WEIGHT DISTRIBUTION FORMULA
FOR SOME CLASS OF CYCLIC CODES

Tadao Kasami

REPORT R-285    APRIL, 1966
This work was supported in part by the Joint Services Electronics Program (U. S. Army, U. S. Navy, and U. S. Air Force) under Contract No. DA 28 043 AMC 00073(E), and in part by the National Science Foundation under Grant NSF GK-690, and in part by the Air Force Cambridge Research Laboratories under Contract AF 19(628)4379.

Reproduction in whole or in part is permitted for any purpose of the United States Government.

Distribution of this report is unlimited. Qualified requesters may obtain copies of this report from DDC.
Weight Distribution Formula for Some Class of Cyclic Codes

Tadao Kasami

Abstract

Let $h_1(X)$ and $h_2(X)$ be different irreducible polynomials such that $h_1(\alpha^{-2^h-1}) = 0$ for some $h (0 < h < m)$ and $h_2(\alpha^{-1}) = 0$, $\alpha$ being a primitive element of $GF(2^m)$. This paper presents the weight distribution formula of the code of length $2^m-1$ generated by $(X^{2^m-1} - 1)/(h_1(X)h_2(X))$ for any $m$ and $h$. Some applications to the cross-correlation problem between two different maximum length sequences are presented.
1. Introduction

W. W. Peterson [1] calculated a number of weight distributions for BCH codes of lengths 63 to 1023 and their dual codes by digital computation. He observed that some BCH codes with large \( t \) for a given \( m \) (5 \( \leq \) \( m \) \( \leq \) 10) have a very simple structure of weight distribution. The result presented here is a theoretical development of his observation.

Let \( C \) be a cyclic code of length \( 2^m-1 \). The extended code of \( C \) is the code with an overall parity check added to \( C \) as the first digit. The first symbol in a code vector is numbered 0, and for \( i > 1 \) the \( i \)-th digit is numbered \( \alpha^{i-2} \), \( \alpha \) being a primitive element of \( GF(2^m) \). Now for \( a \neq 0 \) and \( b \in GF(2^m) \) and for a code vector \( v \) of the extended code, permute the symbol in position \( X \) to position \( aX + b \). Then, the resulting vector is denoted by \( \pi_{ab}v \). W. W. Peterson [1] proved that the extended codes of BCH codes are invariant under doubly transitive group of permutations \( \pi = \{ \pi_{ab} | a \neq 0, b \in GF(2^m) \} \). This paper presents the weight distribution formula for a class of cyclic codes of length \( 2^m-1 \) whose extended codes are invariant under \( \pi \).

Let \( g_1(X) \) and \( g_2(X) \) be different irreducible polynomials such that

1. \( g_1(\alpha^{2^h+1}) = 0 \) for some \( h \) (0 \( \leq \) \( h \) \( < \) \( m \)),
2. \( g_2(\alpha) = 0 \)

The degree of \( g_1(X) \) is a factor \( m' \) of \( m \) and the degree of \( g_2(X) \) is \( m \). Let

\[
 h_1(X) = X^{m'}g_1(X^{-1}), \quad h_2(X) = X^mg_2(X^{-1})
\]

Let \( C_0, C \) and \( C' \) denote binary cyclic codes with length \( 2^m-1 \) generated by

\[
g_1(X)g_2(X), (X^{2^m-1}-1)/(h_1(X)h_2(X)) \quad \text{and} \quad (X^{2^m-1}-1)/(X-1)h_1(X)h_2(X)
\]

respectively. Then \( C \) is the dual code of \( C_0 \) and a subcode of \( C' \). If \( h = 1 \), then \( C_0 \) is a double error correcting BCH code, and if \( m \) is odd and \( h = (m-1)/2 \), then \( C \) is
a BCH code with the second largest t for given m.

In what follows, the weight distribution formula of code $C$ for any m and h will be derived. This problem is closely related to the cross-correlation problem between two different maximum length sequences.* Some applications to the problem will be presented in section 6.

2. Preliminary Lemmas

Lemma 1: The extended code of $C'$ or $C_o$ is invariant under $\pi$.

This lemma follows from the definition of $C'$ or $C_o$ and a general theorem [2]. Let

$$m = m'm''.$$ (1)

Since $a^{2^{m-h}+1}$ is a root of $g_1(X)$, it can be assumed that

$$2h \leq m.$$ (2)

Since $(2^{m'-1})(2^h+1)$ is divisible by $(2^{m'-1}-1)(2^{m'}(m''-1) + 2^{m'}(m''-2) + \ldots + 1)$,

$$h \geq m'(m''-1).$$

From (1) and (2),

$$m'm'' \geq 2h \geq 2m'(m''-1).$$ (3)

Hence,

$$m'' = 1 \text{ or } 2.$$ (4)

If $m'' = 2$, then it follows from (3) that

$$m' = h.$$ (5)

That is, there are only two cases:

$$m' = m$$

and

$$m' = m/2 = h.$$ (6)

* Dr. B. Elspas pointed out this relation.
The following well-known lemmas will be used later.

Lemma 2: Let \( u(\ell) \) denote the smallest positive integer \( u \) such that 
\[ 2^u \equiv 1 \pmod{\ell}. \]
Then, 
\[ 2^{u'} \equiv 1 \pmod{\ell} \]
if and only if \( u' \equiv 0 \pmod{u(\ell)}. \)
Let \((\ell, \ell')\) denote the greatest common divisor of \( \ell \) and \( \ell' \).

Corollary 3: Let \( u = (u_1, u_2) \). Then,
\[ 2^{u_1-1} = 2^{u_2-1}(2^{u_1-1} + 2^{u_2-1}). \]

Lemma 4: \( 2^{u+1} \) (or \( 2^{u-1} \)) is divisible by \( 2^{u+1} + 1 \), if and only if \( u \) is divisible by \( u' \) and \( u/u' \) is odd (or even).

Let \( c' = (m, h) \), \( c = (m, 2h) \) and \( v = (2^m-1, 2^h+1) \). By Corollary 3,
\[ 2^{c'-1} = (2^{m-1}, 2^{h-1}), \]
\[ 2^{c-1} = (2^{m-1}, 2^{2h-1}). \]

Since \( (2^{h+1}, 2^{h-1}) = 1 \),
\[ (2^{m-1}, 2^{2h-1}) = (2^{m-1}, 2^{h+1})(2^{m-1}, 2^{h-1}). \]
Thus,
\[ (2^{c-1})/v = 2^{c'-1}. \]

By definition, \( c = c' \) or \( 2c' \). Therefore, we have:

Lemma 5: If \( c = c' \), then \( v = 1 \). Otherwise,
\[ v = 2^{c'+1} = 2^{c/2}+1. \]

The next lemma is due to Pless [3].

Lemma 6: Let \( a_j \) and \( b_j \) denote the number of code vectors of weight \( j \) in a code \( A \) and the number of code vectors of weight \( j \) in the dual code of \( A \) respectively. If \( b_1 = b_2 = 0 \), then the following power moment identities hold:
\[ \Sigma a_j = 2^k \]
\[ \Sigma a_j = 2^{k-1} \]
\[ \sum j a_j = 2^{k-2} n(n+1) \]
\[ \sum j a_j = 2^{k-3} (n^3 + 3n^2) - 3! 2^{k-3} b_3 \]
\[ \sum j a_j = 2^{k-4} (n^4 + 6n^3 + 3n^2 - 2n) - 4! 2^{k-4} b_4 + 4! 2^{k-4} b_4, \]

where \( k \) denotes the number of information digits.

Let \( C_1 \) and \( C_2 \) denote binary cyclic codes with length \( 2^m-1 \) generated by \( (X^{2^m-1}-1)h_1(X) \) and \( (X^{2^m-1}-1)/h_2(X) \) respectively. Codes \( C_1 \) and \( C_2 \) are subcodes of \( C \) and \( C' \). If the degree of \( g_1(X) \) is \( m \), then the roots of \( h_1(X) = X^m g_1(X^{-1}) \) are:

\[ a^{-2(2^h+1)} = a^{2^m-2^{h+2}}, a^{-2(2^h+1)} = a^{2^m-2^{h+1}-2-1}, \ldots, \]
\[ a^{-2^{m-1}-2^{m-h-1}-1}, a^{-2^{m-h}(2^h+1)} = a^{2^m-2^{m-h-2}}, \]
\[ \ldots, a^{-2^{m-1}-2^{h-1}-1}. \]

There is no \( i \) \((0 \leq i < 2^m)\) with \( h_1(a^i) = 0 \) except for

\[ i_1 = 2^{m-1}-2^{m-h-1}-1 \]

and

\[ i = 2^{m-1}-2^{h-1}-1. \]

By (2), \( i_1 < i \).

If \( m' = \ldots / 2 \), then the roots of \( h_1(X) \) are:

\[ a^{-2^{m+1}} = a^{2^m-2^{m'-2}}, a^{-2^{m+1}} = a^{2^m-2^{m'+1}-2-1}, \ldots, \]
\[ a^{-2^{m-1}-(2^{m'+1})} = a^{2^{m-1}-2^{m'-1}-1}. \]
there is no 1 \( 0 \leq i < 2^{m-1} \) with \( h_1(\alpha^i) = 0 \) except for
\[
i_1 = 2^{m-1}2^{m-1}-1.
\]
The roots of \( h_2(X) \) are \( \alpha^{-1} = \alpha^{2^{m-2}}, \alpha^{-2} = \alpha^{2^{m-3}}, \ldots, \alpha^{-2^{m-1}} = \alpha^{2^{m-1}-1} \).

As it is done above, here we let
\[
i_2 = 2^{m-1}-1.
\]

Let \( X_1, X_2, \ldots, X_w \) be the location numbers of code vector * \( v(x) \) of \( C' \).

Then,
\[
v(\alpha^i) = \sum_{f=1}^{w} X_f^i, \quad 0 \leq i < 2^{m-1}
\]
For any \( B_0 \in \text{GF}(2) \), any \( B_1 \in \text{GF}(2^{m'}) \) and any \( B_2 \in \text{GF}(2^m) \), there exists a unique code vector \( v(x) \) of \( C' \) such that \( v(1) = B_0, v(\alpha^1) = B_1 \) and \( v(\alpha^2) = B_2 \) (Mattson, Solomon [5]). Let \( v(B_0, B_1, B_2; x) \) denote the code vector specified by \( B_0, B_1 \) and \( B_2 \). By definition,
\[
x v(B_0, B_1, B_2; x) = v(B_0, \alpha^{-1} B_1, \alpha^{-2} B_2; x)
\]
If and only if \( B_0 = 0 \), \( v(B_0, B_1, B_2; x) \in C \). If and only if \( B_0 = B_1 = 0 \) (or \( B_0 = B_2 = 0 \)), then \( v(B_0, B_1, B_2; x) \in C_2 \) (or \( C_1 \)). The cyclic permutations on code word symbols induce a permutation group on the code vectors of \( C' \), which divides \( C' \) into disjoint sets of transitivity. Since \( v = (i_1, 2^{m-1}) \), each set consists of \((2^{m-1})/v \) code vectors. In case of \( m' = m \), let \( v(0, \alpha^i, B_2; x) \) \( (0 \leq i < v, B_2 \in \text{GF}(2^m)) \) represent each set. In case of \( m' = m/2 \), let \( v(0, 0, B_2; x) \) represent each set.

A polynomial representation will be used for a code vector [4].
Now, consider the extended code $C_{ex}$ of code $C'$. Let $\bar{v}(B_0, B_1, B_2)$ denote the vector with an overall parity check added to $v(B_0, B_1, B_2; x)$ as the first digit. By definition $C_{ex} = \{ \bar{v}(B_0, B_1, B_2) | v(B_0, B_1, B_2; x) \in C' \}$.

Let $X_1, X_2, \ldots, X_i$ be the location numbers of $\bar{v}(B_0, B_1, B_2)$ and let

$$S_i = \sum_{f=1}^{w} X_i^i, \quad 0 \leq i < 2^{m-1}$$

(7)

Then, by definition

$$S_{i_1} = B_1^1$$

(8)

$$S_{i_2} = B_2^1$$

(9)

$$S_i = 0 \ (i \not\equiv i_1, i_2 \ (mod \ 2^{m-1}), \ 0 \leq i < m)$$

Therefore,

$$S_i = 0 \ (i \not\equiv i_1, i_2, 1 \leq i < 2^{m-1})$$

(10)

By Lemma 1, $-1_b \bar{v}(B_0, B_1, B_2) \in C_{ex}$ for any $b \in GF(2^m)$. Let

$$-1_b \bar{v}(B_0, B_1, B_2) = \bar{v}(B_0', B_1', B_2')$$

(11)

The weights of $\bar{v}(B_0, B_1, B_2)$ and $\bar{v}(B_0', B_1', B_2')$ are the same. By the definition

$$B_1^i = \sum_{f=1}^{w} (X_i + b^i)$$

$$B_2^i = \sum_{f=1}^{w} (X_i + b^i)$$

Hence

$$B_1^i = \sum_{f=1}^{w} X_i^i b^{i-1} = \sum_{f=1}^{w} \binom{i}{i} X_i^i b^{i-1} = \sum_{f=1}^{w} \binom{i}{i} S_i^i b^{i-1}$$

(12)
From (8) and (10),

\[ \beta'_1 = \beta'_1 \]  \hspace{1cm} (12)

Note that \((X_f+b)^2 = (X_f+b)^{2^{m-1}-1} = (X_f^{2^{m-1}} + b^{2^{m-1}})/(X_f+b) = X_f^{2^{m-1}} + \]
\[ X_f^{2^{m-1}}b + \ldots + b^{2^{m-1}-1}. \]

Then,

\[ \beta'_2 = \sum_{i=0}^{2^{m-1}-1} \sum_{i=0}^{2^{m-1}-1} X_f b^{2^{m-1}-1-i} = \sum_{i=0}^{2^{m-1}-1} s_i b^{2^{m-1}-1-i} \]  \hspace{1cm} (13)

Consider the case of \(m' = m\). Since \(i_1 = 2^h i_1 \pmod{2^{m-1}}\), \(S_{i_1} = S_{2^h i_1}\). From

(8), (9), (10) and (13),

\[ \beta'_2 = \beta_1 b^{2^{m-1}-1-i_1} + \beta_1 b^{2^{m-1}-1-i_1} + \beta_2 = \beta_1 b^{2^{m-h-1}} + \]
\[ + \beta_1 b^{2^{h}h-1} + \beta_2. \]  \hspace{1cm} (14)

For the case of \(m' = m/2\), it follows from (8), (9), (10) and (13) that

\[ \beta'_2 = \beta_1 b^{2^{h-1}} + \beta_2. \]  \hspace{1cm} (15)

Hereafter we shall consider the case of \(m' = m\) except for section 5.

For each \(i (0 < i < v)\), \(V_i = \{ \alpha^i b^{2^{m-h-1}} + \alpha^{i2} b^{2^h h-1} \mid b \in GF(2^m) \} \) forms a subspace of \(GF(2^m)\). Let

\[ F_i(X) = \alpha^i X^{2^{m-h-1}} + \alpha^{i2} X^{2^h h-1} \]
\[ = \alpha^i X^{2^h h-1} (X^{2^h h-1} (X^{2^{m-2h-1}} + \alpha^{i(2^h-1)}). \]

If \(i = 0\), the order of a nonzero root in \(GF(2^m)\) of \(F_0(X)\) is a factor of \(2^{m-2h} - 1\). Since \(c = (m,2h) = (m-2h), 2^c - 1 = (2^{m-1},2^{m-2h-1})\). This implies
that the roots in GF\(^{(2^m)}\) of \(F_0(X)\) are in subfield GF\((2^c)\). Conversely, any element in this subfield is a root of \(F_0(X)\). Hence, the dimension of \(V_0\) is \(m-c\). Let \(V_{00}, V_{01}, V_{02}, \ldots, V_{02^{c-1}}\) be the cosets of GF\((2^m)\) with respect to \(V_0\). Each coset has \(2^{m-c}\) elements.

For \(i \neq 0\), assume that \(\alpha^i\) is a root of \(F_1(X)\). Then,
\[
2^h \cdot (2^{m-2h}-1)^j = i(2^{h-1}) \pmod{2^{m-1}}
\]
\[
(1-2^{2h})^j = i2^h(2^{h-1}) \pmod{2^{m-1}}
\]
\[
(2^{h+1})^j = i2^{h+1} \pmod{2^{m-1}}
\]
Since \(v\) divides both \(2^{h+1}\) and \(2^{m-1}\), \(v\) must divide \(i\). However, \(0 < i < v\).

Therefore, there is no root in GF\((2^m)\) of \(F_1(X)\) except for zero. Consequently,
\(v_1 = GF(2^m)\).

Let \(B_{0j} = \{ (\alpha^l, \beta) | 0 \leq l < 2^{m-1}, \beta \in V_{0j} \} \) \((0 \leq j \leq 2^{c-1})\) and
\(B_i = \{ (\alpha^l, \beta) | 0 \leq l < 2^m-1, \beta \in GF(2^m) \} \) \((0 < i < v)\). Then,
\[
|B_{0j}| = (2^{m-1})2^{m-c} / v \quad (0 \leq j < 2^c),
\]
\[
|B_i| = (2^{m-1})2^m / v \quad (0 < i < v)^*.
\]

It follows from the definition of \(B_{0j}\) or \(B_i\) that for any \((B_1, B_2)\) and \((C_1, B_2)\) in the same \(B_{0j}\) or \(B_i\) and for any \(\beta \in GF(2)\), there exists permutation \(\pi_{ab}\) such that \(\pi_{ab}(C_1, B_2) = \nu((B_1, B_2), B_1)\) and \(B' \in GF(2)\). Therefore, \(\nu(C_1, B_2)\) and \(\nu(B_1, B_2)\) have the same weight \(w\). If \(\beta_0\) (or \(\beta_0'\)) is zero,
then \( v(0, B_1, B_2; x) \) (or \( v(0, B'_1, B'_2; x) \)) has weight \( w \). If \( B_0 \) (or \( B'_0 \)) is one, then \( v(1, B_1, B_2; x) \) (or \( v(1, B'_1, B'_2; x) \)) has weight \( w-1 \) by definition. Since \( C' \) contains all one vector \( e = (1,1,\ldots,1) \) and 
\[
\alpha^i = \sum_{f=0}^{m-2} \alpha^i f \quad \text{if} \quad (\alpha^i - 1) = 0 \quad (0 < i < 2^{m-1}),
\]
\[
v(1, B_1, B_2; x) = v(0, B_1, B_2; x) + e(x).
\]
Hence, if \( B_0 \) (or \( B'_0 \)) is one, then \( v(0, B_1, B_2; x) \) (or \( v(0, B'_1, B'_2; x) \)) has weight \( 2^m - w \). Therefore, we have Lemma 8.

**Lemma 8:** For each \( j \) (or \( i \)) \((0 < j < 2^c, 0 < i < v)\), there is \( w_{0j} \) (or \( w_i \)) such that for any \((B_1, B_2) \in B_0j \) (or \( B_i \)) the weight of \( v(0, B_1, B_2; x) \) is either \( w_{0j} \) (or \( w_i \)) or \( 2^m - w_{0j} \) (or \( 2^m - w_i \)).

3. **Case I:** \((m,h) = (m,2h)\)

Hereafter \( a_w \) will denote the number of code vectors of weight \( w \) in \( C \) and \( b_w \) will denote the number of code vectors of weight \( w \) in \( C_0 \).

**Lemma 9:** For \( r \) an \( w \),
\[
\begin{align*}
wa_w &= (2^m - w) a_{2^m - w}, \\
wb_w &= (2^m - w) b_{2^m - w}. 
\end{align*}
\]
This lemma follows from a theorem due to Peterson [1] and Lemma 1. Consequently, if the values of \( w_{0j} \)'s \((0 < j < 2^c)\) and \( w_i \)'s \((0 < i < v)\) are known, the weight distribution of \( C-C_2 \) is completely determined. Furthermore, any nonzero vector of \( C_2 \) has weight \( 2^{m-1} \), because \( C_2 \) is a maximum length sequence code.

**Lemma 10:** \( b_1 = b_2 = 0, \quad b_3 = (2^{c'-1} - 1)(2^{m-1})/3 \).
Proof: Since $C_0$ is a subcode of Hamming code,

$$b_1 = b_2 = 0.$$  

Assume that $a_1$, $a_2$ and $a_3$ are the location numbers of a code vector of weight 3 in $C_0$. Then,

$$a_1 + a_2 = a_3$$  \hspace{1cm} (18)  

$$a_1(2^h + 1) + a_2(2^h + 1) = a_3(2^h + 1)$$  \hspace{1cm} (19)  

From (18),

$$a_3(2^h + 1) = (a_1 + a_2)(2^h + 1) = (a_1 + a_2)(a_1 + a_2)$$

$$= a_1(2^h + 1) + a_2(2^h + 1)$$

By combining with (19),

$$a_1(2^h + 1) + a_2(2^h + 1) = 0,$$

$$a = (a_1 - a_2)(2^h - 1) = 1.$$  \hspace{1cm} (20)  

Thus,

$$(a_1 - a_2)(2^h - 1) = 0 \pmod{2^m - 1}.$$

If $c' = (m, h) = 1$, then $(2^h - 1, 2^m - 1) = 1$. Therefore

$$a_1 = a_2.$$

This is a contradiction, which leads to the conclusion that $b_3 = 0$. If $c' \not= 1$, then $(2^m - 1, 2^h - 1) = 2^{c' - 1}$. Let

$$\mu = (2^m - 1)/(2^{c' - 1}).$$  \hspace{1cm} (21)
Then,
\[ j_1 \equiv j_2 \pmod{\mu} \]
Let \( j_1 = \ell_1 \mu + i \) and \( j_2 = \ell_2 \mu + i \) \((0 \leq i < \mu)\). Since \( \alpha^1 + \alpha^2 = \alpha^3 \) for some \( \ell_3 \), it follows from (18) that \( j_3 = \ell_3 \mu + i \). Conversely, for any \( i \) \((0 \leq i < \mu)\) and for \( \ell_1, \ell_2, \) and \( \ell_3 \) such that
\[
\begin{align*}
\ell_1 \mu & + \ell_2 \mu + \ell_3 \mu \\
\alpha & + \alpha^2 = \alpha \\
0 & \leq \ell_1, \ell_2, \ell_3 < 2^{c'-1}
\end{align*}
\]
(22)
(23)
\( \ell_1 \mu + \ell_2 \mu + \ell_3 \mu \), \( \alpha^1 \), \( \alpha^2 \), and \( \alpha^3 \) satisfy (18) and (19). The number of unordered triplets \((\ell_1, \ell_2, \ell_3)'s\) satisfying (22) and (23) is equal to \( \left( \begin{array}{c} 2^{c'-1} \\ 2 \end{array} \right)/3 \). Consequently,
\[
b_3 = \mu \left( \begin{array}{c} 2^{c'-1} \\ 2 \end{array} \right)/3 = (2^m-1)(2^{c'-1}-1)/3. \]
Q.E.D.

**Lemma 11**: Let \( I_2 \) and \( I_4 \) denote \( \sum_{j \neq 0} (j-2m-1)^2 a_j \) and \( \sum_{j \neq 0} (j-2m-1)^4 a_j \) respectively. Then,
\[
I_2 = 2^{2m-2}(2^m-1), \quad I_4 = 2^{3m+c'-4}(2^m-1). \]

**Proof**: Note that \( k = 2m \). By using the power moment identities of Lemma 6,
\[
I_2 = \sum_{j \neq 0} j^2 a_j - 2^m \sum_{j \neq 0} j a_j + 2^{2m-2} \sum_{j \neq 0} a_j
= 2^{2m-2}(2^m-1) - 2^{2m-2}(2^m-1)
= (2^m-1)(2^{3m-2}-2^{3m-1}+2^{3m-2}+2^{2m-2})
= (2^m-1)2^{2m-2}
\]
\[ I_4 = \sum_j^4 a_j - 2^{m+1} \sum_j^3 a_j + 3 \cdot 2^{2m-1} \sum_j^2 a_j - 2^{3m-1} \sum_j a_j \]
\[ + 2^{4m-4} \sum_{j \neq 0} a_j \]
\[ = 2^{2m-4} \left( \frac{4}{n+6n^3 + 3n^2 - 2n} - 2^{3m-2} \frac{3}{n+3n^2} \right) \]
\[ + 3 \cdot 2^{4m-3} n(n+1) - 2^{5m-2} n + 2^{4m-4} (2^{2m-1}) \]
\[ + 3 \left( 2^{3m-1} - 2^{2m-1} \right) b_3 + 3 \cdot 2^{2m-2} b_4 \]
\[ = n \left[ 2^{2m-4} \left( (n+1)^3 + 3(n+1)(n-1) \right) - 2^{3m-2} \left( (n+1)^2 + n-1 \right) \right] + 3 \cdot 2^{4m-3} (n+1) - 2^{5m-2} + 2^{4m-4} (2^{m+1}) \]
\[ + 3 \cdot 2^{2m-1} (b_3 + b_4) \]
\[ = n \left[ 2^{5m-4} - 2^{5m-2} + 3 \cdot 2^{5m-3} - 2^{5m-2} + 2^{5m-4} \right] \]
\[ + 3 \cdot 2^{3m-4} (2^{m-2}) - 2^{3m-2} (2^{m-2}) + 2^{4m-4} \}
\[ + 3 \cdot 2^{2m-1} (b_3 + b_4) \]
\[ = (2^{m-1}) 2^{3m-3} + 3 \cdot 2^{2m-1} (b_3 + b_4) \]
\[ \] (24)

Since all one vector \((1,1,\ldots,1)\) is in \(C_0\),

\[ b_{2^{m-4}} = b_3. \]

By Lemmas 9 and 10,

\[ b_3 + b_4 = b_{2^{m-4}} + b_4 = 2^{m-2} b_3 + 2^{m-4} = 2^{m-2} b_3 \]
\[ = 2^{m-2} (2^{c+1} - 1) (2^{m-1}) / 3. \]
\[ \] (25)
By substituting the right hand side of (25) into (24),

\[ I_4 = (2^{m-1})2^{3m+c'-4}. \]

Q.E.D.

Let \( j_M \) be the smallest nonzero integer such that

\[ a_j + a_{2^{m-j}j_M} \neq 0. \]

By the definition of \( I_2 \) and \( I_4 \),

\[ (j_M - 2^{m-1})^2 \geq I_4/I_2 = 2^{m+c'-2}. \]  

(26)

Consider the case where \( c = c' \). Then, \( v = 1 \) by Lemma 5. Since all nonzero vectors in \( C_2 \) are of weight \( 2^{m-1} \), it follows from Lemma 8 and (16) that \( a_j + a_{2^{m-j}} (j \neq 0, 2^{m-1}) \) must be divisible by \( 2^{m-c} (2^m - 1) = 2^{m-c} (2^m - 1) \).

Therefore, from (26)

\[ I_2 \geq (j_M - 2^{m-1})^2 (a_j + a_{2^{m-j}j_M}) \geq 2^{2m-2} (2^{m-1}) \]  

(27)

By Lemma 11 and (27),

\[ I_2 = (j_M - 2^{m-1})^2 (a_j + a_{2^{m-j}j_M}) = 2^{2m-2} (2^{m-1}). \]

Consequently,

\[ (j_M - 2^{m-1})^2 = 2^{m+c-2} = 2^{m+c-2} \]  

(28)

\[ a_j + a_{2^{m-j}j_M} = 2^{m-c} (2^{m-1}) \]  

(29)

\[ a_j = 0 \ (j \neq 0, j_M, 2^{m-1}, 2^{m-j}j_M). \]

Hence,
\[ j_M = 2^{m-1} - 2^{(m+c)/2-1} \]  
\[ a_{m-1} = 2^{m-1} - \left( a_j + a_{m-j} \right) \]
\[ = (2^m - 2^{m-c+1})(2^{m-1}) \]

By Lemma 9, (29) and (30),
\[ a_{j_M} = (2^{m-c-1} + 2^{(m-c)/2-1})(2^m - 1) \]
\[ a_{m-j_M} = (2^{m-c-1} - 2^{(m-c)/2-1})(2^m - 1) \]

Thus, we have the following theorem.

**Theorem 1:** If \((m,h) = (m,2h) = c\), then
\[ a_0 = 1 \]
\[ a_{m-1} = 2^{m-1} - 2^{(m+c)/2-1} = (2^{m-c-1} + 2^{(m-c)/2-1})(2^m - 1) \]
\[ a_{m-j} = (2^m - 2^{m-c+1})(2^m - 1) \]
\[ a_{m-1} + 2^{(m+c)/2-1} = (2^{m-c-1} - 2^{(m-c)/2-1})(2^m - 1) \]
\[ a_j = 0 \] for other \( j \).

**Case II:** \(2(m,h) = (m,2h) + m\)

Consider the case in which \(2(m,h) = (m,2h)\). Then, \(v = 2^{c+1}\) by Lemma 5. Since \(v(0,\beta,0,x)\) is in \(C_1\), \(w_{00} = w_0, w_1, \ldots, w_{v-1}\) can be found from the weight distribution of \(C_1\). Each code vector of \(C_1\) is a concatenation of a code vector in cyclic code \(C_1^*\) of length \((2^m-1)/v\) which is generated by \((x^{(2^m-1)/v-1})/h_1(x)\). Let \(v'(\beta;x)\) denote a code vector \(v'(x)\).
in \( C_1 \) such that \( v'(a^{i}) = b \). With the same argument as the one of section 3, set \( C'_{1i} = \{ v(a^{i} + b^j; x) \mid 0 \leq j < (2^m - 1)/\nu \} \) (0 \leq i < \nu) consists of \((2^m - 1)/\nu\) vectors of the same weight \( w'_i \). Since \( v(0, b, 0; x) = (v'(b; x), \ldots, v'(b; x)) \), \( w'_i \) can be given by the following equation:

\[
    w'_i = \nu w_i. \quad (0 \leq i < \nu)
\]

Therefore, by applying Lemma 6 to code \( C_1 \), we have

\[
    (2^m - 1)/\nu \sum_{i=0}^{\nu-1} w_i/\nu = 2^m - 1 (2^m - 1)/\nu ,
\]

\[
    (2^m - 1)/\nu \sum_{i=0}^{\nu-1} (w_i/\nu)^2 = 2^m - 2 (2^m - 1) (2^m - 1 + \nu)/\nu^2 .
\]

Thus,

\[
    \sum_{i=0}^{\nu-1} w_i = 2^{m-1} (31)
\]

\[
    \sum_{i=0}^{\nu-1} w_i^2 = 2^{m-2} (2^m - 1 + \nu) = 2^{m-2} (2^m + 2 c') (32)
\]

Therefore,

\[
    \sum_{i=0}^{\nu-1} (w_i - 2^m - 1)^2 = 2^{m-2} (2^m - 1 + \nu) - 2^m w_i^2 + 2^{m-2} \nu
\]

\[
    = 2^{m-2} (\nu - 1) = 2^{m+c'} - 2 (33)
\]

On the other hand, it follows from Lemma 8, (16), (17) and the definition of \( I_2 \) that

\[
    I_2 = I_{20} + I_{21},
\]

\[
    I_{20} = 2\nu c' (2^m - 1) \sum_{j=1}^{\nu} (w_0 j - 2^m - 1)^2/\nu ,
\]

\[
    I_{21} = 2\nu c' (2^m - 1) (w_0 - 2^m - 1)^2/\nu + 2^m (2^m - 1) \sum_{i=1}^{\nu-1} (w_i - 2^m - 1)^2/\nu .
\]
By Lemma 11 and (33),
\[
I_2 = 2^{2m-2}(2^m-1)
\geq I_{21} = 2^{2m+c'-2}(2^m-1) - (2^m-1)(2^{m-2m-c})(w_0 - 2^m-1)^2/v.
\] (35)

By a simple calculation,
\[
(w_0 - 2^{m-1})^2 \geq 2^{2m-2}(2^c-1)v/(2^{m-2m-c})
\]
\[
= 2^{m+c-2} \quad \text{(by (6)).}
\]

Hence,
\[
w_0 = 2^{m-1} \pm (2^{m+c}/2-1 + \delta), \quad \delta \geq 0
\] (36)

Now, by (31) and (32)
\[
I_2 = \sum_{i=0}^{v-1} (w_i - (2^{m-1} + 2^{m/2-1}))^2
\]
\[
= v2^{m-2}(2^{m-1+v}) - 2(2^{m-1/2}2^{m/2-1})v2^{m-1} + (2^{m-1}2^{m/2-1}v)^2
\]
\[
= v[2^{2m-2}2^m+c'-2 - 2^{m-1}]^2 + 2^{m/2-1} + 2^{2m-2} + 2^{m/2-1}]
\]
\[
= 2^{m-2}(2^c+1)^2
\] (37)

On the other hand,
\[
I_2 \geq (w_0 - (2^{m-1} + 2^{m/2-1}))^2 = [2^{m-1}2^{m+c}/2-1 + \delta - 2^{m-1} + 2^{m/2-1}]^2
\]
\[
= 2^{m-2}(2^c+1+62^{1-m/2})^2
\] (38)

From (35), (36), and (37), we have that
\[
\delta = 0
\]
\[
w_0 = 2^{m-1} \pm 2^{(m+c)/2-1}
\] (39)
\[
w_i = 2^{m-1} \pm 2^{m/2-1} \quad (0 < i < v)
\] (40)
Since \( w_i (0 \leq i < \nu) \) is divisible by \( \nu \), the \( \pm \) sign is determined by Lemma 4.

Thus, we have:

**Theorem 2:** Let \( a_j \) denote the number of code vectors of weight \( j \) in \( C_1^i \).

If \( m/c \) is odd (or even), then

\[
\begin{align*}
a'_0 &= 1 \\
a_{2^{m-1}-2}^{m-1} &+ 2^{m-1} (m+c)/2-1 (\text{or } a_{2^{m-1}+2}^{m-1} (m+c)/2-1) = (2^{m-1})/(2^{c/2}+1) \\
a_{2^{m-1}+2}^{m-1} &+ 2^{m/2-1} (\text{or } a_{2^{m-1}-2}^{m-1} + 2^{m/2-1}) = 2^{c/2}(2^{m-1})/(2^{c/2}+1) \\
a_j &= 0 \text{ for other } j.
\end{align*}
\]

From (35) and (39) it follows that

\[
I_{21} = 2^{2m+c-2}(2^{m-1}) - (2^{m-1})(2^{m-2m-c}) 2^{m+c-2}/\nu = 2^{2m-2}(2^{m-1})(2^c - (2^{c-1})/\nu) = 2^{2m-2}(2^{m-1}) = I_2 \quad \text{(by (35)).}
\]

By (34),

\[
I_{20} = (2^{m-1}) 2^{m-c}/\nu \sum_{j=1}^{2^c-1} (\omega_{0j} - 2^{m-1})^2 = 0
\]

Hence,

\[
\omega_{0j} = 2^{m-1} \quad (1 \leq j < 2^c) \quad (41)
\]

By (16), (17), Lemma 8, (39), (40) and (41), we have:

\[
\begin{align*}
a_{2^{m-1}-2}^{m-1} &+ a_{2^{m-1}+2}^{m-1} = (2^{m-1}) 2^{m+c}/2/(2^{c/2}+1) \\
a_{2^{m-1}} &= (2^{m-1}) 2^{m-c}(2^{c-1})/(2^{c/2}+1) + 2^{m-1}
\end{align*}
\]
Thus, the next theorem follows from Lemma 9.

**Theorem 3**: If $2(m,h) = (m,2h) = c$ and $c \not\equiv m$, then

\[
\begin{align*}
&2^{m-1} - 2^{(m+c)/2} = 2^{m-1} + 2^{(m+c)/2} - 1 = (2^{m-1} + 2^{m-c}/(2^{c/2} + 1))
\end{align*}
\]

Consider the case of $m = 2h$. For any $\beta_1 \not\equiv 0$, $\beta_2$ in $GF(2^m)$, there exists $b \in GF(2^m)$ such that

\[
\beta_1 b^{2^{m-1}} + \beta_2 = 0,
\]

because $(2^{h-1}, 2^{m-1}) = 1$. From (15) and a similar argument to the one for the case of $m = m'$, it follows that there exists $w$ such that the weight of any code vector in $C - C_2$ is either $w$ or $2^m - w$. Since $C_1^\perp$, the cyclic code of length $2^{m/2} - 1$ generated by $(X^{2^{m/2} - 1})/g(X)$, is a maximum length sequence code, $C_1$ consists of one zero vector and $2^{m/2} - 1$ vectors of weight $2^{m/2} - 1$ $(2^{m/2} + 1)$. Therefore,
\[ w = (2^{m/2} + 1)2^{m/2 - 1}. \]

On the other hand, \( C_2 \) is a maximum length sequence code of length \( 2^m - 1 \).

Hence,

\[ a_{2^m - 1} = 2^m - 1. \]

According to Lemma 9, we have:

**Theorem 4:** If \( m = 2h \), then

\[ a_0 = 1 \]

\[ a_{2^m - 1 - 2^m/2 - 1} = (2^{m/2} - 1)(2^{m-1} + 2^{m/2 - 1}) \]

\[ a_{2^m - 1} = 2^h - 1 \]

\[ a_{2^m - 1 + 2^m/2 - 1} = (2^{m/2} - 1)(2^{m-1} - 2^{m/2 - 1}) \]

\[ a_j = 0 \quad \text{for other } j. \]

6. Crosscorrelation Functions of Two Maximum Length Sequences

It follows from Lemma 5 that \( a_2^{2h+1} \) is a primitive element if and only if \( c = c' \). Assume that \( c = c' \). Let

\[ v(0,1,0;x) = \sum_{f=0}^{2^{m-2}} v_1 f^x f \]

\[ v(0,0,1;x) = \sum_{f=0}^{2^{m-2}} v_2 f^x f. \]

Then, \( v_1 = v_{10}, v_{11}, \ldots, v_{12^{m-2}} \) and \( v_2 = v_{20}, v_{21}, \ldots, v_{22^{m-2}} \) are maximum length sequences of length \( 2^m - 1 \). If \( v_1 \) and \( v_2 \), replace 0 by -1. Let

\[ u_1 = u_{10}, u_{11}, \ldots, u_{12^{m-2}} \] and \( u_2 = u_{20}, u_{21}, \ldots, u_{22^{m-2}} \) be the resulting
sequences of real numbers 1 and -1. Correlation function \( \Theta(j) \) of \( u_1 \) and \( u_2 \) is defined by

\[
\Theta(j) = \sum_{f=0}^{2^m-2} u_1^f u_2^{j-f},
\]

where suffix \( f - j \) is to be taken mod \( 2^m-1 \). Note that

\[
v(0,1,0;x) + x^j v(0,0,1;x) = v(0,1,\alpha^j 2;x).
\]

If \( v(0,1,\alpha^j 2;x) \) has weight \( w \), then

\[
\Theta(j) = 2^{m-1-2w}.
\]

Let \( s_i \) denote the number of \( j \)'s (0 \( < \) \( j < 2^m-1 \)) with \( \Theta(j) = i \). Then, \( s_i \) is the number of vectors \( v(0,1,\beta;x) \) with weight \( (2^m-1-i)/2 \). From sections 2 and 3, we have theorem 5.

**Theorem 5:**

\[
s_{(m+c)/2-1} = 2^{m-c-1} 2^{(m-c)/2-1},
\]

\[
s_{-1} = 2^m 2^{-m-c},
\]

\[
s_{2(m+c)/2-1} = 2^{m-c-1} + 2^{(m-c)/2-1},
\]

\[
s_i = 0 \quad \text{for other } i.
\]

For \( 0 \leq j < 2^m-1 \), let

\[
\theta_j = 1 \text{ if } \Theta(j) = -2^{(m+c)/2-1} \text{ or } 2^{(m+c)/2-1},
\]

\[
\theta_j = 0 \quad \text{if } \Theta(j) = -1.
\]

Sequence \( \Theta = \Theta_0, \Theta_1, \ldots, \Theta_{2^m-2} \) will be called the correlation sequence of \( u_1 \) and \( u_2 \). We shall characterize the correlation sequence below. Recall that
\[ V_0 = V_{00} = \{ b^{2^{m-h-1}} + b^{2^h} \mid b \in GF(2^m) \} \]

Since \((2^{h-1}, 2^{m-1}) = 1,\)
\[ V_{00} = \{ b^{2^{m-2h}} + b \mid b \in GF(2^m) \} \]

Since \((m-2h, m) = c,\) the Galois group of \(GF(2^m)\) over \(GF(2^c)\) is generated by the automorphism \(X \rightarrow X^{2^{m-2h}}\) (by Theorem 9, p. 127 of [6]). Therefore, from the trace theorem (p. 121 of [6]) it follows that
\[ V_{00} = \{ b | \sigma(b) = 0, b \in GF(2^m) \}, \]
where \(\sigma(b)\) denotes the trace of \(b\) in \(GF(2^m)\) over \(GF(2^c)\), and
\[ \sigma(b) = b + b^{2^c} + b^{2^{2c}} + \ldots + b^{2^{m-c}}. \]

Hence, any element of each coset \(V_{0j}\) has the same trace \(t_j \in GF(2^c)\), and if \(j \neq j', t_j = t_{j'}\).

Note that \(v_2(0, \beta_1, \beta_2; x) = v(0, \beta_1, \beta_2; x^2) = v(0, \beta_1^2, \beta_2^2; x) \in C\) and that \(v(0, \beta_1, \beta_2; x)\) and \(v(0, \beta_1, \beta_2; x^2)\) have the same weight. Consequently, if \(t_j = t_{j'}^2\), then \(w_{0j'} = w_{0j}\). From the proof of Theorem 1 it follows that there is only one \(j_0\) such that
\[ w_{0j_0} = 2^{m-1} - 2^{(m+c)/2-1} \]
\[ w_{0j} = 2^{m-1}, j \neq j_0. \]

Since \(t_{j_0} = t_{j_0}^2, t_{j_0} = 0\) or 1. Since \(C_1\) is a maximum length sequence code, \(w_{00}\) must be \(2^{m-1}\). Therefore, \(t_{j_0} = 1\). This implies that the weight of \(v(0, 1, \beta; x)\) is not equal to \(2^{m-1}\) if and only if \(\beta + \beta^{2^c} + \beta^{2^{2c}} + \ldots + \beta^{2^{m-c}} = 1\). From (42), \(\theta(j) \parallel -1,\) if and only if \(a + a^{2^c} + a^{2^{2c}} + \ldots + a^{2^{m-c}} = 1\). Since \(a^{2^c} = a^{-1}\) and \(a^{2^{m-1}} = a^{-1}\), we have Theorem 6.
Theorem 6: \( \theta_j = 1 \) if and only if \( \alpha^{-j} + \alpha^{-j2^c} + \alpha^{-j2^2c} + \ldots + \alpha^{-j2^m c} = 1. \)

Now consider the case of \( c = 1. \) By definition, \( v(0,0,1;\alpha^1) = 1. \)

Therefore,
\[
v(0,0,1;\alpha^{-2^l}) = 1 \quad (0 \leq l < m).
\]

On the other hand, for any \( \alpha^{-j} \neq \alpha^{-2^l} \) \((0 \leq l < m),\)
\[
v(0,0,1;\alpha^{-j}) = 0.
\]

By the formula due to Reed and Solomon [7],
\[
v_{2f} = \sum_{j=0}^{2^m-2} v(0,0,1;\alpha^{j}) \alpha^{-jf} = \alpha^f + \alpha^{2f} + \alpha^{2^2f} + \ldots + \alpha^{2^{m-1}f}.
\]

Hence, by Theorem 6
\[
\theta_j = \frac{v}{2^{2m-1-j}}.
\]

This implies the following corollary.

**Corollary 7:** If \( (m,h) = (m,2h) = 1, \) then the correlation sequence of the maximum length sequence generated by \( h_1(X) \) and the one generated by \( h_2(X) \) is the maximum length sequence generated by \( g_2(X) = X^{m} h_2(X^{-1}). \)

R. Gold and E. Kopitzka [8] observed that for some pairs of maximum length sequences the correlation sequences are also maximum length sequences and they listed all such pairs of sequences of length 8191 or less. Among 28 listed pairs, 25 cases are covered by Corollary 7.
Acknowledgment

The author is grateful to Professors W. W. Peterson, R. T. Chien and J. S. Lin for many valuable suggestions and to Professors M. E. Van Valkenburg and H. Ozaki for their support.

References


Let $h_1(X)$ and $h_2(X)$ be different irreducible polynomials such that
$h_1(\alpha^{2^h-1}) = 0$ for some $0 < h < m$ and $h_2(\alpha^{2^h-1}) = 0$, $\alpha$ being a primitive element of $GF(2^m)$. This paper presents the weight distribution formula of the code of length $2^m-1$ generated by $(X^{2^m-1} - 1)/(h_1(X)h_2(X))$ for any $m$ and $h$. Some applications to the cross-correlation problem between two different maximum length sequences are presented.
<table>
<thead>
<tr>
<th>KEY WORDS</th>
<th>LINK A</th>
<th>LINK B</th>
<th>LINK C</th>
</tr>
</thead>
<tbody>
<tr>
<td>weight distribution</td>
<td>HOLE</td>
<td>WT</td>
<td>HOLE</td>
</tr>
<tr>
<td>cyclic codes</td>
<td>WT</td>
<td>HOLE</td>
<td>WT</td>
</tr>
<tr>
<td>cross-correlation</td>
<td>WT</td>
<td>HOLE</td>
<td>WT</td>
</tr>
<tr>
<td>maximum length sequences</td>
<td>WT</td>
<td>HOLE</td>
<td>WT</td>
</tr>
</tbody>
</table>

**Instructions**

1. A REPORT NUMBER MUST BE ENTERED IN BLOCK 1 IN THE FORMAT XXXX-YYYY, WHERE XXXX IS THE CONTRACT OR ORDER NUMBER AND YYYY IS THE YEAR OF REPORT. IN THE LACK OF A CONTRACT OR ORDER NUMBER, ENTER THE REPORT NUMBER ALONE.

2. A REPORT NUMBER MAY BE ENTERED IN BLOCK 1 IN THE FORMAT YYYY-XXXX, WHERE YYYY IS THE YEAR OF REPORT AND XXXX IS AN ARBITRARY NUMBER. IF THE REPORT IS A Nontechnical Report (e.g., ANNUAL REPORT, ANNUAL FINANCIAL REPORT) AND A CONTRACT OR ORDER NUMBER IS NOT APPLICABLE, ENTER THE REPORT NUMBER ALONE.

3. A REPORT NUMBER MAY BE ENTERED IN BLOCK 1 IN THE FORMAT YYYY-XXXX, WHERE YYYY IS THE YEAR OF REPORT AND XXXX IS AN ARBITRARY NUMBER. IF THE REPORT IS A Nontechnical Report (e.g., ANNUAL REPORT, ANNUAL FINANCIAL REPORT) AND A CONTRACT OR ORDER NUMBER IS NOT APPLICABLE, ENTER THE REPORT NUMBER ALONE.

4. KEY WORDS: Key words are standard terms or short phrases that characterize a report and may be used to index entries for catalogs, thesauri, or other literature indexes. Key words must be selected so that the security classification is required. Identification, such as equipment model or classification of technical content, in special cases or identification of technical content, the recipient of the report, and service by the recipient of the report, may be considered in selecting key words.

5. This form is designed to permit the maximum amount of accurate and complete identification of the document, and hence, security classification.

6. The receipt of this form indicates that the recipient has been advised of the report number(s) either by the recipient of this messsage or by the sender of these messages. The recipient is authorized to use this form in accordance with the requirements of the report number(s) and the classification of the report.