On Weight Distribution for Euclidean Image of Binary Linear Codes

Tadashi WADAYAMA, Koichiro WAKASUGI and Masao KASAHARA

Abstract

Some properties of weight distribution for the Euclidean image of binary linear codes are investigated. Many codes defined on Euclidean space can be regarded as the image of binary linear code with a mapping (from binary to signal constellation). We first show the duality of weight distribution for Euclidean image based on a binary linear code C and its dual $C^{\perp}$. In general, weight distribution of Euclidean image is not distance invariant. We present new upper and lower bounds of weight distributions.Furthermore, we present the condition of distance invariance explicitly. Finally, we discuss the computation time of weight enumerator and an extension of upper and lower bounds for group codes.

keywords: weight distribution, linear code, coded modulation

1 Introduction

Many codes defined on Euclidean space are based on a binary linear code C and a mapping ϕ. A codeword of C with length $n = Nb$ is partitioned into consecutive N-segments. Each segment consists of b-bits. The mapping ϕ is a mapping from b-bits to a subconstellation S_i, contained in a signal constellation S. The *Euclidean image of binary linear code* $Img_\phi(C)$ can be naturally defined by the set of codewords which have the following form:

$$(s_0, s_1, \ldots, s_{N-1}) \quad , \quad s_i \in \phi(x_i), \tag{1}$$

$$(x_0, x_1, \ldots, x_{N-1}) \quad \in C, \tag{2}$$

where x_i means the i-th segment of a codeword of C.

In this paper, we shall derive some important properties of the weight distribution of $Img_\phi(C)$. In Section 3, we present the duality of weight enumerators for $Img_\phi(C)$ and its dual $Img_\phi(C^{\perp})$. Our derivation of the duality is based on the proof of binary version of MacWilliams theorem[1)]. We next extend the duality for Euclidean image with time variant mapping. With this extension, we can determine the weight enumerator for the Euclidean image of the translate of binary linear code. In Section 4, we prove lower and upper bounds of weight enumerator with respect to $\succeq$, which is a partial order defined on comparable polynomials. These bounds can be applied for any binary linear code and mapping even if the resulting Euclidean image is not distance-invariant. Furthermore we present the condition of distance-invariance explicitly. In Section 5, an extension of the upper bound is discussed as a concluding remark.

2 Preliminaries

2.1 Byte-wise representation

In this paper, we denote Galois field GF(2) by F_2. The element of the n-times Cartesian product of F_2, $u \in F_2^n$,is denoted by the following bit-wise representation:

$$u = (u_1, u_2, \ldots, u_n)_1, \quad u_i \in F_2. \tag{3}$$

The same element u can be denoted by the following byte-wise representation:

$$u = (u_1, u_2, \ldots, u_N)_b, \quad u_i \in F_2^b, \tag{4}$$

where $N = n/b$. We call $u_i \in F_2^b$,*byte*. We represent an element in F_2^n in various ways. For example, the element in F_2^6:

$$(1, 0, 1, 1, 0, 1)_1 \tag{5}$$

can be denoted in the following ways:

$$(10, 11, 01)_2 \quad \text{or} \quad (101, 101)_3 \quad \text{or} \quad (101101)_6. \tag{6}$$

Moreover, the element can be written as 101101 with no parenthesis.

2.2 Signal constellation

Let us assume that a given signal constellation (a set of points in an L-dimensional Euclidean space) S is partitioned into disjoint subconstellations:

$$S = \bigcup_{i \in F_2^b} S_i. \tag{7}$$

The number of subconstellations is 2^b. We can define the *Euclidean weight enumerator* $E_{S_i}(z)$ by

$$E_{S_i}(z) = \sum_{s \in S_i} z^{||s - s_0||^2}, \tag{8}$$

where the signal point $s_0 \in S$ is referred to as the *origin* of the signal constellation. Except for Section 4, the origin s_0 is assumed to be in S_{0^b}, where 0^b means a b-tuple of zeros. The Euclidean weight enumerator *centered on the point* $p \in S$,$E_S^{(p)}(z)$, is given by

$$E_{S_i}^{(p)}(z) = \sum_{s \in S_i} z^{||s - p||^2}. \tag{9}$$

Thus $E_{S_i}(z)$ is equivalent to $E_{S_i}^{(s_0)}(z)$. In this paper, we often omit the dummy variable z of a weight enumerator for simplicity.

2.3 Euclidean image of binary linear code

Let us consider the following mapping:

$$\phi(x) \mapsto S_x, \quad x \in F_2^b, \tag{10}$$

where S_x is a subconstellations. The Euclidean image of binary linear code C with the mapping ϕ is defined by

$$\begin{aligned} Img_\phi(C) = \{(m_1, m_2, \ldots, m_N) \mid m_i \in \phi(u_i) 1 \leq i \leq N, \\ u = (u_1, u_2, \ldots, u_N)_b \in C\}. \end{aligned} \tag{11}$$

The weight enumerator for $Img_\phi(C)$ is given by

$$E_{Img_\phi(C)} = \sum_{u \in C} E_{\phi(u)}, \tag{12}$$

where $E_{\phi(u)}$ is defined by

$$E_{\phi(u)} = \prod_{1 \leq i \leq N} E_{\phi(u_i)}. \tag{13}$$

3 Duality of Euclidean image of dual code

3.1 Hadamard transform

Let f be any mapping over F_2^n. The Hadamard transform[1)] $\hat{f}$ of f is given by

$$\hat{f}(u) = \sum_{v \in F_2^n} (-1)^{u \cdot v} f(v), \quad u \in F_2^n. \tag{14}$$

Between a binary linear code C and its dual code $C^\perp$, the following important equality holds[1)]:

$$\sum_{w \in C^\perp} f(w) = \frac{1}{|C|} \sum_{u \in C} \hat{f}(u). \tag{15}$$

Substituting Eq.(14) for Eq.(15), we then have

$$\sum_{w \in C^\perp} f(w) = \frac{1}{|C|} \sum_{u \in C} \sum_{v \in F_2^n} (-1)^{u \cdot v} f(v). \tag{16}$$

Let us set

$$f(x) = E_{\phi(x)}. \tag{17}$$

The lefthandside(LHS) of Eq.(16) becomes the weight enumerator of $Img(C^\perp)$:

$$\begin{aligned} (\text{LHS of Eq.16}) &= \sum_{w \in C^\perp} E_{\phi(w)} && (18) \\ &= E_{Img_\phi(C^\perp)}. && (19) \end{aligned}$$

The righthandside(RHS) of Eq.(16) can be transformed as follows:

$$\begin{aligned} (\text{RHS of Eq.16}) &= \frac{1}{|C|} \sum_{u \in C} \sum_{v \in F_2^n} (-1)^{u \cdot v} E_{\phi(v)} && (20) \\ &= \frac{1}{|C|} \sum_{u \in C} \sum_{v \in F_2^n} (-1)^{u \cdot v} \prod_{1 \le i \le N} E_{\phi(v_i)} && (21) \\ &= \frac{1}{|C|} \sum_{u \in C} \sum_{v \in F_2^n} \prod_{1 \le i \le N} (-1)^{u_i \cdot v_i} \cdot E_{\phi(v_i)} && (22) \\ &= \frac{1}{|C|} \sum_{u \in C} \prod_{1 \le i \le N} \sum_{v_i \in F_2^b} (-1)^{u_i \cdot v_i} \cdot E_{\phi(v_i)} && (23) \end{aligned}$$

where

$$\begin{aligned} u &= (u_1, u_2, \ldots, u_N)_b, \quad u_i \in F_2^b, && (24) \\ v &= (v_1, v_2, \ldots, v_N)_b, \quad v_i \in F_2^b. && (25) \end{aligned}$$

Now,we define the Hadamard transform of $E_{\phi(x)}, x \in F_2^b$ by

$$\hat{E}_{\phi(x)} = \sum_{y \in F_2^b} (-1)^{x \cdot y} \cdot E_{\phi(y)}. \tag{26}$$

From the definition of $\hat{E}_{\phi(x)}$, Eq.(23) can be written as

$$\prod_{1 \le i \le N} \{ \sum_{v_i \in F_2^b} (-1)^{u_i \cdot v_i} \cdot E_{\phi(v_i)} \} = \frac{1}{|C|} \sum_{u \in C} \prod_{1 \le i \le N} \hat{E}_{\phi(u_i)}. \tag{27}$$

Consequently,we have the following theorem:

Theorem 1 *For any binary linear code C and mapping ϕ,*

$$E_{Img_\phi(C^\perp)} = \frac{1}{|C|} \sum_{u \in C} \hat{E}_{\phi(u)}, \tag{28}$$

where

$$\hat{E}_{\phi(u)} = \prod_{1 \le i \le N} \hat{E}_{\phi(u_i)}. \tag{29}$$

Now,we see the theorem from another point of view. The following multivariate polynomial:

$$W_C^{(b)}(a_k) = \sum_{u \in C} \prod_{1 \le i \le N} a_{u_i}, \quad k \in F_2^b \tag{30}$$

is referred to as the *byte-weight enumerator of C with byte-width b.* The Hadamard transform on the variables are defined in the same way as weight enumerators. For example, $\hat{a}_{01} = a_{00} - a_{01} + a_{10} - a_{11}$.

From Eq.(12) and Eq.(28), the weight enumerators of $Img_\phi(C)$ and $Img_\phi(C^\perp)$ are given by substituting the weight enumerator corresponding to the variable a_i into $W_C^{(b)}$:

Corollary 1

$$\begin{aligned} E_{Img_\phi(C)} &= W_C^{(b)} \mid_{a_k \to E_{\phi(k)}}, \quad k \in F_2^b, & (31)\\ E_{Img_\phi(C^\perp)} &= W_{C^\perp}^{(b)} \mid_{a_k \to E_{\phi(k)}}, \quad k \in F_2^b, & (32)\\ W_{C^\perp}^{(b)} &= \frac{1}{|C|} W_C^{(b)} \mid_{a_k \to \hat{a}_k} \quad k \in F_2^b. & (33) \end{aligned}$$

where the notation $P \mid_{A \to E}$ means the replacement of the variable A with E in the polynomial P.

Example 1 *Assume that the binary linear code C (code #1 in [1]) has the following generator matrix and the parity check matrix:*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}. \tag{34}$$

The 8-PSK constellation (Fig.1) is defined as

$$\{P_k \mid P_k = exp(j\frac{k\pi}{4}), \quad 0 \le k \le 7\}. \tag{35}$$

The constellation consists of equally spaced 8-signal points on the unit circle. The following 4-subconstellation of 8-PSK and the corresponding weight enumerators are used:

$$\begin{aligned} \phi(00) &= \{P_0, P_4\}, \quad E_{\phi(00)} = 1 + z^4, & (36)\\ \phi(01) &= \{P_3, P_7\}, \quad E_{\phi(01)} = z^{0.586} + z^{3.414}, & (37)\\ \phi(10) &= \{P_2, P_6\}, \quad E_{\phi(10)} = 2z^2, & (38)\\ \phi(11) &= \{P_1, P_5\}, \quad E_{\phi(11)} = z^{0.586} + z^{3.414}. & (39) \end{aligned}$$

The byte-weight enumerator of C is given by

$$W_C^{(2)}(a_{00}, a_{01}, a_{10}, a_{11}) = a_{00}^3 + a_{01}^3 + 3a_{00}a_{10}a_{11} + 3a_{01}a_{10}a_{11}. \tag{40}$$

The Hadamard transform of the variables a_i is given by

$$\begin{aligned}\hat{a}_{00} &= a_{00}+a_{01}+a_{10}+a_{11}, &(41)\\ \hat{a}_{01} &= a_{00}-a_{01}+a_{10}-a_{11}, &(42)\\ \hat{a}_{10} &= a_{00}+a_{01}-a_{10}-a_{11}, &(43)\\ \hat{a}_{11} &= a_{00}-a_{01}-a_{10}+a_{11}. &(44)\end{aligned}$$

From Corollary 1, we have

$$\begin{aligned}W^{(2)}_{C^\perp}(a_{00},a_{01},a_{10},a_{11}) &= \frac{1}{8}W^{(2)}_C(\hat{a}_{00},\hat{a}_{01},\hat{a}_{10},\hat{a}_{11})\\ &= a_{00}^3+a_{10}^3\\ &+ 3a_{00}a_{01}a_{11}+3a_{01}a_{10}a_{11}. \qquad (45)\end{aligned}$$

By substituting $E_{\phi(i)}$ for $W^{(2)}_C$ and $W^{(2)}_{C^\perp}$, we have the Euclidean weight enumerators $E_{Img_\phi(C)}$ and $E_{Img_\phi(C^\perp)}$ as follows:

$$\begin{aligned}E_{Img_\phi(C)} &= 1+z^{1.758}+6z^{2.586}+6z^{3.172}+3z^4\cdots+z^{12},\\ E_{Img_\phi(C^\perp)} &= 1+3z^{1.172}+6z^{3.172}+9z^4\cdots+z^{12}.\end{aligned}$$

3.2 Euclidean image of translate of binary linear code

Let C be a binary linear code with length n. The translate of C by $v\notin C$ is defined by

$$C\oplus v=\{w\oplus v \mid w\in C\}. \qquad (46)$$

For a given mapping ϕ, the Euclidean image of $C\oplus v$ and the corresponding Euclidean weight enumerator $E_{Img_\phi(C\oplus v)}$ can be defined by Eqs (11) and (12) changing C to $C\oplus v$. In the following, we shall derive the relation between $E_{Img_\phi(C\oplus v)}$ and $E_{Img_\phi(C^\perp\oplus v)}$.

For dealing with the translate of linear code, we generalize the definition of the Euclidean image of binary linear code as follows:

$$\begin{aligned}Img_{\boldsymbol{\psi}}(C)=\{(m_1,m_2,\ldots,m_N)\mid m_i\in\psi_i(u_i)\\ u=(u_1,u_2,\ldots,u_N)_b\in C\}.\end{aligned} \qquad (47)$$

$$E_{Img_{\boldsymbol{\psi}}(C)}=\sum_{u\in C}E_{\boldsymbol{\psi}(u)}, \qquad (48)$$

where $E_{\boldsymbol{\psi}}(u)$ is given by

$$E_{\boldsymbol{\psi}(u)}=\prod_{1\le i\le N}E_{\psi_i(u_i)}. \qquad (49)$$

It should be noted that the original definition (11) is for the Euclidean image of binary linear code with *time invariant mapping* and the generalized definition (47), for that of binary linear code with *time variant mapping.*

Letting

$$f(x)=E_{\boldsymbol{\psi}(u)} \qquad (50)$$

in Eq.(16) and transforming the equation in a similar manner, we have the following theorem immediately.

Theorem 2 *(for time variant mapping) The following relation holds:*

$$E_{Img_{\boldsymbol{\psi}}(C^{\perp})} = \frac{1}{|C|} \sum_{u \in C} \hat{E}_{\boldsymbol{\psi}(u)}, \tag{51}$$

where

$$\hat{E}_{\boldsymbol{\psi}(u)} = \prod_{1 \le i \le N} \hat{E}_{\psi_i(u_i)}. \tag{52}$$

The Hadamard transform is given by

$$\hat{E}_{\psi_i(x)} = \sum_{y \in F_2^b} (-1)^{x \cdot y} \cdot E_{\psi_i(y)}. \tag{53}$$

Theorem 2 is a generalization of Theorem 1.

With Theorem 2, we can deal with a translate of binary linear code completely. Let us assume the following mapping:

$$\psi_i(x) = \phi(x \oplus v_i), \quad x \in F_2^b, \tag{54}$$

where $v = (v_1, v_2, \ldots, v_N)_b$. Under this assumption, we see that $Img_\phi(C \oplus v)$ and $Img_\phi(C^\perp \oplus v)$ are equivalent to $Img_{\boldsymbol{\psi}}(C)$ and $Img_{\boldsymbol{\psi}}(C^\perp)$, respectively. Thus we can derive $E_{Img_\phi(C^\perp \oplus v)}$ from Theorem 2.

4 Lower and upper bounds of weight enumerator

The weight enumerator for $Img_\phi(C)$ centered on the $w \in Img_\phi(C)$ is given by

$$E^{(w)}_{Img_\phi(C)} = \sum_{u \in C} E^{(w_1)}_{\phi(u_1)} E^{(w_2)}_{\phi(u_2)} \cdots E^{(w_N)}_{\phi(u_N)}, \tag{55}$$

where

$$w = (w_1, w_2, \ldots, w_N)_b. \tag{56}$$

In general, $E^{(w_1)}_{Img_\phi(C)}$ may not coincide with $E^{(w_2)}_{Img_\phi(C)}$ for $w_1 \neq w_2 \in Img_\phi(C)$. In this section, we shall prove a lower and upper bound of $E^{(w)}_{Img_\phi(C)}$ for $w \in Img_\phi(C)$.

4.1 Partial order on comparable polynomials

Polynomials $A(z)$ and $B(z)$ are called *comparable* if and only if they satisfy the following Conditions 1 and 2:

Condition 1 The polynomials $A(z)$ and $B(z)$ are polynomials with non-negative coefficients such that

$$A(z) = a_{i_n} z^{i_n} + a_{i_{n-1}} z^{i_{n-1}} + \cdots a_{i_0} z^{i_0}, \quad a_{i_s} \in Z^+, \quad i_s \in R^+, \tag{57}$$

$$B(z) = b_{i_n} z^{i_n} + b_{i_{n-1}} z^{i_{n-1}} + \cdots b_{i_0} z^{i_0}, \quad b_{i_s} \in Z^+, \quad i_s \in R^+, \tag{58}$$

where Z^+ is the set of non-negative integer and R^+ is the set of non-negative real number.

Condition 2 For all i_s, the followings holds:

$$a_{i_s} \ge b_{i_s}, \tag{59}$$

or

$$a_{i_s} \le b_{i_s}. \tag{60}$$

When Eq.(59) holds, we denote

$$A(z) \succeq B(z), \tag{61}$$

otherwise

$$A(z) \preceq B(z). \tag{62}$$

Let us consider two sets of M-polynomials $A_i(z)$ and $B_i(z)$, where $A_i(z)$ and $B_i(z)$ are comparable for each i. It is evident that the following lemmas hold, because of the non-negative property of coefficients.

Lemma 1 *If $A_i(z) \succeq B_i(z)$ for each i , then*

$$\prod_i A_i(z) \succeq \prod_i B_i(z). \tag{63}$$

Lemma 2 *If $A_i(z) \succeq B_i(z)$ for each i, then*

$$\sum_i A_i(z) \succeq \sum_i B_i(z). \tag{64}$$

For a given set of polynomials $A_i(z)$,which are not necessarily comparable to each other, the supremum, $\sup_i A_i(z)$, can be defined as the minimum(with respect to $\succeq$) polynomial in the upper bound set of $A_i(z)$:

$$\sup_i A_i(z) = \min_{\forall i, x(z) \succeq A_i(z)} x(z). \tag{65}$$

In a similar manner, we can define the infimum, $\inf_i A_i(z)$, by

$$\inf_i A_i(z) = \max_{\forall i, x(z) \preceq A_i(z)} x(z). \tag{66}$$

Example 2 *If $A_0(z) = 1 + 2z^2, A_1(z) = z + z^2$ then*

$$\underset{i}{sup}\, A_i(z) = 1 + z + 2z^2, \tag{67}$$

$$\underset{i}{inf}\, A_i(z) = z^2. \tag{68}$$

4.2 Lower and upper bounds

We now define the supremum of the weight enumerator corresponding to subconstellation $\phi(i)$ such that

$$E^{(sup)}_{\phi(i)} \triangleq \sup_{\substack{j \in F_2^b \\ s \in \phi(j)}} E^{(s)}_{\phi(i \oplus j)}. \tag{69}$$

By changing the variable $i \oplus j \to i$ in the definition of $E^{(sup)}_{\phi(i)}$, we have an inequality:

$$E^{(sup)}_{\phi(i \oplus j)} \succeq E^{(s)}_{\phi(i)}, \quad i, j \in F_2^b, \quad s \in \phi(j). \tag{70}$$

we have an upper bound of $E^{(w)}_{Img_\phi(C)}$:

$$\begin{aligned} E^{(w)}_{Img_\phi(C)} &= \sum_{u \in C} E^{(w_1)}_{\phi(u_1)} E^{(w_2)}_{\phi(u_2)} \cdots E^{(w_N)}_{\phi(u_N)}, \quad w \in Img(C) \\ &\preceq^1 \sum_{u \in C} E^{(sup)}_{\phi(u_1 \oplus v_1)} E^{(sup)}_{\phi(u_2 \oplus v_2)} \cdots E^{(sup)}_{\phi(u_N \oplus v_N)}, w_i \in \phi(v_i) \\ &=^2 \sum_{u' \in C} E^{(sup)}_{\phi(u'_1)} E^{(sup)}_{\phi(u'_2)} \cdots E^{(sup)}_{\phi(u'_N)} \\ &\triangleq E^{(sup)}_{Img_\phi(C)}, \end{aligned} \tag{71}$$

where $\preceq^1$,$=^2$ hold because
$\preceq^1$: Lemmas 1, 2 and inequality (70),
$=^2$: C is closed under a componentwise mod-2 addition.

In a similar manner, we have a lower bound of $E^{(w)}_{Img(C)}$:

$$E^{(w)}_{Img_\phi(C)} \succeq \sum_{u \in C} E^{(inf)}_{\phi(u_1)} E^{(inf)}_{\phi(u_2)} \cdots E^{(inf)}_{\phi(u_N)} \triangleq E^{(inf)}_{Img_\phi(C)}, \quad (72)$$

where $E^{(inf)}_{\phi(i)}$ is given by

$$E^{(inf)}_{\phi(i)} \triangleq \inf_{\substack{j \in F_2^b \\ s \in \phi(j)}} E^{(s)}_{\phi(i \oplus j)}. \quad (73)$$

We have proved the following theorem:

Theorem 3 *(Upper and lower bounds of weight enumerator) For any $w \in Img(C)$,*

$$E^{(inf)}_{Img_\phi(C)} \preceq E^{(w)}_{Img_\phi(C)} \preceq E^{(sup)}_{Img_\phi(C)}. \quad (74)$$

In terms of coding theory, $E^{(sup)}_{Img_\phi(C)}$ is more important than $E^{(inf)}_{Img_\phi(C)}$, because $E^{(sup)}_{Img_\phi(C)}$ provides information on the lower bound of the minimum Euclidean distance and the upper bound of its multiplicity (the number of codewords which have the minimum Euclidean weight). We shall refer to $E^{(sup)}_{Img(C)}$ as the *worst Euclidean weight enumerator* for $Img_\phi(C)$.

Example 3 *Let us assume that C is generated by G (Eq.34). The mapping ϕ is defined by*

$$\phi(00) = \{P_0, P_6\}, \quad (75)$$
$$\phi(01) = \{P_3, P_5\}, \quad (76)$$
$$\phi(10) = \{P_1, P_7\}, \quad (77)$$
$$\phi(11) = \{P_2, P_4\}. \quad (78)$$

The weight enumerators $E^{(p)}_{\phi(i \oplus j)}$ are given in Table 1. From Table 1, we easily obtain

$$E^{(sup)}_{\phi(00)} = 1 + z^2, \quad (79)$$
$$E^{(sup)}_{\phi(01)} = z^{0.586} + 2z^{3.414}, \quad (80)$$
$$E^{(sup)}_{\phi(10)} = 2z^{0.586} + z^{3.414}, \quad (81)$$
$$E^{(sup)}_{\phi(11)} = z^2 + z^4. \quad (82)$$

By substituting these weight enumerators for Eq.(40), we have the worst weight enumerator:

$$E^{(sup)}_{img_\phi(C)} = 1 + z^{1.758} + 3z^2 + 6z^{2.586} + 6z^{3.172} + 3z^4 + 18z^{4.586} + 6z^{5.172} + 3z^{5.414} + 16z^6 + \cdots. \quad (83)$$

For $a = (0,0,0)$ and $b = (6,6,6)$, the weight enumerators centered on a and b are given by

$$E^{(a)}_{img_\phi(C)} = 1 + 3z^2 + 6z^{2.586} + 3z^4 + 12z^{4.586} + 13z^6 + \cdots, \quad (84)$$

$$E^{(b)}_{img_\phi(C)} = 1 + z^{1.758} + 3z^2 + 3z^{2.586} + 3z^{3.172} + 3z^4 + 9z^{4.586} + 3z^{5.414} + 7z^6 + \cdots. \quad (85)$$

We see that these weight enumerators are upper bounded by $E^{(sup)}_{img_\phi(C)}$ in Eq.(83).

For any $w \in Img_\phi(C)$, if the weight enumerator $E^{(w)}_{Img_\phi(C)}$ is independent of w and equal to the same weight enumerator $E^{(inv)}_{Img_\phi(C)}$, we call $Img_\phi(C)$ *distance-invariant.* Here we prove that $Img_\phi(C)$ becomes distance-invariant.

If $E^{(s)}_{\phi(i\oplus j)}$ is independent of j and s:

$$E^{(inv)}_{\phi(i)} = E^{(s)}_{\phi(i\oplus j)}, \quad {}^\forall j \in F_2^b, \quad {}^\forall s \in \phi(j), \quad (86)$$

then $E^{(sup)}_{\phi(i)}$ coincides with $E^{(inf)}_{\phi(i)}$:

$$E^{(sup)}_{\phi(i)} = E^{(inf)}_{\phi(i)} = E^{(inv)}_{\phi(i)}. \quad (87)$$

Thus $E^{(sup)}_{Img_\phi(C)}$ also coincides with $E^{(inf)}_{Img_\phi(C)}$:

$$E^{(sup)}_{Img_\phi(C)} = E^{(inf)}_{Img_\phi(C)} \triangleq E^{(inv)}_{Img_\phi(C)}. \quad (88)$$

Consequently, from Eq.(88) and Theorem 3,we have

$$E^{(w)}_{Img_\phi(C)} = E^{(inv)}_{Img_\phi(C)} \quad (89)$$

for any $w \in Img_\phi(C)$. This is exactly the condition of the distance invariance.

Corollary 2 *If Eq.(86) holds, then $Img_\phi(C)$ is distance-invariant.*

Example 4 *The Euclidean image $Img_\phi(C)$ in Example 1 is distance-invariant, because the following relations hold for any $j \in F_2^2$ and $s \in \phi(j)$:*

$$E^{(s)}_{\phi(00\oplus j)} = 1 + z^4, \quad (90)$$

$$E^{(s)}_{\phi(01\oplus j)} = z^{0.586} + z^{3.414}, \quad (91)$$

$$E^{(s)}_{\phi(10\oplus j)} = 2z^2, \quad (92)$$

$$E^{(s)}_{\phi(11\oplus j)} = z^{0.586} + z^{3.414}. \quad (93)$$

From Table 1, we see that the Euclidean image $Img_\phi(C)$ in Example 3 is not *distance-invariant.*

5 Conclusion

For trellis-codes including Ungerboeck's code, Zehavi and Wolf[2)] presented the modified transfer function method which enables detail analysis of decoding performance. Our upper bound can be also used for analyzing non-distance-invariant code defined on Euclidean space. Furthermore, our bound requires no symmetric condition of signal constellation unlike the Zehavi-Wolf method.

For proving the upper and lower bounds, the inequality Eq.(70) plays an essential role. Instead of componentwise mod-2 addition, if the code is closed under the componentwise (commutative) group addition $\star$, we can modify the definition Eq.(69) of the supremum corresponding to $\phi(i)$ such that

$$E_{\phi(i)}^{(sup)} \triangleq \sup_{\substack{j \in G^b \\ s \in \phi(j)}} E_{\phi(i \star j)}^{(s)}, \tag{94}$$

where G is an additive group corresponding to $\star$. We then have the upper and lower bounds for the Euclidean image for group code. The condition of distance-invariance becomes

$$E_{\phi(i)}^{(inv)} = E_{\phi(i \star j)}^{(s)}, \quad {}^{\forall} j \in G^b, \quad {}^{\forall} s \in \phi(j). \tag{95}$$

By using Eq.(95), it is easy to check whether a given code is distance-invariant or not.

Department of System Engineering,
Faculty of Computer Science and System Engineering,
Okayama Prefectural University,
111 Kuboki, Soja-shi, Okayama,Japan 719-11 (T.W.)

Department of Electronics and Information Science,
Faculty of Engineering and Design,
Kyoto Institute of Technology,
Matsugasaki,Sakyo-ku, Kyoto,Japan, 606 (K.W.)

Department of Electronics and Information Science,
Faculty of Engineering and Design,
Kyoto Institute of Technology,
Matsugasaki,Sakyo-ku, Kyoto,Japan, 606 (M.K.)

References

1) F. J. MacWiliams and N. J. A.Sloane: "The Theory of Error-Correcting Codes", North Holland (1977).

2) E. Zehavi and J. K. Wolf: "On the performance evaluation of trellis codes", *IEEE Trans. Inform.Theory*, **IT-33**, pp. 196–202 (1989).