Symmetry and Sequence Design I: The Heisenberg-Weyl Group $\mathcal{W}(\mathbb{Z}_2^m)$

Robert Calderbank
Princeton University

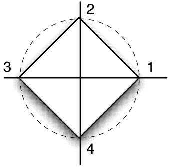
Stephen Howard
Defence Science & Technology Organization Australia

Bill Moran
Melbourne University

Maximal Commutative Subgroup	X $\longrightarrow$	$Z = H^{-1}XH$
Orthonormal Basis	Walsh Sequences $\longrightarrow$	Dirac Sequences

Supported by Defense Advanced Research Projects Agency and Air Force Office of Scientific Research

D_4: The Symmetry Group of the Square



Generated by matrices $x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$

$xz = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ anticlockwise rotation by $\dfrac{\pi}{2}$

$z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ reflection in the horizontal axis

D_4 is the set of eight 2×2 matrices $\varepsilon\, D(a, b)$ given by

$$\varepsilon\, D(a, b) = \varepsilon \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^a \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^b \text{ where } \varepsilon = \pm 1 \text{ and } a, b = 0 \text{ or } 1.$$

$x^2 = z^2 = I_2$

$$\left.\begin{aligned} zx &= \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}\begin{pmatrix} & 1 \\ 1 & \end{pmatrix} = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \\ xz &= \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}\begin{pmatrix} 1 & \\ & -1 \end{pmatrix} = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \end{aligned}\right] \; xz = -zx$$

The Hadamard Transform

$H_2 = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} + & + \\ + & - \end{smallmatrix}\right)$ reflects the lattice of subgroups across the central axis of symmetry

$$
\begin{tikzcd}[column sep=small]
 & & D_4 \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & & \\
 & \langle \pm x \rangle \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \langle xz \rangle \arrow[d, no head] & \langle \pm z \rangle \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\langle x \rangle \arrow[drr, no head] & \langle -x \rangle \arrow[dr, no head] & \langle -I_2 \rangle \arrow[d, no head] & \langle -z \rangle \arrow[dl, no head] & \langle z \rangle \arrow[dll, no head] \\
 & & \langle I_2 \rangle & &
\end{tikzcd}
$$

$$H_2^2 = I_2 \text{ and } H_2^{-1} = H_2$$

$$H_2 x H_2 = z$$

$$H_2 z H_2 = x$$

$$H_2[\varepsilon x^a z^b]H_2 = \varepsilon(H_2 x^a H_2)(H_2 z^b H_2) = \varepsilon z^a x^b = (-1)^{ab} x^b z^a$$

$$H_2[\varepsilon D(a,b)]H_2 = (-1)^{ab}\varepsilon D(b,a)$$

Kronecker Products of Matrices

Given a $p \times p$ matrix $X = [x_{ij}]$ and a $q \times q$ matrix $Y = [Y_{ij}]$, the Kronecker products $X \otimes Y$ is defined by

$$X \otimes Y = \begin{bmatrix} x_{11}Y & \dots & x_{1p}Y \\ \vdots & & \vdots \\ x_{p1}Y & \dots & x_{pp}Y \end{bmatrix}$$

Proposition: $(X \otimes Y)(X' \otimes Y') = (XX') \otimes (YY')$ and in general $(X_1 \otimes \dots \otimes X_m)(Y_1 \otimes \dots \otimes Y_m) = X_1 Y_1 \otimes \dots \otimes X_m Y_m$

$$\begin{pmatrix} x_{11}Y & x_{12}Y \\ x_{21}Y & x_{22}Y \end{pmatrix} \begin{pmatrix} x'_{11}Y' & x'_{12}Y' \\ x'_{21}Y' & x'_{22}Y' \end{pmatrix} = \begin{pmatrix} \bullet & \\ \uparrow & \end{pmatrix}$$

$$x_{11}x'_{11}YY' + x_{12}x'_{21}YY' = (XX')_{11}YY'$$

Walsh-Hadamard Matrix: $H_{2^m} = H_2 \otimes \dots \otimes H_2 \quad (m \text{ copies})$

The Heisenberg-Weyl Group $\mathcal{W}(\mathbb{Z}_2^m)$

$\mathcal{W}(\mathbb{Z}_2^m)$ is the m-fold Kronecker product of D_4 extended by iI_{2^m}.

$i^\lambda p_{m-1} \otimes \ldots \otimes p_0$ where $p_j = I_2, x, z,$ or xz for $j = 0, 1, \ldots, m-1$

There are 2^{2m+2} elements, each represented by a pair of binary m-tuples

$$xz \otimes x \otimes z \otimes xz \otimes I_2 \leftrightarrow D(\overset{a}{11010}, \overset{b}{10110})$$

Example: The Quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ as a subgroup of $\mathcal{W}(\mathbb{Z}_2^2)$

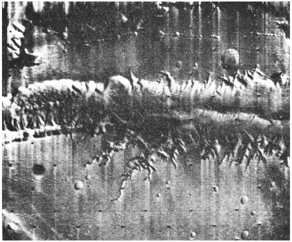
$$\mathbf{i} : -\begin{pmatrix} + & \\ & - \end{pmatrix} \otimes \begin{pmatrix} & - \\ + & \end{pmatrix} = \left(\begin{array}{cc|cc} & + & & \\ - & & & \\ \hline & & & - \\ & & + & \end{array}\right), \quad \mathbf{j} : \begin{pmatrix} & - \\ + & \end{pmatrix} \otimes \begin{pmatrix} + & \\ & + \end{pmatrix} = \left(\begin{array}{cc|cc} & & - & \\ & & & - \\ \hline + & & & \\ & + & & \end{array}\right)$$

$$\text{and } \mathbf{k} : \begin{pmatrix} & + \\ + & \end{pmatrix} \otimes \begin{pmatrix} & - \\ + & \end{pmatrix} = \left(\begin{array}{cc|cc} & & & - \\ & & + & \\ \hline & - & & \\ + & & & \end{array}\right).$$

Walsh Functions

$$H_{2^m}^T = H_2^T \otimes \ldots \otimes H_2^T = H_{2^m}$$

Walsh functions of length 2^m are the rows (columns) of H_{2^m} and their negatives.



Part of the Grand Canyon on Mars. This photograph was transmitted by the Mariner 9 spacecraft on January 19th, 1972 – gray levels are mapped to Walsh functions of length 32.

The closest Walsh function c to the received vector r is the one that maximizes the inner product (r, c):

$$\|r - c\|^2 = \|r\|^2 + \|c\|^2 - 2(r, c).$$

Fast Hadamard Transform

Exhaustive search requires about $2^m \times 2^m = 2^{2m}$ additions and subtractions to find the closest Walsh function to the received vector r.

Fast Hadamard Transform only requires about $m2^m$ operations

Example (m = 3):

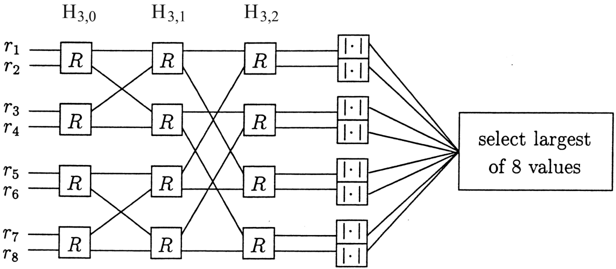
$$H_8 = \underbrace{(I_2 \otimes I_2 \otimes H_2)}_{H_{3,0}} \underbrace{(I_2 \otimes H_2 \otimes I_2)}_{H_{3,1}} \underbrace{(H_2 \otimes I_2 \otimes I_2)}_{H_{3,2}}$$

$$H_8 = \underbrace{\left[\begin{array}{cc|cc|cc|cc} + & + & & & & & & \\ + & - & & & & & & \\ \hline & & + & + & & & & \\ & & + & - & & & & \\ \hline & & & & + & + & & \\ & & & & + & - & & \\ \hline & & & & & & + & + \\ & & & & & & + & - \end{array}\right]}_{2^m \text{ operations}} \underbrace{\left[\begin{array}{cc|cc|cc|cc} + & & + & & & & & \\ & + & & + & & & & \\ \hline + & & - & & & & & \\ & + & & - & & & & \\ \hline & & & & + & & + & \\ & & & & & + & & + \\ \hline & & & & + & & - & \\ & & & & & + & & - \end{array}\right]}_{2^m \text{ operations}} \underbrace{\left[\begin{array}{cc|cc|cc|cc} + & & & & + & & & \\ & + & & & & + & & \\ \hline & & + & & & & + & \\ & & & + & & & & + \\ \hline + & & & & - & & & \\ & + & & & & - & & \\ \hline & & + & & & & - & \\ & & & + & & & & - \end{array}\right]}_{2^m \text{ operations}}$$

Fast Hadamard Transform: Circuit Level Description

The component R produces outputs $(x+y, x-y)$ from inputs (x, y). The component $|\cdot|$ produces $|x|$ from input x and stores the sign.

Received Vector r



The eight outputs of the third stage are the eight inner products of the vector r with the rows of H_8.

Multiplication in the Heisenberg-Weyl Group $\mathcal{W}(\mathbb{Z}_2^m)$

Theorem: $\mathcal{W}(\mathbb{Z}_2^m)$ is a group of order 2^{2m+2}

1. $[\varepsilon D(a,b)][\varepsilon' D(a',b')] = \varepsilon\varepsilon'(-1)^{a'.b} D(a \oplus a', b \oplus b')$
2. $[\varepsilon D(a,b)][\varepsilon' D(a',b')] = (-1)^{a'.b+b'.a}[\varepsilon' D(a',b')][\varepsilon D(a,b)]$
3. Elements $D(a,b)$ with $a.b = 1$ have order 4 and elements $D(a,b)$ with $a.b = 0$ have order 2 (other than the identity $D(0,0)$).

Proof: Look at the i^{th} component

$$x^{a_i} z^{b_i} x^{a'_i} z^{b'_i} = (-1)^{b_i a'_i} x^{a_i + a'_i} z^{b_i + b'_i}$$
$$x^{a'_i} z^{b'_i} x^{a_i} z^{b_i} = (-1)^{a_i b'_i} x^{a_i + a'_i} z^{b_i + b'_i}$$

and so

$$x^{a'_i} z^{b'_i} x^{a_i} z^{b_i} = (-1)^{b_i a'_i + a_i b'_i} x^{a_i} z^{b_i} x^{a'_i} z^{b'_i}$$

The Hadamard Transform and the Heisenberg-Weyl Group

$$
\begin{aligned}
H_{2^m}[\varepsilon D(a,b)]H_{2^m} &= \varepsilon H_{2^m} D(a,0) H_{2^m} H_{2^m} D(0,b) H_{2^m} \\
&= \varepsilon \left(\bigotimes_{i=0}^{m-1} z^{a_i} \right) \left(\bigotimes_{i=0}^{m-1} x^{b_i} \right) \\
&= \varepsilon \bigotimes_{i=0}^{m-1} z^{a_i} x^{b_i} \\
&= \varepsilon \bigotimes_{i=0}^{m-1} (-1)^{a_i b_i} x^{b_i} z^{a_i} \\
&= \varepsilon (-1)^{a.b} D(b,a)
\end{aligned}
$$

Example: $H_{2^m} D(b,0) H_{2^m} = D(0,b)$

$$
\underset{\substack{\uparrow \\ \text{interchanges } 1^{\text{st}} \\ \text{and } b^{\text{th}} \text{ rows}}}{D(b,0)H_{2^m}} \quad = \quad \underset{\substack{\uparrow \\ \text{multiplies } 1^{\text{st}} \text{ row by the} \\ \text{diagonal matrix } D(0,b)}}{H_{2^m} D(0,b)}
$$

Properties of Walsh Functions

Label rows and columns of H_4

$$b \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} \frac{1}{2}\left[\begin{array}{cc|cc} + & + & + & + \\ + & - & + & - \\ \hline + & + & - & - \\ + & - & - & + \end{array}\right] \longleftarrow$$

the v^{th} entry of the $(01)^{\text{th}}$ Walsh function is $\frac{1}{2}(-1)^{(01).v}$

Theorem: (1) The Walsh functions form an orthonormal basis of eigenvectors for each matrix in the commutative subgroup $X = \{\varepsilon D(a, 0)\}$

(2) The v^{th} entry of the Walsh function $2^{-m/2}\mathbf{1}D(0, b)$ is $2^{-m/2}(-1)^{b.v}$

Proof: The v^{th} entry of $\mathbf{1}D(0, b)$ is the first entry of $[\mathbf{1}D(0, b)]D(v, 0)$

$$[\mathbf{1}D(0, b)]D(v, 0) = (-1)^{b.v}\mathbf{1}D(v, 0)D(0, b) = (-1)^{b.v}\mathbf{1}D(0, b)$$

First Order Reed Muller Codes and Walsh Functions

Walsh functions are obtained by exponentiating codewords in the first order Reed Muller code.

Example $(m = 3)$ $RM(1,3)$

$$
(\gamma, b) \quad \begin{array}{c}
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1
\end{pmatrix} \\
v
\end{array}
= \begin{array}{c}
(\ldots\ldots b.v + \gamma \ldots\ldots) \\
| \\
(-1)^{\gamma}(-1)^{b.v} = \varepsilon(-1)^{b.v}
\end{array}
$$

Symmetry: Focus on orthonormal bases of eigenvectors for maximal commutative subgroups.

Maximal Commutative Subgroup	$X = \{\varepsilon D(a,0)\}$	$\xleftrightarrow{H_{2^m}}$	$Z = \{\varepsilon D(0,b)\}$
	|		|
Orthonormal Basis	Walsh Sequences	$\xleftrightarrow{H_{2^m}}$	Dirac Sequences

Local Decoding of $RM(1, m)$

$$(\gamma, b)\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = \Big(\underbrace{\quad}\,|\,\underbrace{\quad}\,|\,\underbrace{\quad}\,|\,\underbrace{\quad}\Big)$$

each pair of entries sums to b_0

e_j: binary vector with a 1 in position i and zeros elsewhere

Local Decoding Algorithm: Input is unknown Walsh Function $\mathbf{1}D(0, b)$

Round $i, i = 0, 1, \ldots, m-1$: select an entry v at random and compare with the entry $v \oplus e_i$: the difference is $(-1)^{b_i}$

Round m: measure any entry to determine the sign γ

$\boxed{\text{We are exploiting how information bits map to codewords}}$

Sequence Design for Wireless Communication: CDMA Downlink

Binary data $a_i(n) = \pm 1$ is transmitted to the i^{th} subscriber in time slot n using a Walsh sequence $w_i(t), t = 0, 1, \ldots, 63 \quad (RM(1,6))$

$$a_i(n)w_i(t) \qquad t = 0, 1, \ldots, 63$$

Signals from different subscribers combine to give

$$r(t) = a_i(n)w_i(t) + \sum_{j \neq i} a_j(n)w_j(t) \qquad t = 0, 1, \ldots, 63$$

The i^{th} receiver computes

$$z_i(n) = \sum_t r(t)w_i(t)$$

and in the absence of noise

$$z_i(n) = a_i(n) + \sum_{j \neq i} a_j(n) \left((w_i(t)), (w_j(t)) \right)$$

Quantum Mechanics

Classical Bits: only take values 0 and 1

Quantum Bits or Qubits: employ superposition of base states e_0 and e_1
A qubit is a 2-dim. Hilbert space and a quantum state is a vector

$$\alpha e_0 + \beta e_1, \text{ where } |\alpha|^2 + |\beta|^2 = 1$$

m qubits are represented by the tensor product of the individual 2-dim. Hilbert spaces.

$$\sum_{v \in \mathbb{Z}_2^m} \alpha_v e_v, \quad \text{where } \sum_{v \in \mathbb{Z}_2^m} |\alpha_v|^2 = 1$$

Measurement: When a measurement is made with respect to the basis $e_v, v \in \mathbb{Z}_2^m$, the probability that the system is found in state e_v is $|\alpha_v|^2$

Quantum Computing: Effectiveness derives from quantum superposition which allows exponentially many instances to be processed at the same time.

Decoherence

No quantum system can be perfectly isolated from the rest of the world and this interaction with the environment causes decoherence.

Error Process: represented mathematically in terms of Pauli matrices

- $x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ bit or flip error in an individual qubit
- $z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ phase error
- $y = ixz = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ flip-phase error

Note: This is the error model for the quantum completely depolarizing channel – a quantum analog for the classical binary symmetric channel.

I_2, x, z and y form an orthonormal basis for the space of linear operators on $\mathbb{C}^2$ wrt the trace inner product – every possible error can be expressed as a linear combination of I_2, x, z and y.

The Heisenberg-Weyl Group $\mathcal{W}(\mathbb{Z}_2^m)$ and Quantum Error Correction

$\mathcal{W}(\mathbb{Z}_2^m)$ is known to mathematicians as an extraspecial 2-group and to physicists as a Pauli group.

$$i^\lambda p_{m-1} \otimes \ldots \otimes p_0 \quad \text{where } \lambda \in \mathbb{Z}_4 \text{ and } p_j = I_2, x, z \text{ or } xz$$
$$i^\lambda D(a, b) \quad \text{where } a, b \in \mathbb{Z}_2^m$$

Commutativity: $D(a, b)$ commutes with $D(a', b')$ if and only if $a'.b + b'.a = 0$

Assumption: The group $\mathcal{W}(\mathbb{Z}_2^m)$ provides a discrete error model for a quantum analog of the classical binary symmetric channel. Any code that corrects these types of quantum errors will be able to correct errors in arbitrary models assuming that the errors are not correlated and the error rate is small.

m-dim. commutative subgroup: common eigenspaces are 1-dim and form an orthonormal basis.

k-dim. commutative subgroup: common eigenspaces are 2^{m-k} dim.

Stabilizer Codes for Quantum Error Correction

Example: $[[5,1,3]]$ Quantum Error Correcting Code

$$\begin{array}{c}\left[\begin{array}{ccccc|ccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array}\right] \\ \qquad a \qquad\qquad\qquad b \end{array}$$

– the rows of this matrix and iI_{32} generate a commutative subgroup G of size 64

– 16 common eigenspaces each 2-dim.

$$\begin{array}{c} \mathcal{W}(\mathbb{Z}_2^5) \\ {\scriptstyle 16}\big\downarrow \\ G^{\perp} \\ {\scriptstyle 4}\big\downarrow \\ G \end{array}$$

Stabilizer Code: the 2-dim eigenspace V fixed by G – view this as a single protected qubit

G is normal in $\mathcal{W}(\mathbb{Z}_2^5)$ so errors in $\mathcal{W}(\mathbb{Z}_2^5)$ permute the 16 common eigenspaces of G

There are $15 = 5 \times 3$ single qubit errors and each moves V to a different eigenspace

Syndrome Detection: Measure the eigenspace (syndrome) without getting any information about the quantum state. Correct single qubit errors by applying the appropriate "coset leader."

Representation of Operators

Inner Products: $(R, S) = Tr(R^\dagger S)$

Hilbert-Schmidt or Frobenius Norm: $\|S\| = Tr(S^\dagger S)^{\frac{1}{2}}$

Orthonormal Basis: $\frac{1}{\sqrt{N}} D(a, b), a, b \in \mathbb{Z}_2^m$ where $N = 2^m$

$$Tr(D(a, b)^\dagger D(a', b')) = N\delta_{a,a'}\delta_{b,b'}$$

Weyl Transform: Given an operator S write

$$\begin{aligned} S &= \frac{1}{N} \sum_{a,b \in \mathbb{Z}_2^m} Tr(D(a, b)^\dagger S) D(a, b) \\ &= \sum_{a,b \in \mathbb{Z}_2^m} S(a, b) \left[\frac{1}{\sqrt{N}} D(a, b) \right] \end{aligned}$$

The Weyl Tranform is the isometry

$$S \longleftrightarrow (S(a, b)) = \left(\frac{1}{\sqrt{N}} Tr(D(a, b)^\dagger S) \right)$$

From Sequences to Rank One Projection Operators

Walsh sequence: $\theta^\dagger = \frac{1}{2}(+-+-) = \frac{1}{2}\mathbf{1}D(00,01)$

Rank One Projection Operator: $\theta\theta^\dagger = \frac{1}{4}\left[\begin{array}{cc|cc} + & - & + & - \\ - & + & - & + \\ \hline + & - & + & - \\ - & + & - & + \end{array}\right]$

$$\theta\theta^\dagger = \frac{1}{4}\left[I_4 - \left[\begin{array}{cc|cc} & 1 & & \\ 1 & & & \\ \hline & & & 1 \\ & & 1 & \end{array}\right] + \left[\begin{array}{cc|cc} & & 1 & \\ & & & 1 \\ \hline 1 & & & \\ & 1 & & \end{array}\right] - \left[\begin{array}{cc|cc} & & & 1 \\ & & 1 & \\ \hline & 1 & & \\ 1 & & & \end{array}\right] \right]$$

$$= \frac{1}{4} \sum_{a \in \mathbb{Z}_2^2} (-1)^{a.(01)} D(a,0)$$

Dirac sequence: $\varphi^\dagger = \theta^\dagger H_4 = (0100)$

Rank One Projection Operator: $\varphi\varphi^\dagger = \left[\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$

$$\varphi\varphi^\dagger = \frac{1}{4} \sum_{b \in \mathbb{Z}_2^2} (-1)^{(01).b} D(0,b)$$

Ambiguity Functions and Moyal's Identity

Let θ be a sequence and $P_\theta = \theta\theta^\dagger$ the corresponding projection operator

Ambiguity Function: $A_\theta(a,b) = Tr(D(a,b)P_\theta) = (\theta, D(a,b)\theta)$
More correct to think of $A_\theta(a,b)$ as the ambiguity function of P_θ rather than θ.

$$P_\theta = \theta\theta^\dagger = \frac{1}{N}\sum_{a,b\in\mathbb{Z}_2^m} \overline{A_\theta(a,b)} D(a,b)$$

Moyal's Identity: follows from a simple property of projection operators:

$$Tr(P_\theta P_\varphi) = Tr(\theta\theta^\dagger\varphi\varphi^\dagger) = |(\theta,\varphi)|^2$$

The Weyl Transform then gives

$$|(\theta,\varphi)|^2 = \frac{1}{N}\sum_{a,b\in\mathbb{Z}_2^m} \overline{A_\theta(a,b)} A_\varphi(a,b)$$

and setting $\theta = \varphi$ gives

$$\|\theta\|^4 = \frac{1}{N}\sum_{a,b\in\mathbb{Z}_2^m} \|A_\theta(a,b)|^2$$

Action of the Hadamard Transform on Ambiguity Functions

Example: $\theta^\dagger = \frac{1}{2}(+-+-)$

Ambiguity Function *Weyl Transform*

$$A_\theta(a,b) = \begin{array}{c c}
\left[\begin{array}{cc|cc} & & & \\ & & & \\ \hline & & & \\ + & - & + & - \end{array}\right] & \begin{array}{c} 11 \\ 10 \\ 01 \\ 00 \end{array} \; b \\
\begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} & \\
a &
\end{array}
\qquad
S_\theta(a,b) = \frac{1}{2}\left[\begin{array}{cc|cc} & & & \\ & & & \\ \hline & & & \\ + & - & + & - \end{array}\right]$$

Example: $\varphi^\dagger = \theta^\dagger H_4 = (0100)$

$$A_\varphi(a,b) = \left[\begin{array}{cc|cc} - & & & \\ + & & & \\ \hline - & & & \\ + & & & \end{array}\right]
\qquad
S_\varphi(a,b) = \frac{1}{2}\left[\begin{array}{cc|cc} - & & & \\ + & & & \\ \hline - & & & \\ + & & & \end{array}\right]$$

Action of the Hadamard Transform $\mathbf{H} = \mathbf{H}_{2^m}$

$$\begin{aligned} Tr(D(a,b)H\theta\theta^\dagger H) &= Tr(HD(a,b)H\theta\theta^\dagger) \\ &= (-1)^{a.b}\, Tr(D(b,a)\theta\theta^\dagger) \end{aligned}$$

More Symmetry gives an Ambiguity Function with Smaller Support

Isotropy Subgroup: $H_\theta = \{g \in \mathcal{W}(\mathbb{Z}_2^m)\,|g\theta = c_g\theta\}$

$\mathbf{H_\theta}$ is commutative

$$\begin{aligned} c_{a',b'}c_{a,b}\theta &= D(a',b')D(a,b)\theta \\ &= (-1)^{a'.b+a.b'}D(a,b)D(a',b')\theta \\ &= (-1)^{a'.b+a.b'}c_{a',b'}c_{a,b}\theta \end{aligned}$$

$\mathbf{A_\theta(a,b) = 0}$ unless $\mathbf{D(a,b)}$ commutes with every $\mathbf{D(a',b')}$ in $\mathbf{H_\theta}$

$A_\theta(a,b) = (D(a',b')\theta, D(a,b)D(a',b')\theta) = (\theta, D(a',b')^\dagger D(a,b)D(a',b')\theta)$

Hence $A_\theta(a,b) = (-1)^{a.b'+a'.b}A_\theta(a,b)$

Note: A_θ is unimodular on H_θ

$$A_\theta(a,b)^2 = \theta^\dagger D(a,b)\theta\theta^\dagger D(a,b)\theta = c_{a,b}^2 = (-1)^{a.b}$$

Generating Maximal Commutative Subgroups of $\mathcal{W}(\mathbb{Z}_2^m)$

Consider subgroups containing iI_N, and call subgroups W_1, W_2 disjoint if $W_1 \cap W_2 = \langle iI_N \rangle$

Theorem:

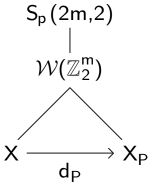
1. Any maximal commutative subgroup disjoint from Z takes the form

$$X_P = \{i^\lambda D(a, aP) | a \in \mathbb{Z}_2^m \text{ and } \lambda \in \mathbb{Z}_4\}$$

   for some binary symmetric matrix P.

2. X_P and X_Q are disjoint if and only if $P - Q$ is nonsingular

Symplectic Group $\mathbf{S_p(2m, 2)}$: all unitary matrices that fix $\mathcal{W}(\mathbb{Z}_2^m)$ by conjugation.



- includes the Hadamard transform H_{2^m}
- acts transitively on disjoint pairs of maximal commutative subgroups
- tool for designing ambiguity functions

Mutually Unbiased Bases

CDMA Wireless Communication: Capacity translates to increasing the number of spreading sequences. Write a new sequence v with $\|v\|^2 = 1$ in terms of the Walsh basis w_i

$$v = \sum_{i=0}^{N-1} \varepsilon_i w_i$$

Since $\sum_{i=0}^{N-1} |\varepsilon_i|^2 = 1$, the average interference is $\frac{1}{N}$.

Theorem: Let A, B be disjoint maxl. comm. subgroups and let $\mathcal{F}_A, \mathcal{F}_B$ be the corresponding orthonormal bases of eigenvectors. If $\theta \in \mathcal{F}_A$ and $\varphi \in \mathcal{F}_B$ then

$$|(\theta, \varphi)| = \frac{1}{\sqrt{N}}$$

Proof (1): Moyal's Identity gives

$$|(\theta, \varphi)|^2 = \frac{1}{N} \sum_{a,b \in \mathbb{Z}_2^m} \overline{A_\theta(a,b)} A_\varphi(a,b) = \frac{1}{N}$$

Proof (2): By transitivity of $S_p(2m, 2)$ we may assume $X = A$ and $Z = B$

Generating Orthonormal Bases of $\mathbb{C}^N$

Remark: One basis for each coset of $RM(1, m+1)$ in $RM(2, m+1)$

$$\begin{array}{lccc}
\text{Maximal Commutative Subgroup} & X & \longrightarrow & X_P = d_P^{-1} X d_P \\
 & | & & | \\
\text{Orthonormal Basis} & H_{2^m} & \longrightarrow & H_{2^m} d_P
\end{array}
\qquad d_P = \mathrm{diag}[i^{vPv^T}]$$

Example: $m = 3$, $P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

$$H_8 = \frac{1}{2\sqrt{2}} \left[\begin{array}{cccc|cccc}
+ & + & + & + & + & + & + & + \\
+ & - & + & - & + & - & + & - \\
+ & + & - & - & + & + & - & - \\
+ & - & - & + & + & - & - & + \\
\hline
+ & + & + & + & - & - & - & - \\
+ & - & + & - & - & + & - & + \\
+ & + & - & - & - & - & + & + \\
+ & - & - & + & - & + & + & -
\end{array}\right]
\quad
d_P = \begin{array}{c}
\left[\begin{array}{cccc|cccc}
1 & & & & & & & \\
 & 1 & & & & & & \\
 & & 1 & & & & & \\
 & & & -1 & & & & \\
\hline
 & & & & i & & & \\
 & & & & & i & & \\
 & & & & & & -i & \\
 & & & & & & & i
\end{array}\right]
\end{array}
\begin{array}{l}
000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111
\end{array}$$

The Geometry of Spreading Sequences

Question: How many vectors can be added to the Walsh basis subject to the condition $|(v, v')|^2 = 0$ or $\frac{1}{N}$ for all vectors v, v'.

Answer: The extremal ensemble is the union of $N + 1$ mutually unbiased bases in $\mathbb{C}^N$

Example ($\mathbf{m = 3}$): Linear space of 8 binary symmetric matrices with the property that all pairwise differences are nonsingular.

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Remark: The extremal ensemble is associated with a $\mathbb{Z}_4$-linear Kerdock code

The Supports of the Associated Ambiguity Functions