Further Results on Polynomial Codes*

C. L. Chen and S. Lin

Department of Electrical Engineering, University of Hawaii, Honolulu, Hawaii 96822

The class of polynomial codes introduced by Kasami, Lin, and Peterson has considerable inherent algebraic and geometric structure. It contains many well known classes of codes as subclasses, such as BCH codes and geometry codes.

The purpose of this paper is to derive further properties of polynomial codes. It is hoped that these properties may impart more algebraic structure to BCH codes and geometry codes.

Firstly, combinatorial expressions for enumerating the number of information digits of certain subclasses of polynomial codes are derived. Secondly, the exact minimum distance of a subclass of BCH codes is established and a tight BCH bound on the minimum distance of the dual of a polynomial code is obtained. Finally, it is shown that a primitive polynomial code is a subcode of the mth power of an extended primitive BCH code where the mth power of a code is defined as the direct-product of a code with itself m times.

1. INTRODUCTION

The class of polynomial codes introduced by Kasami, Lin, and Peterson [1, 2] has considerable inherent algebraic and geometric structure. It contains many well known classes of codes as subclasses, such as BCH codes, Reed–Solomon codes, generalized Reed–Muller codes, projective geometry codes, and Euclidean geometry codes. The purpose of this paper is to investigate further properties of polynomial codes. It is hoped that these properties would enable us to establish further structure of BCH codes and geometry codes.

In Section 2, a brief review of polynomial codes is given. In Section 3, the problem of enumerating the number of information digits of a polynomial code is considered. In Section 4, the exact minimum distance of a

* This work was supported in part by NSF Grant 3594 and by NASA Grant NGR-12-001-046.
subclass of primitive BCH codes is established by using the fact that a polynomial code is a subcode of the BCH code of the same minimum distance. Also, a tight BCH bound on the minimum distance of the dual of a polynomial code is derived. In the last section, it is shown that a primitive polynomial code is a subcode of the \( m \)th power of an extended primitive BCH code where the \( m \)th power of a code is defined as the direct-product of a code with itself \( m \) times.

2. SUMMARIZED RESULTS ON POLYNOMIAL CODES \([1, 2]\)

Consider the field \( GF(q^m) \) which is the extension field of \( GF(q) \). Let \( \alpha \) be a primitive element of \( GF(q^m) \). Then every nonzero element \( \alpha^l \) in \( GF(q^m) \) can be expressed as

\[
\alpha^l = a_{11} + a_{21} \alpha + \cdots + a_{m1} \alpha^{m-1}
\]

for \( 0 \leq l < q^m - 1 \), where \( a_{11} \) is in \( GF(q) \). We call \( (a_{11}, a_{21}, \cdots, a_{m1}) \) the coordinate vector of \( \alpha^l \).

Let \( b \) be a factor of \( q^s - 1 \), and

\[
z = (q^s - 1)/b,
\]

\[
N = (q^m - 1)/b.
\]

Let \( X_1, X_2, \cdots, X_m \) be \( m \) variables over \( GF(q^s) \) and let

\[
\bar{X} = (X_1, X_2, \cdots, X_m).
\]

Define \( Q_m(\mu, b) \) as a set of the following polynomials of \( m \) variables:

\[
f(\bar{X}) = \sum_{r_i \leq i \leq m} C_{r_1r_2 \cdots r_m} X_1^{r_1} X_2^{r_2} \cdots X_m^{r_m}
\]

such that

1. \( C_{r_1r_2 \cdots r_m} \in GF(q^s) \),
2. \( 0 \leq r_i < q^s \) for \( 1 \leq i \leq m \),
3. \( \sum_{i=1}^m r_i = j b \) with \( 0 \leq j \leq \mu \),
4. \( f(a_{11}, a_{21}, \cdots, a_{m1}) \in GF(q) \) for \( 0 \leq l < N \).

where \( (a_{11}, a_{21}, \cdots, a_{m1}) \) is the coordinate vector of \( \alpha^l \).

For each polynomial \( f(\bar{X}) \) in \( Q_m(\mu, b) \), a vector \( v(f) \) is defined as follows:

\[
v(f) = (v_0, v_1, v_2, \cdots, v_{N-1})
\]
with \( l \)th component

\[
v_l = f(a_{1l}, a_{2l}, \ldots, a_{ml}) \in GF(q)
\]

for \( 0 \leq l < N \).

**Definition.** [Kasami–Lin–Peterson]: A \( q \)-ary polynomial code of length \( N \) is defined as the following set of vectors:

\[
c_m(\mu, b) = \{ v(f) | f(\bar{X}) \in Q_m(\mu, b) \}
\]

Let \( h \) be a non-negative integer less than \( q^{m_2} \). Express \( h \) in radix-\( q^s \) form as follows:

\[
h = \delta_0 + \delta_1 q^s + \delta_2 q^{2s} + \cdots + \delta_{m-1} q^{(m-1)s}
\]

where \( 0 \leq \delta_i < q^s \) for \( 0 \leq i < m \). The \( q^s \)-weight of \( h \) is defined as

\[
W_{q^s}(h) = \sum_{i=0}^{m-1} \delta_i
\]

Let \( h' \) be a nonnegative integer less than \( q^{m_2} - 1 \) such that

\[
h' = hq^t (\mod q^{m_2} - 1)
\]

where \( t \) is any nonnegative integer. Then the \( q^s \)-weight of \( hq^t \) is defined as

\[
W_{q^s}(hq^t) = W_{q^s}(h').
\]

**Theorem 1 [Kasami–Lin–Peterson].** The \( q \)-ary polynomial code \( c_m(\mu, b) \) defined by Eq. (5) is a cyclic code of length \( N \) whose generator polynomial has \( \alpha^h \) as a root if and only if

\[
\min_{0 \leq i < s} W_{q^s}(hq^t) = jb
\]

with \( 0 < j < mz - \mu \). The minimum distance of \( c_m(\mu, b) \) is at least

\[
[(R + 1)q^{\sigma_2} - 1]/b
\]

where \( Q \) and \( R \) are quotient and remainder resulting from dividing \( m(q^s - 1) - \mu b \) by \( q^s - 1 \).

It has been shown that a polynomial code \( c_m(\mu, b) \) is either a BCH code or a subcode of the BCH code of length \( N \) and designed distance \([(R + 1)q^{\sigma_2} - 1]/b \).

**Theorem 2 [Kasami–Lin–Peterson]:** The \( q \)-ary dual code of a polynomial code \( c_m(\mu, b) \) has \( \alpha^h \) as a root in its generator polynomial if and only
FURTHER RESULTS ON POLYNOMIAL CODES

41

$U_{\max} W_{q^8}(h_{q^t}) = jb$

with $0 \leq j \leq \mu$.

A BCH lower bound on the minimum distance of the dual of a polynomial code will be derived in Section 4.

3. ON THE ENUMERATION OF INFORMATION DIGITS OF A POLYNOMIAL CODE

It follows from Theorems 1 and 2 that the number of information digits of a polynomial code $C_m(\mu, b)$ is equal to

$$k_m(\mu, b) = \left(\begin{array}{c}
q^m - 1 \\
\text{the number of nonnegative integers } h \text{ less than } q^m - 1 \\
\text{which are divisible by } b \text{ and such that } \\
\max_{0 \leq t < s} W_{q^t}(h_{q^t}) = jb \text{ with } 0 \leq j \leq \mu.
\end{array}\right)$$

A general mathematical formula for enumerating $k_m(\mu, b)$ of any polynomial code has not yet been obtained. For certain subclasses of polynomial codes, combinatorial expressions for $k_m(\mu, b)$ are obtained.

For $m = 1$, a $q$-ary polynomial code $C_1(\mu, b)$ becomes a $q$-ary BCH code of length $N = (q^s - 1)/b$ and designed distance $N - \mu [1, 2, 3]$. The problem of enumerating $k_1(\mu, b)$ has been solved by Mann [4] and Berlekamp [5].

For $b = q^s - 1$, a $q$-ary polynomial code $C_m(\mu, q^s - 1)$ is the null space of a $q$-ary projective geometry code [2, 6, 7]. A general expression for $k_m(\mu, q^s - 1)$ has not yet been found. If $\mu = 1$ and $q$ is a prime, it has been proved that the polynomial code $C_m(1, q^s - 1)$ of length $(q^m - 1)/q^s - 1$ has

$$k_m(1, q^s - 1) = \left(\left(\frac{m + q - 2}{q - 1}\right)^s\right) + 1$$

information digits [5, 7–9].

For $b = 1$ and $\mu = D(q^s - 1)$ with $D < m$, a $q$-ary polynomial code $C_m(D(q^s - 1), 1)$ is the null space of a $q$-ary $(D, s)$th-order Euclidean geometry code [1, 12]. Again, no general expression for $k_m(D(q^s - 1), 1)$ has been found. Some special cases may be found in Ref. [5].

In the following, we shall derive combinatorial expressions for $k_m(\mu, b)$ of two subclasses of polynomial codes.

For $b = 1$ and $s = 1$, a polynomial code $C_m(\mu, 1)$ becomes a $\mu$th order
A recursion formula for enumerating the information digits $k_m(\mu, 1)$ is given in Ref. [10]. A simple combinatorial expression can be obtained by considering this as a problem of distributing $l$ like objects into $m$ different cells with the restriction that no cell may contain more than $q - 1$ objects. Consider a nonnegative integer $h$ which is less than $q^m$. Write $h$ in radix-$q$ form

$$h = \delta_0 + \delta_1 q + \cdots + \delta_{m-1} q^{m-1} \quad (17)$$

where $0 \leq \delta_i \leq q - 1$. The $q$-weight of $h$ is

$$W_q(h) = \sum_{i=0}^{m-1} \delta_i \quad (18)$$

The correspondence

$$h \leftrightarrow (\delta_0, \delta_1, \cdots, \delta_{m-1})$$

is one-to-one. Therefore, to find the total number of integers $h$ less than $q^m$ of weight $l$ is equivalent to enumerating the total number of ways of putting $l$ like objects into $m$ different cells such that each cell may contain no more than $q - 1$ objects. This number is equal to [11]

$$N_i(m, q - 1) = \sum_{t=0}^{m} (-1)^t \binom{m}{l} \binom{l - tq + m - 1}{l - tq} \quad (19)$$

From Eq. (16) and Eq. (19), the number of information digits of a $\mu$th order GRM code is equal to

$$k_m(\mu, 1) = \sum_{i=0}^{\mu} N_i(m, q - 1)$$

$$= \sum_{i=0}^{\mu} \sum_{t=0}^{m} (-1)^t \binom{m}{l} \binom{l - tq + m - 1}{l - tq} \quad (20)$$

A different expression for $k(\mu, 1)$ was found independently by Smith [9]. For $q = 2$, a $\mu$th order GRM code becomes the well known $\mu$th order
Reed–Muller code of length $2^m - 1$ (in cyclic form) with

$$k_m(\mu, 1) = \sum_{i=0}^{\mu} C_i^m$$

information digits.

Now consider the subclass of polynomial codes with $q = 2$ and $s = 2$. A code in this subclass has length and number of information digits as follows:

$$N = \frac{(2^{2m} - 1)}{b},$$

$$k_m(\mu, b) = \left(\begin{array}{c}
\text{the number of nonnegative integers } h \text{ less than } 2^{2m} - 1 \text{ which are divisible by } b \text{ such that} \\
\max_{0 \leq t < s} W_{2^t}(2^t h) = jb \text{ with } 0 \leq j \leq \mu.
\end{array}\right)$$

where $b$ is either equal to 1 or 3.

Let $S_j$ be the set of nonnegative integers $\{h\}$ less than $2^{2m} - 1$ such that, for each $h$ in $S_j$,

$$\max_{0 \leq t < s} W_{2^t}(2^t h) = jb.$$ (23)

Let $k_j$ be the number of integers in the set $S_j$. By Eq. (22), we then have

$$k_m(\mu, b) = \sum_{j=0}^{\mu} k_j$$ (24)

For any integer $h$ in $S_j$, one and only one of the following statements is true:

1. $W_{2^t}(h) = W_{2^t}(2h) = jb$;
2. $W_{2^t}(h) = jb$ and $W_{2^t}(2h) < jb$; or
3. $W_{2^t}(h) < jb$ and $W_{2^t}(2h) = jb$.

Express $h$ in radix-$2^2$ form as follows:

$$h = \delta_0 + \delta_1 2^2 + \delta_2 (2^2)^2 + \cdots + \delta_{m-1} (2^2)^{m-1}$$ (25)

where $0 \leq \delta_i < 2^2$ for $0 \leq i < m$. The $2^2$-weight of $h$ is

$$W_{2^t}(h) = \delta_0 + \delta_1 + \cdots + \delta_{m-1}.$$ (26)

Express each $\delta_i$ in each radix-2 form,

$$\delta_i = \delta_{i0} + \delta_{i1} 2,$$ (26)
where \( \delta_{il} = 0 \) or 1. Thus, we have

\[
W_{2^1}(h) = \sum_{i=0}^{m-1} (\delta_{i0} + \delta_{i1}2) = \sum_{i=0}^{m-1} \delta_{i0} + 2 \sum_{i=0}^{m-1} \delta_{i1}
\]

(28)

Let

\[
e_0 = \sum_{i=1}^{m-1} \delta_{i0}, \quad e_1 = \sum_{i=0}^{m-1} \delta_{i1}
\]

(29)

where \( 0 \leq e_0 \leq m \) and \( 0 \leq e_1 \leq m \).

Then,

\[
W_{2^1}(h) = 2e_1 + e_0
\]

(30)

It is easy to see that the integer \( 2h \pmod{2^{2m} - 1} \) has \( 2^2 \)-weight

\[
W_{2^2}(2h) = 2e_0 + e_1
\]

(31)

and the integer \( 2^{2h} \pmod{2^{2m} - 1} \) has \( 2^2 \)-weight

\[
W_{2^2}(2^h) = 2e_1 + e_0
\]

(32)

From Eqs. (30), (31), and (32), we have that \( h \) is in \( S_j \) if and only if \( 2h \pmod{2^{2m} - 1} \) is in \( S_j \). Therefore, the number of integers \( h \) in \( S_j \) such that \( W_{2^1}(h) = jb \) and \( W_{2^2}(2h) < jb \) is equal to the number of integers in \( S_j \) such that \( W_{2^1}(h) < jb \) and \( W_{2^2}(2h) = jb \).

Let \( h \) be any integer in \( S_j \) such that its \( 2^2 \)-weight is exactly \( jb \),

\[
W_{2^1}(h) = jb = 2e_1 + e_0
\]

(33)

where \( e_1 \) and \( e_0 \) are defined by Eq. (29). Since

\[
W_{2^1}(h) \geq W_{2^2}(2h)
\]

(34)

then, by Eqs. (31), (33), and (34), we obtain

\[
e_1 \geq e_0, \quad 3e_0 \leq jb \leq 3e_1.
\]
If \( e_1 = e_0 \), then \( W_{2^*}(h) = W_{2^*}(2h) \). From Eq. (35), \( e_1 = e_0 \) if and only if \( jb \) is divisible by 3. It follows from Eq. (28) and Eq. (29) that the number of integers in \( S_j \) such that

\[
W_{2^*}(h) = W_{2^*}(2h) = jb
\]

(or \( e_1 = e_0 \)) is equal to

\[
\begin{cases}
(m) \binom{m}{e_1} \binom{m}{e_0} = \left[ \binom{m}{e_1} \right]^2 = \left[ \binom{m}{e_0} \right]^2 & \text{for } 3 | jb, \\
0 & \text{otherwise}
\end{cases}
\]

It follows from Eqs. (28) and (29) that the number of integers in \( S_j \) such that

\( W_{2^*}(h) = jb \) and \( W_{2^*}(2h) < jb \)

\( (e_1 > e_0) \) is equal to

\[
\binom{m}{e_1} \binom{m}{e_0}.
\]

Let \( \sigma_j \) denote the integer part of \( jb/3 \), i.e.,

\[
\sigma_j = \left\lfloor \frac{jb}{3} \right\rfloor,
\]

and let \( \lambda_j \) denote the integer part of \( jb/2 \), i.e.,

\[
\lambda_j = \left\lfloor \frac{jb}{2} \right\rfloor.
\]

Express \( jb \) as follows:

\[
jb = 2e_{1t} + e_{0t}
\]

with

\[
e_{1t} = \sigma_j + l
\]

\[
e_{0t} = jb - 2(\sigma_j + l)
\]

where \( l \) starts from zero to \( \lambda_j - \sigma_j \) if \( jb/3 \) is an integer; otherwise, \( l \) starts from one to \( \lambda_j - \sigma_j \).

It is easy to see that

\[
e_{1t} \geq e_{0t}
\]
where equality holds if and only if $l = 0$ and $jb$ is divisible by 3. Let us define that

$$
\Delta(jb/3) = \begin{cases} 
1 & \text{for } 3 \mid jb \\
0 & \text{for } 3 \nmid jb 
\end{cases}
$$

(43)

Then the total number of integers in $S_1$ such that

$$W_2^1(h) = W_2^1(2h) = jb$$

is equal to

$$\Delta(jb/3) \binom{m}{\sigma_j}^2 = \Delta(jb/3) \binom{m}{\sigma_j}^2$$

(44)

The total number of integers in $S_1$ such that

$$W_2^1(h) = jb \quad \text{and} \quad W_2^1(2h) < jb$$

is equal to

$$\sum_{i=1}^{\lambda_i - \sigma_i} \binom{m}{\sigma_j}^2 = \sum_{i=1}^{\lambda_i - \sigma_i} \binom{m}{\sigma_j}^2\left(jb - 2(\sigma_j + l)\right)$$

(45)

Thus, we have

$$k_j = \Delta(jb/3) \binom{m}{\sigma_j}^2 + 2 \sum_{i=1}^{\lambda_i - \sigma_i} \binom{m}{\sigma_j}^2\left(jb - 2(\sigma_j + l)\right)$$

(46)

By Eq. (24), we obtain

$$k_m(\mu, b) = \sum_{j=0}^{\mu} \Delta(jb/3) \binom{m}{\sigma_j}^2 + 2 \sum_{j=0}^{\mu} \sum_{i=1}^{\lambda_i - \sigma_i} \binom{m}{\sigma_j + l} \left(jb - 2(\sigma_j + l)\right)$$

(47)

where $\sigma_j = [jb/3]$ and $\lambda_j = [jb/2]$.

For $b = 3$, the dual of $C_m(\mu, 3)$ is a projective geometry code [2, 6, 7] and

$$k_m(\mu, 3) = \sum_{j=0}^{\mu} \binom{m}{j}^2 + 2 \sum_{j=0}^{\mu} \sum_{i=1}^{\lambda_i - \sigma_i} \binom{m}{j + l} \left(j - 2l\right).$$

(48)

is the number of parity check digits of the dual code of $C_m(\mu, 3)$.

For $b = 1$ and $\mu = 3D$, the dual of a binary polynomial code $C_m(\mu, 1)$ is an $(m - D - 1, 2)$th order Euclidean geometry code [2, 12] whose
parity check digits are given by

\[ k_m(\mu, 1) = \sum_{j=0}^{\mu} \Delta(j/3) \left( \frac{m}{\sigma_j} \right)^2 + 2 \sum_{j=0}^{\mu} \sum_{l=1}^{\sigma_j} \left( \frac{m}{\sigma_j + l} \right) \cdot \left( j - 2(\sigma_j + l) \right) \]  

\[ (49) \]

The idea for calculating the information digits of a binary polynomial code may be extended to the case where \( s \) is greater than 2. For any \( s \) in general, we may break \( j \) into \( s \) parts as in Eq. (40). A set of \( s-1 \) inequalities have to be satisfied among these \( s \) parts of integers. Then a combinatorial expression for \( k_j \) can be obtained. Of course, the expression for \( k_j \) would be more complicated than that of the case \( s = 2 \).

4. ON THE MINIMUM DISTANCES OF A POLYNOMIAL CODE AND ITS DUAL CODE

A BCH lower bound on the minimum distance of a polynomial code \( C_m(\mu, b) \) is given by Eq. (12). For certain subclasses of polynomial codes, it has shown that this bound gives the exact minimum distance [1]. Since a polynomial code of distance \( d \) is either a \( d \)-BCH code or a subcode of a \( d \)-BCH code, thus if \( d \) is the exact minimum distance of the polynomial code, it is also the exact minimum distance of the \( d \)-BCH code. A theorem which establishes the exact minimum distances of certain subclasses of polynomial codes is proved by Kasami, Lin, and Peterson [1].

**Theorem 3 [Kasami–Lin–Peterson].** A polynomial code \( C_m(\mu, b) \) has minimum distance exactly equal to

\[ \frac{(R + 1)q^{\mu} - 1}{b}, \]

if one of the following conditions holds:

1. \( R = 0 \),
2. \( s = 1 \), or
3. there exists an \( R/b \)-BCH code of length \( (q^\ast - 1)/b \) whose minimum distance is exactly \( R/b \).

Since a \( C_m(\mu, b) \) code is a subcode of the \( \frac{(R + 1)q^\mu - 1}{b} \)-BCH code of length \( (q^{\ast\ast} - 1)/b \), thus the BCH code has minimum distance exactly equal to

\[ \frac{(R + 1)q^{\mu} - 1}{b}. \]
In this section, we shall derive the exact minimum distance of another subclass of polynomial codes, which will enable us to establish the exact minimum distance of certain BCH codes.

Let $Q_0(\mu, b)$ be the set of polynomials in $Q_\mu(\mu, b)$ of Eq. (3) such that, for any $f(\bar{X})$ in $Q_0(\mu, b)$,

$$f(0, 0, \cdots, 0) = 0$$

(51)

Then, the code

$$C_0(\mu, b) = \{v(f) | f(\bar{X}) \in Q_0(\mu, b)\}$$

(52)

is a subcode of the polynomial code $C_\mu(\mu, b)$. Let $g(X)$ be the generator polynomial of $C_\mu(\mu, b)$. Then it is easily shown that the generator polynomial of $C_0(\mu, b)$ is

$$g_0(X) = (X - 1)g(X)$$

(53)

and the minimum distance of $C_0(\mu, b)$ is at least

$$\frac{(R + 1)q^q - 1}{b} + 1$$

In the following, we shall establish the exact minimum distance of a $C_0(\mu, b)$ code with $b = 1$. For $b = 1$, $C_0(\mu, 1)$ has

Length $N = q^{m_0} - 1$,

Minimum Distance $\geq (R + 1)q^{q^*}$.

**Theorem 4.** If an $(R + 1)$-BCH code of length $q^* - 1$ has minimum distance exactly $(R + 1)$, then $C_0(\mu, 1)$ has minimum distance exactly

$$(R + 1)q^{q^*}$.$$

(54)

**Proof.** By the Mattson–Solomon argument, there exists a polynomial $f_0(X)$ of degree $(q^* - 1) - (R + 1) = q^* - R - 2$ such that $f_0(X)$ has $q^* - R - 2$ different roots in $GF(q^*)$. Consider the following polynomial:

$$f(X_1, X_2, \cdots, X_m) = X_1f_0(X_1)(X_2^{q^*-1} - 1) \cdots (X_m^{q^*-1} - 1).$$

(55)

This polynomial has degree

$$(q^* - R - 1) + (m - Q - 1)(q^* - 1)$$

$$= (m - Q)(q^* - 1) - R = \mu$$

(56)

and $f(0, 0, \cdots, 0) = 0$. 
Thus, \( f(X_1, X_2, \ldots, X_n) \) is in \( Q_0(\mu, 1) \). It is easy to see that \( v(f) \) has weight exactly \( (R + 1)q^{\omega_e} \).

Q.E.D.

In the following, only binary codes (\( q = 2 \)) will be considered. We shall show that if \( (R + 1)2^{\omega_e} \) is the exact minimum distance of a binary \( C_m(\mu, 1) \) code, then \( (R + 1)2^{\omega_e} - 1 \) is the exact minimum distance of the binary \( C_m(\mu, 1) \) code. To prove this, we need the following theorems.

**Theorem 5 [Peterson–Prange, 13].** Assume that a binary code \( C_1 \) is invariant under a doubly transitive group and contains only code vectors of even weight. Then, for the code \( C_2 \) which is obtained by dropping the first digit from each code word,

\[
iw_i = (n + 1 - i)w_{i+1} \quad \text{for } i \text{ even}
\]

where \( w_i \) is the number of code words of weight \( i \), and \( n + 1 \) is the length of code vectors in \( C_1 \).

A direct consequence of the above theorem is the following corollary:

**Corollary 6.** Let \( C \) be a primitive binary cyclic code with generator polynomial \( g(X) \) whose extension \( C_0 \) (with an overall parity check digit) is doubly transitive invariant under the affine group of permutations. Let \( C_0 \) be the code whose generator polynomial is \( (X - 1)g(X) \). If code \( C_0 \) has minimum distance exactly \( d + 1 \) (even), then code \( C \) has minimum distance exactly \( d \) (odd).

It is known that an extended primitive code \( C_m(\mu, 1) \) of length \( q^{m_2} \) is doubly transitive invariant under the affine group of permutations [14]. By Theorem 4 and Corollary 6, we obtain:

**Theorem 7.** If a binary \( (R + 1) \)-BCH code of length \( 2^s - 1 \) has minimum distance exactly \( R + 1 \), then the binary polynomial code \( C_m(\mu, 1) \) of length \( 2^{m_2} - 1 \) has minimum distance exactly

\[
(R + 1)2^{\omega_e} - 1,
\]

where \( Q \) and \( R \) are quotient and remainder resulting from dividing \( m(2^s - 1) - \mu \) by \( 2^s - 1 \).

Q.E.D.

Since the polynomial code \( C_m(\mu, 1) \) is a subcode of the \([ (R + 1)2^{\omega_e} - 1 ] \)-BCH code of length \( 2^{m_2} - 1 \), then we have the following corollary:

**Corollary 8.** If a \( d \)-BCH code of length \( 2^s - 1 \) has minimum distance exactly \( d \), then a \([ d \cdot 2^{\omega_e} - 1 ] \)-BCH code of length \( 2^{m_2} - 1 \) has minimum...
distance exactly

\[ d \cdot 2^{\lambda} - 1 \]  

where \( 0 \leq \lambda < m \).

It is known that the dual codes of the class of polynomial codes contain Euclidean geometry codes and projective geometry codes as subclasses. Lower bounds on the minimum distances of the dual codes of polynomial codes have been verified in Refs. [1] and [2]. In the following, we shall derive a BCH bound which is tighter than the previous bounds (Except for the class of projective codes and the class of Euclidean geometry codes).

Let \( D_m(\mu, b) \) be the dual code of the polynomial code \( C_m(\mu, b) \). The generator polynomial of \( D_m(\mu, b) \) has \( \alpha^h \) as a root if and only if

\[
\max_{0 \leq t < s} W_{q^s}(h \alpha^t) = jb
\]

with \( 1 \leq j \leq \mu \) where \( b \) is a factor of \( q^s - 1 \). If \( h_0 \) is the smallest integer which is divisible by \( b \) such that

\[
\max_{0 \leq t < s} Q_{q^s}(h_0 \alpha^t) = (\mu + 1)b,
\]

and

\[
\max_{0 \leq t < s} W_{q^s}(h \alpha^t) < (\mu + 1)b
\]

for any \( h \) less than \( h_0 \) and divisible by \( b \), then the generator polynomial of \( D_m(\mu, b) \) has the following consecutive roots:

\[
\beta^0, \beta^1, \beta^2, \beta^3, \ldots, \beta^{(h_0/b) - 1}
\]

where \( \alpha \) is a primitive element of \( GF(q^m) \). Therefore, \( D_m(\mu, b) \) has minimum distance at least

\[
1 + \frac{h_0}{b}
\]

In the following, we shall construct the integer \( h_0 \).

Let \( Q_0 \) and \( R_0 \) be the quotient and remainder resulting from dividing \( (\mu + 1)b \) by \( (q^s - 1) \), i.e.,

\[
(\mu + 1)b = Q_0(q^s - 1) + R_0
\]

with \( 0 \leq R_0 < q^s - 1 \).
Since $q^* - 1$ is divisible by $b$, $R_0$ is divisible by $b$. Let $j$ be the largest integer such that

$$q^j \leq q^* - R_0$$

(63)

Dividing $q^* - R_0$ by $q^j$, we obtain

$$q^* - R_0 = \sigma_j q^j + r_j$$

(64)

where $1 \leq \sigma_j < q$ and $0 \leq r_j < q^j$.

Let

$$A = R_0 - 1 + \sigma_j q^j$$

(65)

$$B = q^* - \sigma_j q^j.$$ 

Let $A_0$ and $B_0$ be two nonnegative integers less than or equal to $q^* - 1$ which are defined as follows:

$$A_0 = Aq^{*-j} \quad \text{(mod } q^*-1)\text{)} \quad \text{for } A \neq q^*-1$$

$$A_0 = A \quad \text{for } A = q^*-1,$$

(66)

$$B_0 = Bq^{*-j} \quad \text{(mod } q^*-1)\text{)} \quad \text{for } B \neq q^*-1$$

$$B_0 = B \quad \text{for } B = q^*-1.$$ 

Since $A + B$ is divisible by $b$, $A_0 + B_0$ is divisible by $b$.

Now, we construct $h_0$ as follows:

$$h_0 = (q^* - 1) + (q^* - 1)q^* + \cdots + (q^* - 1)q^{(q_0 - 2)s}$$

$$+ A_0 q^{(q_0 - 1)s} + B_0 q^{q_0 s}$$

(67)

$$= B_0 q^{q_0 s} + (A_0 + 1)q^{(q_0 - 1)s} - 1$$

Then, we have the following theorem.

**Theorem 9.** The integer $h_0$ given by Eq. (67) has the following properties:

1. $\max_{0 \leq i < s} W_{q^s}(h_0 q^i) = (\mu + 1)b$,

2. For any integer $h$ which is less than $h_0$ and divisible by $b$, $\max_{0 \leq i < s} W_{q^s}(h q^i) = jb$, with $0 \leq j \leq \mu$.

**Proof.** See appendix. Q.E.D.

Thus, by the Bose argument, the code $D_m(\mu, b)$ has minimum distance
at least

\[ \frac{h_0}{b} + 1. \]  

(68)

Since \( \beta^{h_0/b} \) is not a root of the generator polynomial of \( D_m(\mu, b) \), therefore, \( D_m(\mu, b) \) is a subcode of the \( [1 + (h_0/b)] \)-BCH code of length \( (q^m - 1)/b \) whose generator polynomial has the following roots:

\[ \beta^0, \beta^1, \beta^2, \ldots, \beta^{(h_0/b)-1} \]

and their conjugates.

For \( b = q^s - 1 \), it has been shown that \( D_m(\mu, q^s - 1) \) is a \( \mu \)th order \( q \)-ary projective geometry code which is \((m - \mu - 1)\)-step orthogonizable \([1, 2]\). By Eqs. (62), (63), and (64), we have

\[ Q_0 = \mu + 1, \]
\[ R_0 = 0, \]  

(69)

\[ j = s \quad \text{and} \quad \sigma_j = 1. \]

By Eq. (65), we obtain

\[ A = q^s - 1 \]
\[ B = 0 \]  

(70)

It follows from Eq. (66) that

\[ A_0 = A = q^s - 1 \]
\[ B_0 = B = 0 \]  

(71)

Therefore,

\[ h_0 = q^{(\mu+1)s} - 1, \]  

(72)

and code \( D_m(\mu, q^s - 1) \) has minimum distance at least

\[ \frac{q^{(\mu+1)s}}{q^s - 1} - 1 + 1 \]  

(73)

The BCH bound given by Eq. (73) is exactly the same as the majority-logic decoding bound \([6, 7]\).

For \( b = 1 \) and \( \mu = \ell(q^s - 1) \), \( D_m(\mu, 1) \) is a \( q \)-ary \((m - \ell - 1, s)\)th order Euclidean geometry code \([1, 2]\) which is \((m - \ell - 1)\)-step majority
logic decodable. By Eqs. (62)-(66) it is easy to show that $D_m(\mu, 1)$ has minimum distance at least
\[ q^l + q \cdot q^{(i-1)s} \]  
(74)
The bound given by Eq. (74) was obtained by Lin [2].

5. ON THE RELATIONSHIP BETWEEN AN EXTENDED PRIMITIVE POLYNOMIAL CODE AND THE $m$th POWER OF AN EXTENDED PRIMITIVE $d$-BCH CODE

Let $C_m^*(\mu, 1)$ be the extended code which is obtained from a primitive polynomial code by annexing an overall parity check digit. Each code vector in $C_m^*(\mu, 1)$ is specified by a polynomial $f(X)$ in $Q_m(\mu, 1)$ as follows:

$$v_0(f) = (v_\infty, v_0, v_1, \ldots, v_{q^m-2})$$ \hspace{1cm} (75)

where the overall parity check digit

$$v_\infty = f(0, 0, \ldots, 0)$$ \hspace{1cm} (76)

and the $l$th component

$$v = f(a_1, a_2, \ldots, a_l)$$ \hspace{1cm} (77)

for $0 \leq l < q^m - 1$.

For $m = 1$ and $\mu = q^s - 1 - d$, an extended primitive polynomial code, $C_1^*(q^s - 1 - d, 1)$ is an extended primitive $d$-BCH code of length $q^s$. Let $\xi$ be a primitive element of $GF(q^s)$. Then, $C_1^*(q^s - 1 - d, 1)$ is specified by the following set of polynomials:

\[ Q_1(q^s - 1 - d, 1) = \{ f(X) = \sum_{j=0}^{n-d} C_j X^j \mid C_j \in GF(q^s) \text{ and } f(\xi^l) \in GF(q) \text{ for } 0 \leq l < n \} \]  
(78)

and each code vector in $C_1^*(q^s - 1 - d, 1)$ is

$$v_0(f) = (f(0), f(1), f(\xi), f(\xi^2), \ldots, f(\xi^{n-1}))$$ \hspace{1cm} (79)

where $n = q^s - 1$.

Now, consider the extended primitive polynomial code $C_m^*(\mu, 1)$ with $\mu = q^s - 1 - d$. This code is specified by $Q_m(q^s - 1 - d, 1)$. For any polynomial $f(X)$ in $Q_m(q^s - 1 - d, 1)$, consider the following poly-
nomial:

\[ f'(X_i) = f(\xi^1, \xi^2, \ldots, \xi^{l_i-1}, X_i, \xi^{l_i+1}, \ldots, \xi^{l_m}) \]

\[ = \sum_{i=0}^{q^2-1-d} C_{i} X^{l_i} \]

where \( 0 \leq l_i < q^2 - 1 \). It is obvious that

\[ f'(X_i) \in Q_l(q^2 - 1 - d, 1) \] (81)

It follows from Eqs. (80) and (81) that we obtain the following theorem.

**Theorem 10.** The extended primitive polynomial code

\[ C_m^*(q^2 - 1 - d, 1) \]

is a subcode of the product of an extended primitive d-BCH code with itself \( m \) times.

The product code of a code with itself \( m \) times will be called the \( m \)th power of the code.

The fact of Theorem 10 is most easily seen by considering \( m = 2 \). The extended polynomial code \( C_2^*(q^2 - 1 - d, 1) \) is specified by \( Q_2(q^2 - 1 - d, 1) \) such that each code vector is as follows:

\[ v_0(f) = (v_0, v_0, v_1, v_2, \ldots, v_{q^2-2}) \] (82)

with the overall parity check digit

\[ v_\omega = f(0, 0), \] (83)

and the \( l \)th component

\[ v_l = f(a_{1l}, a_{2l}). \] (84)

Since \( \xi \) is a primitive element of \( GF(q^2) \), \( a_{1l} \) and \( a_{2l} \) must be powers of \( \xi \), say \( \xi^{l_1} \) and \( \xi^{l_2} \). It is obvious that \( a_{1l} \) runs over the set \( 0, 1, \xi, \xi^2, \ldots, \xi^{q^2-2} \) as \( l \) goes through from 0 to \( q^2 - 2 \). Thus, a code vector in \( C_2^*(q^2 - 1 - d, 1) \) can be arranged as a \( q^2 \times q^2 \) array as in Fig. 1. From Eqs. (80) and (81), it can be seen that each row (or each column) of the above array is a code vector in the extended d-BCH code defined by Eqs. (78) and (79). Thus, \( C_2^*(q^2 - 1 - d, 1) \) is a subcode of the product of the extended d-BCH code with itself.

For each polynomial \( f(X_1, X_2) \) in \( Q_2(q^2 - 1 - d, 1) \), we set

\[ X_2 = \xi^l X_1 \] (85)
for $0 \leq t < q^s - 1$. It is easy to see that the polynomial

$$f''(X_1) = f(X_1, \xi X_1)$$

is in $Q_1(q^s - 1 - d, 1)$ of Eq. (78). This implies that the following components

$$(f(1, \xi^t), f(\xi, \xi^t+1), \cdots, f(\xi^{q^s-t-2}, \xi^{q^s-t-2}), f(\xi^{q^s-t-1}, 1), \quad \cdots, f(\xi^{q^s-t}, \xi))$$

form a code vector in the $d$-BCH code specified by $Q_1(q^s - 1 - d, 1)$ of Eq. (78). By the same argument, the polynomial

$$f''(X_2) = f(\xi^t X_1, X_2)$$

is in $Q_1(q^s - 1 - d, 1)$ of Eq. (78). Thus, the following components

$$(f(\xi^t, 1), f(\xi^{t+1}, \xi), \cdots, f(\xi^{q^s-t-2}, \xi^{q^s-t-2}), f(1, \xi^{q^s-t-1}), \quad \cdots, f(\xi^{q^s-t-1}, \xi^{q^s-t-2}))$$

also form a code vector in the $d$-BCH code specified by $Q_1(q^s - 1 - d, 1)$ of Eq. (78).

The property specified by Eqs. (87) and (89) may have some use in decoding.

Define the $m$th power of an extended primitive $d$-BCH code of length $q^s$ as the product of the extended $d$-BCH code with itself $m$ times. Now, it can be seen easily that the $m$th power code $C(m)$ is specified by the following set of polynomials

$$Q(m) = \{f(\bar{X}) = \sum_{r_1=0}^{n-d} \sum_{r_2=0}^{n-d} \cdots \sum_{r_m=0}^{n-d} C_{r_1 r_2 \cdots r_m} X_1^{r_1} X_2^{r_2} \cdots X_m^{r_m} | \quad C_{r_1 r_2 \cdots r_m} \in GF(q^s) \quad \text{and} \quad f(a_{11}, a_{21}, \cdots, a_{m1}) \in GF(q) \}$$

for $0 \leq l < q^{ms} - 1$.

<table>
<thead>
<tr>
<th>$X_1$</th>
<th>0</th>
<th>1</th>
<th>$\xi$</th>
<th>$\xi^2$</th>
<th>$\xi^{q-2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$f(0, 0)$</td>
<td>$f(0, 1)$</td>
<td>$f(0, \xi)$</td>
<td>$f(0, \xi^2)$</td>
<td>$\cdots$</td>
</tr>
<tr>
<td>1</td>
<td>$f(1, 0)$</td>
<td>$f(1, 1)$</td>
<td>$f(1, \xi)$</td>
<td>$f(1, \xi^2)$</td>
<td>$\cdots$</td>
</tr>
<tr>
<td>$\xi$</td>
<td>$f(\xi, 0)$</td>
<td>$f(\xi, 1)$</td>
<td>$f(\xi, \xi)$</td>
<td>$f(\xi, \xi^2)$</td>
<td>$\cdots$</td>
</tr>
<tr>
<td>$\xi^2$</td>
<td>$f(\xi^2, 0)$</td>
<td>$f(\xi^2, 1)$</td>
<td>$f(\xi^2, \xi)$</td>
<td>$f(\xi^2, \xi^2)$</td>
<td>$\cdots$</td>
</tr>
<tr>
<td>$\xi^{q-2}$</td>
<td>$f(\xi^{q-2}, 0)$</td>
<td>$f(\xi^{q-2}, 1)$</td>
<td>$f(\xi^{q-2}, \xi)$</td>
<td>$f(\xi^{q-2}, \xi^2)$</td>
<td>$\cdots$</td>
</tr>
</tbody>
</table>
where \( n = q^s - 1 \). Each code vector in the \( m \)th power code \( C(m) \) is specified by a polynomial in \( Q(m) \) as follows:

\[
v_0(f) = (v_\infty, v_0, v_1, v_2, \cdots, v_{q^m-2}) \tag{91}
\]

where

\[
v_\infty = f(0, 0, \cdots, 0) \tag{92}
\]

and

\[
v_l = f(a_{1l}, a_{2l}, \cdots, a_{ml}) \tag{93}
\]

for \( 0 \leq l < q^{ms} - 1 \).

Since \( Q(m) \) is a subset of \( Q_m(\mu, 1) \) with \( \mu = m(q^s - 1) - md \), the \( m \)th power \( C(m) \) of an extended primitive \( d \)-BCH code is a subcode of the extended primitive polynomial code \( C_m^*(\mu, 1) \) with \( \mu = m(q^s - 1) - md \).

Let \( A \) be an \( m \times m \) nonsingular matrix over \( GF(q^s) \) and \( B \) be an \( m \)-tuple over \( GF(q^s) \). Then, for any \( f(\vec{X}) \) in \( Q_m(\mu, 1) \), there is a polynomial \( f'(\vec{X}) \) in \( Q_m(\mu, 1) \) such that

\[
f'(\vec{X}) = f(\vec{X}A + B) \tag{94}
\]

Consider the permutation \( \pi_{AB} \) on the components of vector \( v_0(f) \) such that

\[
\pi_{AB}v_0(f) = v_0(f') \tag{95}
\]

where \( \pi_{AB} \) is described as follows:

\[
f'(a_{1l}, a_{2l}, \cdots, a_{ml}) = f[(a_{1l}, a_{2l}, \cdots, a_{ml})A + B] \tag{96}
\]

Let \( \pi \) denote the general affine group,

\[
\pi = \{ \pi_{AB} | A \text{ is a nonsingular } m \times m \text{ matrix over } GF(q^s) \text{ and } B \text{ is an } m \text{-tuple over } GF(q^s) \} \tag{97}
\]

It follows from Eq. (94) that we have:

**Theorem 11.** The class of extended primitive polynomial codes are invariant under the general affine group \( \pi \). This theorem implies that an extended primitive polynomial code is doubly transitive invariant under the affine group of permutations [14].

Let \( A \) be an \( m \times m \) nonsingular diagonal matrix over \( GF(q^s) \). Then, for any \( f(\vec{X}) \) in \( Q(m) \) of Eq. (90), there is a polynomial \( f'(\vec{X}) \) in \( Q(m) \) such that

\[
f'(\vec{X}) = f(\vec{X}A + B) \tag{98}
\]

\[
_f(\vec{X}) = f(0, 0, \cdots, 0)
\]

and

\[
v_l = f(a_{1l}, a_{2l}, \cdots, a_{ml})
\]

for \( 0 \leq l < q^{ms} - 1 \).
Let \( \pi_0 \) denote the subgroup of \( \pi \) such that
\[ \pi_0 = \{ \pi_{AB} \mid \pi_{AB} \in \pi \text{ and } A \text{ is an } m \times m \text{ nonsingular diagonal matrix} \} \] (99)

Then we have:

**Theorem 12.** The \( m \)th power of an extended \( d \)-BCH code of length \( q^s \) is invariant under \( \pi_0 \).

**APPENDIX (Proof of Theorem 9)**

Let \( h \) be a nonnegative integer less than \( q^{m_2} - 1 \). Express \( h \) in radix-\( q^s \) form,
\[ h = \sum_{i=0}^{m-1} \delta_i q^i \] (A-1)

where \( 0 \leq \delta_i < q^s \) for \( 0 \leq i < m \).

Define \( \delta_i^{(t)} \) as the nonnegative integer less than \( q^s \) such that
\[ \delta_i^{(t)} = \delta_i q^t \pmod{q^s - 1} \] (A-2a)
for \( 0 \leq \delta_i < q^s - 1 \), and
\[ \delta_i^{(t)} = \delta_i \] (A-2b)
for \( \delta_i = q^s - 1 \). The following lemma is proved by Kasami et al., in Ref. [1].

**Lemma A1.**

\[ W_{q^s}(hq^t) = \sum_{i=1}^{m-1} \delta_i^{(t)} \] (A-3)

for \( 0 \leq t < s \).

It follows from Eqs. (63) and (64) that \( q^s - R_0 \) can be expressed as follows:
\[ q^s - R_0 = \sigma_0 + \sigma_1 q + \sigma_2 q^2 + \cdots + \sigma_j q^j \] (A-4)

where \( 1 \leq \sigma_j \leq q - 1 \) and \( 0 \leq \sigma_i \leq q - 1 \) for \( i = 0, 1, \cdots, j - 1 \).

From Eq. (65), we have
\[
A = (q - 1 - \sigma_0) + (q - 1 - \sigma_1)q + \cdots + (q - 1 - \sigma_{j-1})q^{j-1} \\
+ (q - 1)q^j + \cdots + (q - 1)q^{s-1},
\] (A-5)

\[
B = (q - \sigma_j)q^j + (q - 1)q^{j+1} + \cdots + (q - 1)q^s - 1.
\]

where \( 1 \leq q - \sigma_j \leq q - 1 \).
It follows from Eq. (66) that
\[
1_0 = (q - 1) + (q - 1)q + \cdots + (q - 1)q^{s-j-1}
+ (q - 1 - \sigma_0)q^{s-j} + \cdots + (q - 1 - \sigma_{j-1})q^{s-1} \tag{A-6}
\]
\[
3_0 = (q - \sigma_j) + (q - 1)q + \cdots + (q - 1)q^{s-j-1}
\]

Now, consider the integer \( h_0 \) defined by Eq. (67):
\[
\omega = (q' - 1) + (q' - 1)q' + \cdots + (q' - 1)q^{(Q_0-2)s}
+ A_0q^{(Q_0-1)s} + B_0q^{Q_0s} \tag{A-7}
\]
\[
\text{set}
\]
\[
\bar{A}_0^{(t)} = A_0q^t \pmod{q' - 1}
\]
\[
\bar{B}_0^{(t)} = B_0q^t \pmod{q' - 1} \tag{A-8}
\]

**Lemma A2:**
\[
\max_{0 \leq t < s} W_{q^s}(h_0q^t) = (\mu + 1)b \tag{A-9}
\]

**Proof.** It follows Lemma A1 that
\[
\max_{0 \leq t < s} W_{q^s}(h_0q^t) = (Q_0 - 1)q^s - 1) + \max_{0 \leq t < s} [\bar{A}_0^{(t)} + \bar{B}_0^{(t)}]
\]

From Eq. (A-6), it is easy to see that
\[
\max_{0 \leq t < s} [\bar{A}_0^{(t)} + \bar{B}_0^{(t)}] = A + B = (q^s - 1) + R_0 \tag{A-10}
\]
\[ t = s - j. \] Thus,
\[
\max_{0 \leq t < s} W_{q^s}(h_0q^t) = Q_0(q^s - 1) + R_0
\]

By Eq. (62), we have
\[
\max_{0 \leq t < s} W_{q^s}(h_0q^t) = (\mu + 1)b
\]
Q.E.D.

**Lemma A3:** Let \( h \) be any nonnegative integer less than \( h_0 \) and divisible by \( \nu \). Then,
\[
\max_{0 \leq t < s} W_{q^s}(hq^t) < (\mu + 1)b \tag{A-11}
\]
Proof. Write \( h \) in radix-\( q^s \) form,

\[
h = \delta_0 + \delta_1 q^s + \cdots + \delta_{q_0-2} q^{(q_0-2)s} + C q^{(q_0-1)s} + D q^{q_0s}
\]  
(A-12)

where \( 0 \leq \delta_i \leq q^s - 1 \) and \( D \leq B_0 \).

Then,

\[
W_{q^s}(hq^t) = \sum_{i=0}^{q_0-2} \delta_i^{(t)} + \tilde{C}^{(t)} + \tilde{D}^{(t)}
\]  
(A-13)

It follows from Eqs. (A-2) and (A-13) that we have

\[
\max_{0 \leq t < s} W_{q^s}(hq^t) < (Q_0 - 1)(q^s - 1) + \max_{0 \leq t < s} [\tilde{C}^{(t)} + \tilde{D}^{(t)}]
\]  
(A-14)

There are three cases to be considered:

1. For \( D = B_0 \) and \( C = A_0 \), it is obvious that

\[
\max_{0 \leq t < s} [\tilde{C}^{(t)} + \tilde{D}^{(t)}] = \max_{0 \leq t < s} [\tilde{A}_0^{(t)} + \tilde{B}_0^{(t)}]
\]

Thus,

\[
\max_{0 \leq t < s} W_{q^s}(hq^t) < (Q_0(q^s - 1) + R_0 = (\mu + 1)b
\]  
(A-15)

2. For \( D = B_0 \) and \( C < A_0 \), by Eq. (A-6) it is easy to see that

\[
\max_{0 \leq t < s} [\tilde{C}^{(t)} + \tilde{D}^{(t)}] < \max_{0 \leq t < s} [\tilde{A}_0^{(t)} + \tilde{B}_0^{(t)}]
\]

It follows from Eq. (A-14) that we have

\[
\max_{0 \leq t < s} W_{q^s}(hq^t) < Q_0(q^s - 1) + R_0 = (\mu + 1)b
\]  
(A-16)

3. For \( D < B_0 \), it follows from Eq. (A-5) that

\[
B - \max_{0 \leq t < s} \tilde{D}^{(t)} \geq q^j
\]  
(A-17)

\[
\max_{0 \leq t < s} \tilde{C}^{(t)} - A < q^j
\]  
(A-18)

Combining Eqs. (A-17) and (A-18) yields

\[
A + B > \max_{0 \leq t < s} \tilde{C}^{(t)} + \max_{0 \leq t < s} \tilde{D}^{(t)}
\]  
(A-19)

Thus, we have

\[
(q^s - 1) + R_0 > \max_{0 \leq t < s} [\tilde{C}^{(t)} + \tilde{D}^{(t)}]
\]  
(A-20)
It follows from Eq. (A-14) that
\[
\max_{0 \leq t < s} W_{q^t}(hq') < (\mu + 1)b.
\]
The above three cases conclude the lemma. Q.E.D.

Combining Lemmas A2 and A3, we obtain Theorem 9.

REFERENCES

2. LIN, S., On a Class of Cyclic Codes, Proceedings of the Symposium on Error Correcting Codes, Mathematics Research Center, United States Army, University of Wisconsin, May 6-8, 1968.