Scientiae Mathematicae Japonicae Online, **e-2006**, 567–576

EQUIVALENCE OF LINEAR CODES WITH THE SAME WEIGHT ENUMERATOR

E. J. Cheon *

Received December 4, 2005; revised May 11, 2006

Abstract. Two equivalent linear codes have the same weight enumerator but the converse does not hold. We investigate which code is unique up to equivalence in view of the weight enumerator. The main purpose of this paper is to investigate the weight enumerators associated to the only one equivalent class of linear codes and to construct these codes. Furthermore, we construct non-equivalent linear codes with the same weight enumerator and give the generator matrices of these codes.

1 Introduction and Preliminary. If we know the weight enumerator of a given linear code, then we obtain many information of the code from it, that is, we note the dimension, length, minimum distance of the code, the sum of all weights and the weight enumerator of its dual code, etc. Finding the weight enumerators of linear codes is a very important and interesting problem. Every polynomial can not be a weight enumerator of some code. Though a polynomial is the weight enumerator of some code, we don't know how many codes have the same polynomial as their weight enumerators. Actually, any two equivalent codes always have the same weight enumerator but the converse does not hold. We are interested in finding the linear codes with same weight enumerator, and investigate equivalence of these codes.

A *q-ary* $[n,k]$ *linear code* is a linear subspace of ${\mathbb{F}_q}^n$ over the finite field $\mathbb{F}_q$ of length n, dimension k. A linear code is *non-degenerate* if there is no always-zero coordinate position. The weight $w(\mathbf{x})$ means the number of non-zero positions of a vector $\mathbf{x}$ in ${\mathbb{F}_q}^n$. The *support* of $\mathbf{x}$ means the set of non-zero coordinate positions in $\mathbf{x}$ and is denoted by $\mathrm{Supp}(\mathbf{x})$, i.e., $\mathrm{Supp}(\mathbf{x}) = \{i \mid x_i \neq 0\}$, where $\mathbf{x} = (x_1, \dots, x_n)$. Then $|\mathrm{Supp}(\mathbf{x})| = w(\mathbf{x})$. For $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$ in ${\mathbb{F}_q}^n$, we define the *intersection* of $\mathbf{x}$ and $\mathbf{y}$ by $\mathbf{x} \cap \mathbf{y} = (x_1y_1, \dots, x_ny_n)$. Then $\mathrm{Supp}(\mathbf{x} \cap \mathbf{y}) = \mathrm{Supp}(\mathbf{x}) \cap \mathrm{Supp}(\mathbf{y})$. For any subset S of ${\mathbb{F}_q}^n$, we also define its *support* by $\mathrm{Supp}(S) = \{i \mid x_i \neq 0 \text{ for some } \mathbf{x} \in S\}$.

For a q-ary linear code C, let

$$C^{\perp} = \{\mathbf{x} \in {\mathbb{F}_q}^n \mid \mathbf{x} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in C\}$$

be called the *dual code* of C.

Two $[n,k]_q$ codes C_1 and C_2 are called *equivalent* if there are generator matrices G_1 and G_2 of C_1 and C_2, respectively, such that G_2 may be obtained from G_1 by a sequence of elementary column operations of the following types: (i) transposition of two columns and (ii) multiplication of a column by a non-zero scalar.

For an $[n,k]_q$ code C, let A_r denote the number of codewords in C of weight r. The numbers $A_0, A_1, \dots, A_n$ are referred to as the weight distribution of C, and the formal sum

$$W_C(s) = \sum_{i=0}^{n} A_i s^i$$

2000 *Mathematics Subject Classification.* MSC2000: 94B65, 94B05, 51E20, 05B25.

Key words and phrases. Linear code, Weight enumerator, Equivalence.

*This work was supported by the Korea Research Foundation Grant. (KRF-2004-037-C00004)

is called the *weight enumerator* of C.

The following theorem relates the weight enumerator of a linear code C to the weight enumerator of its dual code $C^{\perp}$.

Theorem 1.1 ([4]) (**The MacWilliams Identity for Linear Codes**) *Let C be a q-ary linear code of length n, $C^{\perp}$ its dual and*

$$W_C(s) = \sum_{i=0}^{n} A_i s^i, \quad W_{C^{\perp}}(s) = \sum_{i=0}^{n} A_i{}^{\perp} s^i,$$

the weight enumerators of C and $C^{\perp}$, respectively. Then

$$W_{C^{\perp}}(s) = \frac{1}{|C|}\,(1+(q-1)s)^n\; W_C\left(\frac{1-s}{1+(q-1)s}\right).$$

Let C_i be an $[n_i,\ k_i]_q$ linear code with a generator matrix G_i for $i = 1, 2$. Then we have a code $C_1 \oplus C_2$ by direct sum,

$$C_1 \oplus C_2 = \{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \in C_1, \mathbf{y} \in C_2\}.$$

Note that $C_1 \oplus C_2$ is an $[n_1+n_2,\ k_1+k_2]_q$ linear code with a generator matrix $\begin{pmatrix} G_1 & \mathbf{0} \\ \mathbf{0} & G_2 \end{pmatrix}$, and the weight enumerator of $C_1 \oplus C_2$ is

$$W_{C_1 \oplus C_2} = W_{C_1}(s) W_{C_2}(s).$$

Theorem 1.2 ([1]) *Let C be a non-degenerate $[n,k]_q$ linear code. Then*

$$n = \frac{1}{q^k - q^{k-1}} \sum_{\mathbf{x} \in C} w(\mathbf{x}).$$

Let $\mathbb{P}^{k-1}$ be the $(k-1)$-dimensional projective space over the finite field $\mathbb{F}_q$. A 0-*cycle* $\mathcal{X}$ means a formal sum of points in $\mathbb{P}^{k-1}$, that is $\mathcal{X} = \sum m_i P_i$ where m_i's are integers and P_i's are points in $\mathbb{P}^{k-1}$. Two 0-cycles $\mathcal{X} = \sum m_i P_i$ and $\mathcal{X}'$ are said to be *projectively equivalent* if there exists a projective transformation $F : \mathbb{P}^{k-1} \to \mathbb{P}^{k-1}$ such that $\sum m_i F(P_i) = \mathcal{X}'$.

For a non-degenerate linear code C, each column of a generator matrix G of C can be regarded as a point in $\mathbb{P}^{k-1}$. The formal sum of all columns of G as points in $\mathbb{P}^{k-1}$ is called a 0-*cycle of the code* C, denoted by $\mathcal{X}_C$. If one chooses another generator matrix G' of the same code C, then two 0-cycles of C corresponding to G and G', respectively, are projectively equivalent. Note that two codes are equivalent if and only if their 0-cycles are projectively equivalent.

Theorem 1.3 ([2]) *Let $\{P_0, P_1, \ldots, P_{n+1}\}$ and $\{Q_0, Q_1, \ldots, Q_{n+1}\}$ be two sets of $(n+2)$ points of $\mathbb{P}^n$. If any $(n+1)$ points in each sets span the whole space $\mathbb{P}^n$, then there exists a unique projective transformation $F : \mathbb{P}^n \to \mathbb{P}^n$ such that $F(P_j) = Q_j$ for $0 \le j \le n+1$.*

From now on, we assume that every code is non-degenerate.

2 The weight enumerators of 2-dimensional codes. In this section, we give some results for 2-dimensional linear codes with the same weight enumerator.

Example 2.1 We find weight enumerators of all linear codes of dimension 2 over $\mathbb{F}_2$ or $\mathbb{F}_3$.
(1) Any 2-dimensional binary linear code C corresponds to the 0-cycle

$$\mathcal{X}_C = m_1\binom{0}{1} + m_2\binom{1}{0} + m_3\binom{1}{1},$$

for some non-negative integers m_1, m_2 and m_3 among which at least two are non-zero. Then we have $W_C(s) = 1 + s^{m_1+m_2} + s^{m_1+m_3} + s^{m_2+m_3}$.
(2) Any 2-dimensional ternary linear code C corresponds to the 0-cycle

$$\mathcal{X}_C = m_1\binom{0}{1} + m_2\binom{1}{0} + m_3\binom{1}{1} + m_4\binom{1}{2},$$

for some non-negative integers m_1, m_2, m_3 and m_4 among which at least two are non-zero. Then we have $W_C(s) = 1 + 2s^{m_1+m_2+m_3} + 2s^{m_1+m_2+m_4} + 2s^{m_1+m_3+m_4} + 2s^{m_2+m_3+m_4}$.

Lemma 2.2 *Let C_1 and C_2 be q-ary $[n, k]$ linear codes.*

(1) *Suppose that $\mathcal{X}_{C_1} = \sum_{i=1}^{k+1} m_i P_i$ and $\mathcal{X}_{C_2} = \sum_{i=1}^{k+1} m_i Q_i$, where $m_i \geq 1$ for $i = 1, \ldots, k+1$, and that any k points in each set $\{P_1, P_2, \ldots, P_{k+1}\}$ and $\{Q_1, Q_2, \ldots, Q_{k+1}\}$ span the whole space $\mathbb{P}^{k-1}$, then C_1 and C_2 are equivalent.*

(2) *Suppose that $\mathcal{X}_{C_1} = \sum_{i=1}^{k} m_i P_i$ and $\mathcal{X}_{C_2} = \sum_{i=1}^{k} m_i Q_i$, where $m_i \geq 1$ for $i = 1, \ldots, k$, then C_1 and C_2 are equivalent.*

Proof. (1) By Theorem 1.3, there is a projective transformation $F : \mathbb{P}^{k-1} \to \mathbb{P}^{k-1}$ such that $F(P_i) = Q_i$ for all $i = 1, \ldots, k+1$. Thus there exists a non-singular matrix $A = (a_{ij})_{k\times k}$ such that $AG_1 = G_2$, which means that G_2 is obtained from G_1 by a sequence of column operations. Recall that any non-singular matrix is expressed as a product of elementary matrices. Thus C_1 and C_2 are equivalent.
(2) Let

$$G_1 = (\underbrace{P_1, \ldots, P_1}_{m_1 \text{ times}}, \ldots, \underbrace{P_k, \ldots, P_k}_{m_k \text{ times}})_{k\times n} \quad \text{and}$$
$$G_2 = (\underbrace{Q_1, \ldots, Q_1}_{m_1 \text{ times}}, \ldots, \underbrace{Q_k, \ldots, Q_k}_{m_k \text{ times}})_{k\times n}.$$

Then the codes C_1 and C_2 are equivalent to codes generated by G_1 and G_2, respectively. Since $\{P_1, \ldots, P_k\}$ and $\{Q_1, \ldots, Q_k\}$ span $\mathbb{P}^{k-1}$, respectively, by Theorem 1.3, there is a projective transformation $F : \mathbb{P}^{k-1} \to \mathbb{P}^{k-1}$ such that $F(P_i) = Q_i$ for all $i = 1, 2, \ldots, k$. Thus there exists a non-singular matrix $A = (a_{ij})_{k\times k}$ such that $AG_1 = G_2$, which means that G_2 is obtained from G_1 by a sequence of column operations. Thus C_1 and C_2 are equivalent. □

The following theorem is the converse of Example 2.1.

Theorem 2.3 *Any two 2-dimensional linear codes over $\mathbb{F}_2$ or $\mathbb{F}_3$ with the same weight enumerator are equivalent.*

Proof. Let C_1 and C_2 be 2-dimensional linear codes over $\mathbb{F}_2$ or $\mathbb{F}_3$ with the same weight enumerator.
(i) For binary case, we let

$$\mathcal{X}_{C_1} = m_1\begin{pmatrix}0\\1\end{pmatrix} + m_2\begin{pmatrix}1\\0\end{pmatrix} + m_3\begin{pmatrix}1\\1\end{pmatrix}, \quad \mathcal{X}_{C_2} = n_1\begin{pmatrix}0\\1\end{pmatrix} + n_2\begin{pmatrix}1\\0\end{pmatrix} + n_3\begin{pmatrix}1\\1\end{pmatrix},$$

for some non-negative integers m_i and n_i. By Lemma 2.2 (1), we may assume that $0 \le m_1 \le m_2 \le m_3$ and $0 \le n_1 \le n_2 \le n_3$. Then, from Example 2.1, we have

$$W_{C_1}(s) = 1 + s^{m_1+m_2} + s^{m_1+m_3} + s^{m_2+m_3},$$
$$W_{C_2}(s) = 1 + s^{n_1+n_2} + s^{n_1+n_3} + s^{n_2+n_3}.$$

Since $W_{C_1}(s) = W_{C_2}(s)$, we get

$$m_1 + m_2 = n_1 + n_2, \quad m_1 + m_3 = n_1 + n_3, \quad m_2 + m_3 = n_2 + n_3.$$

Thus $m_i = n_i$ for $i = 1, 2, 3$. By Lemma 2.2, C_1 and C_2 are equivalent.
(ii) For ternary case, we let

$$\mathcal{X}_{C_1} = m_1\begin{pmatrix}0\\1\end{pmatrix} + m_2\begin{pmatrix}1\\0\end{pmatrix} + m_3\begin{pmatrix}1\\1\end{pmatrix} + m_4\begin{pmatrix}1\\2\end{pmatrix},$$
$$\mathcal{X}_{C_2} = n_1\begin{pmatrix}0\\1\end{pmatrix} + n_2\begin{pmatrix}1\\0\end{pmatrix} + n_3\begin{pmatrix}1\\1\end{pmatrix} + n_4\begin{pmatrix}1\\2\end{pmatrix},$$

for some non-negative integers m_i and n_i. By Theorem 1.3, for any subsets $\{P_1, P_2, P_3\}$ and $\{Q_1, Q_2, Q_3\}$ in $\mathbb{P}^1$, there exists a projective transformation satisfying $P_i \to Q_i$, $i = 1, 2, 3$. This means that any bijection from $\mathbb{P}^1$ to $\mathbb{P}^1$ is a projective transformation, since the projective line $\mathbb{P}^1$ over $\mathbb{F}_3$ has only 4 points. Thus we may assume that $0 \le m_1 \le m_2 \le m_3 \le m_4$ and $0 \le n_1 \le n_2 \le n_3 \le n_4$. Then, from Example 2.1, we have

$$W_{C_1}(s) = 1 + 2s^{m_1+m_2+m_3} + 2s^{m_1+m_2+m_4} + 2s^{m_1+m_3+m_4} + 2s^{m_2+m_3+m_4},$$
$$W_{C_2}(s) = 1 + 2s^{n_1+n_2+n_3} + 2s^{n_1+n_2+n_4} + 2s^{n_1+n_3+n_4} + 2s^{n_2+n_3+n_4}.$$

Since $W_{C_1}(s) = W_{C_2}(s)$, we get

$$m_1 + m_2 + m_3 = n_1 + n_2 + n_3, \quad m_1 + m_2 + m_4 = n_1 + n_2 + n_4,$$
$$m_1 + m_3 + m_4 = n_1 + n_3 + n_4, \quad m_2 + m_3 + m_4 = n_2 + n_3 + n_4.$$

From this linear system of equations, we obtain $m_i = n_i$ for $i = 1, 2, 3, 4$. Similarly above, we can take a projective transformation $F : \mathbb{P}^1(F_3) \to \mathbb{P}^1(F_3)$ such that $F(P_i) = Q_i$ and $m_i = n_i$ for $i = 1, 2, 3, 4$. Therefore C_1 and C_2 are equivalent. □

The next example shows that Theorem 2.3 can not be extended to the case $q \ge 4$.

Example 2.4 ([3]) For $q \ge 4$, let C_i be a code with a generator matrix

$$G_i = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & \alpha_i \end{pmatrix} \quad \text{for} \quad i = 1, 2,$$

where $\alpha_i \in \mathbb{F}_q \setminus \{0, 1\}$. Then $W_{C_1}(s) = W_{C_2}(s)$ but C_1 and C_2 are not equivalent when $\alpha_1 \ne \alpha_2$.

3 The weight enumerators associated to the only one equivalent class of codes.

The main purpose of this section is to investigate the weight enumerators associated to the only one equivalent class of linear codes and to construct these codes.

From now on, by abuse of notation, we also write the notation $W_B(s)$, even if B is any subset of $\mathbb{F}_q{}^n$. Let I_n be an $n \times \uplus n$ identity matrix. For vectors $\mathbf{x}_1, \ldots, \mathbf{x}_n$, $\langle \mathbf{x}_1, \ldots, \mathbf{x}_n \rangle$ denotes the linear span of $\mathbf{x}_1, \ldots, \mathbf{x}_n$, and a vector $(1, 1, \ldots, 1)$ is simply denoted by $1 \ldots 1$.

Lemma 3.1 *Suppose that C is a q-ary $[n, k]$ linear code and $\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k\}$ is a basis of C. If $\deg W_C(s) = n = \sum_{i=1}^{k} w(\mathbf{x}_i)$, then C is equivalent to the code*

$$\langle \underbrace{1\ldots1}_{w(\mathbf{x}_1)\text{times}} \rangle \oplus \langle \underbrace{1\ldots1}_{w(\mathbf{x}_2)\text{times}} \rangle \oplus \cdots \oplus \langle \underbrace{1\ldots1}_{w(\mathbf{x}_k)\text{times}} \rangle,$$

and we have $W_C(s) = \prod_{i=1}^{k} (1 + (q-1)s^{w(\mathbf{x}_i)})$.

Proof. Since $\deg W_C(s) = n$, there is a codeword $\mathbf{c}$ of weight n. Let $\mathbf{c} = a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \cdots + a_k\mathbf{x}_k$ for some $a_1, a_2, \ldots, a_k \in \mathbb{F}_q$. Since

$$n = w(\mathbf{c}) = w(\sum_{i=1}^{k} a_i\mathbf{x}_i) \leq \sum_{i=1}^{k} w(a_i\mathbf{x}_i) \leq \sum_{i=1}^{k} w(\mathbf{x}_i) = n,$$

all a_i's are non-zero and $\mathrm{Supp}(\mathbf{x}_i) \cap \mathrm{Supp}(\mathbf{x}_j) = \emptyset$ for $1 \leq i < j \leq k$. Hence C is equivalent to the code

$$\langle \underbrace{1\ldots1}_{w(\mathbf{x}_1)\text{times}} \rangle \oplus \langle \underbrace{1\ldots1}_{w(\mathbf{x}_2)\text{times}} \rangle \oplus \cdots \oplus \langle \underbrace{1\ldots1}_{w(\mathbf{x}_k)\text{times}} \rangle.$$

Obviously, we obtain

$$W_C(s) = (1 + (q-1)s^{w(\mathbf{x}_1)})(1 + (q-1)s^{w(\mathbf{x}_2)}) \ldots (1 + (q-1)s^{w(\mathbf{x}_k)}).$$

□

Theorem 3.2 *Let C be a q-ary linear code with*

$$W_C(s) = (1 + (q-1)s^a)^k.$$

If a is odd or $q \neq 2$, then C is equivalent to the code generated by $(\underbrace{I_k \ldots I_k}_{a \text{ times}})$.

Proof. Since $W_C(s) = (1 + (q-1)s^a)^k$, by using Theorem 1.2, we can compute that the length of C is ka. Hence C is a $[ka, k]$ linear code. We divide the proof into two cases.

Case 1. Suppose $q \neq 2$.

For $k = 1$, the assertion is true. Now, we assume $k \geq 2$. Let $A = \{\mathbf{x} \in C \mid w(\mathbf{x}) = a\}$. Then we have $|A| = k(q-1)$. We claim that for any two elements $\mathbf{x}$ and $\mathbf{y}$ in A,

$$\mathbf{x} \in \langle \mathbf{y} \rangle \quad \text{or} \quad \mathrm{Supp}(\mathbf{x}) \cap \mathrm{Supp}(\mathbf{y}) = \emptyset.$$

Suppose that $\mathbf{x} \notin \langle \mathbf{y} \rangle$ and $\mathrm{Supp}(\mathbf{x}) \cap \mathrm{Supp}(\mathbf{y}) \neq \emptyset$. We set $r = |\mathrm{Supp}(\mathbf{x}) \cap \mathrm{Supp}(\mathbf{y})|$, $0 < r < a$. On the other hand, from $W_C(s)$, we note that there is an element $\mathbf{z}$ of weight

ka in C. By applying a sequence of column operations to the code C, we may assume that $\mathbf{z}$ has the 1 in the ka columns, i.e., $\mathbf{z} = \underbrace{1\ldots1}_{ka\ \text{times}}$. So we may let as follows:

$$\begin{array}{llllllllll}
\mathbf{z} = 1, \ \ldots, \ 1, & 1, & \ldots, \ 1, & 1, & \ldots, \ 1, & 1, \ \ldots, \ 1 \\
\mathbf{x} = b_1, \ldots, \ b_{a-r}, & b_{a-r+1}, & \ldots, \ b_a, & 0, & \ldots, \ 0, & 0, \ \ldots, \ 0 \\
\mathbf{y} = 0, \ \ldots, \ 0, & c_1, & \ldots, \ c_r, & c_{r+1}, & \ldots, \ c_a, & 0, \ \ldots, \ 0
\end{array}$$

Then $(k-1)a \le w(-b_1\mathbf{z}+\mathbf{x}), w(-c_1\mathbf{z}+\mathbf{y}) < ka$. Thus $w(-b_1\mathbf{z}+\mathbf{x}) = (k-1)a = w(-c_1\mathbf{z}+\mathbf{y})$ which implies that $b_1 = b_2 = \cdots = b_a$ and $c_1 = c_2 = \cdots = c_a$. Since $0 < w(\alpha\mathbf{x}+\beta\mathbf{y}) < 2a$ for any $\alpha, \beta \in \mathbb{F}_q$ with $(\alpha,\beta) \ne (0,0)$, $w(\alpha\mathbf{x}+\beta\mathbf{y}) = a$. Thus $a = w(\mathbf{x} - c_1^{-1}b_1\mathbf{y}) = 2a - 2r$ and $a = w(\mathbf{x}+\gamma\mathbf{y}) = 2a - r$ for some $\gamma \in \mathbb{F}_q \setminus \{0, -c_1^{-1}b_1\}$. This is a contradiction. Thus we proved the claim. Therefore we conclude that there exist k vectors in A whose supports are mutually disjoint, and hence these k vectors form a basis of the code C. By Lemma 3.1, C is equivalent to the code generated by $(\underbrace{I_k \ldots I_k}_{a\ \text{times}})$.

Case 2. Suppose that $q = 2$ and a is odd.
Consider $A = \{\mathbf{x} \in C \mid w(\mathbf{x}) = a\}$. Then we have $|A| = k$. It suffices to show that A is a basis of C. For any $\mathbf{x}$ and $\mathbf{y}$ in A with $\mathbf{x} \ne \mathbf{y}$, we get $0 < w(\mathbf{x}+\mathbf{y}) \le 2a$. From $W_C(s)$, we have $w(\mathbf{x}+\mathbf{y}) = a$ or $2a$. If $w(\mathbf{x}+\mathbf{y}) = a$, then $2w(\mathbf{x}\cap\mathbf{y}) = a$. Since a is odd, this is a contradiction. Thus $w(\mathbf{x}+\mathbf{y}) = 2a$ and $w(\mathbf{x}\cap\mathbf{y}) = 0$, i.e.,

$$\mathrm{Supp}(\mathbf{x}) \cap \mathrm{Supp}(\mathbf{y}) = \emptyset.$$

Therefore, any two elements in A have mutually disjoint supports. Thus A is a basis of C. By Lemma 3.1, the proof is complete. □

Remark 3.3 *We will show in Theorem 4.1 that if $q = 2$ and $a(\ge 2)$ is even, there exist at least two non-equivalent codes.*

Theorem 3.4 *Suppose C is a q-ary linear code with*

$$W_C(s) = \prod_{i=1}^{k} (1 + (q-1)s^{a_i}),$$

where $\sum_{j=1}^{i-1} a_j < a_i$ for any $i = 2, \ldots, k$. Then C is equivalent to the code $\langle \underbrace{1\ldots1}_{a_1\ \text{times}} \rangle \oplus \langle \underbrace{1\ldots1}_{a_2\ \text{times}} \rangle \oplus \cdots \oplus \langle \underbrace{1\ldots1}_{a_k\ \text{times}} \rangle$.

Proof. For each $i = 1, \ldots, k$, take a vector $\mathbf{x}_i \in C$ with $w(\mathbf{x}_i) = a_i$. Since $\sum_{j=1}^{i-1} a_j < a_i$, we can prove easily that $\mathbf{x}_i \notin \langle \mathbf{x}_1, \ldots, \mathbf{x}_{i-1} \rangle$ for each i. Thus $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ is a basis of C. By Lemma 3.1, C is equivalent to the code $\langle \underbrace{1\ldots1}_{a_1\text{times}} \rangle \oplus \langle \underbrace{1\ldots1}_{a_2\ \text{times}} \rangle \oplus \cdots \oplus \langle \underbrace{1\ldots1}_{a_k\ \text{times}} \rangle$. □

The following corollary is a special case of Theorem 3.4.

Corollary 3.5 *Suppose C is a binary linear code with*

$$W_C(s) = \prod_{i=0}^{k-1} (1 + s^{2^i}) = 1 + s + s^2 + s^3 + s^4 + \cdots + s^{2^k - 1}.$$

Then C is equivalent to the code

$$\langle 1\rangle \oplus \langle 11\rangle \oplus \langle 1111\rangle \oplus \cdots \oplus \langle \underbrace{1\ldots 1}_{2^{k-1}\text{times}} \rangle.$$

The next example shows that the condition $\sum_{j=1}^{i-1} a_j < a_i$ for all $i = 2, \ldots, k$ in Theorem 3.4 is necessary.

Example 3.6 Let $\mathcal{X}_{C_1} = 3\binom{1}{\substack{0\\0}} + 4\binom{0}{\substack{1\\0}} + 5\binom{0}{\substack{0\\1}}$ and $\mathcal{X}_{C_2} = \binom{1}{\substack{0\\0}} + 2\binom{0}{\substack{1\\0}} + 3\binom{0}{\substack{0\\1}} + 6\binom{1}{\substack{1\\1}}$. Then

$$W_{C_1}(s) = (1+s^3)(1+s^4)(1+s^5) = W_{C_2}(s),$$

and obviously, C_1 and C_2 are not equivalent.

Theorem 3.7 *Suppose C is a q-ary $[n,k]$ linear code and C_1 is a $(k-1)$-dimensional subcode of C. If $W_C(s) = g(s)W_{C_1}(s)$, then $g(s) = 1 + (q-1)s^a$ for some positive integer a and there exists $\mathbf{x}$ in $C \setminus C_1$ of weight a such that* $\mathrm{Supp}(C_1) \cap \mathrm{Supp}(\mathbf{x}) = \emptyset$.

Proof. Let $\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{k-1}\}$ be a basis of C_1 and $\mathbf{x}$ be a codeword of the minimum weight a in $C \setminus C_1$. Then

$$C = \langle \mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{k-1}, \mathbf{x}\rangle = \bigcup_{\alpha \in \mathbb{F}_q} (\alpha\mathbf{x} + C_1).$$

Let $A = C \setminus C_1$. Since $\mathbf{x}$ has the minimum weight a in A, let $W_A(s) = s^a(b + sh(s))$, for some $b \neq 0$ and a polynomial $h(s)$. Since $W_C(s) = W_{C_1}(s) + W_A(s) = g(s)W_{C_1}(s)$, we have $W_A(s)$ is a multiple of $W_{C_1}(s)$. Since

$$\gcd(W_{C_1}(s), s^a) = 1,$$

we have $b + sh(s)$ is a multiple of $W_{C_1}(s)$, that is, $b + sh(s) = W_{C_1}(s)f(s)$ for some $f(s)$, $\deg f(s) \geq 0$. Thus $g(s) = 1 + s^a f(s)$ and $\deg g(s) \geq a$. On the other hand, since C_1 is a subcode and $\alpha\mathbf{x} + C_1 = \alpha\mathbf{x} + \alpha C_1$ for any $\alpha \neq 0$, we get $W_A(s) = (q-1)W_{\mathbf{x}+C_1}(s)$. Since $\deg W_A(s) = \deg W_{\mathbf{x}+C_1}(s) \leq w(\mathbf{x}) + \deg W_{C_1}(s) = a + \deg W_{C_1}(s)$ and

$$\begin{aligned}\deg g(s) + \deg W_{C_1}(s) &= \deg W_C(s) = \deg(W_{C_1}(s) + W_A(s)) \\ &= \max\{\deg W_{C_1}(s), \deg W_A(s)\} \leq a + \deg W_{C_1}(s),\end{aligned}$$

we get $\deg g(s) \leq a$. Therefore, $\deg g(s) = a$, hence $g(s) = 1 + us^a$. Since $\dim C_1 = k-1$, we have $g(1) = q$. Thus $u = q-1$ and $g(s) = 1 + (q-1)s^a$.

Since $W_C(s) = W_{C_1}(s) + W_A(s) = W_{C_1}(s) + (q-1)W_{\mathbf{x}+C_1}(s)$ and $W_C(s) = (1 + (q-1)s^a)W_{C_1}(s) = W_{C_1}(s) + (q-1)s^a W_{C_1}(s)$, we have $W_{\mathbf{x}+C_1}(s) = s^a W_{C_1}(s)$. Now we will show that $w(\mathbf{x}+\mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y})$ for any $\mathbf{y} \in C_1$. Suppose that there is a codeword $\mathbf{y} \in C_1$ such that $w(\mathbf{x}+\mathbf{y}) \neq w(\mathbf{x}) + w(\mathbf{y})$. Take $\mathbf{c} \in C_1$ of maximum weight l such that $w(\mathbf{x}+\mathbf{c}) \neq w(\mathbf{x}) + w(\mathbf{c})$, that is, $\mathrm{Supp}(\mathbf{c}) \cap \mathrm{Supp}(\mathbf{x}) \neq \emptyset$. Let $\mathbf{u} \in C_1$ with $w(\mathbf{u}+\mathbf{x}) = l + a$. If $w(\mathbf{u}) > l$, then $w(\mathbf{u}+\mathbf{x}) = w(\mathbf{u}) + w(\mathbf{x}) > l + a$ by the definition of l. If $w(\mathbf{u}) < l$, then $w(\mathbf{u}+\mathbf{x}) \leq w(\mathbf{u}) + w(\mathbf{x}) < l + a$. Hence $w(\mathbf{u}) = l$ and $\{\mathbf{u} \in C_1 \mid w(\mathbf{u}+\mathbf{x}) = l + a\} \subseteq \{\mathbf{u} \in C_1 \mid w(\mathbf{u}) = l\}$. Since $|\{\mathbf{u} \in C_1 \mid w(\mathbf{u}+\mathbf{x}) = l + a\}| = |\{\mathbf{u} \in C_1 \mid w(\mathbf{u}) = l\}|$ by $W_{\mathbf{x}+C_1}(s) = s^a W_{C_1}(s)$, we have $\{\mathbf{u} \in C_1 \mid w(\mathbf{u}+\mathbf{x}) = l + a\} = \{\mathbf{u} \in C_1 \mid w(\mathbf{u}) = l\}$. Since $\mathbf{c} \in \{\mathbf{u} \in C_1 \mid w(\mathbf{u}) = l\}$ and $\mathbf{c} \notin \{\mathbf{u} \in C_1 \mid w(\mathbf{u}+\mathbf{x}) = l + a\}$, we have a contradiction. Hence $w(\mathbf{x}+\mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y})$ for any $\mathbf{y} \in C_1$. Therefore we have $\mathrm{Supp}(C_1) \cap \mathrm{Supp}(\mathbf{x}) = \emptyset$. $\square$

Remark 3.8 *If we assume that $g(s)$ has only non-negative coefficients, then we can prove the above theorem easily as follows; Since $W_C(1) = g(1)W_{C_1}(1)$ and $1 = W_C(0) = g(0)W_{C_1}(0) = g(0)$, we get $g(1) = q$ and $g(0) = 1$. Since all coefficients in the polynomials $W_C(s)$ and $W_{C_1}(s)$ except their constant terms are multiples of $q-1$, so are those of $g(s)$. Thus if all coefficients of $g(s)$ are non-negative, then $g(s)$ must have only two non-zero terms, and hence $g(s)$ is of the form $1 + (q-1)s^a$ for some positive integer a.*

Theorem 3.9 *Suppose C is a q-ary $[n, k]$ linear code with*

$$W_C(s) = (1 + (q-1)s^a)f(s), \quad \text{where} \quad a > 2 \deg f(s).$$

Then C is equivalent to the code $\langle \underbrace{1 \dots 1}_{a \text{ times}} \rangle \oplus A'$ for some code A'.

Proof. Note that $W_C(s) = f(s) + (q-1)s^a f(s)$ and every term of $f(s)$ is that of $W_C(s)$ and hence every coefficient of $f(s)$ is a non-negative integer. Let A and B be the following two disjoint sets:

$$A = \{\mathbf{x} \in C \mid w(\mathbf{x}) \leq \deg f(s)\} = \{\mathbf{x} \in C \mid w(\mathbf{x}) < a\},$$
$$B = \{\mathbf{x} \in C \mid w(\mathbf{x}) > \deg f(s)\} = \{\mathbf{x} \in C \mid w(\mathbf{x}) \geq a\}.$$

Then $C = A \cup B$. For any $\mathbf{x}_1$, $\mathbf{x}_2 \in A$, note that

$$w(\mathbf{x}_1 + \mathbf{x}_2) \leq w(\mathbf{x}_1) + w(\mathbf{x}_2) \leq 2 \deg f(s) < a.$$

Hence $\mathbf{x}_1 + \mathbf{x}_2 \in A$. Thus A is a subcode of C and $W_A(s) = f(s)$. Note that $f(1) = q^{k-1}$ and hence $\dim A = k - 1$. Now the result follows from Theorem 3.7. □

Note that for q-ary $[n, k]$ linear codes C_1 and C_2, if C_1 and C_2 are equivalent, then ${C_1}^\perp$ and ${C_2}^\perp$ are also equivalent. Thus by Theorem 1.1, we also conclude that the weight enumerators of the dual of the codes in previous theorems correspond to the only one equivalent class of linear codes.

4 The weight enumerators with non-equivalent codes. Now, we construct non-equivalent linear codes with the same weight enumerator and give the generator matrices of these codes.

Theorem 4.1 *There exist at least two non-equivalent binary linear codes with the same weight enumerator $(1 + s^a)^k$, for any even $a \geq 2$ and any integer $k \geq 3$.*

Proof. Let

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

and let C_i be the code generated by G_i for $i = 1, 2$, where

$$G_1 = (\overbrace{I_k, \dots, I_k}^{a \text{ times}}) \quad \text{and} \quad G_2 = \begin{pmatrix} \overbrace{A \dots A}^{\frac{a}{2} \text{ times}} & \overbrace{\mathbf{0} \quad \dots \quad \mathbf{0}}^{a \text{ times}} \\ \mathbf{0} \dots \mathbf{0} & I_{(k-3)} \dots I_{(k-3)} \end{pmatrix}.$$

Then $W_{C_1}(s) = (1 + s^a)^k = W_{C_2}(s)$. For any distinct elements $\mathbf{x}_1, \mathbf{x}_2$ in C_1 of weight a, we have $w(\mathbf{x}_1 + \mathbf{x}_2) = 2a$, while there exist two distinct elements $\mathbf{x}'_1, \mathbf{x}'_2$ in C_2 of weight a such that $w(\mathbf{x}'_1 + \mathbf{x}'_2) = a$. Thus C_1 and C_2 are not equivalent. □

Theorem 4.2 *Suppose C is a binary linear code with $W_C(s) = (1+s)(1+s^2)(1+s^4)\ldots(1+s^{2^{a-1}})$. Then the following hold:*
(1) *There exists only one code up to equivalence with the weight enumerator $W_C(s)^r$ for* (i) $r = 1,$ (ii) $a = 1$ *or* (iii) $a = 2$ *and* $r = 2$.
(2) *There exist at least two non-equivalent codes with the weight enumerator $W_C(s)^r$ for* (i) $r = 2$ *and* $a \geq 3$ *or* (ii) $r \geq 3$ *and* $a \geq 2$.

Proof. (1) (i) If $r = 1$, then by Corollary 3.5, it is obvious. (ii) If $a = 1$, then the corresponding code is the whole space ${F_2}^r$. (iii) If $a = 2$ and $r = 2$, then the weight enumerator is $(1+s)^2(1+s^2)^2 = 1+2s+\cdots$. Hence the code contains two unit vectors, say, e_1 and e_2. Then C is equivalent to the code $\langle e_1\rangle \oplus \langle e_2\rangle \oplus C'$ for some C' of dimension 2. Thus $W_{C'} = (1+s^2)^2$. By Theorem 2.3, C' is uniquely determined up to equivalence.
(2) (i) If $r = 2$ and $a \geq 3$, then we have two codes as follows:

$$C_1 = \langle I_2\rangle \oplus \langle I_2, I_2\rangle \oplus \langle I_2, I_2, I_2, I_2\rangle \oplus D,$$
$$C_2 = \langle I_2\rangle \oplus \langle A\rangle \oplus D,$$

where

$$D = \begin{cases} 0, & \text{for } a = 3, \\ \langle \underbrace{I_2, \ldots, I_2}_{2^3 \text{ times}}\rangle \oplus \cdots \oplus \langle \underbrace{I_2, \ldots, I_2}_{2^{a-1} \text{ times}}\rangle, & \text{for } a \geq 4 \end{cases}$$

and

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Here, for a matrix M, the notation $\langle M\rangle$ means the linear code with a generator matrix M. Then $W_{C_1}(s) = W_{C_2}(s) = W_C(s)^2$. For any two elements $\mathbf{x}_1$ and $\mathbf{x}_2$ in C_1 of weight 2 and 4, respectively, we have $w(\mathbf{x}_1 + \mathbf{x}_2) = 6$, while there exist two elements $\mathbf{x}'_1$ and $\mathbf{x}'_2$ in C_2 of weight 2 and 4, respectively, such that $w(\mathbf{x}'_1 + \mathbf{x}'_2) = 4$. Thus C_1 and C_2 are not equivalent.
(ii) If $r \geq 3$ and $a \geq 2$, then $(1+s^2)^3$ is a factor of $W_C(s)^r$. By Theorem 4.1, it is obvious. □

In the following theorem, we provide a class of polynomials in which every member is the weight enumerator of at least two non-equivalent binary linear codes.

Theorem 4.3 *There are at least two non-equivalent binary linear codes with the weight enumerator*

$$f(s) = 1 + s^{b_1+b_2} + s^{b_1+b_3} + s^{b_2+b_3} + s^{b_1+b_4} + s^{b_2+b_4} + s^{b_3+b_4} + s^{b_1+b_2+b_3+b_4},$$

where b_i's are any natural numbers satisfying $b_4 = b_1 + b_2 + b_3$.

Proof. We may assume $b_1 \leq b_2 \leq b_3$. Let

$$P_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, P_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, P_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, P_4 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Let C_1 be a code corresponding to the positive 0-cycle $\sum_{i=1}^4 b_i P_i$. Then we obtain $W_{C_1}(s) = f(s)$ by elementary calculation. Let C_2 be a code corresponding to the positive 0-cycle $\mathcal{X}_{C_2} = \sum_{j=1}^3 a_j P_j$, where $a_j \geq 1$ for $j = 1, 2, 3$. Then

$$W_{C_2}(s) = 1 + s^{a_1} + s^{a_2} + s^{a_3} + s^{a_1+a_2} + s^{a_1+a_3} + s^{a_2+a_3} + s^{a_1+a_2+a_3}.$$

Now, if we let $a_1 = b_1 + b_2$, $a_2 = b_1 + b_3$, and $a_3 = b_2 + b_3$, then it is easy to show $W_{C_1}(s) = W_{C_2}(s)$. However, C_1 and C_2 are not equivalent, since the corresponding 0-cycles are not projectively equivalent. □

Remark 4.4 *Using Theorem 4.3, we can construct various polynomials which are weight enumerators of two non-equivalent binary linear codes as follows:*
Let $f(s)$ be a polynomial appeared in Theorem 4.3 which is the common weight enumerator of non-equivalent binary linear codes C_1 and C_2. Let $g(s)$ be the weight enumerator of a binary linear code C of any dimension. Then $f(s)g(s)$ is the weight enumerator of non-equivalent binary linear codes $C_1 \oplus C$ and $C_2 \oplus C$

Acknowledgement. The author is deeply grateful to the referee for his valuable comments, suggestion and careful reading which made much improvement in the presentation of this manuscript.

References

[1] G. van der Geer and M. van der Vlugt, Generalized Reed-Muller codes and curves with many points, Journal of Number Theory 72, 1998, 257–268.

[2] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Clarendon Press, Oxford, 1998.

[3] Y. Kashiwagi, I. Kikumasa, O. Miyagawa and A. Ohbuchi, A note on equivalence and weight enumerators of codes, Hiroshima Journal of Math. Education 4, 1996, 109 –116.

[4] S. Roman, Coding and Information Theory, Springer-Verlag, 1992.

Department of Mathematics, Korea Advanced Institute of Science and Technology Daejeon 305-701, Korea

enju1000@naver.com