DUKE UNIVERSITY

Understanding Operator Reed-Muller Codes Through the Weyl Transform

by

Weiyao Wang

A thesis submitted to in partial fulfillment of the requirements for graduating with distinction in the Department of Mathematics degree of Duke University

Department of Mathematics, Duke University, Durham, North Carolina

2018

DUKE UNIVERSITY

Abstract

This paper expands the framework on the multidimensional generalizations of binary Reed-Muller code, operator Reed-Muller codes, where the codewords are projection operators through the Weyl Transform. The Weyl Transform of these operator Reed-Muller codes maps the operators to vectors, and it is isometric. This nice property gives new proofs for some known results and produce a simpler decoding algorithm. In particular, the property provides a different framework to analyze the distance spectrum of second operator Reed-Muller codes without using the Dickson's Theorem.

Acknowledgements

This paper is based on my independent research studies conducted under the mentorship of my academic advisor Dr. Robert Calderbank. The works in this paper are collaborative work of me and my advisor.

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. He is always willing to spend lots of time discussing problems with me, even on weekends. I am deeply inspired by the passions and attitude he has towards researches, teaching and mentorship during my time at Duke. I cannot hope for a better advisor.

I thank Dr. Jungsang Kim for his great lectures about quantum information theory. I learned a lot of background knowledge of the project from his lectures.

I also thank Dr. David Kraines and Dr. Leslie Saper for their help in general during my path to my research and degree in mathematics.

Special thanks to my thesis committee members: Dr. Calderbank and Dr. Kraines.

Finally, I thank my parents for their continuous support during my life and my studies.

Contents

Chapter 1

Background Introduction

A central problem in coding theory is how to pack as many points as possible on a real or complex surface so that they are most equally spread. There is literature on finding good packings ([SS98]), and literature on finding upper bounds on the size of packings. One can reformulate the problem as packing 1-dimensional subspaces by connecting points to the origin and use the angles of the line as measure of distance ([CSB87]). Finding a good packing then becomes finding as many subspaces as possible with angles between them as large as possible.

It is natural to generalize the packing problem to higher dimensions: we might consider arranging M-dimensional subspaces in T-dimensional real or complex space so that they are far from each other with respect to some defined metric. The set of M-dimensional subspaces of T-dimensional space forms the Grassmannian space $G(T, M)$, and we may consider packings in this space. Such packing problems have broad applications in wireless communications, statistics as well as quantum information theory. In particular, quantum error correcting codes are eigenspaces of commutative subgroups of the Heisenberg-Weyl group.

[AC10] gives several constructions of Grassmannian packings in the complex space, and generalizes the binary Reed-Muller codes to operator codes based on Heisenberg-Weyl (HW_N). Based on the theory developed in [AC10], we hope to have a deeper understanding by looking at them in a different way through the perspective of the Weyl Transform, which is an isometry between two inner product spaces. The first is $N \times N$ Hermitian matrices with the trace inner product, and the second is real valued vectors of length N^2 with the standard Euclidean inner product. Highly symmetric collections of matrices map to vectors that are highly sparse (few nonzero entries) in the Weyl transform. The collections of matrices constructed in [AC10] are highly symmetric, and we will show that it is possible to infer their properties from the Weyl transform.

In this paper, we will derive properties of the first and second order operator Reed-Muller code, then conjecture properties of higher order codes, using the intuition built up from the first and second order codes. We will use the Weyl transform to provide simple proofs for results presented in [AC10]. We also provide a simpler decoding algorithm for the first order operator Reed-Muller codes and derive the distance spectrum for the second order operator Reed-Muller codes. We start by reviewing the construction of the Heisenberg-Weyl group.

1.1 The Heisenberg-Weyl or Pauli Group

1.1.1 Pauli Matrices

The Pauli Matrices are

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

1.1.2 The Heisenberg-Weyl Group

The Heisenberg-Weyl Group HW_N ($N = 2^m$) is defined by m-fold Kronecker products of $I, X, Y,$ and Z with coefficients in $1, -1, i, -i$. The group is important in the construction of quantum error-correction codes given by [AK01] and [CRSS97].

A linear operator $E \in HW_N$ takes the following 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 center of the group is thus $\mathcal{Z} = \{I_{2^m}, -I_{2^m}, iI_{2^m}, -iI_{2^m}\}$, and the quotient group $\bar{\mathcal{E}} = \mathcal{E}/\mathcal{Z}$ is isomorphic to the binary vector space $\mathbb{F}_2^{2m}$. The isomorphism is given by indexing $E \in \bar{\mathcal{E}}$ with vectors $(a, b) \in \mathbb{F}_2^{2m}$ such that:

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

where

$$e_i = \begin{cases} I_2, \ a_i = 0, b_i = 0 \\ X, \ a_i = 1, b_i = 0 \\ Y, \ a_i = 1, b_i = 1 \\ Z, \ a_i = 0, b_i = 1 \end{cases} \tag{1.1}$$

1.1.3 Properties of Operators in the Heisenberg-Weyl Group

These linear operators $E_v \in \bar{\mathcal{E}}$ satisfy the following properties:

1. E_v is Hermitian, that is $E_v = E_v^\dagger$
2. If $v \neq 0$, we have $Tr(E_v) = 0$
3. From Property 2, it is not difficult to show that $Tr(E_v E_w) \neq 0$ if and only if $v = w$.
4. Since $Y = iXZ$, $E_{(a,b)} = i^{ab} E_{(a,0)} E_{(0,b)}$.
5. $E_{(a,b)} E_{(a',b')} = (-1)^{ab'+a'b} E_{(a',b')} E_{(a,b)}$, which describes the commutativity of the operators.
6. Using the property of Kronecker product that $(A \otimes B)(C \otimes D) = AC \otimes BD$ and Property 4, we derive the multiplication formula for $E_{(a,b)} E_{(a',b')} = \alpha E_{(a+a',b+b')}$, where $\alpha = i^{a'b-ab'}$.
7. Combining Property 5 and Property 6, if E_v and E_w commute, then $E_v E_w = \pm E_{v+w}$; if they anti-commute, we have $E_v E_W = \pm i E_{v+w}$.

From Property 5, the commutativity of operators is determined by the symplectic inner product $(a, b) * (a', b') = ab' \oplus ba'$. It is easy to verify that $E_{(a,b)} E_{(a',b')}$ commutes if and only if (a, b) and (a', b') are orthogonal with respect to the symplectic inner product (i.e. $(a, b) * (a', b') = 0$).

1.2 Projection Operators P_v of E_v

1.2.1 Constructions of P_v

We define the projection matrices for the eigenspaces of E_v: $P_{v,1} = \frac{1}{2}(I + E_v)$ for the eigenspace of E_v with eigenvalue 1 and $P_{v,-1} = \frac{1}{2}(I - E_v)$ for the eigenspace of E_v with

eigenvalue -1. It is easy to verify that such projection operators P_v satisfy the properties of projection operators (i.e. $P_v P_v = P_v$) by the properties of E_v in the previous section.

We further define projection operators $P_{S,\epsilon}$, such that S is a k-dimensional commutative group generated by E_{a_j,b_j}, $j = 1, ..., k$ (i.e. $S = \langle E_{(a_j,b_j)} | i = 1, ..., k \rangle$) and $\epsilon = (\epsilon_1, ..., \epsilon_k)$, where $\epsilon_i = \pm 1, i = 1, ..., k$. Define

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

1.2.2 Properties of P_v

Lemma 1.1. *The operators $P_{S,\epsilon}$ satisfy:*

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

Proof. Since $E_{(a_i,b_i)}$ and $E_{(a_j,b_j)}$ commute, we can show that $(I + \epsilon_i E_{(a_i,b_i)})$ and $(I + \epsilon_j E_{(a_j,b_j)})$ commute.

$$\begin{aligned}(I + \epsilon_i E_{(a_i,b_i)})(I + \epsilon_j E_{(a_j,b_j)}) &= I + \epsilon_j E_{(a_j,b_j)} + \epsilon_i E_{(a_i,b_i)} + \epsilon_i \epsilon_j E_{(a_i,b_i)} E_{(a_j,b_j)} \\ &= I + E_{(a_j,b_j)} + \epsilon_i E_{(a_i,b_i)} + \epsilon_i \epsilon_j E_{(a_j,b_j)} E_{(a_i,b_i)} \\ &= (I + \epsilon_j E_{(a_j,b_j)})(I + \epsilon_i E_{(a_i,b_i)})\end{aligned}$$

Then, we show that $(I + \epsilon_i E(a_i, b_i))^2 = 2(I + \epsilon_i E(a_i, b_i))$.

$$\begin{aligned}(I + \epsilon_i E_{(a_i,b_i)})^2 &= I + 2\epsilon_i E_{(a_i,b_i)} + E_{(a_i,b_i)}^2 \\ &= I + 2\epsilon_i E_{(a_i,b_i)} + I \\ &= 2(I + \epsilon_i E_{(a_i,b_i)})\end{aligned}$$

Finally, we show $P_{S,\epsilon}^2 = P_{S,\epsilon}$:

$$\begin{aligned}P_{S,\epsilon}^2 &= (\frac{1}{2^k} \Pi_{j=1}^{k} (I + \epsilon_j E_{(a_j,b_j)}))^2 \\ &= \frac{1}{2^k} \Pi_{j=1}^{k} \frac{1}{2} (2(I + \epsilon_j E_{(a_j,b_j)}) \\ &= \frac{1}{2^k} \Pi_{j=1}^{k} (I + \epsilon_j E_{(a_j,b_j)}) \\ &= P_{S,\epsilon}\end{aligned} \tag{1.2}$$

Next we prove $\| P_{C,\epsilon} \|_F^2 = 2^{m-k}$:

$$\begin{aligned} Tr(P_{S,\epsilon}) &= \frac{1}{2^k} Tr(I + \sum_{g \in S} \epsilon_g g) \\ &= \frac{1}{2^k} (Tr(I) + \sum_{g \in S} \epsilon_g Tr(g)) \quad (1.3) \\ &= \frac{1}{2^k} Tr(I) + 0 \quad (1.4) \\ &= 2^{m-k} \end{aligned}$$

(1.3) is true due to linearity of the trace operator. (1.4) is true since each $g \in S$ can be written in a unique product of $E_{(a_j,b_j)}$, the generators of S. By Property 3 in 1.1.3, $E_{(a,b)}$ are orthogonal with respect to the trace inner product, and the product of $E_{(a,b)}$ is again an element of HW_N up to some coefficients. For the terms $S \in C$ where $g = E_{(a_j,b_j)}$ is a generator, $Tr(E_{(a_j,b_j)}) = 0$, thus making the sum $(\sum_{g \in S} \epsilon_g Tr(g))$ zero.

Therefore, $\|P_{S,\epsilon}\|_F^2 = Tr(P_{S,\epsilon}^\dagger P_{S,\epsilon}) = Tr(P_{S,\epsilon} P_{S,\epsilon}) = Tr(P_{S,\epsilon}) = 2^{m-k}$

□

1.2.3 Addition Operation $\oplus$ of P_v

Before we introduce the operator Reed-Muller code, we define a commuting operation $\oplus$ between two commuting operators P, P' as follows:

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

The idea to use Boolean logic for commuting operators came from [AC05] and [ACK06]. This definition follows naturally from the fact that two commuting projection operators P and P' can be simultaneously diagonalized, and thus $\oplus$ defined above is equivalent to modulo 2 summation of the diagonal entries of P and P'. This is useful because Theorem 1 in [AC10] states that after diagonalization the diagonal entries of P form a binary Reed-Muller code, and therefore $P \oplus P'$ is equivalent to the modulo 2 sum of the two corresponding binary codes.

Example 1.2.1. Consider $v_1 = (0,0,1,0,1,1)$, $v_2 = (0,1,0,1,0,1)$, and $v_3 = (1,0,0,0,1,0)$. They are linearly independent and pairwise orthogonal with respect to symplectic inner

product. Their corresponding operator codes are given by:

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

$$P_{v_2,1} = \begin{bmatrix} 0.5 & & 0.5 & & & & & \\ & 0.5 & & -0.5 & & & & \\ 0.5 & & 0.5 & & & & & \\ & -0.5 & & 0.5 & & & & \\ & & & & 0.5 & & -0.5 & \\ & & & & & 0.5 & & 0.5 \\ & & & & -0.5 & & 0.5 & \\ & & & & & 0.5 & & 0.5 \end{bmatrix}$$

$$P_{v_3,1} = \begin{bmatrix} 0.5 & & & & 0.5 & & & \\ & 0.5 & & & & 0.5 & & \\ & & 0.5 & & & & -0.5 & \\ & & & 0.5 & & & & -0.5 \\ 0.5 & & & & 0.5 & & & \\ & 0.5 & & & & 0.5 & & \\ & & -0.5 & & & & 0.5 & \\ & & & -0.5 & & & & 0.5 \end{bmatrix}$$

The three matrices $P_{v_1,1}$, $P_{v_2,1}$ 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 $(0,1,0,1,0,1,0,1)$. These are also binary Reed-Muller codewords.

It is easy to verify that $\oplus$ is commutative and $P \oplus P'$ is a projection operator. This operation is important for constructing the operator Reed-Muller codes.

1.2.4 Distance Between Two Operators

Following [AC10], we give a slightly different version of chordal distance to measure the distance between two subspaces Q_1, Q_2 defined in [CHS96]. Given the projection

operators P_1, P_2 for the two subspaces, the distance $d(Q_1, Q_2)$ is given by the following definition:

$$d(Q_1, Q_2)^2 = d(P_1, P_2)^2 = Tr(P_1) + Tr(P_2) - 2Tr(P_1 P_2) \tag{1.5}$$

Since P_1 and P_2 are Hermitian from 1.1.3, $d(P_1, P_2)$ is a real number.

1.3 Operator Reed-Muller Code

We follow the construction of the operator Reed-Muller codes given by [AC10] using boolean functions. 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 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 $O - RM(r, m)$ is the set of all operators P associated with boolean functions f of degree at most r with m inputs. The inputs x_i for the boolean function are replaced by projection operators defined in 1.2. Multiplication in f is replaced by operator multiplication, and the binary addition is replaced by $\oplus$ defined in 1.2.3. It follows from 1.1.3 that these operators commute with each other with respect both to multiplication and addition.

1.4 The Weyl Transform

The Weyl transform represents a Hermitian operator in terms of an orthonormal basis with respect to the trace inner product:

Lemma 1.2. *The matrices $\frac{1}{2^{\frac{m}{2}}} E_{(a,b)}$, where $E_{(a,b)} \in \bar{\mathcal{E}}_m$ ($(a, b) \in \mathbb{F}_2^{2m}$), 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.*

Proof. First, we prove that each such operator $\frac{1}{2^{\frac{m}{2}}} E_{(a,b)}$ is unitary. Since $E_{(a,b)}$ is Hermitian,

$$Tr(\frac{1}{2^{\frac{m}{2}}}E_{(a,b)}(\frac{1}{2^{\frac{m}{2}}}E_{(a,b)})^{\dagger}) = Tr(\frac{1}{2^m}I) = 1$$

Second, the operators are orthogonal, that is $Tr(\frac{1}{2^{\frac{m}{2}}}E_{(a,b)}\frac{1}{2^{\frac{m}{2}}}E_{(a',b')}) \neq 0$ if and only if $(a,b) = (a',b')$. Since $E_{(a,b)}E_{(a',b')} = i^{a'b-ab'}E(a+a', b+b')$, $Tr(a+a', b+b') \neq 0$ if and only if $(a+a', b+b') = 0$, which is equivalent to $(a,b) = (a',b')$.

Since the operators are unitary and orthogonal, they form an orthonormal set.

The dimension of the Hermitian operators is 2^{2m}, which is the same as the set of all operators of the form $\frac{1}{2^{\frac{m}{2}}}E_{(a,b)}$. Since each operator is Hermitian and the set of the operators is linearly independent, the set forms an orthonormal basis for the Hermitian operators. □

Lemma 1.2 implies that any Hermitian linear operator S can be written as a linear combination of projection operators $E_{(a,b)}$ as follows:

$$\begin{aligned} S &= \sum_{(a,b)\in\mathbb{F}_2^{2m}} [\frac{1}{2^{\frac{m}{2}}}Tr(E_{(a,b)}S)](\frac{1}{2^{\frac{m}{2}}}E_{(a,b)}) \\ &= \sum_{(a,b)\in\mathbb{F}_2^{2m}} S(a,b)\frac{1}{2^{\frac{m}{2}}}E_{(a,b)} \end{aligned} \tag{1.6}$$

where $S(a,b) = \frac{1}{2^{\frac{m}{2}}}Tr(E_{(a,b)}S)$.

Equation 1.6 defines the Weyl Transform of S at index (a,b). Therefore, 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.

The following corollary summarizes the above discussion:

Corollary 1.3. *Weyl transform is an isometry between Hermitian matrices with respect to the Frobenius norm (defined in equation (1.5)) and* $\mathbb{R}^{2^{2m}}$ *with respect to the Euclidean norm.*

Since the operator Reed-Muller codes defined in 1.3 are Hermitian, we would like to consider their Weyl Transforms and understand their properties through their Weyl Transforms in the Euclidean space.

Chapter 2

Invariant Distance Spectrum of Operator Reed-Muller Codes

Let $B_t(P') = |\{P \in O - RM(r,m) : d(P,P')^2 = t\}|$ for $P' \in O - RM(r,m)$, the set of operator Reed-Muller codes with distance $\sqrt{t}$ to P'. We use this set to characterize the distance spectrum for operator Reed-Muller codes:

Lemma 2.1. *Fix any $P \in O-RM(r,m)$. The map $\pi_p : O-RM(r,m) \to O-RM(r,m)$, defined by $\pi_P(P') = P' \oplus P$, is a bijection.*

Proof. The proof follows from the fact that $\pi_P(\pi_P(P')) = P'$, since $P' \oplus P \oplus P = P'$. □

Lemma 2.1 implies that π is a permutation map.

Lemma 2.2. *For any $P \in O - RM(r,m)$, $\forall t, B_t(P) = B_t(0)$.*

Proof. Fix any $P' \in O - RM(r,m)$,

$$\begin{aligned} \| P, P' \|_F^2 &= Tr(P) + Tr(P') - 2Tr(PP') \\ &= Tr(P \oplus P') \\ &= Tr(P \oplus P') + Tr(0) - 2Tr(0) \\ &= \| P \oplus P', 0 \|_F^2 \end{aligned}$$

Therefore, the distance of P to any other operator code P' is the distance of 0 to any $P' \oplus P$.

In addition, $P \oplus P = 0$. Thus, π_P defined in lemma 2.1 permutes $O - RM(r,m)$ and send P to 0. The distance spectrum of P is essentially the distance spectrum of 0

in $\pi_P(O - RM(r,m))$. By lemma 2.1, $f(O - RM(r,m)) = O - RM(r,m)$, and thus, $B_t(P) = B_t(0)$ for any P. □

Lemma 2.2 implies that for $P \in O - RM(r,m)$, the size of the set with a given distances does not depend on the choice of P. Therefore, the distance spectrum of operator Reed-Muller codes is invariant for all operator codes.

Theorem 2.3. *For any* $Q, Q' \in O - RM(r,m)$, $B_t(Q) = B_t(Q')$.

Chapter 3

First Order Operator Reed-Muller Code

In this chapter, we describe and analyze the first order operator Reed-Muller code $O - RM(1, m)$ by their Weyl transforms. Section 3.1 calculates the explicit form of the Weyl transform of the first order operator codes. Section 3.2 calculates the distance spectrum using the Weyl transforms in Section 3.1. Section 3.3 and 3.4 digresses a little to give alternative proofs of some known result using induction, which comes from the intuition built from 3.1 and 3.2. Section 3.5 applies the Weyl transform and gives a simpler decoding algorithm.

3.1 Weyl Transform of the First Order Operator Reed-Muller Code O-RM(1,m)

Let C be the linear subspace generated by G. Then every operator in $O - RM(1, m)$ is either $P_{v,1}$ or $P_{v,-1}$, where $v \in C$ because $P_{v_1,1} \oplus P_{v_2,1} = P_{v_1+v_2,\pm 1}$ and $v_1 + v_2 \in C$. The Weyl transform of $P_{v,1}$, $v \neq 0$ takes the form

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

where the second non-zero element is at index i whose binary representation is v. Similarly the Weyl transform of $P_{v,-1}$ takes the form

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

Additionally, if $v = 0$, the Weyl transform is $(2^{\frac{m}{2}}, 0, ..., 0)$ for $P_{\mathbf{0},1}$ and $\mathbf{0}$ for $P_{\mathbf{0},-1}$.

3.2 The Distance Spectrum by The Weyl Transform

We use the distance of the Weyl transforms in Euclidean space to derive the distance spectrum of $O - RM(1, m)$

Theorem 3.1. *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. Using Theorem 2.3, we only need to consider the case when $P = P_{0,-1} = 0$, the matrix with all zero entries.

Consider any non-trivial projection matrix $P' = \frac{1}{2}(I + \lambda E_v)$ where $v \neq 0$, the Weyl transform of P' is a vector w, with value $\pm 2^{\frac{m}{2}-1}$ on v's coordinate and $2^{\frac{m}{2}-1}$ on 0 coordinate.

Since the Weyl transform is isometric to the operator norm (equation (1.5)) by Corollary 1.3, the distance between P and P' is equal to the Euclidean distance between 0 and w, which is just the norm of w. Therefore, the distance squared is 2^{m-1}. There are $2^{2m+1} - 2$ such nontrivial projection operators (i.e. $P_v, v \neq 0$).

Consider the case for $P_{v,e}$ when $v = 0$, the Weyl transform w would be 0 if $e = -1$ and $(2^{\frac{m}{2}}, 0, .., 0)$ if $e = 1$. Therefore, the Euclidean distance squared between w and 0 would be 0 and 2^m respectively.

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

3.3 The Principal Angles Between Subspaces

The Heisenberg-Weyl Group can be defined inductively as in [SS98] and section 1.1, and we may use this construction to determine principal angles between subspaces determined by the projection operators in $O - RM(1, m)$.

Let $P_1 = \frac{1}{2}(I_{2^m} + E_{v_1}) \oplus a_1 I_{2^m}$ and $P_2 = \frac{1}{2}(I_{2^m} + E_{v_2}) \oplus a_2 I_{2^m}$. Further let $\theta_1, ..., \theta_{2^m}$ be the principal angles between the subspaces defined by P_1 and P_2 respectively. Denote by U_1 and U_2 arbitrary chosen orthonormal bases of theses subspaces and let d_i be the singular values of the matrix $U_1^\dagger U_2$ in increasing order. Recall that $d_i = cos\theta_i$.

Theorem 3.2. *The principal angles θ_i between subspaces determined by operators $P_{v_1,\epsilon}$ and $P_{v_2,\epsilon}$ are as follows:*

- *if $v_1 = v_2$ and $P_1 \neq P_2$ then $d_i = 0, i = 1, ..., 2^m$*
- *if $v_1 \neq v_2$ and $v_1 * v_2 = 0$, then half of d_i are equal to 1 and another half are equal to 0*
- *if $v_1 \neq v_2$ and $v_1 * v_2 = 1$, then $d_i = \frac{1}{\sqrt{2}}, i = 1, ..., 2^{m-1}$, the other half equal to 0.*

Proof. The row vectors $\{r_1, ..., r_{2^m}\}$ of P_v form a basis for the eigenspace of P_v because $P_v P_v = P_v$ and thus $P_v r_i = r_i$. Therefore, the principal angles between U_1 and U_2 can be thought as the principal angles between the orthonormal bases for P_1 and P_2.

The Heisenberg-Weyl group HW_{2^m} is constructed through the Kronecker Product of $\{I, X, Y, Z\}$, where

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

If $v_1 = v_2$ and $P_1 \neq P_2$ then $P_1 P_2 = 0$ and the subspaces determined by P_1 and P_2 are orthogonal. Hence, the principal angles are all $\frac{\pi}{2}$ and $d_i = 0$ for all i.

When $v_1 \neq v_2$, we will prove by induction: for the base case, where $m = 1$, there are four possibilities for v_1 and four possibilities for v_2: $\{(0,0), (1,0), (0,1), (1,1)\}$. If $v_1 = (0,0)$, $P_1 = I$ and $P_1 P_2 = P_2$, whose singular values are 1 and 0. For the other cases, we can re-scale $P_{(1,0)}$ and $P_{(1,1)}$ by multiplying $\sqrt{2}$ to get matrices of norm 1 rows. Then up to transpose and $\pm$, there are two possibilities for $P_1' P_2'$, where P_1' and P_2' are re-scaled P_1 and P_2 with norm 1 rows, and the possibilities are

$$\begin{bmatrix} \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} \frac{1+i}{2} & 0 \\ 0 & 0 \end{bmatrix}$$

and their singular values are $\frac{\sqrt{2}}{2}$.

For inductive hypothesis, assume that the statement is true for operators in $O-RM(1,i)$ $i = 1, ..., m$, and we prove the case $m+1$.

Since the normalizer of HW_N in the group of unitary matrices acts transitively on HW_N, it is enough to consider any fixed projection operator $E_{v_1} \in O-RM(1, m+1)$ ([AC10]). Fix $v_1 = (0, ..., 0|1, 0, ..., 0)$, then

$$P_{v_1} = \begin{bmatrix} I_{2^m} & 0 \\ 0 & 0 \end{bmatrix}$$

If $v_1 * v_2 = 1$, the first index for v_2 is 1. Suppose $v_2 = (1, a|0, b)$, and $v_2' = (1, a|1, b)$ and $v = (a, b)$, we have

$$P_{v_2} = \frac{1}{2}\begin{bmatrix} I & E_v \\ E_v & I \end{bmatrix}, P_{v_2'} = \frac{1}{2}\begin{bmatrix} I & E_v \\ -E_v & I \end{bmatrix}$$

Re-scale P_{v_2} and $P_{v_2'}$ to $\sqrt{2}P_{v_2}$ and $\sqrt{2}P_{v_2'}$ to have norm 1 rows, the first 2^m rows of $\sqrt{2}P_{v_2}$ and $\sqrt{2}P_{v_2'}$ are linearly independent and pairwise orthogonal. Since the dimension of P_{v_2} and $P_{v_2'}$ are 2^m, the first 2^m rows form an orthonormal basis for P_{v_2} and $P_{v_2'}$. The product of P_{v_1} and $\sqrt{2}P_{v_2}$ or $\sqrt{2}P_{v_2'}$ gives a matrix as $\frac{\sqrt{2}}{2}P_{v_1}$, which has 2^m singular values with value $\frac{1}{\sqrt{2}}$.

If $v_1 * v_2 = 0$, the first index of v_2 is 0. Suppose $v_2 = (0, a|0, b)$, and $v_2' = (0, a|1, b)$ and $v = (a, b)$, we have

$$P_{v_2} = \frac{1}{2}\begin{bmatrix} I + E_v & 0 \\ 0 & I + E_v \end{bmatrix}, P_{v_2'} = \frac{1}{2}\begin{bmatrix} I + E_v & 0 \\ 0 & I - E_v \end{bmatrix}$$

The orthonormal basis for P_{v_2} and $P_{v_2'}$ can be obtained by finding the orthonormal basis for the first 2^m rows combined with the orthonormal basis for the the last 2^m rows. Since both the first 2^m rows and the last 2^m rows have dimension 2^{m-1}, we may give the first 2^{m-1} rows the basis for the first 2^m rows, the second 2^{m-1} rows as the basis for the last 2^m rows. The remaining part as zero vectors. This is a basis for P_{v_2} or $P_{v_2'}$. Denote it by U_{v_2}. Then $P_{v_1}U_{v_2} = U_{v_2}$.

Using our induction hypothesis, we have $\frac{1}{2}(I + E_v) = P_v P_0$, thus, by our induction hypothesis, we have half of the singular values are 1 since $0 * v = 0$ for $\frac{1}{2}(I + E_v)$. Since U_{v_2} have the basis for two such matrices, there are $2 \times 2^{m-1} = 2^m$ singular values of 1, and the rest are 0.

□

3.4 Basis Characterization Using Induction

Following the idea of induction demonstrated in the previous proof, we also give an alternative proof on the basis of the operator codes.

Theorem 3.3. *$U_i \in O - RM(1, m)$ can be chosen in such a way that all their entries will be proportional to elements of the set $\{0, 1, -1, i, -i\}$*

Proof. To find orthogonal bases for these projection operators, we only need to find eigenvectors with eigenvalue 1 that form an orthogonal bases. Additionally, the eigenvectors for the projection operators are the same as the eigenvectors for E_v. Thus, we are finding the orthogonal bases formed by the eigenvectors of E_v with eigenvalues 1 and -1, where 1 corresponds to $I + E_v$ and -1 corresponds to $I - E_v$.

We will prove by induction. For the base case where $m = 1$, we need to consider $\frac{1}{2}(I)$, $\frac{1}{2}(X)$, $\frac{1}{2}(Y)$, and $\frac{1}{2}(Z)$. Therefore, we have:

1. I has eigenvectors $(1, 0)$ and $(0, 1)$
2. X has eigenvectors $(1, 1)$ and $(1, -1)$
3. Y has eigenvectors $(1, -i)$ and $(1, i)$
4. Z has eigenvectors $(1, 0)$ and $(0, 1)$

where the first eigenvector has eigenvalue 1 and the second has eigenvalue -1, except both eigenvectors of I have eigenvalue 1.

Induction Hypothesis: We assume the eigenvectors for E_v, where $v \in F_2^{2^m}$ have entries in $\{0, 1, i, -i\}$, have eigenvalues 1 or -1.

We want to prove the case for E_v where $v \in F_2^{2^{m+1}}$. Write $E_v = e \otimes E_w$, where $e = I, X, Y, Z$. E_v has eigenvectors with the form $u \otimes g$, where u is an eigenvector of e and g is an eigenvector of E_w, because $E_v(u \otimes g) = (e \otimes E_w)(u \otimes g) = (eu) \otimes (E_w g) = \lambda_1 u \otimes \lambda_2 g = \lambda_1\lambda_2(u \otimes g)$, where λ_1 and λ_2 are the corresponding eigenvalues. Let u be any eigenvector of e whose possibilities are listed above and λ is 1 or -1, the eigenvalue $\lambda_1\lambda_2$ is 1 or -1 since $\lambda_2 = 1, -1$ by induction hypothesis. Since u and g both have entries in $\{0, 1, i, -i\}$, their Kronecker product also have entries in $\{0, 1, i, -i\}$.

□

3.5 Decoding Algorithm

Following [HM00], decoding a first order Reed-Muller operator code is equivalent to:

Given a perturbed operator X, we need to find the projection operator $P_{(a,b),\lambda}$ such that

$$P_{(a,b),\lambda} = argmin_{\lambda=\pm1, a,b\in F_2^{2^m}} \parallel P_{(a,b),\lambda}, XX^\dagger \parallel_F$$

Since Weyl Transform is isometric (Corollary 1.3), this is equivalent to find the minimizer for the Euclidean distance between the Weyl Transform of the two operators. Based on this observation, we propose the following decoding algorithm:

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 $P = \frac{1}{2}(I + eE_{(a,b)})$;

The time complexity for computing $XX^\dagger$ is 2^{3m}. Naively, the time complexity for computing $Tr(XX^\dagger E_{(a,b)})$ is 2^{2m}, and we have 2^{2m} possibilities for $E_{(a,b)}$, so the time complexity is upper bounded by 2^{4m}. However, computing $Tr(XE_{(a,b)})$ can be reduced to 2^m: since operator $E_{(a,b)}$ is sparse (there is one element in each row and column): we only need to do one computation for each row using the element in the row of X at the non-zero element index of the row for $E_{(a,b)}$. Since there are 2^m rows, and we only need to use the diagonal elements, we only need to compute 2^m times. Thus, the overall time complexity is 2^{3m}.

The new algorithm is much simpler in form compared to the known best algorithm in [AC10], and has the same time complexity. It also avoids fast Hadamard transform. The time complexities of both algorithms is lower bounded by calculations of $XX^\dagger$, but if the computation can be reduced, our algorithm has the potential to be faster since the time complexity of the algorithm in [AC10] is also lower bounded by fast Hadamard transform.

Chapter 4

Second Order Operator Reed-Muller Code

In this chapter, we focus on the second order operator Reed-Muller code $O-RM(2,m)$. We begin by reviewing McWilliams' method of calculating the distance spectrum for binary Reed-Muller code $RM(2,m)$ by enumerating via Dickson's Theorem in [MS77]. Since there is a bijection between binary Reed-Muller code $RM(2,m)$ and operator Reed-Muller code $O-RM(2,m)$, McWilliams' approach can also be used to calculate the distance spectrum of $O-RM(2,m)$.

Next, we propose a new method using the Weyl transform. We begin by directly classifying $O-RM(2,m)$ by the supports of their Weyl transforms. For each category of $O-RM(2,m)$, we calculate the distance using the Euclidean distance of their Weyl transforms. Finally, we count the number of operator codes in each category.

4.1 Enumeration via Dickson's Theorem

Similar to operator Reed-Muller codes, binary Reed-Muller codes $RM(2,m)$ are generated by the boolean functions of degree ≤ 2 with m inputs $x_1,...,x_m$. Therefore, the boolean function that generates a codeword in $RM(2,m)$ can be written as

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

where $q_{ij} = 0, 1$, $l_i = 0, 1$, and $\epsilon = 0, 1$. Since the linear part $(\sum_{i=1}^{m} l_i x_i + \epsilon) \in RM(1, m)$, $RM(2, m)$ is a union of cosets of $RM(1, m)$. Therefore, classifying $RM(2, m)$ requires classifying the quadratic part $\sum_{i,j=1}^{m} q_{ij} x_i x_j$.

4.1.1 Dickson's Theorem

We begin by introducing Dickson's Theorem given in [Dic01] that classifies the quadratic forms in finite field $GF[2^n]$:

Theorem 4.1. *(Dickson's Theorem) If a quadratic form with coefficients in $GF[2^n]$ (i.e. $\sum_{i \leq j}^{i,j=1,...,M} q_{ij} x_i x_j$, $q_{ij} \neq 0$) cannot be expressed in the field as a quadratic form with fewer than M linear homogeneous functions of $x_1, ..., x_M$, it can be reduced by a linear homogeneous substitution belonging to the field to one of the canonical forms*

1. $x_1 x_2 + x_3 x_4 + ... + x_{M-2} x_{M-1} + x_M^2$ *if M is odd*
2. $x_1 x_2 + x_3 x_4 + ... + x_{M-1} x_M + \lambda x_{M-1}^2 + \lambda x_M^2$ *if M is even*

where λ is zero or is a particular one of the values for which $x_{M-1} x_M + \lambda x_{M-1}^2 + \lambda x_M^2$ is irreducible.

We apply Theorem 4.1 in the case of $GF[2]$ for boolean functions. We have the following version of Theorem 4.1 from [MS77]:

Theorem 4.2. *(Dickson's Theorem on $GF[2]$)*

1. *If B is a symplectic $m \times m$ matrix of rank $2M$, then there exists an invertible binary matrix R such that RBR^T has zeros everywhere except on the two diagonals immediately above or below the main diagonal with entries $1010...100...0$ that has M ones.*
2. *Any boolean function of degree ≤ 2,*

$$xQx^T + Lx + \epsilon$$

where Q is an upper triangular matrix, can be written as

$$\sum_{i=1}^{M} y_{2i-1} y_{2i} + L'y + \epsilon$$

where $y = xR^{-1}$ and R is given by 1 above with $B = Q + Q^T$. Moreover, inputs $y_1, ..., y_{2M}$ are linearly independent.

3. *If $L'y$ is linearly dependent on $y_1, .., y_{2M}$, we may by an affine transformation of inputs write the boolean function as*

$$\sum_{i=1}^{M} z_{2i-1} z_{2i} + \epsilon$$

where $z_1, ..., z_{2M}$ are linearly independent.

Theorem 4.2 is proved inductively on the dimension of B.

Theorem 4.2 shows two important properties of the binary Reed-Muller codes. First, each codeword can be uniquely determined by a symplectic binary matrix B. Second, the boolean function that generates the form is characterized by the rank and the dimension of B in the quadratic part.

Since the generating boolean function of a codeword also determines the weight of the codeword, we can count the number of the codewords with a fixed rank and a fixed dimension of B, and determine the number of such codewords by the count of symplectic binary matrices B given its rank and dimension.

4.1.2 Three Categories Given by Dickson's Theorem

The following lemma in [AC10] summarizes the classification of boolean function given by Theorem 4.2 into three categories:

Lemma 4.3. *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. $x_1x_2 \oplus x_3x_4 \oplus ... \oplus x_{2t-1}x_{2t}$
2. $x_1x_2 \oplus x_3x_4 \oplus ... \oplus x_{2t-1}x_{2t} + 1$
3. $x_1x_2 \oplus x_3x_4 \oplus ... \oplus x_{2t-1}x_{2t} \oplus x_{2t+1}$

4.2 Classifying O-RM(2,m)

In this section, we will classify the second order operator Reed-Muller codes $O - RM(2, m)$. We will prove a similar classification as Lemma 4.3.

For convenience, let $P_a = \frac{1}{2}(I \pm E_a)$, $P_{a,1} = \frac{1}{2}(I + E_a)$, and $P_{a,-1} = \frac{1}{2}(I - E_a)$. When we use P_a, the calculations or the proofs will be focused on a and the sign can be either $+$ or $-$.

In this section, we use an example of $m = 2$: $G_{ex} = \{v_1 = (1,0,0,0), v_2 = (0,1,0,0), v_3 = (0,0,1,0), v_4 = (0,0,0,1)\}$, a set of four linearly independent vectors.

4.2.1 Operator as Sum of Products

First, any boolean function may be re-written in the form of sum of products. Since there is a bijective correspondence between boolean functions and operator functions, an operator code can also be written as a sum of products.

4.2.2 Combining Two Products with a Common Operator

The following example shows that we may combine two products if they share a same operator.

Example 4.2.1. Given G_{ex}, consider the boolean function $F = x_1x_2 \oplus x_2x_3 \oplus x_3x_4$ that generates the operator function $f = P_{(1,0,0,0)}P_{(0,1,0,0)} \oplus P_{(0,1,0,0)}P_{(0,0,1,0)} \oplus P_{(0,0,1,0)}P_{(0,0,0,1)}$, we may reduce f as:

$$\begin{aligned} f &= P_{(1,0,0,0)}P_{(0,1,0,0)} \oplus P_{(0,1,0,0)}P_{(0,0,1,0)} \oplus P_{(0,0,1,0)}P_{(0,0,0,1)} \\ &= P_{(0,1,0,0)}(P_{(1,0,0,0)} \oplus P_{(0,0,1,0)}) \oplus P_{(0,0,1,0)}P_{(0,0,0,1)} \\ &= P_{(0,1,0,0)}P_{(1,0,1,0)} \oplus P_{(0,0,1,0)}P_{(0,0,0,1)} \end{aligned} \tag{4.1}$$

Note that the reduced form is still a sum of products.

There is a corresponding observation in Dickson's Theorem (Theorem 4.2).

Example 4.2.2. Let $x = (x_1, x_2, x_3, x_4)$, and let R be

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ 1 & & 1 & \\ & & & 1 \end{bmatrix}$$

Then $xR = (x_1 \oplus x_3, x_2, x_3, x_4)$ and $F(x_1, x_2, x_3, x_4) = x_2(x_1 \oplus x_3) \oplus x_3x_4 = H(xR)$, such that $H(v_1, v_2, v_3, v_4) = v_2v_1 \oplus v_3v_4$. This corresponds to the reduced form of f.

Lemma 4.4. *Any operator F in $O - RM(2, m)$ can be written as sum of products such that for each pair of products, they do not share common operators up to a sign flip.*

Proof. First,we write the operator as a sum of products: $\oplus_{k=1}^{M} f_k$, such that f_k has degree at most 2. There are three cases for f_k: P_aP_b, P_a, and I. Suppose two of these f_k share common elements, then there are two cases: $P_aP_b \oplus P_aP_c$ and $P_aP_b \oplus P_a$. For the first case,

$$\begin{aligned}
P_aP_b \oplus P_aP_c &= P_a(P_b \oplus P_c) \\
&= P_a(P_b + P_c - 2P_bP_c) \\
&= P_a(P_b + P_c - \frac{1}{2}(I \pm E_a \pm E_b \pm E_aE_b)) \\
&= P_a(P_b + P_c - \frac{1}{2}(2I \pm E_a \pm E_b) + (I \pm E_aE_b)) \\
&= P_a(P_b + P_c - (P_b + P_c) + \frac{1}{2}(I \pm E_aE_b)) \\
&= P_a(\frac{1}{2}(I \pm E_aE_b)) \\
&= P_aP_d
\end{aligned}$$

where P_d is some first order operator code.

For the second case P_aP_b with P_a,

$$\begin{aligned}
P_b(P_a \oplus I) &= P_b(I + P_a - 2P_a) \\
&= P_b(I - P_a) \\
&= P_b(I - \frac{1}{2}(I \pm E_a)) \\
&= P_b(\frac{1}{2}(I - \pm E_a)) \\
&= P_bP_a
\end{aligned}$$

The operation of combining two products into one if two products share the same elements reduces the length of the sum by one. Since the length of the sum is finite, we can only perform finite number of such combining operations, and there will be no product in the sum that shares a common operator. □

4.2.3 Combining Two Products with Non-Trivial Intersection on Support of the Weyl Transform

We would like to generalize the idea of combining operations in lemma 4.4 from the sharing operators of the products to the intersections of the support of the Weyl transforms

of the products.

Example 4.2.3. Consider $f = P_{(1,1,0,0),1}P_{(0,0,1,1),1} \oplus P_{(0,1,1,0),1}P_{(1,0,0,1),1}$. The two products share no operators. Their Weyl transforms are respectively

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

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

The supports of their Weyl transforms intersect on $E_{(1,1,1,1)}$ and I. Their sum can be re-written as follows:

$$\begin{aligned} f &= P_{(1,1,0,0),1}P_{(0,0,1,1),1} \oplus P_{(0,1,1,0),1}P_{1,0,0,1,1} \\ &= P_{(1,1,1,1),1}P_{(1,1,0,0),1} \oplus P_{(1,1,1,1),1}P_{(0,1,1,0),1} \\ &= P_{(1,1,1,1),1}(P_{(1,1,0,0),1} \oplus P_{(0,1,1,0),1}) \\ &= P_{(1,1,1,1),1}P_{(1,0,1,0),-1} \end{aligned}$$

where we reduce the number of products by one.

Lemma 4.5. *Any operator F in $O-RM(2,m)$ can be written as sum of products such that for each pair of products, the supports of their Weyl transform have no intersections besides I.*

Proof. From lemma 4.4, we may assume the products share no common elements. Suppose for some pairs of products, the supports of their Weyl transform some share elements besides I, we have two situations: $P_aP_b \oplus P_cP_d$ and $P_aP_b \oplus P_{a+b}$. The second case is simpler, since $P_aP_b = \pm P_aP_{a+b}$, and we can combine the two products into one product to reduce the number of products by one. The first case is trickier. Without loss of generality, we assume $E_{a+b} = E_{c+d}$, where $a+b = c+d$. We can re-write P_aP_b as follows:

$$\begin{aligned} P_aP_b &= \frac{1}{4}(I \pm E_a \pm E_b \pm E_{a+b}) \\ &= \frac{1}{2}(I + E_a)\frac{1}{2}(I + E_{a+b}) \\ &= P_aP_{a+b} \end{aligned}$$

Similarly, we can re-write P_cP_d as P_cP_{c+d}, and$P_aP_b \oplus P_cP_d = P_{a+b}P_{a+c}$. Therefore we may reduce to a case where the products intersect trivially with respect to their Weyl transforms. □

4.2.4 Re-writing Products of Operators

The idea of re-writing the product P_aP_b as P_aP_{a+b} in lemma 4.5 can be generalized:

Example 4.2.4. Consider $f = P_{(1,0,0,0),1}P_{(0,1,0,0),1} \oplus P_{(0,0,1,0),1}P_{(0,0,0,1),1}$. The support of the Weyl Transform of f covers all possible operators E that is generated by

$$E_{(1,0,0,0)}, E_{(0,1,0,0)}, E_{(0,0,1,0)}, E_{(0,0,0,1)}$$

By symmetry, it suffices to show that it's possible to have $P_{(1,1,0,0)}$, $P_{(1,0,1,0)}$, $P_{(1,1,1,0)}$ and $P_{(1,1,1,1)}$ as one of its products as follows:

1. $P_{(1,1,0,0)}$: $f = P_{(1,1,0,0),1}P_{(1,0,0,0),1} \oplus P_{(0,0,1,0),1}P_{(0,0,0,1),1}$
2. $P_{(1,0,1,0)}$: $f = P_{(1,0,1,0),-1}P_{(0,1,0,0),1} \oplus P_{(0,1,1,0),-1}P_{(0,0,1,1),1}$
3. $P_{(1,1,1,0)}$: $f = P_{(1,1,0,0),1}P_{(1,0,0,0),1} \oplus P_{(0,0,1,0),1}P_{(0,0,0,1),1} = P_{(1,1,1,0),-1}P_{(1,0,0,0)} \oplus P_{(1,0,0,1),-1}P_{(0,0,1,0),1}$
4. $P_{(1,1,1,1)}$: $f = P_{(1,1,0,0)}P_{(1,0,0,0)} \oplus P_{(0,0,1,1)}P_{(0,0,1,0)} = P_{(1,1,1,1),-1}P_{(1,0,0,0)} \oplus P_{(1,0,1,0)}P_{(0,0,1,1)}$

Lemma 4.6. *For any second order operators, $F = \oplus_{i=1}^{k} P_{v_{2i-1}}P_{v_{2i}}$ is a sum of product with only quadratic terms of $\{P_{v_1}, ..., P_{v_{2k}}\}$ such that $\{v_1, ..., v_{2k}\}$ is linearly independent. We can re-write F as a sum of products where one product contains $P_{v'}$ such that v' can be any linear combination of $v_1, ..., v_{2k}$.*

Proof. We use induction of k. The base case with $k = 1$, $P_{v_1}P_{v_2} = \pm P_{v_1+v_2}P_{v_1}$.

Suppose the statement is true for $k = p$, and we now prove for $k = p + 1$.

Given $F = \oplus_{i=1}^{p+1} P_{v_{2i-1}}P_{v_{2i}}$. For $v' \in span(\{v_1, ..., v_{2p}\})$, we can use inductive hypothesis to re-write the first p products of F.

So it remains to show for $v' \notin span(\{v_1, ..., v_{2p}\})$ but $v' \in span(\{v_1, ..., v_{2p+2}\})$, which implies that v_{2p+1} or v_{2p+2} or both are in the linear combination of $\{v_1, ..., v_{2p+2}\}$ that constructs v'.

If both are in, re-write the last product as $P_{v_{2p+1}+v_{2p+2}}P_{v_{2p+1}}$ using the base case. By symmetry, without loss of generality, we assume only v_{2p+1} is in the linear combination.

Suppose $v' = v'' + v_{2p+1}$ such that $v'' \in span(\{v_1, ..., v_{2p}\})$, then by inductive hypothesis we can re-write the first p products in F so that one of theses product is $P_{v''}P_{v'''}$. Without loss of generality, assume $E_{v''} = E_{v'',1}, E_{v'''} = E_{v''',1}, E_{v_{2p+1}} = E_{v_{2p+1},1}, E_{v_{2p+2}} = E_{v_{2p+2},1}$ commute.

$$P_{v'',1}P_{v''',1} \oplus P_{v_{2p+1},1}P_{v_{2p+2},1} = P_{v''+v_{2p+1},-1}P_{v''',1} \oplus P_{v'''+v_{2p+2},-1}P_{v_{2p+1},1}$$

Therefore, we can re-write the sum of products to let one product contain $v' = v'' + v_{2p+1}$. □

An immediate corollary from Lemma 4.6 gives a general principle of the intersection of the support of the Weyl transforms of operator Reed-Muller codes:

Corollary 4.7. *Given two operators whose set of indexes of the operators in their forms of sum of products are linearly independent, their Weyl transforms intersect trivially on I and only on I.*

4.2.5 Classifying Second Order Operator Codes by the Length of Quadratic Part

Using lemma 4.6, we are able to generalize the combining operations:

Theorem 4.8. *For any operator F that constructs $O-RM(2,m)$ as a sum of quadratic product, we may write it as a sum of products such that for each product, the support of its Weyl transform intersects trivially with the Weyl transform of the sum of any other products of F.*

Proof. We prove by induction on the length of the product. The base case has length one in the form P_aP_b, and it is true by definition.

Suppose the statement is true for operators with sum of length k .

In case $k+1$, arrange first k products that satisfies the statement using induction hypothesis. If there is some non-trivial intersection with the support of the Weyl transform of the $k+1^{th}$ product, re-write the first k products using lemma 4.6 to get a product in the first k sum that contains P_v, which is in the $k+1^{th}$ product.

Combining the two products into one, the number of products after the combination is less than or equal to k. By induction hypothesis we may re-write the operator code to satisfy the statement. □

Theorem 4.8 gives the explicit forms of the second order operator Reed-Muller codes, and there will be three categories ($\{a_1, ..., a_M, b_1, ..., b_M, c\}$ is linearly independent):

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

Case two generalizes since $\oplus_{k=1}^{r} P_{v_k}$ is a first order code.

4.3 The Weyl Transform of the Second Order Operator Reed-Muller Code O-RM(2,m)

We use the classification we derive from Theorem 4.8 to calculate the Weyl Transform of $O - RM(2, m)$. We first calculate the Weyl transform of the first category in the classification: $\oplus_{k=1}^{M} P_{a_k} P_{b_k}$.

4.3.1 Expanding as an Additive Sum of Operators in the Heisenberg-Weyl Group

Example 4.3.1. When $m = 2$, without loss of generality, we only consider $v_1 v_2$ and $v_1 v_2 \oplus v_3 v_4$, since we may switch v_1, v_2, v_3, v_4 as well as $v_1 + v_2$ with v_1 by symmetry.

1. $P_{v_1,1} P_{v_2,1} = \frac{1}{4}(I + E_{v_1} + E_{v_2} \pm E_{v_1+v_2})$
2. $P_{v_1,1} P_{v_2,1} \oplus P_{v_3,1} P_{v_4,1} = \frac{1}{8}(3I + E_{v_1} + E_{v_2} + E_{v_3} + E_{v_4} \pm E_{v_1+v_2} \pm E_{v_3+v_4} - (E_{v_1+v_3} \pm E_{v_1+v_4} \pm E_{v_2+v_3} \pm E_{v_2+v_4} \pm E_{v_1+v_2+v_3} \pm E_{v_1+v_2+v_4} \pm E_{v_1+v_3+v_4} \pm E_{v_2+v_3+v_4} \pm E_{v_1+v_2+v_3+v_4}))$

Based on the observations from the example above,

Lemma 4.9. *For any $P \in O - RM(2, m)$ such that $P = \oplus_{k=1}^{M} P_{a_k} P_{b_k}$, satisfying the requirement of the classification in theorem 4.8, then P is equivalent to an additive sum $(+)$ of all elements in the subgroup generated by $\{E_{a_1}, E_{b_1}, ..., E_{a_M}, E_{b_M}\}$. The coefficient of I is $\frac{2^M - 1}{2^{M+1}}$, and the coefficients of other operators is $\pm\frac{1}{2^{M+1}}$.*

Proof. The proof follows from an inductive argument. The base case is $M = 1$, where $P_{a_1}P_{b_1} = \frac{1}{4}(I + E_{a_1} + E_{b_1} + E_{a_1+b_1})$.

Assume the result holds for any $M \leq K$, and consider the case $K+1$. For simplicity, define S_K to be the set of vectors generated by $\{a_1, b_1, .., a_K, b_K\}$, and G_K to be the set of vectors generated by $\{a_K, b_K\}$

$$\begin{aligned}
P &= \oplus_{k=1}^{K+1} P_{a_k}P_{b_k} \\
&= \oplus_{k=1}^{K} P_{a_k}P_{b_k} \oplus P_{a_{K+1}}P_{b_{K+1}} \\
&= \frac{1}{2^{K+1}}((2^K-1)I + \sum_{v\in S_k} \pm E_v) \oplus \frac{1}{4}(I + E_{a_{K+1}} + E_{b_{K+1}} + E_{a_{K+1}+b_{K+1}}) \\
&= \frac{1}{2^{K+1}}((2^K-1)I + \sum_{v\in S_K} \pm E_v) + \frac{1}{4}(I + E_{a_{K+1}} + E_{b_{K+1}} + E_{a_{K+1}+b_{K+1}}) \\
&\quad -\frac{1}{2^{K+2}}((2^K-1)I + \sum_{v\in S_K} \pm E_v)(I + E_{a_{K+1}} + E_{b_{K+1}} + E_{a_{K+1}+b_{K+1}}) \\
&= \frac{1}{2^{K+2}}((2^{K+1}-1)I + \sum_{v\in S_K} \pm E_v + \sum_{v\in G_{K+1}} \pm E_v) \\
&\quad -\frac{1}{2^{K+2}}(\sum_{v\in S_K, w\in G_{K+1}} \pm E_vE_w) \\
&= \frac{1}{2^{K+2}}((2^{K+1}-1)I + \sum_{v\in S_{K+1}} \pm E_v)
\end{aligned}$$

□

An immediate corollary of lemma 4.9 gives the coefficient of the operators in the additive sum for other categories of the second order operator Reed Muller codes:

Corollary 4.10. *For the third case ($(\oplus_{k=1}^{M} P_{a_k}P_{b_k}) \oplus I$), an additive sum of all elements is given by the operators in the subgroup generated by $\{E_{a_1}, E_{b_1}, ..., E_{a_M}, E_{b_M}\}$. The coefficient for I is $\frac{2^M+1}{2^{M+1}}$, and the coefficients for other operators are $\pm\frac{1}{2^{M+1}}$ (total 2^{2M} of them)*

Corollary 4.11. *For the second case ($(\oplus_{k=1}^{M} P_{a_k}P_{b_k}) \oplus P_c$), an additive sum of all elements is given by I and the products of E_c and the operators in the support of $\oplus_{k=1}^{M} P_{a_k}P_{b_k}$ (total $2^{2M}+1$ of them). The coefficient of I is $\frac{1}{2}$ and the coefficients for the other operators are $\pm\frac{1}{2^{M+1}}$.*

Example 4.3.2. Continuing the previous example, consider $P_{v_1,1}P_{v_2,1} \oplus P_{v_3,1}$ and $P_{v_1,1}P_{v_2,1} \oplus P_{v_3,1}P_{v_4,1} \oplus I$.

1. $P_{v_1,1}P_{v_2,1} \oplus P_{v_3,1} = \frac{1}{4}(I + E_{v_1} + E_{v_2} \pm E_{v_1+v_2}) \oplus \frac{1}{2}(I + E_{v_3}) = \frac{1}{4}(2I + E_{v_3} \pm E_{v_1+v_3} \pm E_{v_2+v_3} \pm E_{v_1+v_2+v_3})$

2. $P_{v_1,1}P_{v_2,1} \oplus P_{v_3,1}P_{v_4,1} \oplus I = I - (P_{v_1,1}P_{v_2,1} \oplus P_{v_3,1}P_{v_4,1}) = \frac{1}{8}(5I - E_{v_1} + E_{v_2} + E_{v_3} + E_{v_4} \pm E_{v_1+v_2} \pm E_{v_3+v_4} - (E_{v_1+v_3} \pm E_{v_1+v_4} \pm E_{v_2+v_3} \pm E_{v_2+v_4} \pm E_{v_1+v_2+v_3} \pm E_{v_1+v_2+v_4} \pm E_{v_1+v_3+v_4} \pm E_{v_2+v_3+v_4} \pm E_{v_1+v_2+v_3+v_4}))$

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

Using lemma 4.9 and its corollaries, we give an explicit formula of the Weyl transform with $Tr(I_{2^m}) = 2^m$:

Theorem 4.12. *For any $Q \in O - RM(2,m)$ such that the projection operator $P = \oplus_{k=1}^{M} P_{a_k}P_{b_k}$ satisfies the requirement in theorem 4.8, we have the Weyl transform of P at the first index being $\frac{2^M-1}{2^{M+1-\frac{m}{2}}}$ and the other index as $\pm\frac{1}{2^{M+1-\frac{m}{2}}}$, and the support is a commutative subgroup generated by $\{E_{a_1}, E_{b_1}, ..., E_{a_M}, E_{b_M}\}$.*

The Weyl Transform of the third case is $\frac{2^M+1}{2^{M+1-\frac{m}{2}}}$ for first index and $\pm\frac{1}{2^{M+1-\frac{m}{2}}}$ for other indexes (total 2^{2M} of them).

The Weyl Transform of the second case is $\frac{1}{2^{1-\frac{m}{2}}}$ for the first index and $\pm\frac{1}{2^{M+1-\frac{m}{2}}}$ for other indexes, which are the products of E_c and the operators in the support of $\oplus_{k=1}^{M} P_{a_k}P_{b_k}$. (total $2^{2M}+1$ of them)

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

Using theorem 2.3, it suffices to consider the distance spectrum of 0. Therefore, we do not need to consider the sign patterns in the coordinates of the Weyl transform and only need to compute the magnitude.

From the discussions in section 4.3, we derive the corollary on the possible value for distance of the code

Corollary 4.13. *The possible value for t^2 such that $B_t(0) > 0$ includes $\{\frac{2^{M+m}-2^m}{2^{M+1}}, 2^{m-1}, \frac{2^{M+m}+2^m}{2^{M+1}}\}$, respectively for first, second and third case, where $2M \leq m$*

Example 4.4.1. Consider $RM(2,4)$, then $M \leq 2$, and there are three possible values for M:

If $M = 0$, from corollary 4.13, possible values of t^2 include 0, 8, 16 for the first, second and third case respectively. The first case has only one possibility, and so does the third.

Since $M = 0$ is the same as $RM(1, 4)$, the total number of operators is $2^{\binom{4}{0}+\binom{4}{1}} = 32$. Thus, there are $32 - 2 = 30$ for the second case.

If $M = 1$, then the possible values of t^2 include 4, 8, 12. The total number of such operators are given by $\frac{(2^4-2^0)(2^4-2^1)}{(2^2-2^0)(2^2-2^1)} \times 4 \times (2^{4-2+1} - 2) = 35 \times 32$, where 35 is the number of possibilities of the subspace formed by the vectors chosen for the quadratic part, 4 is the sign flip for the selected 2 operators, and $2^{4-2+1}-2$ is the available selection for a first order operator. The number of the first case can be given by the sign flips of the operators (i.e. $P_{v,1} \to P_{v,-1}$ and vice versa). Thus, there are 4 possibilities for each subspace in the 35 possibilities. For each first case, it can be mapped to a third case by operation $\oplus I$. For the second case, it can be thought as finding the vector that is not in the subspace in the quadratic part, which has $2^4 - 2^2 = 12$ possibilities. Considering sign flip, there are 24 possibilities. In summary, the first case and third case both have 35×4 possibilities, and the second case has 35×24 possibilities.

If $M = 2$, the only possibilities are the first and third case with distance t^2 equal to 6 and 10. Since we know the total number of operators in O-RM(2,4) is $2^{\binom{4}{0}+\binom{4}{1}+\binom{4}{2}}$, we may subtract all possibilities for $M = 1$ and $M = 0$, where we have 28×32 total possibilities. Since each first case operator can be mapped to a third case operator, the total number of possibilities of both the first case and the third case is 28×16.

From the example above, we may have two combinatorial countings. First, given a vector space spanned by m vectors, we need to select a $2M$-dimensional subspace using the linear combinations of the m vectors (i.e. select $2M$ linearly independent vectors from the set of all 2^m possible linear combinations of the m vectors). We would like to know how many unique subspaces there are given fixed M and m. Call this number $g(m, M)$.

Second, given the $2M$-dimensional subspace from the previous step, we need to divide the space into M 2-dimensional subspaces, each spanned by 2 vectors selected from the $2M$-dimensional subspace. These 2-dimensional subspaces need to intersect trivially. Call this number $f(M)$.

Lemma 4.14. $g(m, M) = \frac{\Pi_{i=0}^{2M-1}(2^m-2^i)}{\Pi_{i=0}^{2M-1}(2^{2M}-2^i)}$

Proof. We may select any vectors among the 2^m vectors except 0 at the beginning. Then the next one would be any vector not in the span of the previously selected vectors. Thus, for the i^{th} vector, we have selected $i - 1$ linearly independent vectors, leaving $2^m - 2^{i-1}$ available vector not in the subspace formed by the first $i - 1$ vectors.

In the counting above, we have counted the permutations of a same selection $\Pi_{i=0}^{2M-1}(2^{2M} - 2^i)$ times, and thus need to divide by the number. □

Lemma 4.15. $f(M) = 2^{M(M-1)}(\Pi_{i=1}^{M}(2^{2i-1}-1))$

Proof. At the beginning, we may pick any vector, and to put a vector not in the span of that vector, we have $2^{2M}-2$ choices (excluding the selected vector and 0). Then, again, we may pick a random vector, and choose a vector that is not in the span of the previously selected 3 vectors: $2^{2M}-2^3$.

Following this logic, if we have picked i 2-dimensional subspaces, we may randomly pick a vector, then we can choose a vector from the space that is linearly independent of the selected vectors, leaving $2^{2M}-2^{2i+1}$ choices.

In the counting above, suppose we have selected v_1 randomly for a 2-dimensional subspace, and then we chose v_2. The operator we formulate will be $P_{v_1}P_{v_2}$, which has the same support as $P_{v_1}P_{v_1+v_2}$. Therefore, we have counted the same choice twice. Thus, we need to divide the result by 2^M since we selected the 2-dimensional subspace M times. □

Using the two formula above, we may give the following formula for calculating the distance spectrum of second order operator Reed-Muller Code.

Theorem 4.16. *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* $t^2=\frac{2^{M+m}+2^m}{2^{M+1}}$

Proof. Both the first case and the third case can be thought as selecting $2M$-dimensional subspace from m-dimensional space to construct the quadratic part (i.e. $g(m,M)$), then divide the space into M 2-dimensional subspace (i.e. $f(M)$). 2^{2M} represents the possibility for sign flip for the $2M$ operators selected for the quadratic part.

The second case can be thought as the first case with a first order operator Reed-Muller code, whose support in Weyl transform intersects trivially with the quadratic part. Additionally, two vectors whose difference is in the support of the Weyl transform of the quadratic part are the same. For example, suppose P_b intersects non-trivially with the support of the Weyl transform of the quadratic part, and P_a, P_{a+b} intersects trivially with the support of the Weyl transform of the quadratic part. Then $P_{a+b}=P_a\oplus P_b$, and

P_b may be moved into the quadratic part by our categorization of second order operator Reed-Muller code. In this case, P_a and P_{a+b} are equivalent.

This gives us 2^{m-2M+1} possibilities for the first order operator Reed-Muller code considering a sign flip, and we need to exclude 0 and I. □

Chapter 5

Sign Patterns of the Weyl Transform

In this chapter, we prove a theorem on the sign patterns of the Weyl transform of operator Reed-Muller Codes for any order. The theorem further demonstrates that the Weyl transform offers a nice framework of understanding operator Reed-Muller codes.

Theorem 5.1. *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.

We observe that $\epsilon_{(a+c,b+d)} = \epsilon_{(a,b)}\epsilon_{(c,d)}(i^{ad^T - bc^T})$ is well defined for $\epsilon \in \{1, -1\}$. By well-defined, we require two different ways of expanding $\epsilon_{(a+c,b+d)}$ is the same: $\epsilon_{(a+c,b+d)} = \epsilon_{(a,b)}\epsilon_{(c,d)}(i^{ad^T - bc^T})$ and $\epsilon_{(a+c,b+d)} = \epsilon_{(c+a,d+b)} = \epsilon_{(c,d)}\epsilon_{(a,b)}(i^{bc^T - ad^T})$. This implies that $i^{bc^T - ad^T} = i^{ad^T - bc^T}$ has to be true. This is indeed true since we are working with a commutative group $\{E_{(a,b)}\}$ where $\{(a,b)\}$ is orthogonal with respect to symplectic inner product. Therefore, we may interchange $ad^T - bc^T$ and $bc^T - ad^T$.

Proof. Let $S_j = \langle (a_i, b_i) | i = 1, ..., j \rangle$ and $S'_j = S_j \setminus S_{j-1}$.

If $\epsilon_{(a+c,b+d)} = \epsilon_{(a,b)}\epsilon_{(c,d)}(i^{bc^T - ad^T})$ for all $0 \neq (a,b),(c,d) \in S$, we want to show that

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

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

Given $p \leq k$, we have:

$$\sum_{(a,b)\in S_p} \epsilon_{a,b}E_{a,b} \quad = \quad \sum_{(a,b)\in S_{p-1}} \epsilon_{a,b}E_{a,b} + \sum_{(a,b)\in S'_p} \epsilon_{a,b}E_{a,b}$$

For any $(a,b) \in S'_p$, by definition of S_p and S'_p, $E_{(a,b)} = i^{a'b_p^T - a_pb'^T}E_{(a',b')}E_{(a_p,b_p)}$, where $(a',b') \in S_{p-1}$. Therefore,

$$\begin{aligned}
\sum_{(a,b)\in S_p} \epsilon_{(a,b)}E_{(a,b)} &= \sum_{(a,b)\in S_{p-1}} \epsilon_{(a,b)}E_{(a,b)} + \sum_{(a,b)\in S'_p} \epsilon_{(a,b)}E_{(a,b)} \\
&= \sum_{(a,b)\in S_{p-1}} \epsilon_{(a,b)}E_{(a,b)} + \sum_{(a',b')\in S_{p-1}} \epsilon_{(a,b)}i^{a'b_p^T - a_pb'^T}E_{(a',b')}E_{(a_p,b_p)} \\
&= \sum_{(a,b)\in S_{p-1}} \epsilon_{(a,b)}E_{(a,b)} \\
&\quad + \sum_{(a',b')\in S_{p-1}} (i^{a'b_p^T - a_pb'^T}\epsilon_{(a',b')}\epsilon_{(a_p,b_p)})i^{a_pb'^T - a'b_p^T}E_{(a',b')}E_{(a_p,b_p)} \\
&= \sum_{(a,b)\in S_{p-1}} \epsilon_{(a,b)}E_{(a,b)} + \sum_{(a',b')\in S_{p-1}} (\epsilon_{(a',b')}\epsilon_{(a_p,b_p)})E_{(a',b')}E_{(a_p,b_p)} \\
&= \sum_{(a,b)\in S_{p-1}} \epsilon_{(a,b)}E_{(a,b)} + (\sum_{(a,b)\in S_{p-1}} \epsilon_{(a,b)}E_{(a,b)})\epsilon_{(a_p,b_p)}E_{(a_p,b_p)} \\
&= (\sum_{(a,b)\in S_{p-1}} \epsilon_{(a,b)}E_{(a,b)})(I_N + \epsilon_{(a_p,b_p)}E_{(a_p,b_p)})
\end{aligned}$$

Taking $p = k, k-1, ..., 1$, we can continuously separate $(I_N + \epsilon_{(a_p,b_p)}E_{(a_p,b_p)})$, and therefore, we have $O = \Pi_{i=1}^{k}(I_N + \epsilon_{(a_i,b_i)}E_{(a_i,b_i)})$.

Conversely, if $O = \Pi_{i=1}^{k}(I_N + \epsilon_{(a_i,b_i)}E_{(a_i,b_i)})$, we can prove that $\epsilon_{(a+c,b+d)} = \epsilon_{(a,b)}\epsilon_{(c,d)}(i^{cb^T - ad^T})$ for all $0 \neq (a,b),(c,d) \in S$. Consider any $(a,b),(c,d) \neq 0$ and $(a,b) \neq (c,d)$. We may choose basis of S as follows: $\{(a,b),(c,d),(a_3,b_3),...,(a_k,b_k)\}$ and $\{(a,b),(a+c,b+d),(a_3,b_3),...,(a_k,b_k)\}$. We can write

$$\begin{aligned} O &= (I+\epsilon_{(a,b)}E_{(a,b)})(I+\epsilon_{(c,d)}E_{(c,d)})\Pi_{i=3}^{k}(I_N+\epsilon_{(a_i,b_i)}E_{(a_i,b_i)}) \\ &= (I+\epsilon_{(a,b)}E_{(a,b)})(I+\epsilon_{(a+c,b+d)}E_{(a+c,b+d)})\Pi_{i=3}^{k}(I_N+\epsilon_{(a_i,b_i)}E_{(a_i,b_i)}) \end{aligned}$$

Therefore,

$$(I+\epsilon_{(a,b)}E_{(a,b)})(I+\epsilon_{(c,d)}E_{(c,d)}) = (I+\epsilon_{(a,b)}E_{(a,b)})(I+\epsilon_{(a+c,b+d)}E_{(a+c,b+d)})$$

which implies

$$\epsilon_{(a,b)}E_{(a,b)}\epsilon_{(c,d)}E_{(c,d)} = \epsilon_{(a+c,b+d)}E_{(a+c,b+d)}$$

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

□

Bibliography

[AC05] A. Ashikhmin and A. R. Calderbank. Space-time reed-muller codes for noncoherent mimo transmission. In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, pages 1952–1956, Sept 2005.

[AC10] A. Ashikhmin and A. R. Calderbank. Grassmannian packings from operator reed muller codes. *IEEE Transactions on Information Theory*, 56(11):5689–5714, Nov 2010.

[ACK06] A. Ashikhmin, A. R. Calderbank, and W. Kewlin. Multidimensional second order reed-muller codes as grassmannian packings. In *2006 IEEE International Symposium on Information Theory*, pages 1001–1005, July 2006.

[AK01] A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Transactions on Information Theory*, 47(7):3065–3072, Nov 2001.

[CHS96] John H. Conway, Ronald H. Hardin, and Neil J. A. Sloane. Packing lines, planes, etc.: Packings in grassmannian spaces. *Experimental Mathematics*, 5(2):139–159, 1996.

[CRSS97] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over gf(4). In *Proceedings of IEEE International Symposium on Information Theory*, pages 292–, Jun 1997.

[CSB87] J. H. Conway, N. J. A. Sloane, and E. Bannai. *Sphere-packings, Lattices, and Groups*. Springer-Verlag New York, Inc., New York, NY, USA, 1987.

[Dic01] L.E. Dickson. *Linear Groups: With an Exposition of the Galois Field Theory*. B.G. Teubner's Sammlung von lehrbüchern auf dem gebiete der mathematischen wissenschaften mit einschluss ihrer anwendungen. bd. VI. B. G. Teubner, 1901.

[HM00] B. M. Hochwald and T. L. Marzetta. Unitary space-time modulation for multiple-antenna communications in rayleigh flat fading. *IEEE Transactions on Information Theory*, 46(2):543–564, Mar 2000.

[MS77] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-correcting Codes*. North-Holland mathematical library. North-Holland Publishing Company, 1977.

[SS98] P.W. Shor and N.J.A. Sloane. A family of optimal packings in grassmannian manifolds. *Journal of Algebraic Combinatorics*, 7(2):157–163, Mar 1998.