THE WEIGHT ENUMERATOR POLYNOMIALS OF SOME CLASSES OF CODES WITH COMPOSITE PARITY-CHECK POLYNOMIALS

TøR HELLESETH

Matematisk Institut, aed. A, Universitetet i Bergen, 5014 Bergen, Norway

Received 5 January 1976
Revised 30 November 1976

We find the Hamming weight distribution of some classes of linear codes. The cyclic codes in these classes have composite parity-check polynomials.

1. Introduction

Let \( F = \text{GF}(q) \), and let \( F^k \) be a \( k \)-dimensional vector space over \( F \). Elements of \( F^k \) are regarded as column vectors of length \( k \). Let \( G \) be a \( k \times n \) generator matrix for a linear code \( V \) of block length \( n \) and dimension \( k \) over \( \text{GF}(q) \). Such a code will be called an \([n, k]\) code over \( \text{GF}(q) \).

In this paper we find the Hamming weight enumerators of an infinite number of linear codes. The codes which are investigated here include a class of codes whose Hamming weight enumerator polynomials have earlier been found by Oganesyan, Yagdzyan, and Tairyari [6].

The method applied here is related to the method which Helleseth, Kløve, and Mykkeltveit [4], used in obtaining the weight enumerator polynomials of some irreducible cyclic codes.

2. Preliminaries

Let \( V \) be an \([n, k]\) code over \( F \) which has a \( k \times n \) generator matrix \( G \). We first give a construction which gives us an infinite class of codes \( V_l \) over \( F \), which have weight enumerator polynomials which are related in a very nice way. This construction consists of two steps.

Step 1. For every integer \( l \geq 1 \) we can consider \( G \) as a \( k \times n \) generator matrix for an \([n, k]\) code over \( \text{GF}(q^l) \). We call these codes \( V_l \) for \( l \geq 1 \).

Step 2. Let \( B \) be an irreducible cyclic \( [(q^l - 1)/(q - 1), l] \) code over \( \text{GF}(q) \) where \( \gcd(l, q - 1) = 1 \). Then every vector has weight \( q^{l-1} \). Also \( B \) is isomorphic to the
field $GF(q')$. If $\alpha$ is an element of order $(q^i - 1)/(q - 1)$ such that $\alpha, \alpha^2, \ldots, \alpha^{q^i-1}$ are the nonzeros (roots of the parity-check polynomial) of $B$, the isomorphism can be defined as in Goethals [3]: $b(x) \in B$ maps onto $b(\alpha) \in GF(q')$ and $\xi \in GF(q')$ maps onto the codeword $(a_0, a_1, \ldots, a_{(q^i-1)/(q-1)-1})$, where

$$a_i = \text{Tr}_i(\xi \alpha^{-i}) \quad \text{and} \quad \text{Tr}_i(x) = \sum_{j=0}^{i-1} x^{q^j}.$$  

A typical codeword of $V_i$ is $(\delta_0, \delta_1, \ldots, \delta_{n-1}, \delta_i \in GF(q')$. Map each $\delta_i$ onto a vector of length $(q^i - 1)/(q - 1)$ by the isomorphism described above. Then $V_i$ becomes an $[n(q^i - 1)/(q - 1), k]$ code which we call $\hat{V}_i$ and a vector of weight $i$ in $V_i$ becomes a vector of weight $q^{i-1}i$ of $\hat{V}_i$.

Hence, starting from an $[n, k]$ code $V_i$ over $F$ we have constructed a sequence of $[n(q^i - 1)/(q - 1), k]$ codes $\hat{V}_i$ over $F$ via a sequence of $[n, k]$ codes $V_i$ over $GF(q')$.

If we let $A_i(z)$ and $\hat{A}_i(z)$ denote the weight enumerator polynomials of $V_i$ and $\hat{V}_i$ respectively we note that

$$\hat{A}_i(z) = A_i(z^{q^{i-1}}).$$  

It is therefore easy to find the weight distribution of $\hat{V}_i$ from the weight distribution of $V_i$.

A very interesting fact is that the weight distribution of the codes $V_i$ are related in a nice way and can be found by considering the generator matrix $G$ only. The following theorem which connects the weight distribution $A_i(z)$ of the various $V_i$ is proved in Helleseth, Kløve, and Mykkeltveit [4].

**Theorem 2.1.** Let $V_i$ be an $[n, k]$ code with generator matrix $G = (g_{ij}), g_{ij} \in F$. Let $A_i(z)$ denote the weight enumerator polynomial of $V_i$. Then

$$A_i(z) = \sum_{i=0}^{n} \sum_{j=0}^{k} A_{ij} (q^i - 1)(q^i - q) \cdots (q^i - q^{i-1})z^i,$$

where $A_{ij}$ is the number of $(k - j)$-dimensional subspaces of $F^n$ which contain exactly $n - i$ of the $n$ columns of $G$.

The case $l = 1$ has been known for some time. See MacWilliams [5].

Note that the $A_{ij}$'s depend on $G$ only and are independent of $l$. We can arrange the $A_{ij}$'s in an array:

$$
\begin{array}{c|cccccc}
\hline
i & 0 & 1 & \cdots & k-1 & k \\
\hline
0 & 1 & 0 & \cdots & 0 & 0 \\
1 & 0 & A_{11} & \cdots & A_{1,k-1} & A_{1,k} \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
n & 0 & A_{n1} & \cdots & A_{n,k-1} & A_{n,k} \\
\hline
\end{array}
$$
Finding $A_i(z) = 1 + \sum_{i=1}^n A_i(q-1)z^i$ is equivalent of finding the first column of the array, (i.e. to find how many $(k-1)$-dimensional subspaces of $F^k$ which contains $n-i$ of the $n$ columns of $G$). To find $A_i(z)$ we also need to find the second column etc. We also note that $A_i(z)$ is determined for every $i \geq 1$ if we know all $A_1(z), \ldots, A_k(z)$ or $A_0$ for $0 \leq i \leq n$, $0 \leq j \leq k$.

In this paper we will consider generator matrices of two types $G^{(1)}$ and $G^{(2)}$.

Case 1. We let

$$G^{(1)} = [s_1, s_2, \ldots, s_n],$$

where $s_i = (\cdot)$ and $u$ runs through all nonzero vectors in $F^k$, $v$ through all nonzero vectors in $F^{k'}$. Thus $k = k_1 + k_2$ and $n = (q^{k_1} - 1)(q^{k_2} - 1)$.

Case 2. We let

$$G^{(2)} = [s_1, s_2, \ldots, s_n],$$

where $s_i = (\cdot)$ and $u$ runs through $S \subset F^k$ where $S$ has the property that every subset of $k_1$ vectors from $S_1$ contains $k_1$ linearly independent vectors $v$ through all nonzero vectors in $F^{k_2}$. Thus $k = k_1 + k_2$ and $n = n_1(q^{k_1} - 1)$ where $|S_i| = n_1$.

As above we will construct infinite sequences of codes $\hat{V}^{(1)}$ and $\hat{V}^{(2)}$ from $G^{(1)}$ and $G^{(2)}$ respectively. In Section 3 we will find the $A_n$'s for $G^{(1)}$ and $G^{(2)}$. Using Theorem 2.1 and (1) we find $\hat{A}_i(z)$ for every $i \geq 1$ in the two cases above.

Let $\mathcal{F}^k$ denote the family of subspaces of $F^k$. Let $Z$ denote the set of integers. In Section 3 we need the following results.

**Theorem 2.2.** Let $f$ and $g$ be mappings from $\mathcal{F}^k$ into $Z$. Let $X, U \in \mathcal{F}^k$. If

$$f(X) = \sum_{\phi(U) \subseteq X} g(U),$$

then

$$g(X) = \sum_{\phi(U) \subseteq X} (-1)^{\dim_X X - \dim_U X} q^{\dim_X X - \dim_U X} f(U).$$

**Lemma 2.3.** Let $[n] = \{W \in \mathcal{F}^k \mid \dim W = k\}$. Then

$$\prod_{i=0}^{n-k} (x - q^i) = \sum_{i=0}^n \binom{n}{i} (-1)^i q^i x^{n-i}. $$

Theorem 2.2, which is the Möbius inversion formula on the lattice $\mathcal{F}^k$, and Lemma 2.3, can be found in Bender and Goldman [1].

**Lemma 2.4.** Let $X \in \mathcal{F}^k$, and let

$$g_i(X) = \frac{|\{(v_1, \ldots, v_i) \in F^k \mid \dim_F \langle v_1, \ldots, v_i \rangle = X\}|}{|Z^i|}.$$ 

Then we have

$$g_i(X) = \prod_{i=0}^{\dim X - 1} (q^i - q^i).$$
Proof. We define \( f_i(X) \) such that \( f_i(X) = \sum_{\sigma \subseteq U \subseteq X} g_i(U) \). Then \( f_i(X) = \| \{ v_1, \ldots, v_i \} \| \), \( v_i \in F^k \), and \( \langle v_1, \ldots, v_i \rangle \subseteq X \), and therefore \( f_i(X) = q^{|X|} \). By Theorem 2.2 we have

\[
g_i(X) = \sum_{\sigma \subseteq U \subseteq X} (-1)^{|X|-|U|} q^{(|X|-|U|)+t} qt^{\dim U - |U|},
\]

where \( n = \dim X \). Hence we have

\[
g_i(X) = \sum_{\sigma \subseteq U \subseteq X} \binom{n}{|U|} (-1)^{|U|} q^{|U| + t} qt^{\dim U - |U|}.
\]

By Lemma 2.3 we get

\[
g_i(X) = \prod_{\sigma \subseteq U \subseteq X} q^{|U|-|\sigma|},
\]

which was to be proved.

3. Determination of \( A_i \)

Let \( \mathcal{F}_i \) denote the family of \( j \)-dimensional subspaces of \( F^k \), with \( \mathcal{F}_i = \bigcup_{j=0}^{n} \mathcal{F}_i^j \).

Let \( k = k_1 + k_2 \). When we write \( s = (s) \), we let \( u \in F^{k_1} \) and \( v \in F^{k_2} \).

Let \( W \in \mathcal{F}_i \). We define \( U_w = \{ u \ (s) \subseteq W \} \in \mathcal{F}_i^j \) and \( T_w = \{ t \ (s) \subseteq W \} \in \mathcal{F}_i^j \). It is then easy to see that

\[
\left( \begin{array}{c}
u_1 \\ \vdots \\ \nu_i \\ 0 \\ t_1 \\ \cdots \\ t_i \\
\end{array} \right)
\]

is a basis for \( W \) whenever \( u_1, \ldots, u_i, t_1, \ldots, t_i \) are bases for \( U_w \) and \( T_w \) respectively and \( (s_1) \subseteq W \).

Note that \( (s) \subseteq W \) and \( (s') \subseteq W \) implies that \( (s, s') \subseteq W \) and therefore \( v - v' \in T_w \).

Let \( W, W' \in \mathcal{F}_i \). It is then straightforward to check the following:

Lemma 3.1. We have \( W = W' \) if and only if \( U_w = U_w' \), \( T_w = T_w' \), and \( v - v' \in T_w = T_w' \) for \( i = 1, 2, \ldots, j \).

This means that when \( W \) runs through \( \mathcal{F}_i \), then \( U_w, T_w, v_1, v_2, \ldots, v_i \) run through all combinations with \( U_w \in \mathcal{F}_i^j \), \( T_w \in \mathcal{F}_i^k \), and every \( v \), runs through a complete set of representatives of \( F^*/T_w \) for \( i = 1, 2, \ldots, j \).

Let \( G_i \) be a \( k_i \times n_i \) matrix with components from \( F \), let \( S_i \) denote the set of column vectors of \( G_i \), and let \( n_i - |S_i| \).
Let $G$ be the $k \times n_i(q^{k_2} - 1)$ matrix with components from $F$ such that

$$G = [s_1, s_2, \ldots, s_n],$$

where $s_i = (\cdot)$ and $u, v$ run through all possible combinations $u \in S_i, v \in F^{k_2} - \{0\}$. We let $S$ denote the set of column vectors of $G$.

If $S_i$ consists of all nonzero vectors in $F^{k_1}$, then $G = G^{(i)}$ as defined in (2).

If $S_i$ has the property that every set of $k_1$ vectors from $S_i$ are linear independent, then $G = G^{(2)}$ as defined in (3). Note that in this case $G_i$ is the generator matrix of an $[n, k]$ maximum distance separable code.

In this section we find the $A_y$'s of Theorem 2.1 for $G^{(i)}$ and $G^{(2)}$. To simplify notations we let $B_y = A_{n-k, 0}$. Hence $B_y = \{|W \in \mathcal{F}_y^k||W \cap S_i| = i\}$. We let $B_y^* = A_{n-k, 0}^*$ where $A_y^*$ refers to $G_i$.

Using the basis for $W \in \mathcal{F}_y^k$ given in (4) we get:

**Lemma 3.2.** We have

$$|W \cap S_i| = |U_w \cap S_i|q^{k_2} - \left| \left\{ a \in F^{k_1} \left| \sum_{i=1}^{k_1} a_u, u \in S_i \text{ and } \sum_{i=1}^{k_2} a_v, v \in T_w \right. \right\} \right|.$$

**Proof.** By (4) we get

$$|W \cap S_i| = \left| \left\{ a \in F^{k_1}, b \in F^{k_2} \left| \sum_{i=1}^{k_1} a_u, u \in S_i \text{ and } \sum_{i=1}^{k_2} a_v, + \sum_{i=1}^{k_2} t_v, \neq 0 \right. \right\} \right|$$

$$= \left| \left\{ a \in F^{k_1} \left| \sum_{i=1}^{k_1} a_u, u \in S_i \text{ and } \sum_{i=1}^{k_2} a_v, v \in T_w \right. \right\} \right| (q^{k_2} - 1)$$

$$+ \left| \left\{ a \in F^{k_1} \left| \sum_{i=1}^{k_1} a_u, u \in S_i \text{ and } \sum_{i=1}^{k_2} a_v, v \notin T_w \right. \right\} \right| q^{k_2}$$

$$= \left| \left\{ a \in F^{k_1} \left| \sum_{i=1}^{k_1} a_u, u \in S_i \right. \right\} \right| q^{k_2}$$

$$- \left| \left\{ a \in F^{k_1} \left| \sum_{i=1}^{k_1} a_u, u \in S_i \text{ and } \sum_{i=1}^{k_2} a_v, v \in T_w \right. \right\} \right|$$

$$= |U_w \cap S_i|q^{k_2} - \left| \left\{ a \in F^{k_1} \left| \sum_{i=1}^{k_1} a_u, u \in S_i \text{ and } \sum_{i=1}^{k_2} a_v, v \in T_w \right. \right\} \right|,$$

which was to be proved.

**Theorem 3.3.** Let $G^{(i)}$ be as in (2). Then

$$B_y = \sum_{i=0}^{k_1} \left[ k_1 \right] \left[ k_2 \right] \sum_{j=0}^{k_2-j} \left[ k_2 - j + j_1 \right] \prod_{i=0}^{j_i} \left( q^{k_i} - q^i \right), \quad i = q^i - q^{i-1} - q^{i-2} + 1.$$

**Remark.** Note that the expression for $B_y$ contains at most two nonzero terms and is therefore easy to calculate.
Proof. Since, in this case, \( S_i \) consists of every nonzero vector of \( F^{k_i} \) we get by Lemma 3.2 when \( W \in F_{i}^{\beta} \):

\[
| W \cap S_i | = | U_w \cap S_i | q^{h_j} - \left| \left\{ a \in F_i \right\} | \sum_{i=1}^{l} a u_i \in S_i \text{ and } \sum_{i=1}^{l} a v_i \in T_w \right| \]
\[
= (q^{l-1}) q^{h_j} - \left| \left\{ a \in F_i \cdot \{0 \} \right\} \sum_{i=1}^{l} a v_i \in T_w \right| \]
\[
= q^{l} - q^{h_j} - q^{l-1 \cdot \dim \mathcal{C} - h_j + 1},
\]

where \( \mathcal{C} = v_i + T_w \in F^{k_j}/T_w \).

By Lemma 3.1 we note that when \( W \) runs through \( F_{i}^{\beta} \), then \( U_w, T_w \), and \( \mathcal{C} \) run through all combinations \( U_w \in F_{i}^{\beta}, T_w \in F_{i}^{\beta} \), and \( \mathcal{C} \in F^{k_j}/T_w \) for \( i = 1, 2, \ldots, l \), such that \( j = j_1 + j_2 \). The number of \( W \in F_{i}^{\beta} \) such that \( \dim U_w = j_1 \), \( \dim T_w = j_2 \), and \( \dim (\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_l) = p \) is therefore

\[
\left[ k_1 \right] \left[ j_1 \right] \left[ k_2 \right] \left[ j_2 \right] \prod_{i=0}^{l} (q^{h_j} - q^{p_i}),
\]

since \([k_i]\) and \([j_i]\) are the number of choices of \( U_w \) and \( T_w \) respectively and \([k_i, j_i]\) \( \prod_{i=0}^{l} (q^{h_j} - q^{p_i}) \) is, by Lemma 2.4, the number of choices of \( \mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_l \), such that \( \dim (\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_l) = p \). All these choices of \( W \) give \( | W \cap S_i | = q^l - q^{h_j} - q^{l-1 \cdot p_i} + 1 \). Hence

\[
B_{n1} = \left\{ \left| W \in F_{i}^{\beta} \right| \mid | W \cap S_i | = i \right\} = \sum_{i=0}^{k_2} \left[ k_1 \right] \left[ k_2 \right] \prod_{i=0}^{l} \left[ k_i - j_1 \right] \prod_{i=0}^{l} (q^{h_j} - q^{p_i}), \quad i = q^l - q^{h_j} - q^{l-1 \cdot p_i} + 1,
\]

which was to be proved.

We next will determine \( B_{n1} \) for \( G^{(2)} \) defined in (3). Then since \( G_{1} \) is a maximum distance separable code we get

\[
B_{n1}^{*} = \binom{n_1}{i} \sum_{i=0}^{n_1} (-1)^i \binom{n_1 - i}{h} \binom{k_1 - i - h}{k_1 - j}, \quad \text{for } j < k_1,
\]

\( B_{n1,1}^{*} = 1 \) and \( B_{n1,0}^{*} = 0 \) when \( i < n_1 \). See Helleseth, Kløve, and Mykkeltveit [4].

Theorem 3.4. Let \( G^{(2)} \) be as defined in (3). Then

\[
B_{n} = \sum_{i=n_1}^{k_2} \left[ k_1 \right] \sum_{i=0}^{k_1} B_{n1}^{*} q^{n_1 \cdot 1 + n_1 \cdot 1} \left( \frac{\rho}{\gamma} \right) (q^l - 1)^{p_{i}},
\]

\[
+ \left[ k_2 \right] \sum_{i=0}^{k_2} \sum_{i=0}^{k_2} B_{n1}^{*} q^{n_1 \cdot 1} \prod_{i=0}^{l} (q^{h_j} - q^{p_i}),
\]

where
For $U \in \mathcal{F}_k^+$, we choose a basis $u_1, u_2, \ldots, u_n$ for $U$ as follows. If $j_1 = k_1$, let $u_1 = s_1^t, u_2 = s_2^t, \ldots, u_{k_1} = s_{k_1}^t$. If $j_1 < k_1$ and $U \cap S_1 = \{s_1^t, s_2^t, \ldots, s_n^t\}$, then $s_1^t, s_2^t, \ldots, s_n^t$ are linear independent and we choose $u_1 = s_1^t, u_2 = s_2^t, \ldots, u_n = s_n^t$ and let $u_{n+1}, u_{n+2}, \ldots, u_{k_1}$ be arbitrary such that $u_1, u_2, \ldots, u_{k_1}$ is a basis for $U$.

Let $W \in \mathcal{F}_k^+$. Using the basis in (4) for $W$ we divide $\mathcal{F}_k^+$ into two classes depending on $\dim U_w$.

**Class 1.** Let $\dim U_w = j_1 < k_1$. If we let $|U_w \cap S_1| = \rho$ then we get from Lemma 3.2, since we have chosen the basis for $U_w$ as above

$$|W \cap S| = \rho q^{j_1^2} - \gamma,$$

where $\gamma = \{|i| \in T_w, 1 \leq i \leq \rho\}$. We have $0 \leq \gamma \leq \rho \leq j_1 < k_1$.

The number of $W \in \mathcal{F}_k^+$ such that $\dim U_w = j_1, |U_w \cap S_1| = \rho$, $\dim T_w = j_2$, and $|\{i \in T_w, 1 \leq i \leq \rho\}| = \gamma$ is by Lemma 3.1

$$B_{\rho j_1} [k_2_{j_2}] q^{(k_2^2 + 2k_1 \rho \gamma)}/(q^\gamma - 1)^{\rho - \gamma},$$

(5)

since $B_{\rho j_1}^*$ is the number of choices of $U_w$ such that $\dim U_w = j_1$ and $|U_w \cap S_1| = \rho$. $[k_2_{j_2}]$ is the number of choices of $T_w$ such that $\dim T_w = j_2$. $q^{(k_2^2 + 2k_1 \rho \gamma)}/(q^\gamma - 1)^{\rho - \gamma}$ is the number of of choices of $v_1, v_2, \ldots, v_{j_2}$ such that exactly $\gamma$ of these belong to $T_w$, when every $v_i$ for $i = 1, 2, \ldots, j_2$ runs through a complete set of representatives of $F^{k_2}/T_w$. Every such $W \in \mathcal{F}_k^+$ give $|W \cap S| = \rho q^{j_1^2} - \gamma$.

**Class 2.** Let $\dim U_w = k_1$. Then our basis for $U_w$ is

$$\begin{bmatrix}
1 & 0 \\
0 & 1 \\
\vdots & \vdots \\
0 & 0 \\
\end{bmatrix} \begin{bmatrix}
0 & 0 \\
0 & 0 \\
\vdots & \vdots \\
1 & 1 \\
\end{bmatrix}$$

Hence $S_1 \subseteq U_w$ and $\Sigma_{i=1}^n a_i u_i = a$. By Lemma 3.2 we get $|W \cap S| = n q^{j_1^2} - \gamma$, where $\gamma = \{|a| \in S_1, \Sigma_{i=1}^n a_i b_i = \bar{b}\}$. 

\[B_{\rho j_1} = \begin{pmatrix} n_1 \end{pmatrix} \sum_{k=0}^{j_1} (-1)^{j_1} {n_1 \choose h} \left[ k_1 - i - h \right] \begin{pmatrix} k_1 - j - h \end{pmatrix} \text{ for } j < k_1, \ B_{\rho j_1} = 1 \text{ and } B_{\rho j_1} = 0 \text{ when } i < n_1.\]
Here, $\delta_i = \delta + T_w \in F^{k_i}/T_w$. When $v_i$ runs through a complete set of representatives, then $\delta_i$ runs through the vectorspace $F^{k_i}/T_w$ of dimension $k_i - j$. We consider $\delta_i$ as elements of $F^{k_i - j}$; for $i = 1, 2, \ldots, j$. Let $V_i = \{ \delta \in F^{k_i} | \sum_{i=1}^{k_i} a_i \delta_i = 0 \}$. Then $V_i$ is the orthogonal complement of the rowspace of the $(k_i - j) \times k_i$ matrix $[\delta_1, \delta_2, \ldots, \delta_{k_i}]$. When $\delta_i$, for $i = 1, 2, \ldots, k_i$, runs through $F^{k_i - j}$ independent of each other, then the row vectors $r_i$ of this matrix run through every $k_i$-dimensional vector independent of each other for $i = 1, 2, \ldots, k_i - j$. By Lemma 2.4 every rowspace of dimension $r$ occurs $\prod_{i=1}^{r} (q^{k_i - j} - q^r)$ times. Hence every $V_i$ of dimension $k_i - r$ also occurs $\prod_{i=0}^{j} (q^{k_i - j} - q^r)$ times.

The number of $W \in F^k$ such that $\dim U_W = k_1$, $\dim T_w = j_2$, $\gamma = |V^i \cap S|$, and $\dim V^i = k_1 - r$ is by Lemma 3.1

$$B_{k_1,k_2}^{*} \prod_{i=0}^{j} (q^{k_i - j} - q^r) \left[ \begin{array}{c} k_2 \\ j_2 \end{array} \right].$$

(6)

since $[\delta_i]$ is the number of choices of $T_w$ such that $\dim T_w = j_2$, and $B_{k_1,k_2}^{*}$ is the number of $V^i$ such that $\dim V^i = k_1 - r$ and $\gamma = |V^i \cap S|$. Since $V^i$ runs through $F^k$, exactly $\prod_{i=0}^{j} (q^{k_i - j} - q^r)$ times when every $\delta_i$ for $i = 1, 2, \ldots, k_i$, runs through a complete set of representatives of $F^{k_i}/T_w$, we get (6). Every such $W \in F^k$ give $|W \cap S| = n q^r - \gamma$.

Since every $W \in F^k$ belongs to class 1 or class 2 we get Theorem 3.4 when we combine (5) and (6).

4. Applications

In this section we will apply the results obtained in Sections 2 and 3, and we will find the Hamming weight enumerator polynomials of some cyclic codes which have composite parity-check polynomials, and whose weight enumerating polynomials have not been reported earlier except in a few cases.

Using Theorem 2.1, Theorem 3.3, Theorem 3.4, and (1) we are able to construct a sequence of codes $V_n$, $l \geq 1$, with known weight distribution, starting from a code $V_1$ with generator matrix $G^{(1)}$ or $G^{(2)}$.

We next show that if $V_1$ is a cyclic $[n, k]$ code then $V_1$ can be taken to be a cyclic $[n(q^l - 1)/(q - 1), k]_2$ code over $F$ when $\gcd(n,(q^l - 1)/(q - 1)) = 1$.

If $V_1$ is a cyclic $[n, k]$ code over $F$ with parity-check polynomial $h(x) \in F[x]$, then $V_1$ is a cyclic $[n, k]$ code over $GF(q^l)$ with $h(x)$ as parity-check polynomial for every $l > 1$.

If $V_1$ is a cyclic code, and $n$ and $(q^l - 1)/(q - 1)$ are relatively prime, the code $V_1$ can be arranged as a cyclic code as follows: Let $(\delta_n, \delta_{n-1}, \ldots, \delta_{n-2}) \in V_n$, map each $\delta_i$ onto a column vector of length $(q^l - 1)/(q - 1)$ and weight $q^{l-1}$ by the isomorphism described in Section 2. The codeword $(\delta_n, \delta_{n-1}, \ldots, \delta_{n-2})$ becomes a $(q^l - 1)/(q - 1) \times n$ array
Label the rows of this array by $1, x, \ldots, x^{q^l - 1}$ and the columns by $1, y, \ldots, y^{n - 1}$ ($y^n = 1$). A codeword of $\tilde{V}_l$ is then $f(x, y)$ a polynomial in $x$ and $y$.

Set $xy = z$. For each $s, r, 0 \leq s \leq (q^l - 1)/(q - 1) - 1$, $0 \leq r \leq n(q^l - 1)/(q - 1) - 1$ such that $r \equiv s \pmod{(q^l - 1)/(q - 1)}$, $r \equiv t \pmod{n}$, and $z' = x^ry'$, then $f(x, y) = \sum_{j=0}^{(q^l - 1)/(q - 1) - 1} a_jz^j$, and $(a_0, a_1, \ldots, a_{(q^l - 1)/(q - 1) - 1})$ is a codeword of the cyclic code $V_l$.

If $\alpha, \alpha^n, \ldots, \alpha^{n^{q^l - 1}}$ are the nonzeros of $B$ and $\gamma_1, \gamma_2, \ldots, \gamma_n$ the nonzeros of $V$, then by Berlekamp and Justesen [2] the nonzeros of $V_l$ are

$$\alpha \gamma_{1i}, (\alpha \gamma_1)^n_{1i}, \ldots, (\alpha \gamma_1)^{n^{q^l - 1}}_{1i}, \ldots, \alpha \gamma_{ki}, (\alpha \gamma_k)^n_{ki}, \ldots, (\alpha \gamma_k)^{n^{q^l - 1}}_{ki}.$$ 

Hence, if $V_l$ is a cyclic code, and $\gcd(n, (q^l - 1)/(q - 1)) = 1$, and $\gamma_1, \gamma_2, \ldots, \gamma_n$ are the nonzeros of $V$, then the nonzeros of $V_l$ are $(\alpha \gamma_i)^n_{ji}, 1 \leq j \leq k, 0 \leq i < l$.

Case 1. Construction of cyclic codes from $G^{(1)}$. Let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be the nonzero elements of $F$. Let $G^{(1)} = \lambda_1H | \lambda_2H | \cdots | \lambda_nH$. If $\gcd(k_1, k_2) = 1$, then $H$ may be taken to be a cyclic code as follows: Let $C_1$ be a $[(q^{k_1} - 1)/(q - 1), k]_q$ cyclic code with $\gcd(k, q - 1) = 1$. Let $C_2$ be a $[(q^{k_2} - 1), k]_q$ cyclic code. Let $H_1$ be a generator matrix for $C_1$, $i = 1, 2$. Then we can take $H$ as the $(k_1 + k_2) \times n((q^{k_1} - 1)(q^{k_2} - 1))/(q - 1)$ matrix

$$H = \begin{pmatrix} H_1 & H_1 & \cdots & H_1 \\ H_2 & H_2 & \cdots & H_2 \\ \vdots & \vdots & \ddots & \vdots \\ H_n & H_n & \cdots & H_n \end{pmatrix}.$$ 

Let now $H$ be the generator matrix of $V_l$. Let $n = ((q^{k_1} - 1)/(q^{k_2} - 1))(q - 1)$ and let $\beta$ be a primitive $n$th root of unity such that $\beta^{q^{k_1} - 1}$ is a nonzero of $C_1$ and $\beta^{q^{k_2} - 1}$ is a nonzero of $C_2$. The code generated by $H$ has the $k_1 + k_2$ nonzeros

$$(\beta^{q^{k_1} - 1})^i, (\beta^{q^{k_2} - 1})^{n - 1}j, 0 \leq i < k_1, 0 \leq j < k_2.$$ 

If $\gcd(k_1, k_2) = \gcd(k_1, l) = \gcd(k_2, l) = \gcd(k_1, q - 1) = 1$, then $\gcd(n, (q^l - 1)/(q - 1)) = 1$ and the nonzeros of $V_l$ fall in two conjugacy classes

$$(\alpha \beta^{q^{k_1} - 1})^i, (\alpha \beta^{q^{k_2} - 1})^{n - 1}j, 0 \leq i < k_1, 0 \leq j < k_2.$$ 

Thus the parity check polynomial of $V_l$ is a product of two irreducible polynomials of degree $k_1l$ and $k_2l$ respectively. Since $G^{(1)}$ and $H$ are closely related, the weight distribution of $V_l$ for every $l \geq 1$ can easily be calculated from Theorem 2.1, Theorem 3.3, and (1).

Case 2. Construction of cyclic codes from $G^{(2)}$. Let $C_1$ be an $[n_1, k_1]$ cyclic maximum distance separable code. Let $C_2$ be a $[q^{k_2} - 1, k_2]$ cyclic code where $\gcd(n_1, q^{k_2} - 1) = 1$. Let $H_1$ be a generator matrix for $C_1$, $i = 1, 2$. Then we can take $G^{(2)}$ as the $(k_1 + k_2) \times n_1(q^{k_2} - 1)$ matrix
\( G^{(q)} = (H_1, H_1, \ldots, H_1). \)

Let now \( G^{(q)} \) be the generator matrix of \( V_1 \). Let \( \gamma_1, \gamma_2, \ldots, \gamma_k \) and \( \gamma_{k-1}, \gamma_{k-2}, \ldots, \gamma_k \) be the nonzeros of \( C_1 \) and \( C_2 \) respectively, then \( \gamma_1, \gamma_2, \ldots, \gamma_k \) are the nonzeros of \( V_1 \). Thus we easily find the nonzeros of \( \hat{V}_i \) for every \( I \geq 1 \). The weight distribution of \( \hat{V}_i \) can easily be calculated from Theorem 2.1, Theorem 3.4, and (1).

**Example.** Let \( q = 2, k_1 = 1, k_2 = 2 \), and let

\[
H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},
\]

be a generator matrix for a \([3, 3]\) code over GF(2). Let \( B \) be a \([7, 3]\) code. The isomorphism between \( B \) and \( \text{GF}(2^7) \) can be taken to be

\[
1 \leftrightarrow 11110100,
\]

\[
\alpha \leftrightarrow 01110100,
\]

\[
\alpha^2 \leftrightarrow 00110101. \text{ etc.}
\]

Thus the codeword \((1, \alpha, \alpha^2)\) of the \([3, 3]\) code \( V_3 \) becomes the array

\[
1 \begin{array}{c} y \ y^2 \\
1 \left[ \begin{array}{ccc} 1 & 0 & 0 \\
1 & 1 & 0 \\
x^2 & 1 & 1 \\
x^4 & 0 & 1 \\
x^5 & 1 & 0 \\
x^6 & 0 & 1 \\
x^7 & 0 & 0 \end{array} \right] \end{array}
\]

\[
f(x, y) = 1 + x + xy + x^2y + x^2y^2 + x^3y + x^3y^2 + x^4 + x^4y^2 + x^5y + x^6y^2. \]

The exponents of \( x, y, z \) are shown in the following table

<table>
<thead>
<tr>
<th>x</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>7</td>
<td>14</td>
</tr>
<tr>
<td>1</td>
<td>15</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>9</td>
<td>16</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>10</td>
<td>17</td>
</tr>
<tr>
<td>4</td>
<td>18</td>
<td>4</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>12</td>
<td>19</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>13</td>
<td>20</td>
</tr>
</tbody>
</table>

\[ f(x, y) = 1 + z + z^7 + z^{10} + z^{11} + z^{15} + z^{16} + z^{17} + z^{18} + z^{19} + z^{20}. \]
The nonzeros of $B$ are $\alpha, \alpha^2, \alpha^4$ where $\alpha^7 = 1$, and of $V, 1, \beta, \beta^2$ where $\beta^4 = 1$. Let $\gamma$ be a primitive 21st root of unity with $\alpha = \gamma^5, \beta = \gamma^7$. The nonzeros of $\hat{V}$, are

$$\gamma, \gamma^5, \gamma^{12},$$

$$\gamma^{10}, \gamma^{20}, \gamma^{10}, \gamma^{17}, \gamma^{13}, \gamma^5,$$

which are roots of two irreducible polynomials of degree 3 and 6.

The weight distribution of $\hat{V}_3$ is according to Theorem 3.3 (or Theorem 3.4) and (1)

$$\hat{A}_3(z) = 1 + 21z^4 + 147z^6 + 343z^{12}.$$ 

Acknowledgment

The author is grateful for the suggestions of the anonymous referee. Due to his criticism the original version of this paper has been considerably improved.

References