Weight Enumerator Analysis for $(2, P)$- and $(3, P)$-SFA LDPC Codes

Manabu Hagiwara
Research Institute for Secure Systems (RISEC)
National Institute of
Advanced Industrial Science and Technology (AIST),
Central 2, 1-1-1 Umezono, Tsukuba City,
Ibaraki, 305-8568, JAPAN
Email: hagiwara.hagiwara@aist.go.jp

J. B. Nation
Department of Mathematics
University of Hawaii at Manoa,
2565 McCarthy Mall, Honolulu, Hawaii 96822, USA
Email: jb@math.hawaii.edu

***Abstract*—Let C and C' be (J, P)-SFA LDPC codes with $J = 2$ or 3. Then the weight enumerator polynomials of C and C' are identical: $W(C; X, Y) = W(C'; X, Y)$.**

I. Introduction

The weight enumerator for binary codes has been widely studied, and has influenced both engineering and pure mathematics. One direct application for engineering is to estimate the probability of undetectable error over a binary symmetric channel. For a linear code C transmitted over a binary symmetric channel with cross-over probability p, the probability of undetectable error is equal to $W(C; 1-p, p)-(1-p)^n$, where $W(C; X, Y)$ is the weight enumerator of C and we assume the codewords are chosen from a uniform distribution. A typical research examples from pure mathematics is the classification problem for extremal type II codes [1]. The classification problem is purely mathematically interesting, and therefore it has been spreading in unexpected directions, *e.g.*, vertex operator algebras [2], even lattices [3].

In general, an LDPC code is defined as "a kernel of a sparse matrix." This definition is meaningful from the point of view of coding theory, but it is difficult to use for calculating weight distributions. On the other hand, the definition of SFA LDPC codes is given in algebraic terms, which allows for a more analytical study of these codes. For example, the Tanner graph of the parity-check matrix of an SFA LDPC code never contains a cycle of size 4. For another example, the minimum weight of SFA LDPC codes has been investigated by Yang and Helleseth [4], and Sugiyama and Kaji [5]. Yang and Helleseth [4] determined that for cases with column weight 4 and block size 5 or 7, the minimum weight is 8, and for cases with the same column weight and with larger block sizes, it is possibly 10 [4]. Sugiyama and Kaji [5] determined that the minimum weights for cases with column weight 5 and block size > 7, the minimum weight is 10 or 12.

Although the minimum weights of codes may be a valuable indicator of the performance of linear block codes, it is not the only way to evaluate the efficiency of codes. In this paper, we show that for cases with column weight 2 and 3 and with block size a prime number, all (generalized) SFA LDPC codes have the same weight enumerator. A standard technique to show two linear codes have the same weight enumerator has been to construct an index permutation for code space. Our technique in this paper has different aspect from it. As a novel technique to show that, we apply a "row-index" permutation of their "parity-check matrices".

II. Preliminaries

Throughout this paper, let $\mathbb{F}_2 = \{0, 1\}$ denote a binary field, $\mathbb{Z}$ the integer set, and $\mathbb{Z}_P$ the residue ring modulo a positive integer P.

SFA (simple full-length array) **LDPC** (low-density parity-check) codes are defined as instances of **QC** (quasi-cyclic) LDPC codes [6], [7], [8], [9], [10]. Let us start by introducing QC LDPC codes.

Let P be a positive integer. For each integer x, we define a square matrix $I(x)$ of degree P by putting

$$I(1) := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & & 1 \\ 1 & 0 & \dots & & 0 \end{pmatrix}, \quad I(x) := I(1)^x.$$

We call $I(x)$ a **circulant matrix**.

Definition (Quasi-Cyclic LDPC Matrix with Circulant Matrices)**.** Let J, L and P be positive integers. We call a matrix H over $\mathbb{F}_2$ a QC LDPC matrix if H consists of the same size circulant matrices, *i.e.*,

$$H = \begin{pmatrix} I(a_{1,1}) & I(a_{1,2}) & \dots & I(a_{1,L}) \\ I(a_{2,1}) & I(a_{2,2}) & \dots & I(a_{2,L}) \\ \vdots & & \ddots & \vdots \\ I(a_{J,1}) & I(a_{J,2}) & \dots & I(a_{J,L}) \end{pmatrix},$$

where $a_{j,l} \in \mathbb{Z}$.

Definition (SFA LDPC Matrix)**.** Let J and P be positive numbers. For a pair (J, P) and a vector $a := (a_1, a_2, \dots, a_J) \in$

$\mathbb{Z}_P^J$ such that each entry is distinct from other, a matrix H_a is defined as follows:

$$H_a := (I(a_j(l-1)))_{1\le j\le J, 1\le l\le P},$$

where $I(x)$ is a circulant matrix of size P-by-P. The matrix H_a is called a (J,P) **SFA-LDPC matrix with respect to** a, or simply is called a **generalized SFA-LDPC matrix**.

Thus H_a is a $JP \times LP$ matrix.

Remark II.1. A (J,P) SFA-LDPC matrix H_δ with respect to $\delta = (0,1,\dots,J-1)$ is known as a (J,P)-SFA LDPC matrix in the sense of [5], [11].

Example II.2. *Let* $J = 2, P = 5$.
For $a = (2,4)$,

$$H_a = \begin{pmatrix} I(0) & I(2) & I(4) & I(1) & I(3) \\ I(0) & I(4) & I(3) & I(2) & I(1) \end{pmatrix}.$$

For $\delta = (0,1)$,

$$H_\delta = \begin{pmatrix} I(0) & I(0) & I(0) & I(0) & I(0) \\ I(0) & I(1) & I(2) & I(3) & I(4) \end{pmatrix}.$$

Definition (SFA LDPC Codes)**.** Let H_a be a (J,P) SFA-LDPC matrix with respect to a vector a. An **SFA LDPC code** C_a is defined as the kernel of H_a, *i.e.*,

$$C_a := \{c \in \mathbb{F}_2^{P^2} \mid H_a c^T = 0\},$$

where c^T is the transpose of c.

Our primary interest is to determine the weight enumerator (or the weight distribution) of a given LDPC code [12].

Definition (Weigh Enumerator)**.** Let n be a positive integer. For a subset $C \subset \mathbb{F}_2^n$, the following polynomial

$$W(C;X,Y) := \sum_{c\in C} X^{\mathrm{wt}(c)} Y^{n-\mathrm{wt}(c)}$$

is called the **weight enumerator** (or the weight distribution) of C, where $\mathrm{wt}(c)$ is Hamming weight of c.

The following is our main contribution.

Theorem II.3. *Let P and J be positive integers.*
Let $a = (a_1,\dots,a_J)$, $\delta \in \mathbb{Z}_P^J$ be vectors such that all the entries of a are distinct from each other, and $\delta = (0,1,\dots,J-1)$. For (J,P)-SFA LDPC codes C_a and C_δ, if P is a prime number and $J = 2, 3$, we have

$$W(C_a;X,Y) = W(C_\delta;X,Y).$$

In other words, our theorem implies that the weight distribution does not depend on the choice of a and we can focus on the case δ. In particular, once we determine the minimum weight of a (J,P)-SFA code, then we determine the minimum weight of any (J,P)-SFA codes for $J = 2,3$. The proof is given in the next section.

III. Weight Enumerator of SFA LDPC Codes

A. Canonical Representation

A weight enumerator is invariant for index-permutations of rows and columns for a parity-check matrix. Formally, for a linear code C with respect to a parity-check matrix H, a row-index permutation σ and a column-index permutation τ for H, we have

$$W(C;X,Y) = W(C';X,Y),$$

where C' is a linear code with respect to a parity-check matrix $\sigma H \tau$. In this paper, we call two matrices H_1, H_2 **equivalent** if there exists a row (resp. column) index permutation σ (resp. τ) such that $H_1 = \sigma H_2 \tau$. The following observations are fundamental for equivalence on SFA-LDPC matrices.

Theorem III.1. *Let $(a_1,a_2,\dots,a_J) \in \mathbb{Z}_P^J$ be a vector.*
A (J,P)-SFA LDPC matrix H_a is equivalent to

i) $H_{(a_{\sigma(1)},a_{\sigma(2)},\dots,a_{\sigma(J)},)}$ *for a permutation σ on a set $\{1,2,\dots,J\}$.*
ii) $H_{(a_1-x,a_2-x,\dots,a_J-x)}$ *for any $x \in \mathbb{Z}_P$,*
iii) $H_{(a_j^{-1}a_1,a_j^{-1}a_2,\dots,a_j^{-1}a_J)}$ *if $a_j \neq 0$.*

The statement i) is directly obtained from the definition of equivalence.

The following observation helps to prove ii). Let s (resp. t) denote a cyclic shift for the row (resp. column) indices of a $P \times P$ matrix. In other words, s permutes the i-th row to the $i+1 \pmod P$-th row. Then we have

$$s^y I(x) t^z = I(x-y+z).$$

Let $\sigma := s^{y_1} \times s^{y_2} \times \cdots \times s^{y_J}$ denote a row index permutation of $JP \times P^2$ matrix H such that it acts on the jth block of $H = (I(a_{j,l}))$ as y_j. Similarly we define an action of $\tau := t^{z_1} \times \cdots \times t^{z_P}$ to column indices of P^2. Then we have

$$\sigma H \tau = (I(a_{j,l} - y_j + z_l)).$$

Lemma III.2. *Let $H_a(J,P)$ be a (J,P)-SFA LDPC matrix with respect to a vector $a \in \mathbb{Z}_P^J$. Put $\tau := t^0 \times t^1 \times \cdots \times t^{P-1}$. Then*

$$H_a \tau = H_{a'}$$

where $a' := (a_1+1, a_2+1, \dots, a_J+1)$.

Proof:

$$H_a\tau = (I(a_j(l-1)+(l-1))) = (I((a_j+1)(l-1))) = H_{a'}.$$

■

By applying the proposition above $P - a_1$ times, we have the statement ii). The following is the direct corollary of ii).

Corollary III.3. *For any SFA LDPC matrix $H_{(a_1,a_2,\dots,a_J)}$, there exists a column index permutation τ_1 such that*

$$H_{(a_1,a_2,a_3,\dots,a_J)}\tau_1 = H_{(0,a_2-a_1,a_3-a_1,\dots,a_J-a_1)}.$$

Next we prove iii). By Corollary III.3, there exists a column permutation t_1 such that the jth block row of $H_{(a_1,a_2,\dots,a_J)}$ is $I(0), I(a_j), I(2a_j), \dots, I((P-1)a_j)$, where $a_j \neq 0$.

By our assumption that P is a prime number, the set $\{0, a_j, 2a_j, \ldots, (P-1)a_j\}$ is equal to $\mathbb{Z}_P = \{0, 1, \ldots, P-1\}$. Thus there exists a block-wise column index permutation τ_2 such that the jth block row of $H_{(a_1,a_2,\ldots,a_J)}\tau_2$ is $I(0), I(1), I(2), \ldots, I(P-1)$.

Our claim is that the (j', l)th block of $H_{(a_1,a_2,\ldots,a_J)}\tau_2$ is $I(\frac{a_{j'}}{a_j}(l-1))$. In other words,

$$H_{(a_1,a_2,\ldots,a_J)}\tau_2 = H_{(a_j^{-1}a_1, a_j^{-1}a_2, a_j^{-1}a_3, a_j^{-1}a_4, \ldots, a_j^{-1}a_J)}.$$

The claim is obtained by observation of the (j, l)-th and (j', l)-th blocks of $H_{(a_1,a_2,\ldots,a_J)}$. These blocks are $I(a_j(l-1))$ and $I(a_{j'}(l-1))$. If $a_j(l-1)$ is $m \in \mathbb{Z}_P$, we have $a_{j'}(l-1) = \frac{a_{j'}}{a_j}a_j(l-1) = m\frac{a_{j'}}{a_j}$. Therefore, after permuting the columns by τ_2, the j'th block row becomes

$$I(0), I(\frac{a_{j'}}{a_j}), I(2\frac{a_{j'}}{a_j}), \ldots, I((P-1)\frac{a_{j'}}{a_j}).$$

Hence we obtain the statement iii).

As an application of III.1, we give a canonical representation of an SFA-LDPC matrix as follows.

Theorem III.4. *Let P be a prime number. Any SFA LDPC matrix is equivalent to*

$$H_{(0,1,b_3,b_4,\ldots,b_J)},$$

where $b_l \in \mathbb{Z}_P$ and $0, 1, b_3, \ldots, b_J$ are distinct from each other.

Proof: Let $H := H_{(a_1,a_2,\ldots,a_J)}$ be an SFA LDPC matrix. By ii) of Theorem III.1, H is equivalent to

$$H_{(0,a_2-a_1,a_3-a_1,\ldots,a_J-a_1)}.$$

By iii) of Theorem III.1, H is equivalent to

$$H_{(0,1,\frac{a_3-a_1}{a_2-a_1},\ldots,\frac{a_J-a_1}{a_2-a_1})}.$$

It is easy to check that all entries are distinct. ∎

Hence, when P is any positive integer, it is enough to consider the cases where $a_0 = 0$ for determining the weight enumerator of an SFA LDPC code. However, if P is a prime number, it suffices to consider the cases where $b = (0, 1, b_3, b_4, \ldots, b_J)$.

In a case $J = 2$, every $(2, P)$-SFA LDPC matrix is equivalent to $H_{(0,1)}$. Therefore we have the following:

Corollary III.5. *Theorem II.3 holds for $J = 2$.*

To prove our main contribution (Theorem II.3), we will give a deeper argument. For two specific cases $(J, P) = (3, 3)$ and $(3, 5)$, we can prove the statement in a simpler way.

Proposition III.6. *For $(J, P) = (3, 3)$ and $(3, 5)$ cases, we found that all SFA-LDPC matrices are equivalent.*

Proof: For a case $(J, P) = (3, 3)$, every SFA-LDPC matrix has a canonical representation $H_{(0,1,2)}$. Therefore the proposition holds.

For the case $(J, P) = (3, 5)$, there are three canonical representations; $H_{(0,1,2)}, H_{(0,1,3)}$ and $H_{(0,1,4)}$.

First, we prove $H_{(0,1,2)}$ and $H_{(0,1,4)}$ are equivalent. By performing a block row index permutation to $H_{(0,1,4)}$, we have $H_{(4,0,1)}$ is equivalent to $H_{(0,1,4)}$. By performing $t^0 \times t^1 \times \cdots \times t^4$, we have $H_{(4,0,1)}(t^0 \times t^1 \times \cdots \times t^4) = H_{(4+1,0+1,1+1)} = H_{(0,1,2)}$.

Next we prove $H_{(0,1,2)}$ and $H_{(0,1,3)}$ are equivalent. By performing a block row index permutation to $H_{(0,1,3)}$, we have $H_{(0,3,1)}$ is equivalent to $H_{(0,1,3)}$. The canonical representation of $H_{(0,3,1)}$ is $H_{(0,\frac{3}{3},\frac{1}{3})} = H_{(0,1,2)}$.

Thus the statement holds. ∎

B. From the Dual Code

The following is a well-known identity for the weight enumerator for a linear code.

Theorem III.7 (MacWilliams Identity [13])**.** *Let C be a linear code of length n over a binary field $\mathbb{F}_2$, and $C^\perp$ the dual code of C with the standard inner product $\langle , \rangle$ over $\mathbb{F}_2$, i.e. $\langle (c_1, c_2, \ldots c_n), (x_1, x_2, \ldots, x_n)\rangle := \sum_{1\le j\le n} c_j x_j$.*

Then the following equation holds:

$$W(C^\perp; X, Y) = \frac{1}{|C|}W(C; X - Y, X + Y).$$

Therefore, it is enough for proving our main contribution to show that for a fixed P, any dual code of a $(3, P)$-SFA LDPC code has the same weight enumerator.

The code space of a dual code $C^\perp$ of a linear code with respect to a $(3, P)$-SFA LDPC matrix H is given as

$$C^\perp := \{wH \mid w \in \mathbb{F}_2^{3P}\}.$$

Instead of calculating $W(C^\perp; X, Y)$, we investigate

$$\sum_{w\in\mathbb{F}_2^{3P}} X^{P^2-\mathrm{wt}(wH)}Y^{\mathrm{wt}(wH)}.$$

There exists an integer α such that

$$W(C^\perp; X, Y) = \frac{1}{\alpha}\sum_{w\in\mathbb{F}_2^{3P}} X^{P^2-\mathrm{wt}(wH)}Y^{\mathrm{wt}(wH)},$$

where α is a normalizer such that the coefficient on X^{P^2} of the right hand is 1.

Let us divide a vector $w \in \mathbb{F}_2^{3P}$ into $x, y, z \in \mathbb{F}_2^P$ so that $w = (x, y, z)$. Then we have

$$\begin{aligned}
&\sum_{w\in\mathbb{F}_2^{3P}} X^{P^2-\mathrm{wt}(wH)}Y^{\mathrm{wt}(wH)} \\
=\ &\sum_{x,y,z\in\mathbb{F}_2^P} X^{P^2-\mathrm{wt}((x,y,z)H_{(0,1,c)})}Y^{\mathrm{wt}((x,y,z)H_{(0,1,c)})} \\
=\ &\sum_{1\le p,l\le P} (X^{P^2-\mathrm{wt}(x_p+y_{p+(l-1)}+z_{p+c(l-1)})} \\
&\qquad \times Y^{\mathrm{wt}(x_p+y_{p+(l-1)}+z_{p+c(l-1)})}),
\end{aligned}$$

where the addition is taken over modulo P, and x_p is the pth entry of x.

We define a natural map$^-$: $\mathbb{F}_2 \to \mathbb{Z}$ as $\overline{0_{\mathbb{F}_2}} := 0_{\mathbb{Z}}, \overline{1_{\mathbb{F}_2}} := 1_{\mathbb{Z}}$ so that $\overline{1} + \overline{1} = 2$. Then we have

$$\begin{aligned}
&\sum_{1\le p,l\le P} \mathrm{wt}(x_p + y_{p+(l-1)} + z_{p+c(l-1)}) \\
= &\sum_{1\le p,l\le P} (\overline{x_p} + \overline{y_{p+(l-1)}} + \overline{z_{p+c(l-1)}} - 2\overline{x_p z_{p+c(l-1)}} \\
&-2\overline{x_p y_{p+(l-1)}} - 2\overline{z_{p+c(l-1)} y_{p+(l-1)}} \\
&+4\overline{x_p y_{p+(l-1)} z_{p+c(l-1)}}) \\
= &\sum_{1\le p,l\le P} (\overline{x_p} + \overline{y_{p+(l-1)}} + \overline{z_{p+c(l-1)}}) \\
&-2\sum_{1\le p,l\le P} (\overline{x_p z_{p+c(l-1)}} + \overline{x_p y_{p+(l-1)}} \\
&+\overline{z_{p+c(l-1)} y_{p+(l-1)}}) + 4\sum_{1\le p,l\le P} \overline{x_p y_{p+(l-1)} z_{p+c(l-1)}}
\end{aligned}$$

Lemma III.8. $\sum_{1\le p,l\le P}(\overline{x_p} + \overline{y_{p+(l-1)}} + \overline{z_{p+c(l-1)}}) = P\mathrm{wt}(x) + P\mathrm{wt}(y) + P\mathrm{wt}(z)$.

Proof: By the definition of $\overline{x_p}$ and Hamming weight, we have $\sum_{1\le p,l\le P} \overline{x_p} = P\mathrm{wt}(x)$. Similarly, we have $\sum_{1\le p,l\le P} \overline{y_{p+(l-1)}} = P\mathrm{wt}(y)$ and $\sum_{1\le p,l\le P} \overline{z_{p+c(l-1)}} = P\mathrm{wt}(z)$. ∎

Lemma III.9. $\sum_{1\le p,l\le P}(\overline{x_p z_{p+c(l-1)}} + \overline{y_{p+(l-1)} x_p} + \overline{z_{p+c(l-1)} y_{p+(l-1)}}) = \mathrm{wt}(x)\mathrm{wt}(z) + \mathrm{wt}(y)\mathrm{wt}(x) + \mathrm{wt}(z)\mathrm{wt}(y)$

Proof: Here we prove $\sum_{1\le p,l\le P} \overline{x_p z_{p+c(l-1)}} = \mathrm{wt}(x)\mathrm{wt}(z)$.

$$\begin{aligned}
\sum_{1\le p,l\le P} \overline{x_p z_{p+c(l-1)}} &= \sum_{1\le p\le P} \overline{x_p} \sum_{1\le l\le P} \overline{z_{p+c(l-1)}} \\
&= \sum_{1\le p\le P} \overline{x_p} \sum_{1\le p_z\le P} \overline{z_{p_z}} \\
&= \mathrm{wt}(x)\mathrm{wt}(z).
\end{aligned}$$

Similarly we can prove $\sum_{1\le p,l\le P} \overline{y_{p+(l-1)} x_p} = \mathrm{wt}(y)\mathrm{wt}(x)$ and $\sum_{1\le p,l\le P} \overline{z_{p+c(l-1)} y_{p+(l-1)}} = \mathrm{wt}(z)\mathrm{wt}(y)$. ∎

Lemma III.10. $\sum_{1\le p,l\le P} \overline{x_p y_{p+(l-1)} z_{p+c(l-1)}} = \#\{(p,l) \mid 1 \le p,l \le P, x_p = y_{p+(l-1)} = z_{p+c(l-1)} = 1\}$

Proof: $\overline{x_p y_{p+(l-1)} z_{p+c(l-1)}} = 1$ if and only if $x_p = y_{p+(l-1)} = z_{p+c(l-1)} = 1$ ∎

Let us define $\mathrm{Supp}(x) := \{1 \le p \le P \mid x_p = 1\}$ and call it the **support** of x. Then we have

$$\begin{aligned}
&\#\{(p,l) \mid 1 \le p,l \le P, x_p = y_{p+(l-1)} = z_{p+c(l-1)} = 1\} \\
= &\#\{(p,l) \mid 1 \le p,l \le P, p \in \mathrm{Supp}(x), \\
&p + (l-1) \in \mathrm{Supp}(y), p + c(l-1) \in \mathrm{Supp}(z)\} \\
= &\#\{(p_x,p_y,p_z) \in \mathrm{Supp}(x) \times \mathrm{Supp}(y) \times \mathrm{Supp}(z) \\
&\mid 1 \le \exists l \le P, (p_y,p_z) = (p_x + (l-1), p_x + c(l-1))\} \\
= &\#\{(p_x,p_y,p_z) \in \mathrm{Supp}(x) \times \mathrm{Supp}(y) \times \mathrm{Supp}(z) \\
&\mid (1-c)p_x + cp_y - p_z = 0\}.
\end{aligned}$$

Hence we have the following:

Theorem III.11. $\mathrm{wt}((x,y,z)H_{(0,1,c)}) = P\mathrm{wt}(x) + P\mathrm{wt}(y) + P\mathrm{wt}(z) - 2\mathrm{wt}(x)\mathrm{wt}(y) - 2\mathrm{wt}(y)\mathrm{wt}(z) - 2\mathrm{wt}(z)\mathrm{wt}(x) + 4\#\{1 \le p_x,p_y,p_z \le P \mid (1-c)p_x + cp_y - p_z = 0, (p_x,p_y,p_z) \in \mathrm{Supp}(x) \times \mathrm{Supp}(y) \times \mathrm{Supp}(z)\}$.

Geometrically speaking, the weight of codeword of the dual code for $(0,1,c)$ relates to a plane $\{1 \le p_x,p_y,p_z \le P \mid (1-c)p_x + cp_y - p_z = 0\}$. If we have a weight invariant bijection from a plane $\{1 \le p_x,p_y,p_z \le P \mid (1-c)p_x + cp_y - p_z = 0\}$ to another plane $\{1 \le p_x,p_y,p_z \le P \mid (1-\gamma)p_x + \gamma p_y - p_z = 0\}$, we obtain our main contribution, *i.e.*, Theorem II.3 for $J = 3$. Let us construct such a bijection from here.

For $2 \le c,\gamma \le P-1$, we define a bijection $f_{c,\gamma} : \mathbb{Z}_P^3 \to \mathbb{Z}_P^3$ as

$$f_{c,\gamma} : (p_x,p_y,p_z) \mapsto (\frac{1-c}{1-\gamma}p_x, \frac{c}{\gamma}p_y, p_z).$$

Then $f_{c,\gamma}$ is also a bijection from $\{1 \le p_x,p_y,p_z \le P \mid (1-c)p_x + cp_y - p_z = 0\}$ to $\{1 \le p_x,p_y,p_z \le P \mid (1-\gamma)p_x + \gamma p_y - p_z = 0\}$.

Next, we define a bijection $F_{c,\gamma} : \mathbb{F}_2^{3P} \to \mathbb{F}_2^{3P}$ as

$$\begin{aligned}
F_{c,\gamma} \quad : \quad &(x_1,x_2,\ldots,x_P,y_1,y_2,\ldots,y_P,z_1,z_2,\ldots,z_P) \\
\mapsto \quad &(x_{\frac{1-c}{1-\gamma}1}, x_{\frac{1-c}{1-\gamma}2}, \ldots, x_{\frac{1-c}{1-\gamma}P}, \\
&y_{\frac{c}{\gamma}1}, y_{\frac{c}{\gamma}2}, \ldots, y_{\frac{c}{\gamma}P}, \\
&z_1, z_2, \ldots, z_P).
\end{aligned}$$

The definition of $F_{c,\gamma}$ is motivated by $f_{c,\gamma}$.

Since $F_{c,\gamma}$ is a permutation of indices of each component $x,y,z \in \mathbb{F}_2^{3P}$, for $(x',y',z') := F_{c,\gamma}(x,y,z)$ we have $\mathrm{wt}(x') = \mathrm{wt}(x), \mathrm{wt}(y') = \mathrm{wt}(y)$, and $\mathrm{wt}(z') = \mathrm{wt}(z)$.

These imply that

$$\begin{aligned}
&\sum_{w\in\mathbb{F}_2^{3P}} X^{P^2 - \mathrm{wt}(wH_{(0,1,c)})} Y^{\mathrm{wt}(wH_{(0,1,c)})} \\
= &\sum_{w\in\mathbb{F}_2^{3P}} X^{P^2 - \mathrm{wt}(wH_{(0,1,\gamma)})} Y^{\mathrm{wt}(wH_{(0,1,\gamma)})},
\end{aligned}$$

for any $2 \le c,\gamma \le P-1$. As a corollary, we have

$$W(C^{\perp}_{(0,1,c)}; X, Y) = W(C^{\perp}_{(0,1,\gamma)}; X, Y).$$

By combining MacWilliams identity, we obtain our main contribution, that is Theorem II.3, for $J = 3$ case.

IV. Weight Enumerator of $(2,P)$-SFA LDPC codes

By routine calculation, we can obtain the weight enumerator of the dual code of the $(2,P)$-SFA LDPC code with respect to $H_{(0,1)}$. Using the MacWilliams identity, we have the following:

Theorem IV.1. *Let $H_{0,1}(2,P)$ be a generalized $(2,P)$-SFA LDPC matrix with respect to $H_{(0,1)}$ and C the linear code with respect to H.*

The weight enumerator for C is

$$\sum_{0\le p_0\le P^2} \frac{\sum_{0\le p_1,p_2\le P} \sum_{0\le p_3\le p_0} \psi(p_1,p_2,p_3)}{2^{2P}} X^{P^2-p_0} Y^{p_0},$$

where $\phi(p_1,p_2) := (P-p_1)p_2 + p_1(P-p_2)$ *and* $\psi(p_1,p_2,p_3) := (-1)^{p_3}\binom{P}{p_1}\binom{P}{p_2}\binom{\phi(p_1,p_2)}{p_0-p_3}\binom{P^2-\phi(p_1,p_2)}{p_3}$.

We omit the proof here since it is just a routine but long calculation.

If we fix p_0, move P, and focus on the coefficient of $X^{P^2-p_0}Y^{p_0}$, we obtain the following:

Corollary IV.2. *Let* $w_p(P)$ *denote the coefficient of* $X^{P^2-p}Y^p$ *for the weight enumerator* $W(C_{a_1,a_2}(P,2);X,Y)$. *Then* $w_p(P)$ *is a polynomial in* P *over* $\mathbb{Q}$ *for any non-negative integer* p. *Furthermore, the degree of* $w_p(P)$ *is at most* $2p$.

Corollary IV.2 implies that "if there is a prime number P_0 such that the coefficient of $X^{P_0^2-p_0}Y^{p_0}$ is not zero, there exist infinitely many prime numbers P_1 which have the same property." In particular, if the minimum weight of P_0 is p_0, infinitely many $(2,P_1)$-SFA LDPC codes' minimum weight is p_0.

We like to note that we have similar but more complex formulas to Theorem IV.1 and Corollary IV.2 for $P=3$.

V. Conclusion

After we obtained Theorem II.3, we tried to prove any $(3,P)$-SFA LDPC matrices are equivalent for a prime number P. To determine $(3,P)$-SFA LDPC matrices are equivalent for a given prime number is an interesting problem. But this failed for all primes $P \geq 7$.

We may of course confine our attention to matrices $H_{(0,1,b)}$ with $2 \leq b \leq P-1$. Theorem III.1 implies that $H_{(0,1,b)}$ is equivalent to $H_{(0,1,1-b)}$ and $H_{(0,1,\frac{1}{b})}$. In particular, for any odd prime P, the matrices $H_{(0,1,2)}$, $H_{(0,1,P-1)}$ and $H_{(0,1,\frac{P+1}{2})}$ are equivalent, and possibly this could constitute one equivalence class. For example, with $P=7$ we know that $H_{(0,1,2)}$, $H_{(0,1,6)}$, $H_{(0,1,4)}$ are equivalent, and likewise $H_{(0,1,3)}$, $H_{(0,1,5)}$, but it is uncertain whether $H_{(0,1,2)}$ is equivalent to $H_{(0,1,3)}$.

In [14], the explicit formula for word error-rate over binary symmetric channel with fixed initialization decoding has been obtained for the $(3,11)$-SFA LDPC code. If any $(3,11)$-SFA LDPC matrices are equivalent, it means we obtain the explicit formula for any $(3,11)$-SFA LDPC codes under the same condition. We leave this problem open.

We have another open problem if we have similar results for larger column weight $J \geq 4$.

Acknowledgment

This work was supported by KAKENHI 22760286.

References

[1] V. Pless and N. J. A. Sloane, On the classification and enumeration of self-dual codes, J. Combin. Theory Ser. A 18 (1975), pp.313-335.

[2] I.B. Frenkel, J. Lepowsky and A. Meurman, Vertex Operator Algebras and the Monster, Academic Press, New York, 1988.

[3] C. Dong, Vertex algebras associated with even lattices, J. Algebra 161 (1993), pp.245-265.

[4] K.Yang, T.Helleseth, On the Minimum Distance of Array Codes as LDPC Codes, IEEE Trans. on Information Theory, vol.49, no.12, pp.3268-3271, 2003.

[5] Kenji Sugiyama, Yuichi Kaji, "On the Minimum Weight of Simple Full-Length Array LDPC Codes," IEICE Trans. on Fundam. of ECCS, Vol. E91-A Issue 6, June 2008.

[6] M.Blaum, R.M.Roth, New Array Codes for Multiple Phased Burst Correction, IEEE Trans. on Information Theory, vol.39, no.1, pp.66-77, 1993.

[7] J.L.Fan, "Array codes as low-density parity-check codes," Proc. 2nd Int.Symp. on Turbo Codes, pp.543-546, 2000.

[8] T.Mittelholzer, Efficient Encoding and Minimum Distance Bounds of Reed-Solomon-Type Array Codes, Proc. of ISIT 2002, Lausanne, Switzerland, page 282, 2002.

[9] T.Mittelholzer, Minimum Distance of Column-Weight-4 LDPC Codes Derived from Array Codes, IBM Research Report, RZ3556, 2006.

[10] Marc P. C. Fossorier, Quasi-Cyclic Low-Density Parity-Check Codes From Circulant Permutation Matrices, IEEE Trans. on Information Theory, vol.50, no.8, pp.1788-1793, 2004.

[11] Yuichi Kaji, "On the Number of Minimum Weight Codewords of SFA-LDPC Codes," Proc. of the 2009 IEEE Inter. Sym. on Inform. Theory, Seoul, Korea, pp.70-74, June 2009.

[12] W. Wesley Peterson and E. J. Weldon, Jr., Error-Correcting Codes Second Edition, New York,1961, 285, M.I.T. Press

[13] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes North-Holland Mathematical Library, Volume 16, 1977 (11th reprint, 2003)

[14] M. Hagiwara, Marc P. C. Fossorier, H. Imai, Fixed Initialization Decoding of LDPC Codes Over a Binary Symmetric Channel, IEEE Trans. on Information Theory 58(4), pp.2321-2329, 2012.