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

Hajime Tanaka

Graduate School of Information Sciences
Tohoku University

Designs and Codes
June 23, 2009

Convention

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

Reference

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 $\mathrm{Sp}(2m, 2)$-space with pairwise trivial intersection
- Σ' : used to construct an affine plane

Topic 2: MUBs (mutually unbiased bases)

- $\mathscr{C}_i = \{\boldsymbol{x}_j^{(i)}\}_{j=1}^N$ $(i = 1, 2, \ldots, s)$: orthonormal bases for $\mathbb{C}^N$
- $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_s$: mutually unbiased

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

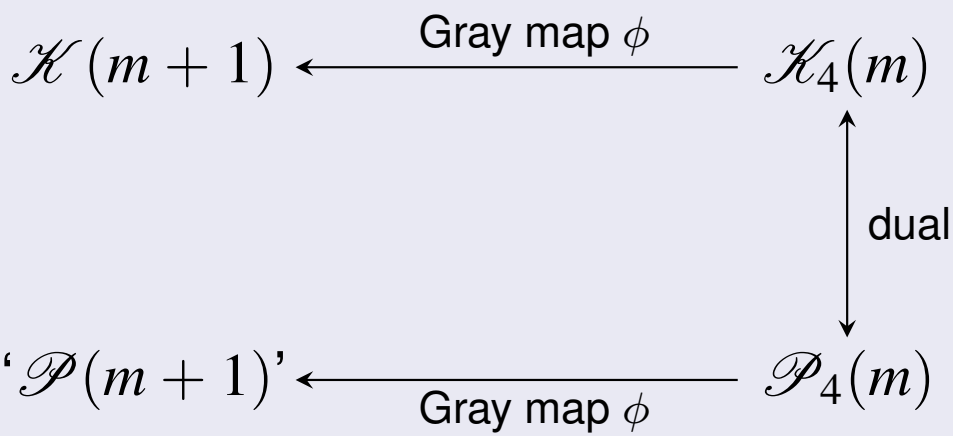
Remark

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



where

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

Overview

We shall deepen our understanding of the following relations:

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

The key is the following inclusion:

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

We shall "realize" the above inclusion in:

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

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

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

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

  - Q : non-degenerate $\overset{\text{def}}{\Leftrightarrow}$ $(\ |\ )$: 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")

Example

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

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

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

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

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

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

Example

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

- $(\overline{\boldsymbol{u}}|\overline{\boldsymbol{v}}) := (\boldsymbol{u}|\boldsymbol{v})$: an alternating form on $\langle \boldsymbol{w} \rangle^{\perp}/\langle \boldsymbol{w} \rangle$, where $\overline{\boldsymbol{u}} = \boldsymbol{u} + \langle \boldsymbol{w} \rangle$ and $\overline{\boldsymbol{v}} = \boldsymbol{v} + \langle \boldsymbol{w} \rangle$
- $\langle \boldsymbol{w} \rangle^{\perp}/\langle \boldsymbol{w} \rangle$: an "$\mathrm{Sp}(2m,2)$-space" (or "$[C_m(2)]$-space")

Example

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

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

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

Example

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

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

$\overset{\text{def}}{\Leftrightarrow}$

1. $|\Sigma| = 2^m + 1$
2. $A \cap B = 0$ for distinct $A, B \in \Sigma$

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

$\Leftrightarrow$

1. $|\Sigma| = 2^m + 1$
2. $A \cap B = 0$ for distinct $A, B \in \Sigma$

Remark

- Recall $Q((a,b)) = a \cdot b$.
- Ξ : the set of isotropic (projective) points of $\mathbb{Z}_2^{2m+2}$
- $|\Xi| = \underbrace{1 \cdot (2^{m+1}-1)}_{a=0} + \underbrace{(2^{m+1}-1) \cdot 2^m}_{a \neq 0} = (2^m+1)(2^{m+1}-1)$
- $\Xi = \bigcup_{A \in \Sigma} (A \backslash \{0\})$: a partition of Ξ

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

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

Example

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

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

$\overset{\text{def}}{\Leftrightarrow}$

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

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

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

$\Leftrightarrow$

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

Remark

- $|(\langle \boldsymbol{w} \rangle^\perp / \langle \boldsymbol{w} \rangle) \backslash \{\bar{0}\}| = 2^{2m} - 1 = (2^m + 1)(2^m - 1)$
- $(\langle \boldsymbol{w} \rangle^\perp / \langle \boldsymbol{w} \rangle) \backslash \{\bar{0}\} = \bigcup_{A' \in \Sigma'} (A' \backslash \{\bar{0}\})$: a partition of $\langle \boldsymbol{w} \rangle^\perp / \langle \boldsymbol{w} \rangle$

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

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

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

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) $(i = 0,1,\ldots,m+1)$
- Σ : a maximal clique of (Λ, R_{m+1})

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

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

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

Remark*

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

Example

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

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

- 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. $(\ |\ )_1 := \mathrm{Tr}(\ |\ )_m$, where $\mathrm{Tr} : \mathrm{GF}(2^m) \to \mathbb{Z}_2$ is the trace map:

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

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

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

- $\langle \boldsymbol{w} \rangle^{\perp}$: an $\Omega(2m+1, 2)$-space (equipped with $Q|_{\langle \boldsymbol{w} \rangle^{\perp}}$)
- $\langle \boldsymbol{w} \rangle^{\perp} / \langle \boldsymbol{w} \rangle$: an $\mathrm{Sp}(2m, 2)$-space (equipped with $(\ |\ )$)

- ${}^{\forall} A \in \Lambda$ (i.e., maximal isotropic in $\mathbb{Z}_2^{2m+2}$)
- $A \cap \langle \boldsymbol{w} \rangle^{\perp}$: maximal isotropic in $\langle \boldsymbol{w} \rangle^{\perp}$ (of dimension m)
- $A' := \overline{A \cap \langle \boldsymbol{w} \rangle^{\perp}} \in \Lambda'$ (i.e., maximal isotropic in $\langle \boldsymbol{w} \rangle^{\perp} / \langle \boldsymbol{w} \rangle$)

- $A \mapsto A \cap \langle \boldsymbol{w} \rangle^{\perp} \mapsto A' := \overline{A \cap \langle \boldsymbol{w} \rangle^{\perp}}$
- $\Sigma \mapsto \Sigma' := \{A' \mid A \in \Sigma\}$

Example

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

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

Example

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

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 $[C_m(2)]$

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

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

- Observe $K^\flat := \left(\begin{smallmatrix} K & O \\ O & K^{-T} \end{smallmatrix}\right) \in O^+(2m+2,2)$ $(K \in \mathrm{GL}(V))$
  - $Q((a,b)K^\flat) = Q((aK, bK^{-T})) = (aK)\cdot(bK^{-T}) = a\cdot b$
- ${}^\forall A \in \Sigma\backslash\{Z\}$ ${}^\exists g \in O^+(2m+2,2)$ s.t. $(X,Z)g = (A,Z)$
- ${}^{\exists 1} M_A$: $(m+1)\times(m+1)$ alternating s.t. $X\left(\begin{smallmatrix} I & M_A \\ O & I \end{smallmatrix}\right) = A$
  - The above g is of the form $\left(\begin{smallmatrix} K & M \\ O & K^{-T} \end{smallmatrix}\right)$.
  - Replace g by $K^{\flat -1}g$.
  - $\underbrace{Q\left((a,b)\left(\begin{smallmatrix} I & M_A \\ O & I \end{smallmatrix}\right)\right)}_{=Q((a,b))=a\cdot b} = Q((a, aM_A+b)) = a\cdot(aM_A) + a\cdot b$
- $\mathrm{rank}(M_A - M_B) = m+1$ $({}^\forall A, B \in \Sigma\backslash\{Z\},\ A \neq B)$
  - $A =$ row space of $(I\ M_A)$; $B =$ row space of $(I\ M_B)$
  - $\boldsymbol{a}(I\ M_A) = \boldsymbol{b}(I\ M_B) \Leftrightarrow \boldsymbol{a} = \boldsymbol{b},\ \boldsymbol{a}(M_A - M_B) = 0$

- $\Sigma(\ni X, Z) \overset{1:1}{\longleftrightarrow} \{M_A \mid A \in \Sigma \backslash \{Z\}\}$
- $\{M_A \mid A \in \Sigma \backslash \{Z\}\}$: a Kerdock set, i.e.,

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

Remark*

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

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

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

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

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

- ${}^{\forall}A' \in \Sigma \backslash \{Z'\}$ ${}^{\exists 1}P_{A'}$: $m \times m$ symmetric s.t. $X' \begin{pmatrix} I & P_{A'} \\ O & I \end{pmatrix} = A'$
- $\mathrm{rank}(P_{A'} - P_{B'}) = m \quad ({}^{\forall}A', B' \in \Sigma' \backslash \{Z'\},\ A' \neq B')$
- $\Sigma'(\ni X', Z') \overset{1:1}{\longleftrightarrow} \{P_{A'} \mid A' \in \Sigma' \backslash \{Z'\}\}$

Remark*

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

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

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

- $((v_{m+1}, v_{m+1} M_A) |\ \boldsymbol{w}) = 1$
- $((v_i, v_i M_A) |\ \boldsymbol{w}) = (M_A)_{i,m+1} \quad (i = 1, 2, \ldots, m)$

We conclude:

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

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

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

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

Example

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

$$X(b) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{b_1} \otimes \cdots \otimes \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{b_{m+1}},$$
$$Z(b) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)^{b_1} \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)^{b_{m+1}}.$$

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

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

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 $2^{1+(2m+2)}$

- $E = X(V)Z(V)\langle -I \rangle$: extraspecial of order $2^{1+(2m+2)}$
- $\boldsymbol{e}^2 \in \langle -I \rangle \quad (\boldsymbol{e} \in E)$
- $X(a)Z(b)X(a)Z(b) = (-1)^{a \cdot b}\, I$

- $\widetilde{E} := E/\langle -I \rangle \cong \mathbb{Z}_2^{2m+2}$: a vector space over $\mathbb{Z}_2$
- $\widetilde{\boldsymbol{e}} := \boldsymbol{e}\langle -I \rangle$ for $\boldsymbol{e} \in E$
- $\widetilde{E} = \widetilde{X}(V)\widetilde{Z}(V) \cong V \oplus V$

- $Q : \widetilde{E} \to \mathbb{Z}_2 \quad (\widetilde{X}(a)\widetilde{Z}(b) \mapsto a \cdot b)$: a quadratic form on $\widetilde{E}$
- $\boldsymbol{e}^2 = (-I)^{Q(\widetilde{\boldsymbol{e}})} \quad (\boldsymbol{e} \in E)$

- $\boldsymbol{e}^2 = (-I)^{Q(\widetilde{\boldsymbol{e}})} \quad (\boldsymbol{e} \in E)$
- $(\ |\ )_{\widetilde{E}}$: the associated alternating form of Q:

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

- $[\boldsymbol{e}_1, \boldsymbol{e}_2] = (-I)^{(\widetilde{\boldsymbol{e}}_1|\ \widetilde{\boldsymbol{e}}_2)_{\widetilde{E}}} \quad (\boldsymbol{e}_1, \boldsymbol{e}_2 \in E)$

  - $(\boldsymbol{e}_1\boldsymbol{e}_2)(\boldsymbol{e}_1\boldsymbol{e}_2) = (-I)^{Q(\widetilde{\boldsymbol{e}}_1+\widetilde{\boldsymbol{e}}_2)} = (-I)^{Q(\widetilde{\boldsymbol{e}}_1)+Q(\widetilde{\boldsymbol{e}}_2)+(\widetilde{\boldsymbol{e}}_1|\ \widetilde{\boldsymbol{e}}_2)_{\widetilde{E}}}$
  - $\boldsymbol{e}_1^2\boldsymbol{e}_2^2 = (-I)^{Q(\widetilde{\boldsymbol{e}}_1)+Q(\widetilde{\boldsymbol{e}}_2)}$

- $e^2 = (-I)^{Q(\widetilde{e})} \quad (e \in E)$
- $[e_1, e_2] = (-I)^{(\widetilde{e}_1 | \widetilde{e}_2)_{\widetilde{E}}} \quad (e_1, e_2 \in E)$
- $Q(g^{-1}\widetilde{e}g) = Q(\widetilde{e}) \quad (g \in N_{O(\mathbb{R}^{2^{m+1}})}(E), e \in E)$
  - $(g^{-1}eg)^2 = g^{-1}(-I)^{Q(\widetilde{e})}g = (-I)^{Q(\widetilde{e})}$

Proposition

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

Example

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

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

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

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

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

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

Example

- Suppose $m = 1$; $V = \mathbb{Z}_2^2 = \langle 10, 01 \rangle$, $V' = \langle 10 \rangle$
- $\boldsymbol{w} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} 00 \\ 10 \\ 01 \\ 11 \end{matrix}$
- $e_{00} = (1,0,0,0)$; $\quad \sqrt{-1}\, e_{00} = e_{00}\boldsymbol{w} = -e_{01} = (0,0,-1,0)$
- $e_{10} = (0,1,0,0)$; $\quad \sqrt{-1}\, e_{10} = e_{10}\boldsymbol{w} = -e_{11} = (0,0,0,-1)$
- $\alpha e_{00} + \beta e_{10} = (\mathrm{Re}\alpha, \mathrm{Re}\beta, -\mathrm{Im}\alpha, -\mathrm{Im}\beta) \quad (\alpha, \beta \in \mathbb{C})$

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

- $(x_1 + y_1\sqrt{-1} \mid x_2 + y_2\sqrt{-1})_{\mathbb{C}}$

$$= (x_1x_2 + y_1y_2) + (x_2y_1 - x_1y_2)\sqrt{-1}$$

$$= ((x_1, -y_1)|(x_2, -y_2))_{\mathbb{R}} + ((x_1, -y_1)|(-y_2, -x_2))_{\mathbb{R}}\sqrt{-1}$$

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

- $(\boldsymbol{u}|\boldsymbol{v})_{\mathbb{C}} = (\boldsymbol{u}|\boldsymbol{v})_{\mathbb{R}} + (\boldsymbol{u}|\boldsymbol{v}\boldsymbol{w})_{\mathbb{R}}\sqrt{-1}$
- $U(\mathbb{C}^{2^m}) = C_{O(\mathbb{R}^{2^{m+1}})}(\boldsymbol{w})$
- $\boldsymbol{e} \in E \cap U(\mathbb{C}^{2^m}) \Leftrightarrow I = [\boldsymbol{e}, \boldsymbol{w}] = (-I)^{(\widetilde{e}|\widetilde{w})_{\widetilde{E}}} \Leftrightarrow \widetilde{\boldsymbol{e}} \in \langle \widetilde{\boldsymbol{w}} \rangle^{\perp}$
- $\langle \widetilde{\boldsymbol{w}} \rangle^{\perp} / \langle \widetilde{\boldsymbol{w}} \rangle = (E \cap U(\mathbb{C}^{2^m})) / \langle \sqrt{-1}\, I \rangle$ (Recall $\sqrt{-1}\, I = \boldsymbol{w}$.)

- $X(V') := \{X(b) \mid b \in V'\} = X(V) \cap U(\mathbb{C}^{2^m})$
- $Z(V') := \{Z(b) \mid b \in V'\} = Z(V) \cap U(\mathbb{C}^{2^m})$
- $X(V'), Z(V') \cong V'$

- $\overline{\boldsymbol{e}} := \boldsymbol{e}\langle \sqrt{-1}\, I \rangle$ for $\boldsymbol{e} \in E \cap U(\mathbb{C}^{2^m})$
- $\langle \widetilde{\boldsymbol{w}} \rangle^{\perp} / \langle \widetilde{\boldsymbol{w}} \rangle = \overline{X}(V')\overline{Z}(V') \cong V' \oplus V'$

- 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:

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

Proposition

$N_{U(\mathbb{C}^{2^m})}(\langle \widetilde{\boldsymbol{w}} \rangle^{\perp} / \langle \widetilde{\boldsymbol{w}} \rangle) \twoheadrightarrow \mathrm{Sp}(2m, 2)$ (surjective)

- $N_{O(\mathbb{R}^{2^m+1})}(E) \twoheadrightarrow O^+(2m+2, 2)$ (surjective)
- $O^+(2m+2, 2)_{\boldsymbol{w}} = 2 \cdot O(2m+1, 2) \cong 2 \cdot \mathrm{Sp}(2m, 2)$

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

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

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

Example

- $T_P(u) := \hat{u}\hat{P}\hat{u}^T$ $(u \in V')$: associated with P
- Recall $\left(\begin{smallmatrix} I & P \\ O & I \end{smallmatrix}\right) \in \mathrm{Sp}(2m, 2)$.
- $d'_P := \mathrm{diag}[(\sqrt{-1})^{T_P(v)}]_{v \in V'} \in U(\mathbb{C}^{2^m})$
- $d'^{-1}_P (\overline{X}(a)\overline{Z}(b)) d'_P = \overline{X}(a)\overline{Z}(aP)\overline{Z}(b) = \overline{X}(a)\overline{Z}(b) \left(\begin{smallmatrix} I & P \\ O & I \end{smallmatrix}\right)$

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

Remark

- $T_1, T_2 : V' \to \mathbb{Z}_4$: $\mathbb{Z}_4$-valued quadratic forms associated with P
- $T_1 - T_2 : V' \to 2\mathbb{Z}_4 \cong \mathbb{Z}_2$: 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

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

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

- $e_v X(b) = e_{v+b}$
- $e_v Z(b) = (-1)^{b \cdot v} e_v$
- $\langle e_v \rangle_{\mathbb{R}} \ \ (v \in V)$: 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

- Σ : an orthogonal spread of $\widetilde{E}$
- We shall always assume $\widetilde{X}(V), \widetilde{Z}(V) \in \Sigma$.

- A : a subgroup of E s.t. $\widetilde{A} \in \Sigma \backslash \{\widetilde{Z}(V)\}$
  (Note that $\langle A, -I \rangle$ is the preimage of $\widetilde{A}$.)
- $\mathscr{F}_{\mathbb{R}}(A)$: the set of A-irreducible submodules of $\mathbb{R}^{2^{m+1}}$
- $^{\exists}\boldsymbol{g} \in N_{O(\mathbb{R}^{2^{m+1}})}(E)$ s.t. $\boldsymbol{g}^{-1}\widetilde{X}(V)\boldsymbol{g} = \widetilde{A}$
- $\mathscr{F}_{\mathbb{R}}(A) = \{\langle e_u^* \rangle_{\mathbb{R}}\boldsymbol{g} \mid u \in V\}$: an orthogonal frame

Remark

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

- $\mathscr{F}_{\mathbb{R}}(\Sigma) := \bigcup_{\widetilde{A} \in \Sigma} \mathscr{F}_{\mathbb{R}}(A)$

Example

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

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

- $\widetilde{A} \in \Sigma$; $\quad \mathscr{F}_{\mathbb{R}}(A) = \{\ell_1^{(A)}, \ell_2^{(A)}, \ldots, \ell_{2^{m+1}}^{(A)}\}$
- Pick a unit vector $\boldsymbol{x}_i^{(A)} \in \ell_i^{(A)}$ $(i = 1, 2, \ldots, 2^{m+1})$.
- $\mathscr{C}_A := \{\boldsymbol{x}_i^{(A)}\}_{i=1}^{2^{m+1}}$: an orthonormal basis for $\mathbb{R}^{2^{m+1}}$
- $\{\mathscr{C}_A \mid \widetilde{A} \in \Sigma\}$: $(2^m + 1)$ real MUBs

  - Pick distinct $\widetilde{A}, \widetilde{B} \in \Sigma$.
  - $^{\exists}\boldsymbol{g} \in N_{O(\mathbb{R}^{2^{m+1}})}(E)$ s.t. $\boldsymbol{g}^{-1}\widetilde{X}(V)\boldsymbol{g} = \widetilde{A}$, $\boldsymbol{g}^{-1}\widetilde{Z}(V)\boldsymbol{g} = \widetilde{B}$
  - $\mathscr{F}_{\mathbb{R}}(A) = \{\langle e_u^* \rangle_{\mathbb{R}}\boldsymbol{g} \mid u \in V\}$, $\mathscr{F}_{\mathbb{R}}(B) = \{\langle e_v \rangle_{\mathbb{R}}\boldsymbol{g} \mid v \in V\}$

Remark*

- $\bigcup_{\tilde{A}\in\Sigma}(\mathscr{C}_A \cup (-\mathscr{C}_A))$ 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.

Lemma

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

$\boldsymbol{g} \in N_{O(\mathbb{R}^{2^{m+1}})}(E)$ if
1. $\mathscr{F}_{\mathbb{R}}(X(V))\boldsymbol{g} = \mathscr{F}_{\mathbb{R}}(X(V))$
2. $\mathscr{F}_{\mathbb{R}}(Z(V))\boldsymbol{g} = \mathscr{F}_{\mathbb{R}}(Z(V))$

Proposition

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

$\mathscr{F}_{\mathbb{R}}(\Sigma_1)\boldsymbol{g} = \mathscr{F}_{\mathbb{R}}(\Sigma_2) \Leftrightarrow$
1. $\boldsymbol{g} \in N_{O(\mathbb{R}^{2^{m+1}})}(E)$
2. $\boldsymbol{g}^{-1}\Sigma_1\boldsymbol{g} = \Sigma_2$

Proof.

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

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

- $V' = \langle v_1, v_2, \ldots, v_m \rangle$
- $X(V') = \{X(b) \mid b \in V'\}$
- $Z(V') = \{Z(b) \mid b \in V'\}$
- $\langle \widetilde{w} \rangle^{\perp} / \langle \widetilde{w} \rangle = \overline{X}(V')\overline{Z}(V')$: an $\mathrm{Sp}(2m, 2)$-space

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

- $(\boldsymbol{u}|\boldsymbol{v})_{\mathbb{C}} = (\boldsymbol{u}|\boldsymbol{v})_{\mathbb{R}} + (\boldsymbol{u}|\boldsymbol{v}\boldsymbol{w})_{\mathbb{R}}\sqrt{-1}$
- $(\boldsymbol{u}|\boldsymbol{u}\boldsymbol{w})_{\mathbb{R}} = 0$

  - $(\boldsymbol{u}|\boldsymbol{u}\boldsymbol{w})_{\mathbb{R}} = (\boldsymbol{u}\boldsymbol{w}|\boldsymbol{u}\boldsymbol{w}^2)_{\mathbb{R}} = -(\boldsymbol{u}\boldsymbol{w}|\boldsymbol{u})_{\mathbb{R}}$

- $(\boldsymbol{u}|\boldsymbol{v})_{\mathbb{C}} = (\boldsymbol{u}|\boldsymbol{v})_{\mathbb{R}} + (\boldsymbol{u}|\boldsymbol{v}\boldsymbol{w})_{\mathbb{R}}\sqrt{-1}$
- $(\boldsymbol{u}|\boldsymbol{u}\boldsymbol{w})_{\mathbb{R}} = 0$

- Σ : an orthogonal spread of $\widetilde{E}$
- Recall $\Sigma' = \left\{ \overline{\widetilde{A} \cap \langle \widetilde{\boldsymbol{w}} \rangle^{\perp}} \;\middle|\; \widetilde{A} \in \Sigma \right\}$.

- $\widetilde{A} \in \Sigma$
- $\mathscr{F}_{\mathbb{R}}(A)\boldsymbol{w} = \mathscr{F}_{\mathbb{R}}(A)$
- $\ell \neq \ell\boldsymbol{w}$ $(^{\forall}\ell \in \mathscr{F}_{\mathbb{R}}(A))$ $(\because (\ell|\ell\boldsymbol{w})_{\mathbb{R}} = 0)$
- A' : a subgroup of $E \cap U(\mathbb{C}^{2^m})$ s.t. $\overline{A'} = \overline{\widetilde{A} \cap \langle \widetilde{\boldsymbol{w}} \rangle^{\perp}}$
- $\mathscr{F}_{\mathbb{C}}(A') := \{\mathbb{C}\ell = \ell + \ell\boldsymbol{w} \mid \ell \in \mathscr{F}_{\mathbb{R}}(A)\}$: the set of A'-irreducible submodules of $\mathbb{C}^{2^m}$; an orthogonal frame
- $\mathscr{F}_{\mathbb{C}}(\Sigma') := \bigcup_{\overline{A'} \in \Sigma'} \mathscr{F}_{\mathbb{C}}(A') = \{\mathbb{C}\ell = \ell + \ell\boldsymbol{w} \mid \ell \in \mathscr{F}_{\mathbb{R}}(\Sigma)\}$

- $\widetilde{A}, \widetilde{B} \in \Sigma \ \ (\widetilde{A} \neq \widetilde{B})$
- $\ell^{(A)} \in \mathscr{F}_{\mathbb{R}}(A), \ \ell^{(B)} \in \mathscr{F}_{\mathbb{R}}(B)$
- $\boldsymbol{x}^{(A)} \in \ell^{(A)}, \boldsymbol{x}^{(B)} \in \ell^{(B)}$: unit vectors
- $$\left|(\boldsymbol{x}^{(A)}|\boldsymbol{x}^{(B)})_{\mathbb{C}}\right| = \left|(\boldsymbol{x}^{(A)}|\boldsymbol{x}^{(B)})_{\mathbb{R}} + (\boldsymbol{x}^{(A)}|\boldsymbol{x}^{(B)}\boldsymbol{w})_{\mathbb{R}}\sqrt{-1}\right|$$
$$= \sqrt{\left(\frac{1}{\sqrt{2^{m+1}}}\right)^2 + \left(\frac{1}{\sqrt{2^{m+1}}}\right)^2}$$
$$= \frac{1}{\sqrt{2^m}}$$

- $\overline{A'} \in \Sigma'; \quad \mathscr{F}_{\mathbb{C}}(A') = \{\ell_1'^{(A')}, \ell_2'^{(A')}, \ldots, \ell_{2^m}'^{(A')}\}$
- Pick a unit vector $z_i^{(A')} \in \ell_i'^{(A')} \ \ (i = 1, 2, \ldots, 2^m)$.
- $\mathscr{C}'_{A'} := \{z_i^{(A')}\}_{i=1}^{2^m}$: an orthonormal bases for $\mathbb{C}^{2^m}$
- $\{\mathscr{C}'_{A'} \mid \overline{A'} \in \Sigma'\}$: $(2^m + 1)$ complex MUBs

Example

- Suppose $m = 1$, and recall $\boldsymbol{w} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$.
- $\ell_1 := \langle (1,0,0,0) \rangle_{\mathbb{R}} \in \mathscr{F}_{\mathbb{R}}(Z(V))$
- $\ell_1 \boldsymbol{w} = \langle (0,0,-1,0) \rangle_{\mathbb{R}} \in \mathscr{F}_{\mathbb{R}}(Z(V))$
- $\mathbb{C}\ell_1 = \langle (1,0) \rangle_{\mathbb{C}}$
- $\ell_2 := \langle (1,1,1,1) \rangle_{\mathbb{R}} \in \mathscr{F}_{\mathbb{R}}(X(V))$
- $\ell_2 \boldsymbol{w} = \langle (1,1,-1,-1) \rangle_{\mathbb{R}} \in \mathscr{F}_{\mathbb{R}}(X(V))$
- $\mathbb{C}\ell_2 = \langle (1-\sqrt{-1}, 1-\sqrt{-1}) \rangle_{\mathbb{C}} = \langle (1,1) \rangle_{\mathbb{C}}$
- $(1,0) \in \mathbb{C}\ell_1$, $\frac{1}{\sqrt{2}}(1,1) \in \mathbb{C}\ell_2$: unit vectors
- $\left| ((1,0) | \frac{1}{\sqrt{2}}(1,1))_{\mathbb{C}} \right| = \frac{1}{\sqrt{2}}$

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))

We relate "$\mathscr{K}_4(\Sigma') \overset{\phi}{\longmapsto} \mathscr{K}(\Sigma)$" with "$\mathscr{F}_{\mathbb{R}}(\Sigma) \longmapsto \mathscr{F}_{\mathbb{C}}(\Sigma')$".

- $\widetilde{A} \in \Sigma \backslash \{\widetilde{Z}(V)\}$
- $\exists^1 M_A : (m+1) \times (m+1)$ alternating s.t. $\widetilde{X}(V) \begin{pmatrix} I & M_A \\ O & I \end{pmatrix} = \widetilde{A}$
- $Q_{M_A} : V \to \mathbb{Z}_2$: a quadratic form with associated alternating form uM_Av^T
- $\mathscr{K}(\Sigma) := \left\{ (Q_{M_A}(v) + s \cdot v + \epsilon)_{v \in V} \middle| \begin{array}{c} \widetilde{A} \in \Sigma \backslash \{\widetilde{Z}(V)\}, \\ s \in V,\ \epsilon \in \mathbb{Z}_2 \end{array} \right\} \subseteq \mathbb{Z}_2^{2^{m+1}}$: a Kerdock code

Remark

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

- $\mathscr{K}(\Sigma) = \left\{ (Q_{M_A}(v) + s \cdot v + \epsilon)_{v \in V} \;\middle|\; \begin{array}{c} \widetilde{A} \in \Sigma \backslash \{\widetilde{Z}(V)\}, \\ s \in V,\ \epsilon \in \mathbb{Z}_2 \end{array} \right\}$

Proposition

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

Proof.

- Recall $\mathscr{F}_{\mathbb{R}}(X(V)) = \{ \langle e_u^* \rangle_{\mathbb{R}} \mid u \in V \}$ where
$$e_u^* = \frac{1}{\sqrt{2^{m+1}}} \sum_{v \in V} (-1)^{u \cdot v} e_v.$$
- $d_{M_A} = \mathrm{diag}[(-1)^{Q_{M_A}(v)}]_{v \in V}$ $(\widetilde{A} \in \Sigma \backslash \{\widetilde{Z}(V)\})$
- $\mathscr{F}_{\mathbb{R}}(A) = \mathscr{F}_{\mathbb{R}}(X(V)) d_{M_A}$ and
$$e_s^* \, d_{M_A} = \frac{1}{\sqrt{2^{m+1}}} \sum_{v \in V} (-1)^{Q_{M_A}(v) + s \cdot v} e_v.$$ □

- $V' = \langle v_1, v_2, \ldots, v_m \rangle$
- $\overline{A'} \in \Sigma' \backslash \{\overline{Z}(V')\}$
- $\exists 1 P_{A'}$: $m \times m$ symmetric s.t. $\overline{X}(V') \begin{pmatrix} I & P_{A'} \\ O & I \end{pmatrix} = \overline{A'}$
- $T_{P_{A'}} : V' \to \mathbb{Z}_4$: a $\mathbb{Z}_4$-quadratic form associated with $P_{A'}$
- $\mathscr{K}_4(\Sigma') := \left\{ (T_{P_{A'}}(v) + 2\hat{s} \cdot \hat{v} + \epsilon)_{v \in V'} \middle| \begin{matrix} A' \in \Sigma' \backslash \{\overline{Z}(V')\}, \\ s \in V', \ \epsilon \in \mathbb{Z}_4 \end{matrix} \right\} \subseteq \mathbb{Z}_4^{2^m}$
  : a $\mathbb{Z}_4$-Kerdock code

Remark

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

- $\mathscr{K}_4(\Sigma') = \left\{ (T_{P_{A'}}(v) + 2\hat{s}\cdot\hat{v} + \epsilon)_{v\in V'} \,\middle|\, \begin{array}{c} A' \in \Sigma'\backslash\{\overline{Z}(V')\}, \\ s \in V',\ \epsilon \in \mathbb{Z}_4 \end{array} \right\} \subseteq \mathbb{Z}_4^{2^m}$

Proposition

$$\mathscr{K}_4(\Sigma') = \left\{ (z_v)_{v\in V'} \in \mathbb{Z}_4^{2^m} \,\middle|\, \left\langle ((\sqrt{-1})^{z_v})_{v\in V'} \right\rangle \in \mathscr{F}_{\mathbb{C}}(\Sigma') \right\}$$

Proof.

- $\mathscr{F}_{\mathbb{C}}(\overline{X}(V')) = \{\langle e'^*_u \rangle_{\mathbb{C}} \mid u \in V'\}$ where
$$e'^*_u := \frac{1}{\sqrt{2^m}} \sum_{v\in V'} (-1)^{u\cdot v} e_v.$$
- $d'_{P_{A'}} = \mathrm{diag}[(\sqrt{-1})^{T_{P_{A'}}(v)}]_{v\in V'}$ $(\overline{A'} \in \Sigma'\backslash\{\overline{Z}(V')\})$
- $\mathscr{F}_{\mathbb{C}}(A') = \mathscr{F}_{\mathbb{C}}(\overline{X}(V'))d'_{P_{A'}}$, and
$$e'^*_s\, d'_{P_{A'}} = \frac{1}{\sqrt{2^m}} \sum_{v\in V'} (\sqrt{-1})^{T_{P_{A'}}(v) + 2\hat{s}\cdot\hat{v}} e_v.$$ □

Lemma

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

$$\mathbb{C}^{2^m} \supseteq \{\pm 1,\ \pm\sqrt{-1}\}^{2^m} \underset{\times\left(\frac{1+\sqrt{-1}}{2}\right)}{\overset{\times(1-\sqrt{-1})}{\rightleftarrows}} \{\pm 1\}^{2^{m+1}} \subseteq \mathbb{R}^{2^{m+1}}$$

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

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

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

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

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

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

- $\mathscr{K}_4(\Sigma') = \left\{(z_v)_{v\in V'} \in \mathbb{Z}_4^{2^m} \,\middle|\, \left\langle((\sqrt{-1})^{z_v})_{v\in V'}\right\rangle \in \mathscr{F}_{\mathbb{C}}(\Sigma')\right\}$
- $\mathscr{K}(\Sigma) = \left\{(x_v)_{v\in V} \in \mathbb{Z}_2^{2^{m+1}} \,\middle|\, \left\langle((-1)^{x_v})_{v\in V}\right\rangle \in \mathscr{F}_{\mathbb{R}}(\Sigma)\right\}$

Proposition

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

Proof.

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

Kerdock and Preparata codes

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

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

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

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

defines an isometry:

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

Kerdock and Preparata codes

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

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

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

Proposition

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

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

Proof.

- $\mathscr{K}_4(\Sigma') = \left\{ (T_{P_{A'}}(v) + 2\hat{s}\cdot\hat{v} + \epsilon)_{v\in V'} \;\middle|\; \begin{array}{c} A' \in \Sigma'\backslash\{\overline{Z}(V')\}, \\ s \in V',\ \epsilon \in \mathbb{Z}_4 \end{array} \right\}$
- Let $\oplus$ denote the binary addition in $\mathbb{Z}_2$.
- Recall $\hat{}\,: \mathbb{Z}_2 = \{0,1\} \hookrightarrow \mathbb{Z}_4 = \{0,1,2,3\}$.
- Note $\hat{a} + \hat{b} = a \oplus b + 2\hat{a}\hat{b} \quad (a,b \in \mathbb{Z}_2)$.

- $T_{P_{A'}}(v) + T_{P_{B'}}(v)$

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

□

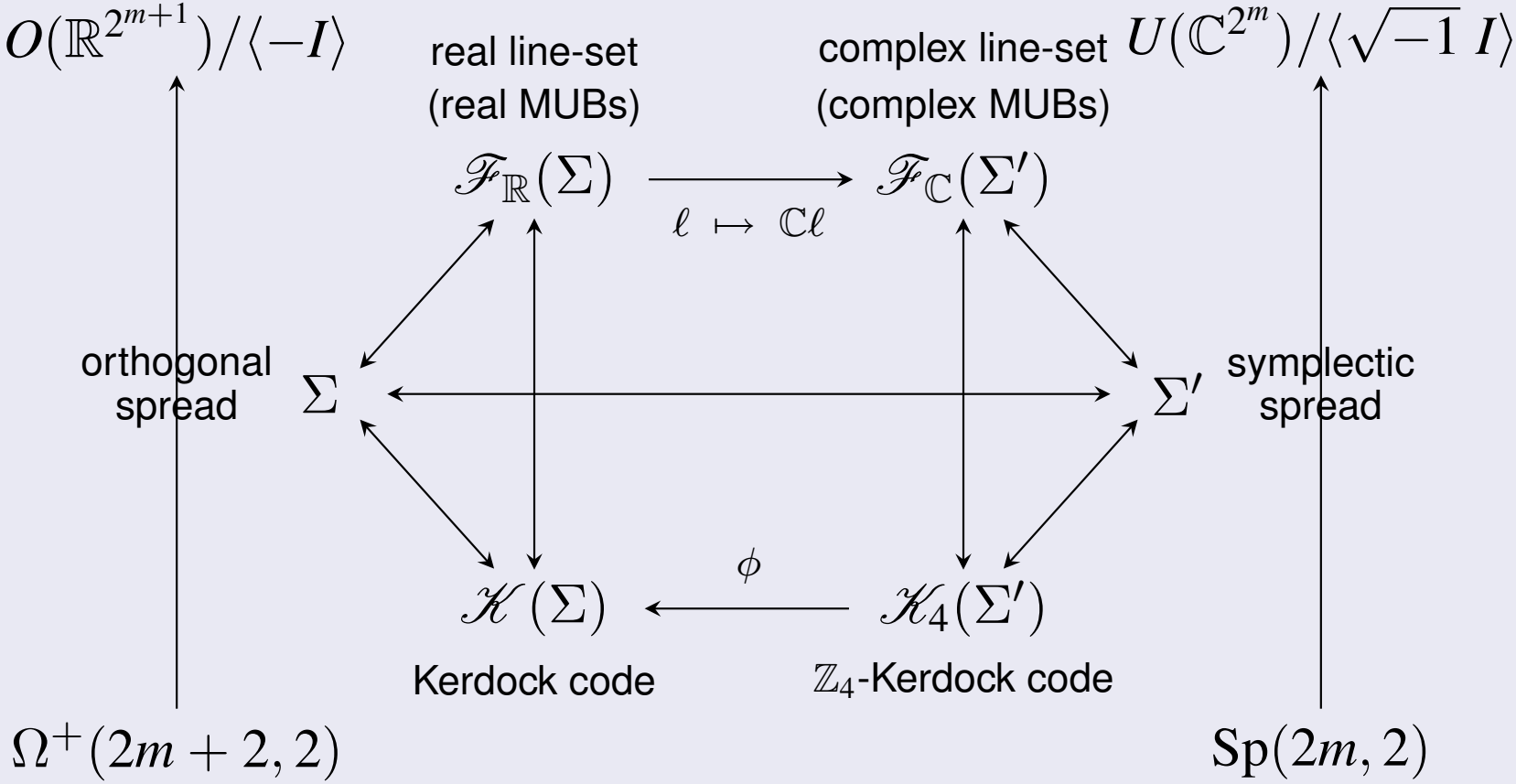
Kerdock and Preparata codes

- The determination of equivalence among various Kerdock or $\mathbb{Z}_4$-Kerdock codes is not simple. (For example it is possible that $\mathscr{K}_4(\Sigma_1') \ncong \mathscr{K}_4(\Sigma_2')$ even if $\Sigma_1' \cong \Sigma_2'$.)
- But it is proved for example that

$$\phi(\mathscr{K}_4(\Sigma_1')) \cong \phi(\mathscr{K}_4(\Sigma_2')) \Leftrightarrow \mathscr{K}_4(\Sigma_1') \cong \mathscr{K}_4(\Sigma_2')$$

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

Summary


$O(\mathbb{R}^{2^{m+1}})/\langle -I \rangle$
real line-set
(real MUBs)
complex line-set
(complex MUBs)
$U(\mathbb{C}^{2^m})/\langle \sqrt{-1}\, I \rangle$
$\mathscr{F}_{\mathbb{R}}(\Sigma)$
$\ell \mapsto \mathbb{C}\ell$
$\mathscr{F}_{\mathbb{C}}(\Sigma')$
orthogonal
spread
Σ
Σ'
symplectic
spread
ϕ
$\mathscr{K}(\Sigma)$
$\mathscr{K}_4(\Sigma')$
Kerdock code
$\mathbb{Z}_4$-Kerdock code
$\Omega^+(2m+2,2)$
$\mathrm{Sp}(2m,2)$

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 $\phi^{\natural} : \mathbb{Z}_4 \to \mathbb{Z}_2^2$:

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

- Consider the following correspondence:

$$\mathbb{C}^{2^m} \supseteq \{\pm 1, \pm\sqrt{-1}\}^{2^m} \underset{\times\left(\frac{1-\sqrt{-1}}{2}\right)}{\overset{\times(1+\sqrt{-1})}{\rightleftarrows}} \{\pm 1\}^{2^{m+1}} \subseteq \mathbb{R}^{2^{m+1}}$$