Understanding Operator Reed-Muller Code Through the Weyl Transform

Senior Thesis Presentation

Weiyao Wang[1] Mentor: Robert Calderbank[1]

[1]Duke University

April 17

Table of Contents

Table of Contents

Overview: Generalizing Packing Problem

A main problem of the theory of error-correcting codes is the packing problem:

- How to arrange as many points as possible on the surface of a real or complex sphere so that they would be as far apart as possible
- Arranging as many 1-D subspaces in the embedding real or complex space with angle as large as possible

We can generalize the problem to subspaces of dimension higher than 1:

- How to arrange as many M-dimensional subspaces of T-dimensional real or complex space so that they would be as far apart as possible
- Consider packing in Grassmannian space $G(T, M)$

Overview: Motivation

- Generalization of binary Reed-Muller codes to operator Reed-Muller Codes ($N \times N$ Hermitian matrices) based on Heisenberg-Weyl Group
- Weyl Transform:
  - $N \times N$ Hermitian matrices $\rightarrow$ real valued vectors of length N^2
  - Trace Inner Product Space $\rightarrow$ Euclidean Space
  - Isometry

Table of Contents

The Heisenberg-Weyl or Pauli Group HW_N

The Pauli Matrices are

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}, \text{and } Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

A linear operator E of Heisenberg-Weyl Group HW_N ($N = 2^m$) takes the form:

$$E = \alpha e_1 \otimes e_2 \otimes ... \otimes e_m, \text{ where } e_i = I, X, Y, \text{or } Z, \ \alpha = \pm 1, \pm i$$

The Heisenberg-Weyl or Pauli Group HW_N

We define $E_{(a,b)} \in HW_N$ where vectors $(a, b) \in \mathbb{F}_2^{2m}$ indexes the operator:

$$E_{(a,b)} = e_1 \otimes e_2 \otimes ... \otimes e_m$$

where

$$e_i = \begin{cases} I_2, & a_i = 0, b_i = 0 \\ X, & a_i = 1, b_i = 0 \\ Y, & a_i = 1, b_i = 1 \\ Z, & a_i = 0, b_i = 1 \end{cases} \tag{1}$$

The Heisenberg-Weyl or Pauli Group HW_N

These linear operators satisfy the following properties:

- E_v is Hermitian, that is $E_v = E_v^\dagger$
- If $v \neq 0$, we have $Tr(E_v) = 0$; $Tr(E_v E_w) \neq 0$ if and only if $v = w$
- $E_{(a,b)} E_{(a',b')} = (-1)^{a(b')^T \oplus a' b^T} E_{(a',b')} E_{(a,b)}$
  - symplectic inner product:

$$(a, b) * (a', b') = a(b')^T \oplus a' b^T$$

  - $E_{(a,b)} E_{(a',b')}$ commutes if and only if (a, b) and (a', b') are orthogonal with respect to the symplectic inner product (i.e. $(a, b) * (a', b') = 0$)
- Multiplication formula for $E_{(a,b)} E_{(a',b')} = \alpha E_{(a+a',b+b')}$, where $\alpha = i^{a'b - ab'}$

Projection Operators P

$P_{v,\pm 1}$ as the projection matrix of the eigensapces of E_v:

- $P_{v,1} = \frac{1}{2}(I + E_v)$: eigenspace of E_v with eigenvalue 1
- $P_{v,-1} = \frac{1}{2}(I - E_v)$ eigenspace of E_v with eigenvalue -1.

Define projection operators $P_{S,\epsilon}$:

- S is a k-dimensional commutative group generated by E_{a_j,b_j}, $j = 1, ..., k$ (i.e. $S = \langle E_{(a_j,b_j)} | i = 1, ..., k \rangle$)
- $\epsilon = (\epsilon_1, ..., \epsilon_k)$, where $\epsilon_i = \pm 1, i = 1, ..., k$

$$P_{S,\epsilon} = \frac{1}{2^k} \Pi_{j=1}^{k} (I + \epsilon_j E_{a_j,b_j}), \ E_{a_j,b_j} \in S$$

- $\| P_{S,\epsilon} \|_F^2 = 2^{m-k}$

Example of P

Let $v_1 = (0, 0, 1|0, 1, 1)$, the corresponding operator is $P_{v_1,I} = \frac{1}{2}(I + I \otimes Z \otimes Y)$:

$$P_{v_1,1} = \begin{bmatrix} 0.5 & 0.5i & & & & & & \\ -0.5i & 0.5 & & & & & & \\ & & 0.5 & -0.5i & & & & \\ & & 0.5i & 0.5 & & & & \\ & & & & 0.5 & 0.5i & & \\ & & & & -0.5i & 0.5 & & \\ & & & & & & 0.5 & -0.5i \\ & & & & & & 0.5i & 0.5 \end{bmatrix}$$

Further let $v_2 = (0, 1, 0|1, 0, 1)$ and $v_3 = (1, 0, 0|0, 1, 0)$.
Note: $P_{v_1,1}$, $P_{v_2,1}$ and $P_{v_3,1}$ can be simultaneously diagonalized, with diagonal entries as $(0, 0, 0, 0, 1, 1, 1, 1)$, $(0, 0, 1, 1, 0, 0, 1, 1)$, and $(0, 1, 0, 1, 0, 1, 0, 1)$. They are first-order binary Reed-Muller codewords.

Projection Operators P

- Commuting operation $\oplus$ between two commuting operators P, P':

$$P \oplus P' = P + P' - 2PP'$$

- Distance between the subspaces defined by P_1 and P_2 (Frobenius Norm):

$$d(P_1, P_2)^2 = Tr(P_1) + Tr(P_2) - 2\,Tr(P_1 P_2)$$

Operator Reed-Muller Code

Let $G = \{v_1, ..., v_m\}, v_i \in \mathbb{F}_2^{2m}$ be a set of pairwise orthogonal and linearly independent binary vectors with respect to the symplectic inner product. Define operators $\{P_{v,\lambda}\}$ as follows:

$$P_{v,\lambda} = \frac{1}{2}(I_{2^m} + \lambda E_v), \ \lambda = \pm 1, \text{ where } v \in G$$

The operator Reed-Muller code $O - RM(r, m)$:

- The commutative set of all operators P associated with boolean functions f of degree at most r with m inputs
- Inputs x_i for the boolean function are replaced by projection operators in $\{P_{v,\lambda}\}$
- Multiplication in f is replaced by operator multiplication
- Binary addition is replaced by $\oplus$

Distance Spectrum of $O - RM(r, m)$

- Let $B_t(P') = |\{P \in O - RM(r, m) : d(P, P')^2 = t\}|$ for $P' \in O - RM(r, m)$, the cardinality of the set of operator Reed-Muller codes with distance $\sqrt{t}$ to P'.
- The $B_t(P')$'s for all possible t describes the distance spectrum of P'
- **Theorem:** For any $Q, Q' \in O - RM(r, m)$, $B_t(Q) = B_t(Q')$.
- The Theorem implies that the distance spectrum is invariant with respect to operator code

The Weyl Transform

- **Lemma:** The matrices $\frac{1}{2^{\frac{m}{2}}} E_{(a,b)}$ form an orthonormal basis for the real vector space of $N \times N$ ($N = 2^m$) Hermitian matrices with respect to the trace inner product.
- Any Hermitian linear operator S can be written as a linear combination of projection operators $E_{(a,b)}$ as follows:

$$S = \sum_{(a,b) \in \mathbb{F}_2^{2m}} S(a,b) \frac{1}{2^{\frac{m}{2}}} E_{(a,b)} \tag{2}$$

  $S(a,b) = \frac{1}{2^{\frac{m}{2}}} Tr(E_{(a,b)} S)$, the Weyl Transform of S at index (a,b).
- The Weyl transform of S is a vector of length 2^{2m}, where index i (counting from left to right) has value $S(a,b)$ such that (a,b) is the binary representation of integer i.
- It is an **isometry** between the Trace Inner Product Space of Hermitian Vectors and the Euclidean Space.

Table of Contents

First Order Operator Code $O - RM(1, m)$

- Let C be the linear subspace generated by $G = \{v_1, ..., v_m\}$.
- $P \in O - RM(1, m)$ has the form $\oplus P_{v_i, \pm 1}$: it is a linear combination of the set $\{P_0, P_{v_1}, ..., P_{v_m}\}$
- The cardinality of $O - RM(1, m)$, $|O - RM(1, m)| = 2^{2m+1}$
- P is either $P_{v,1}$ or $P_{v,-1}$, where $v \in C$ because

$$P_{v_1, \pm 1} \oplus P_{v_2, \pm 1} = P_{v_1 + v_2, \pm 1}, \ v_1 + v_2 \in C$$

The Weyl Transform of $O - RM(1, m)$

- The Weyl transform of $P_{v,1} = \frac{1}{2}(I + E_v)$, $v \neq 0$ is

$$(2^{\frac{m}{2}-1}, 0, ...0, 2^{\frac{m}{2}-1}, 0, ..., 0)$$

  where the second non-zero element is at index v.
- The Weyl transform of $P_{v,-1} = \frac{1}{2}(I - E_v)$, $v \neq 0$ is

$$(2^{\frac{m}{2}-1}, 0, ...0, -2^{\frac{m}{2}-1}, 0, ..., 0)$$

- The Weyl transform is $(2^{\frac{m}{2}}, 0, ..., 0)$ for $P_{\mathbf{0},1}$ and $\mathbf{0}$ for $P_{\mathbf{0},-1}$

Distance Spectrum of $O - RM(1, m)$

Theorem: For any $P \in O - RM(1, m)$, we have

$$B_0(P) = 1, B_{2^m}(P) = 1, B_{2^{m-1}}(P) = 2^{2m+1} - 2$$

Proof: By invariance of distance spectrum, let $P = P_{0,-1} = \mathbf{0}$; consider $P' = P_{v',\lambda'}$. Let $W(\cdot)$ denotes the Weyl Transform. Then $d(\mathbf{0}, P') = \| W(P') \|$

- $v' = 0$, $\lambda' = 1$. $W(P') = (2^{\frac{m}{2}}, 0, ..., 0)$. $\| W(P') \|^2 = 2^m$.
- $v' = 0$, $\lambda' = -1$. $P' = P$. $\| W(P') \|^2 = 0$.
- $v' \neq \mathbf{0}$. $W(P') = (2^{\frac{m}{2}-1}, 0, ...0, \pm 2^{\frac{m}{2}-1}, 0, ..., 0)$. $\| W(P') \|^2 = 2^{m-2} + 2^{m-2} = 2^{m-1}$.

Decoding $O - RM(1, m)$

Decoding $O - RM(1, m)$ is equivalent to: Given a perturbed operator X (X is perturbed from some $P_{(a,b),\lambda} \in O - RM(1, m)$), we need to recover the projection operator $P_{(a,b),\lambda}$ such that

$$P_{(a,b),\lambda} = argmin_{\lambda=\pm 1, a,b \in F_2^{2m}} \parallel P_{(a,b),\lambda} - XX^\dagger \parallel_F$$

The isometric property of Weyl Transform $\rightarrow$ decoding is equivalent to

$$P_{(a,b),\lambda} = argmin_{\lambda=\pm 1, a,b \in F_2^{2m}} \parallel W(P_{(a,b),\lambda}) - W(XX^\dagger) \parallel$$

Decoding Objective: find the largest index of $W(XX^\dagger)$ in absolute value (first index needs to subtract $2^{\frac{m}{2}-1}$)

Decoding Algorithm of $O - RM(1, m)$

Algorithm 1: New Decoding Algorithm of $O - RM(1, m)$

Given perturbed input X ;
Compute $XX^\dagger$;
for $(a, b) \in \mathbb{F}_2^{2m}$ **do**
    Compute $Tr(XX^\dagger E_{(a,b)})$ as the Weyl transform of X at index (a, b) ;
end
Find the largest index in terms of absolute value in the Weyl transform computed before (first index subtract $2^{\frac{m}{2}-1}$), record it at index (a^*, b^*), and its sign e ;
Output $P = \frac{1}{2}(I + eE_{(a,b)})$;

Time Complexity: Total: $O(2^{3m}) + 2^{2m}O(2^m) = O(2^{3m})$

- $O(2^{3m})$ for $XX^\dagger$
- $O(2^m)$ for $Tr(XX^\dagger E_{(a,b)})$ since $E_{(a,b)}$ is sparse; total 2^{2m} times

Table of Contents

Dickson's Theorem in From Binary Code

Binary Reed-Muller Codes $RM(2, m)$ are generated by boolean functions of degree ≤ 2 with m inputs $x_1, ..., x_m$, $x \in \mathbb{F}_2^n$:

$$\sum_{i,j=1,i\leq j}^{m} q_{ij}x_ix_j + \sum_{i=1}^{m} l_ix_i + \epsilon = xQx^T + Lx + \epsilon$$

Traditionally, Dickson's Theorem provides a normal form for quadratic functions:

Theorem: Let $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$ be a quadratic function with the symmetric matrix B of rank $2t$. There exists an affine transformation s, so that $f \circ s$ has one of the following algebraic forms:

1. $y_1y_2 \oplus y_3y_4 \oplus ... \oplus y_{2t-1}y_{2t}$
2. $y_1y_2 \oplus y_3y_4 \oplus ... \oplus y_{2t-1}y_{2t} + 1$
3. $y_1y_2 \oplus y_3y_4 \oplus ... \oplus y_{2t-1}y_{2t} \oplus y_{2t+1}$

Classifying $O - RM(2, m)$

Theorem: Let $\{P_{v_1}, ..., P_{v_m}\}$ be the input operators of boolean functions with degree ≤ 2 that generate $O - RM(2, m)$. Let C be the linear subspace generated by $\{v_1, ..., v_m\}$. Each operator code $P \in O - RM(2, m)$ belong to one of the following three categories:

1. $\oplus_{k=1}^{M} P_{a_k} P_{b_k}$
2. $(\oplus_{k=1}^{M} P_{a_k} P_{b_k}) \oplus P_c$
3. $(\oplus_{k=1}^{M} P_{a_k} P_{b_k}) \oplus I$

where $\{a_1, ..., a_M, b_1, ..., b_M, c\} \subset C$ is linearly independent

Classifying $O - RM(2, m)$

Proof Intuition:

- Observe: $P_a P_b = P_a P_{a+b} = P_b P_{a+b}$
- Generalize: $P_a P_b \oplus P_c P_d = P_{a+c} P_b \oplus P_c P_{b+d}$
- Generalize: Any $\oplus_{i=1}^{r} P_{a_r} P_{b_r}$ can be re-written as $P_{a_1'} P_{b_1'} \oplus_{i=2}^{r} P_{a_i} P_{b_i}$ for any $a_1' \in span(\{a_i, b_i\})$

Given any $\oplus_{i=1}^{r} P_{a_i} P_{b_i}$, if $\{a_i, b_i\}$ not independent, we can reduce the sum by 1: eg. $a_r = \oplus_{i=1}^{r-1} a_i$,

$$\oplus_{i=1}^{r} P_{a_i} P_{b_i} = P_{a_r} P_{b_1'} (\oplus_{i=2}^{r-1} P_{a_i'} P_{b_i'}) \oplus P_{a_r} P_{b_r} = P_{a_r} P_{b_1'+b_r} (\oplus_{i=2}^{r-1} P_{a_i'} P_{b_i'})$$

The process will terminate when the operators are "irreducible"

The Weyl Transform of $O - RM(2, m)$

1. $\oplus_{k=1}^{M} P_{a_k} P_{b_k}$:
   - Index 0: $\frac{2^M - 1}{2^{M+1-\frac{m}{2}}}$
   - Index $v \in span(\{a_k, b_k\})$: $\pm \frac{1}{2^{M+1-\frac{m}{2}}}$
2. $(\oplus_{k=1}^{M} P_{a_k} P_{b_k}) \oplus P_c$:
   - Index 0: $\frac{1}{2^{1-\frac{m}{2}}}$
   - Index $c + v$, $v \in span(\{a_k, b_k\})$: $\pm \frac{1}{2^{M+1-\frac{m}{2}}}$
3. $(\oplus_{k=1}^{M} P_{a_k} P_{b_k}) \oplus I$
   - Index 0: $\frac{2^M + 1}{2^{M+1-\frac{m}{2}}}$
   - Index $v \in span(\{a_k, b_k\})$: $\pm \frac{1}{2^{M+1-\frac{m}{2}}}$

Distance Spectrum of $O - RM(2, m)$

Invariance of Distance Spectrum $\rightarrow$ Fix $\mathbf{0}$ $\rightarrow$ Computing Euclidean Norm of the Weyl Transform

Theorem: Given $O - RM(2, m)$ and a fixed M, the number of operator codes are given as follows:

1. Case One: $\oplus_{k=1}^{M} P_{a_k} P_{b_k}$: $f(M)g(m, M)2^{2M}$; distance $t^2 = \frac{2^{M+m} - 2^m}{2^{M+1}}$
2. Case Two: $(\oplus_{k=1}^{M} P_{a_k} P_{b_k}) \oplus P_c$: $g(m, M)f(M)2^{2M}(2^{m-2M+1} - 2)$; distance $t^2 = 2^{m-1}$
3. Case Three: $(\oplus_{k=1}^{M} P_{a_k} P_{b_k}) \oplus I$: $\oplus_{k=1}^{M} P_{a_k} P_{b_k}$: $f(M)g(m, M)2^{2M}$; distance $t^2 = \frac{2^{M+m} + 2^m}{2^{M+1}}$

where $g(m, M) = \frac{\Pi_{i=0}^{2M-1}(2^m - 2^i)}{\Pi_{i=0}^{2M-1}(2^{2M} - 2^i)}$ and $f(M) = 2^{M(M-1)}(\Pi_{i=1}^{M}(2^{2i-1} - 1))$

Table of Contents

Sign Patterns

Theorem: Let $O = \sum_{(a,b)\in S} \epsilon_{a,b} E(a,b)$, where S is a $k - dim$ isotropic subspace with respect to the symplectic inner product. Suppose $S = \langle (a_i, b_i) | i = 1, ..., k \rangle$. Then

$$\epsilon_{(a+c,b+d)} = \epsilon_{(a,b)}\epsilon_{(c,d)}(i^{ad^T - bc^T})$$

for all $0 \neq (a,b),(c,d) \in S$ if and only if

$$O = \Pi_{i=1}^{k}(I_N + \epsilon_{(a_i,b_i)} E_{(a_i,b_i)})$$

for any basis $\{(a_1,b_1), ..., (a_k,b_k)\}$ of S.

Acknowledgment

This paper is based on my independent research studies conducted under the mentorship of my academic adviser Dr. Robert Calderbank. I thank Dr. Calderbank for his great help bringing me into the field of algebra and error-correction codes and his continuous and insightful inputs to the project overall. I also thank Dr. Jungsang Kim for his great lectures about quantum information theory. Special thanks to Dr. David Kraines and Dr. Leslie Saper for their help in general during my path to my research and degree in mathematics.