcal{K}_4(\Sigma') \xrightarrow{\phi} \mathcal{K}(\Sigma)$$

$$\blacktriangleright \mathcal{K}(\Sigma) = \left\{ (Q_{M_A}(v) + s \cdot v + \epsilon)_{v \in V} \mid \begin{array}{l} \tilde{A} \in \Sigma \setminus \{\tilde{Z}(V)\}, \\ s \in V, \epsilon \in \mathbb{Z}_2 \end{array} \right\}$$

Proposition

$$\mathcal{K}(\Sigma) = \left\{ (x_v)_{v \in V} \in \mathbb{Z}_2^{2^{m+1}} \mid \langle ((-1)^{x_v})_{v \in V} \rangle \in \mathcal{F}_{\mathbb{R}}(\Sigma) \right\}$$

Proof.

\blacktriangleright Recall $\mathcal{F}_{\mathbb{R}}(X(V)) = \{ \langle e_u^* \rangle_{\mathbb{R}} \mid u \in V \}$ where

$$e_u^* = \frac{1}{\sqrt{2^{m+1}}} \sum_{v \in V} (-1)^{u \cdot v} e_v.$$

$\blacktriangleright d_{M_A} = \text{diag} [(-1)^{Q_{M_A}(v)}]_{v \in V}$ ($\tilde{A} \in \Sigma \setminus \{\tilde{Z}(V)\}$)

$\blacktriangleright \mathcal{F}_{\mathbb{R}}(A) = \mathcal{F}_{\mathbb{R}}(X(V)) d_{M_A}$ and

$$e_s^* d_{M_A} = \frac{1}{\sqrt{2^{m+1}}} \sum_{v \in V} (-1)^{Q_{M_A}(v) + s \cdot v} e_v. \quad \square$$

$$\mathcal{K}_4(\Sigma') \xrightarrow{\phi} \mathcal{K}(\Sigma)$$

- ▶ $V' = \langle v_1, v_2, \dots, v_m \rangle$
- ▶ $\bar{A}' \in \Sigma' \setminus \{\bar{Z}(V')\}$
- ▶ $\exists! P_{A'} : m \times m$ symmetric s.t. $\bar{X}(V') \begin{pmatrix} I & P_{A'} \\ O & I \end{pmatrix} = \bar{A}'$
- ▶ $T_{P_{A'}} : V' \rightarrow \mathbb{Z}_4$: a \mathbb{Z}_4 -quadratic form associated with $P_{A'}$
- ▶ $\mathcal{K}_4(\Sigma') := \left\{ (T_{P_{A'}}(v) + 2\hat{s} \cdot \hat{v} + \epsilon)_{v \in V'} \mid \begin{array}{l} A' \in \Sigma' \setminus \{\bar{Z}(V')\}, \\ s \in V', \epsilon \in \mathbb{Z}_4 \end{array} \right\} \subseteq \mathbb{Z}_4^{2^m}$
 : a **\mathbb{Z}_4 -Kerdock code**

Remark

The maps $v \mapsto T_{P_{A'}}(v) + 2\hat{s} \cdot \hat{v}$ ($s \in V'$) are the \mathbb{Z}_4 -valued quadratic forms associated with P .

$$\mathcal{K}_4(\Sigma') \xrightarrow{\phi} \mathcal{K}(\Sigma)$$

$$\blacktriangleright \mathcal{K}_4(\Sigma') = \left\{ (T_{P_{A'}}(v) + 2\hat{s} \cdot \hat{v} + \epsilon)_{v \in V'} \mid \begin{array}{l} A' \in \Sigma' \setminus \{\bar{Z}(V')\}, \\ s \in V', \epsilon \in \mathbb{Z}_4 \end{array} \right\} \subseteq \mathbb{Z}_4^{2^m}$$

Proposition

$$\mathcal{K}_4(\Sigma') = \{ (z_v)_{v \in V'} \in \mathbb{Z}_4^{2^m} \mid \langle ((\sqrt{-1})^{z_v})_{v \in V'} \rangle \in \mathcal{F}_{\mathbb{C}}(\Sigma') \}$$

Proof.

$$\blacktriangleright \mathcal{F}_{\mathbb{C}}(\bar{X}(V')) = \{ \langle e_u^* \rangle_{\mathbb{C}} \mid u \in V' \} \text{ where}$$

$$e_u^* := \frac{1}{\sqrt{2^m}} \sum_{v \in V'} (-1)^{u \cdot v} e_v.$$

$$\blacktriangleright d'_{P_{A'}} = \text{diag}[(\sqrt{-1})^{T_{P_{A'}}(v)}]_{v \in V'} \quad (A' \in \Sigma' \setminus \{\bar{Z}(V')\})$$

$$\blacktriangleright \mathcal{F}_{\mathbb{C}}(A') = \mathcal{F}_{\mathbb{C}}(\bar{X}(V')) d'_{P_{A'}}, \text{ and}$$

$$e_s^* d'_{P_{A'}} = \frac{1}{\sqrt{2^m}} \sum_{v \in V'} (\sqrt{-1})^{T_{P_{A'}}(v) + 2\hat{s} \cdot \hat{v}} e_v. \quad \square$$

$$\mathcal{K}_4(\Sigma') \xrightarrow{\phi} \mathcal{K}(\Sigma)$$

Lemma

With the identification $\mathbb{C} \cong \mathbb{R}^2$,

$$\mathbb{C}^{2^m} \supseteq \{\pm 1, \pm\sqrt{-1}\}^{2^m} \begin{array}{c} \xrightarrow{\times(1-\sqrt{-1})} \\ \xleftarrow{\times\left(\frac{1+\sqrt{-1}}{2}\right)} \end{array} \{\pm 1\}^{2^{m+1}} \subseteq \mathbb{R}^{2^{m+1}}$$

$$\begin{array}{l} (1 - \sqrt{-1}) \times 1 = 1 - \sqrt{-1} = (1, -1) \\ (1 - \sqrt{-1}) \times \sqrt{-1} = 1 + \sqrt{-1} = (1, 1) \\ (1 - \sqrt{-1}) \times (-1) = -1 + \sqrt{-1} = (-1, 1) \\ (1 - \sqrt{-1}) \times (-\sqrt{-1}) = -1 - \sqrt{-1} = (-1, -1) \end{array}$$

$$\mathcal{K}_4(\Sigma') \xrightarrow{\phi} \mathcal{K}(\Sigma)$$

$$\begin{aligned} (1 - \sqrt{-1}) \times 1 &= 1 - \sqrt{-1} = (1, 1) \\ (1 - \sqrt{-1}) \times \sqrt{-1} &= 1 + \sqrt{-1} = (1, -1) \\ (1 - \sqrt{-1}) \times (-1) &= -1 + \sqrt{-1} = (-1, -1) \\ (1 - \sqrt{-1}) \times (-\sqrt{-1}) &= -1 - \sqrt{-1} = (-1, 1) \end{aligned}$$

Why choose $1 - \sqrt{-1}$?

► corresponds to the Gray map $\phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2$:

$$\phi(0) = 00, \quad \phi(1) = 01, \quad \phi(2) = 11, \quad \phi(3) = 10$$

$$\begin{array}{ccc} \mathbb{Z}_4 & \xrightarrow{z \mapsto (\sqrt{-1})^z} & \{\pm 1, \pm\sqrt{-1}\} \\ \downarrow \phi & & \downarrow \begin{array}{l} \times(1 - \sqrt{-1}) \\ \mathbb{C} \cong \mathbb{R}^2 \end{array} \\ \mathbb{Z}_2^2 & \xrightarrow{(x, y) \mapsto ((-1)^x, (-1)^y)} & \{(\pm 1, \pm 1)\} \end{array}$$

$$\mathcal{K}_4(\Sigma') \xrightarrow{\phi} \mathcal{K}(\Sigma)$$

- ▶ $\mathcal{K}_4(\Sigma') = \{(z_v)_{v \in V'} \in \mathbb{Z}_4^{2^m} \mid \langle ((\sqrt{-1})^{z_v})_{v \in V'} \rangle \in \mathcal{F}_{\mathbb{C}}(\Sigma')\}$
- ▶ $\mathcal{K}(\Sigma) = \{(x_v)_{v \in V} \in \mathbb{Z}_2^{2^{m+1}} \mid \langle ((-1)^{x_v})_{v \in V} \rangle \in \mathcal{F}_{\mathbb{R}}(\Sigma)\}$

Proposition

$$\mathcal{K}(\Sigma) = \phi(\mathcal{K}_4(\Sigma')).$$

Proof.

Recall $\mathcal{F}_{\mathbb{C}}(\Sigma') = \{\mathbb{C}l \mid l \in \mathcal{F}_{\mathbb{R}}(\Sigma)\}$. □

Kerdock and Preparata codes

- ▶ the **Lee weight** $w_L : \mathbb{Z}_4 \rightarrow \mathbb{N} \cup \{0\}$:

$$w_L(0) = 0, \quad w_L(1) = w_L(3) = 1, \quad w_L(2) = 2$$

- ▶ the **Lee weight** on \mathbb{Z}_4^N : $w_L(\mathbf{a}) = \sum_{i=1}^N w_L(a_i)$
- ▶ the **Lee distance** on \mathbb{Z}_4^N : $d_L(\mathbf{a}, \mathbf{b}) = w_L(\mathbf{a} - \mathbf{b})$
- ▶ the Gray map $\phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2$

$$\phi(0) = 00, \quad \phi(1) = 01, \quad \phi(2) = 11, \quad \phi(3) = 10$$

defines an isometry:

$$\phi : \begin{array}{c} \mathbb{Z}_4^N \\ \text{(Lee metric)} \end{array} \longrightarrow \begin{array}{c} \mathbb{Z}_2^{2N} \\ \text{(Hamming metric)} \end{array}$$

Kerdock and Preparata codes

- ▶ the **Lee weight enumerator** of $C \subseteq \mathbb{Z}_4^N$:

$$\text{Lee}_C(x, y) = \sum_{c \in C} x^{2N - w_L(c)} y^{w_L(c)}$$

- ▶ $\text{Lee}_C(x, y) = \text{Ham}_{\phi(C)}(x, y)$
- ▶ $C : \mathbb{Z}_4$ -linear $\Rightarrow \text{Lee}_{C^\perp}(x, y) = \frac{1}{|C|} \text{Lee}_C(x + y, x - y)$
- ▶ $\text{Ham}_{\phi(C^\perp)}(x, y) = \frac{1}{|C|} \text{Ham}_{\phi(C)}(x + y, x - y)$: a “formal duality”

Proposition

$\mathcal{K}_4(\Sigma')$: \mathbb{Z}_4 -linear $\Leftrightarrow \{P_{A'} \mid \overline{A'} \in \Sigma'\}$: closed under addition

- ▶ An example was constructed by Hammons et al. (1994).
- ▶ $\mathcal{P}_4(\Sigma') := \mathcal{K}_4(\Sigma')^\perp$: a **\mathbb{Z}_4 -Preparata code**
- ▶ $\phi(\mathcal{P}_4(\Sigma'))$: a ‘**Preparata**’ code

Proof.

$$\blacktriangleright \mathcal{K}_4(\Sigma') = \left\{ (T_{P_{A'}}(v) + 2\hat{s} \cdot \hat{v} + \epsilon)_{v \in V'} \mid \begin{array}{l} A' \in \Sigma' \setminus \{\bar{Z}(V')\}, \\ s \in V', \epsilon \in \mathbb{Z}_4 \end{array} \right\}$$

\blacktriangleright Let \oplus denote the binary addition in \mathbb{Z}_2 .

\blacktriangleright Recall $\hat{\cdot} : \mathbb{Z}_2 = \{0, 1\} \hookrightarrow \mathbb{Z}_4 = \{0, 1, 2, 3\}$.

\blacktriangleright Note $\hat{a} + \hat{b} = a \oplus b + 2\hat{a}\hat{b}$ ($a, b \in \mathbb{Z}_2$).

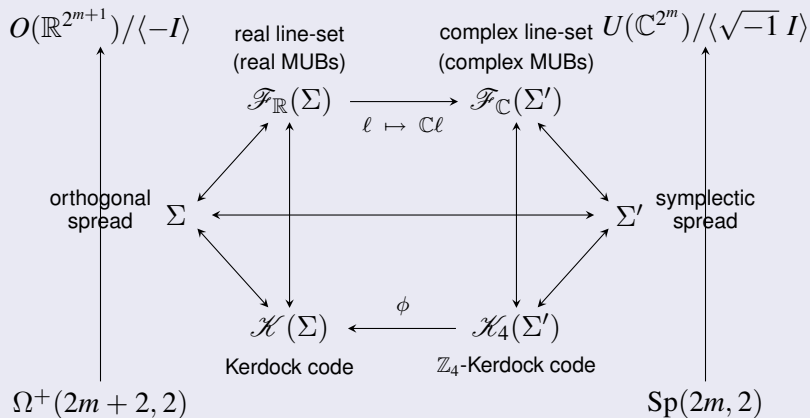
$$\begin{aligned} \blacktriangleright T_{P_{A'}}(v) + T_{P_{B'}}(v) &= \hat{v}\hat{P}_{A'}\hat{v}^T + \hat{v}\hat{P}_{B'}\hat{v}^T \\ &= \sum_{i=1}^m ((\hat{P}_{A'})_{ii} + (\hat{P}_{B'})_{ii})\hat{v}_i^2 + 2 \sum_{i < j} ((\hat{P}_{A'})_{ij} + (\hat{P}_{B'})_{ij})\hat{v}_i\hat{v}_j \\ &= \sum_{i=1}^m (\widehat{P_{A'} \oplus P_{B'}})_{ii}\hat{v}_i^2 + 2 \sum_{i < j} (\widehat{P_{A'} \oplus P_{B'}})_{ij}\hat{v}_i\hat{v}_j \\ &\quad + 2 \sum_{i=1}^m (\hat{P}_{A'})_{ii}(\hat{P}_{B'})_{ii}\hat{v}_i \\ &= T_{P_{A' \oplus P_{B'}}}(v) + 2\hat{s} \cdot \hat{v} \text{ where } s := ((P_{A'})_{ii}(P_{B'})_{ii})_{i=1}^m. \quad \square \end{aligned}$$

- ▶ The determination of equivalence among various Kerdock or \mathbb{Z}_4 -Kerdock codes is not simple. (For example it is possible that $\mathcal{K}_4(\Sigma'_1) \not\cong \mathcal{K}_4(\Sigma'_2)$ even if $\Sigma'_1 \cong \Sigma'_2$.)
- ▶ But it is proved for example that

$$\phi(\mathcal{K}_4(\Sigma'_1)) \cong \phi(\mathcal{K}_4(\Sigma'_2)) \Leftrightarrow \mathcal{K}_4(\Sigma'_1) \cong \mathcal{K}_4(\Sigma'_2)$$

(There remains a gap in the proof which I have not succeeded in filling.)

Summary



What if identify $\mathbb{C} \cong \mathbb{R}^2$ by $x + y\sqrt{-1} \leftrightarrow (x, y)$?

Everything works if:

- ▶ Replace the Gray map by $\phi^{\natural} : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2$:

$$\phi^{\natural}(0) = 00, \quad \phi^{\natural}(1) = 10, \quad \phi^{\natural}(2) = 11, \quad \phi^{\natural}(3) = 01$$

- ▶ Consider the following correspondence:

$$\mathbb{C}^{2^m} \supseteq \{\pm 1, \pm\sqrt{-1}\}^{2^m} \begin{array}{c} \xrightarrow{\times(1+\sqrt{-1})} \\ \xleftarrow{\times\left(\frac{1-\sqrt{-1}}{2}\right)} \end{array} \{\pm 1\}^{2^{m+1}} \subseteq \mathbb{R}^{2^{m+1}}$$