5-1975

Some Results on the Weight Structure of Cyclic Codes of Composite Length

Carlos R.P. Hartmann
Syracuse University, chartman@syr.edu

T. Y. Hwang
Syracuse University

1-75

SOME RESULTS ON THE WEIGHT STRUCTURE OF CYCLIC CODES OF COMPOSITE LENGTH

C. R. P. Hartmann

T. Y. Hwang

May 1975

SYSTEMS AND INFORMATION SCIENCE
SYRACUSE UNIVERSITY

Some Results on the Weight Structure of Cyclic Codes of Composite Length

C. R. P. Hartmann

T. Y. Hwang

This work was supported by the National Science Foundation Grant GK-37449,

Systems and Information Science

Syracuse University

Syracuse, New York 13210

(315) 423-2368

Abstract

In this work we investigate the weight structure of cyclic codes of composite length $n = n_1 n_2$, where n_1 and n_2 are relatively prime. The actual minimum distances of some classes of binary cyclic codes of composite length are derived. For other classes new lower bounds on the minimum distance are obtained. These new lower bounds improve on the BCH bound for a considerable number of binary cyclic codes.

I. Introduction

The problem of constructing cyclic product codes has been considered by Burton and Weldon [1] and by Abramson [2]. The factoring of cylic codes was considered by Assmus and Mattson [3,4], and Goethals [5]. Goethals found new lower bounds on the minimum weight of a subclass of cyclic codes of composite length $n = n_1 n_2$ with $GCD(n_1, n_2) = 1$. Kasami [6] extended Goethals result. In both papers [5,6] a factorization is applied to the polynomials obtained from the Mattson-Solomon formulation [7].

By using a factorization applied directly to code vectors the actual minimum distances of some classes of binary cyclic codes of composite length are derived. For other classes new lower bounds on the minimum distance are obtained. The minimum distance and the lower bounds are given in terms of the minimum distance of cyclic codes of length n_1 and n_2. In many cases, the new lower bounds improve on the BCH bound, d_0 [8].

Some preliminaries are introduced in Section II. In Section III the minimum distances and the lower bounds are derived. In Section IV tables with numerical examples are presented. Concluding remarks are contained in Section V.

II. Preliminaries

Let V_n be a cyclic code over GF(q) of length $n = n_1 n_2$, $\mathrm{GCD}(n_1, n_2) = 1$, and minimum distance d generated by g(x). Since n_1 and n_2 are relatively prime, there exist integers a and b such that

$$an_1 + bn_2 = 1 .$$

Let β be an element of order n in an extension field $GF(q^m)$ of GF(q) and let

$$\alpha = \beta^{bn_2}, \ \gamma = \beta^{an_1} .$$

Then, α and γ are primitive n_1^{th} and n_2^{th} roots of unity respectively, and

$$\alpha\gamma = \beta$$

Let $\rho(\theta,\phi)$, $0 \leq \rho(\theta,\phi) < n$, be the unique solution of the following congruences given by the Chinese remainder theorem:

$$\rho(\theta,\phi) \equiv \begin{cases} \theta (\mathrm{mod}\ n_1), & 0 \leq \theta < n_1 \\ \phi (\mathrm{mod}\ n_2), & 0 \leq \phi < n_2 \end{cases} .$$

It follows that $\beta^{\rho(\theta,\phi)} = \alpha^{\theta}\gamma^{\phi}$.

Let

$$v(x) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a_{\rho(i,j)} x^{\rho(i,j)}, \ a_{\rho(i,j)} \in GF(q)$$

be a code vector of V_n. Associated with the polynomial v(x), polynomials V(y,z), $V_j(y)$ and $\bar{V}_i(z)$ are defined as follows:

$$V(y,z) = \sum_{j=0}^{n_2-1} V_j(y) z^j$$

$$= \sum_{i=0}^{n_1-1} \bar{V}_j(z) y^i,$$

where

$$V_j(y) = \sum_{i=0}^{n_1-1} a_{\rho(i,j)} y^i \text{ and } \bar{V}_i(z) = \sum_{j=0}^{n_2-1} a_{\rho(i,j)} z^j .$$

Similar to Kasami's derivation [6], it can be shown that

$$v(\beta^{\rho(\theta,\phi)}) = V(\alpha^\theta, \gamma^\phi) .$$

In the next section we will derive the minimum distances and the lower bounds on the minimum distance of some classes of cyclic codes of composite length $n = n_1 n_2$, $GCD(n_1,n_2) = 1$.

III. Theorems

At first we will present a new lower bound on d which is a generalization of Elias' bound [9] for cylic product codes. In order to prove this bound we require two technical lemmas. The proofs of these lemmas are similar to the proofs of [10, Lemma 1] and [10, Lemma 2], respectively.

Lemma 1: If $V_j(\alpha^\theta) = \sum_{i=0}^{n_1-1} a_{\rho(i,j)} \alpha^{i\theta} = 0$ for $\theta = 0,1,\ldots,n_1-1$, then $a_{\rho(i,j)} = 0$ for $i = 0,1,\ldots,n_1-1$.

Lemma 2: If $v(\beta^{\rho(\theta,\phi)}) = \sum_{j=0}^{n_2-1} V_j(\alpha^\theta)\gamma^{j\phi} = 0$ for $\phi = 0,1,\ldots,n_2-1$, then $V_j(\alpha^\theta) = 0$ for $j = 0,1,\ldots,n_2-1$.

Let V_n be a cyclic code over GF(q) of length $n = n_1 n_2$ and minimum distance d generated by g(x), where $GCD(n_1,n_2) = 1$. For each θ, $0 \leq \theta < n_1$, we define $J_\theta = \{\phi | g(\beta^{\rho(\theta,\phi)}) = 0\}$ and define m_θ to be the least nonzero integer such that $\theta q^{m_\theta} \equiv \theta (\text{mod } n_1)$. Thus if $\phi \in J_\theta$, then $\phi_1 \in J_\theta$, where $\phi_1 \equiv q^{m_\theta} \phi (\text{mod } n_2)$. Define $S_1 = \{\theta | J_\theta = \{0,1,\ldots,n_2-1\}\}$. For each $\theta \notin S_1$ and such that J_θ is nonempty we define $V_{n_2}^{(\theta)}$ to be the cyclic code over $GF(q^{m_\theta})$ of length n_2 and minimum distance $d_2^{(\theta)}$ generated by

$$g_2^{(\theta)}(x) = \prod_{\phi \in J_\theta} (x-\gamma^\phi) .$$

For each $\theta \notin S_1$ and such that J_θ is empty we define $V_{n_2}^{(\theta)}$ to be the cyclic code over $GF(q^{m_\theta})$ of length n_2 and minimum distance $d_2^{(\theta)} = 1$

generated by

$$g_2^{(\theta)}(x) = 1 \ .$$

Further, for each $\theta \notin S_1$ define $S_\theta = S_1 \cup S_1^{(\theta)}$, where $S_1^{(\theta)} = \{\hat{\theta} | 0 \leq \hat{\theta} < n_1;\ \hat{\theta} \notin S_1 \text{ and } d_2^{(\hat{\theta})} > d_2^{(\theta)}\}$. Now, for each θ such that S_θ is nonempty define $V_{n_1}^{(\theta)}$ to be the cyclic code over GF(q) of length n_1 and minimum distance $d_1^{(\theta)}$ generated by

$$g_1^{(\theta)}(x) = \text{LCM}\{\prod_{i \varepsilon S_\theta} m_i(x)\}$$

where $m_i(x)$ is the minimum polynomial of α^i over GF(q). Further, for each θ such that S_θ is empty define $V_{n_1}^{(\theta)}$ to be the cyclic code over GF(q) of length n_1 and minimum distance $d_1^{(\theta)} = 1$ generated by

$$g_1^{(\theta)}(x) = 1 \ .$$

We are now in the position to prove the following theorem.

<u>Theorem 1</u>: $d \geq \min(d_1^{(\theta)}\ d_2^{(\theta)} | \theta \notin S_1)$

<u>Proof</u>: Let $v(x)$ be a nonzero code polynomial of weight w in V_n. Then

$$v(\beta^{\rho(\theta,\phi)}) = \sum_{j=0}^{n_2-1} V_j(\alpha^\theta)\gamma^{j\phi} \ .$$

First, we note, by Lemma 2, that for each $\theta \ \varepsilon \ S_1$ we have $V_j(\alpha^\theta) = 0$ for $j = 0,1,\ldots,n_2-1$. By Lemma 1, if $V_j(\alpha^\theta) = 0$ for $j = 0,1,\ldots,n_2-1$ and for $\theta = 0,1,\ldots,n_1-1$, then $v(x) \equiv 0$, contradicting the assumption that $v(x)$ is a nonzero code polynomial of V_n. Hence $S_1 \neq \{0,1,\ldots,n_1-1\}$ and there must exist at least one $\theta \notin S_1$, $0 \leq \theta < n_1$ such that $V_j(\alpha^\theta) \neq 0$ for some j, $0 \leq j < n_2$. In general for each θ such that J_θ is nonempty and $\theta \not\in S_1$ we have

$$v(\beta^{\rho(\theta,\phi)}) = \sum_{j=0}^{n_2-1} V_j(\alpha^\theta)\gamma^{j\phi} = 0$$

for $\phi \in J_\theta$. Now since $(V_j(\alpha^\theta))^{q^{m_\theta}} = V_j(\alpha^\theta)$, $v_2(z) = \sum_{j=0}^{n_2-1} V_j(\alpha^\theta)z^j$ is a code polynomial of $V_{n_2}^{(\theta)}$. For cases where $V_j(\alpha^\theta) \neq 0$, for some j, $0 \leq j < n_2$, we actually must have $V_j(\alpha^\theta) \neq 0$ for $j = j_1, j_2, \ldots, j_\mu$ where $\mu \geq d_2^{(\theta)}$. So it is possible that $V_j(y) \not\equiv 0$ for $j = j_1, j_2, \ldots, j_\mu$ for $\mu = d_2^{(\theta)}$ and $V_j(y) \equiv 0$ for $j = j_{\mu+1}, j_{\mu+2}, \ldots, j_{n_2}$. But in this case $V_j(\alpha^{\hat{\theta}}) = 0$ for $j = 0,1,\ldots,n_2-1$ and for all $\hat{\theta} \in S_\theta$. Thus, $V_j(y)$ is a code polynomial of $V_{n_1}^{(\theta)}$ for $j = 0,1,\ldots,n_2-1$. Hence the weight of $V_j(y)$, for $j = j_1, j_2, \ldots, j_\mu$ is at least $d_1^{(\theta)}$. It follows that $w \geq d_1^{(\theta)} d_2^{(\theta)}$. The case where $V_j(y) \not\equiv 0$ for $j = j_1, j_2, \ldots, j_\mu$ for $\mu > d_2^{(\theta)}$ is considered when we analyze the case $V_j(\alpha^{\theta_1}) \neq 0$ for some j, $0 \leq j < n_2$, and θ_1 is such that $d_2^{(\theta_1)} > d_2^{(\theta)}$. By a similar argument, when θ is such that J_θ is empty and $\theta \not\in S_1$, we obtain $w \geq d_1^{(\theta)}$ since $d_2^{(\theta)} = 1$. Thus we conclude that

$$d \geq \min(d_1^{(\theta)} d_2^{(\theta)} \mid \theta \not\in S_1)$$

Q.E.D.

We remark that [10, Theorem 2] is a weak version of this theorem.

We now give an example of the application of Theorem 1.

<u>Example 1</u>: Consider the (55,35) binary BCH code generated by $g(x) = m_1(x)$. For this code $n_1 = 5$, $n_2 = 11$, J_0 = empty set, $J_1 = J_4 = \{1,3,4,5,9\}$, $J_2 = J_3 = \{2,6,7,8,10\}$, S_1 = empty set, and

$d_0 = 4$. Thus $V_{n_2}^{(0)}$ is the (11,11) binary cyclic code with $d_1^{(0)} = 1$, $V_{n_2}^{(1)} = V_{n_2}^{(4)}$ is a (11,6) quadratic residue code over GF(4) with $d_2^{(1)} = d_2^{(4)} = 5$ and $V_{n_2}^{(2)} = V_{n_2}^{(3)}$ is also a (11,6) cyclic code over GF(4) with $d_2^{(2)} = d_2^{(3)} = 5$ since it is equivalent to $V_{n_2}^{(1)}$. Thus we obtain the following table:

θ	$d_1^{(\theta)}$	$d_2^{(\theta)}$
0	5	1
1	1	5
2	1	5
3	1	5
4	1	5

Hence, by Theorem 1, $d \geq 5$. We remark that for this example the generalized BCH bound [11] also gives $d \geq 5$ and that in this case both bounds achieve the actual minimum distance [12]. If we apply [10, Theorem 2] to this code we obtain only $d \geq 1$.

We are now interested in the investigation of the minimum weight of odd-weight code vectors and the minimum weight of even-weight code vectors of binary cyclic codes of composite length $n = n_1 n_2$, $GCD(n_1, n_2) = 1$. Thus from now on we assume $q = 2$.

In order to continue our development we need to introduce some definitions. Let d_{odd}, d_{even} be the minimum weight of odd-weight and the minimum weight of even-weight code vectors of V_n, respectively. Further, for i = 1 and 2, let d_i be the minimum distance of V_{n_i} and let d_{iodd}, d_{ieven} be the minimum weight of odd-weight and minimum weight of even-weight code vectors of V_{n_i}, respectively. Where V_{n_i} is a binary cyclic code of length n_i generated by $g_i(x)$.

The next theorem gives the exact value on d_{odd} and d_{even} when V_n is a binary cyclic product code of V_{n_1} and V_{n_2}.

<u>Theorem 2</u>: Let V_n be the binary cyclic product code of V_{n_1} and V_{n_2} generated by g(x) such that $g(1) \neq 0$. Then,

$$d_{odd} = d_{1odd}\, d_{2odd}$$

and

$$d_{even} = \min(d_{1even}\, d_2,\ d_1\, d_{2even})$$

<u>Proof</u>: Let v(x) be a nonzero code vector of V_n. Thus, we have that

$$v(\beta^{\rho(\theta,\phi)}) = V(\alpha^\theta,\gamma^\phi) = \sum_{j=0}^{n_2-1} V_j(\alpha^\theta)\gamma^{j\phi} .$$

Let

$$v_2(z) = \sum_{j=0}^{n_2-1} V_j(1) z^j ,$$

then

$$v_2(\gamma^\phi) = v(\beta^{\rho(0,\phi)}) .$$

According to [13, Theorem 3] we have that

$$v(\beta^{\rho(0,\phi)}) = 0 \text{ for } \phi \in S_2$$

where $S_2 = \{\phi | g(\beta^{\rho(\theta,\phi)}) = 0 \text{ for } \theta = 0,1,\ldots,n_1-1\}$. Thus, by [13] $v_2(z)$ is a code polynomial of V_{n_2}. Furthermore, by [13, Theorem 3]

$$v(\beta^{\rho(\theta,\phi)}) = \sum_{j=0}^{n_2-1} V_j(\alpha^\theta)\gamma^{j\phi} = 0$$

for $\theta \in S_1$, where $S_1 = \{\theta | g(\beta^{\rho(\theta,\phi)}) = 0 \text{ for } \phi = 0,1,\ldots,n_2-1\}$. Thus, by Lemma 2, $V_j(\alpha^\theta) = 0$ for $\theta \in S_1$ and $j = 0,1,\ldots,n_2-1$. Hence by [13], $V_j(y)$ is a code polynomial of V_{n_1} for $j = 0,1,\ldots,n_2-1$. First let us assume that $v(x)$ has odd weight. Hence, $V_j(1) \neq 0$ for at least one j, $0 \leq j < n_2$. So, $v_2(z)$ has weight at least d_{2odd} and since $V_j(y)$ is a code polynomial of V_{n_1} we can conclude that $d_{odd} \geq d_{1odd}\, d_{2odd}$. Now we assume that $v(x)$ has even weight. Two cases must be analyzed, $V_j(1) \neq 0$ for some j, $0 \leq j < n_2$ and $V_j(1) = 0$ for $j = 0,1,\ldots,n_2-1$. If $V_j(1) \neq 0$ for some j, $0 \leq j < n_2$, then $v_2(z) \not\equiv 0$ and $v_2(z)$ must have even weight. Thus, $d_{even} \geq d_{1odd}\, d_{2even}$. Now, if $V_j(1) = 0$ for $j = 0,1,\ldots,n_2-1$, then

$$v(\beta^{\rho(0,\phi)}) = \sum_{j=0}^{n_2-1} V_j(1)\, \gamma^{j\phi} = 0$$

for $\phi = 0,1,\ldots,n_2-1$. Thus, $v(x)$ is divisible by $x^{n_2} + 1$. According to [13] $v(x)$ is a code polynomial of the binary cyclic product code of V_{n_2} and $V_{n_1}^{(E)}$, where $V_{n_1}^{(E)}$ is the binary cyclic code of length n_1 generated by $(x+1)g_1(x)$, $g_1(x)$ is the generator of V_{n_1}. Hence, by the Elias bound [9] for cyclic product codes we obtain $d_{even} \geq d_{1even}\, d_2$. In conclusion

$d_{even} \geq \min(d_{1odd}\, d_{2even}, d_{1even}\, d_2) = \min(d_1\, d_{2even}, d_{1even}\, d_2)$.

Now we will show that if $w(v_1(x)) = w_1$ is the Hamming weight of $v_1(x)$, a nonzero code polynomial of V_{n_1} and $w(v_2(x)) = w_2$ is the Hamming weight of $v_2(x)$, a nonzero code polynomial of V_{n_2}, then there exists a code polynomial $v(x)$ of V_n such that $w(v(x)) = w_1w_2$. Let

$$v_1(x) = 1 + \sum_{i=1}^{w_1-1} x^{k_i},\ 0 < k_i < n_1 ,$$

$$v_2(x) = 1 + \sum_{j=1}^{w_2-1} x^{\ell_j},\ 0 < \ell_j < n_2 ,$$

$$M_1 = \{0,k_1,k_2,\ldots,k_{w_1-1}\} \text{ and } M_2 = \{0,\ell_1,\ell_2,\ldots,\ell_{w_2-1}\}.$$

Now we construct the following polynomial

$$\hat{v}(x) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a_{\rho(i,j)}\, x^{\rho(i,j)}$$

such that $a_{\rho(i,j)} = 1$ if $i \in M_1$ and $j \in M_2$, otherwise $a_{\rho(i,j)} = 0$. Hence $w(\hat{v}(x)) = w_1w_2$. Associated with the polynomial $\hat{v}(x)$ we have

$$\hat{V}(y,z) = \sum_{j=0}^{n_2-1} \hat{V}_j(y) z^j ,$$

where

$$\hat{V}_j(y) = \sum_{i=0}^{n_1-1} a_{\rho(i,j)} y^i .$$

In this case we have

$$\hat{V}_0(y) = \hat{V}_{\ell_1}(y) = \ldots. = \hat{V}_{\ell_{w_2-1}}(y) = 1 + \sum_{i=1}^{w_1-1} y^{k_i}$$

and $\hat{V}_j(y) \equiv 0$ for $j \notin M_2$ and $0 < j < n_2$. Hence

$$\hat{V}(y,z) = (1 + \sum_{i=1}^{w_1-1} y^{k_i})(1 + \sum_{j=1}^{w_2-1} z^{\ell_j})$$

and

$$\hat{v}(\beta^{\rho(\theta,\phi)}) = \hat{V}(\alpha^\theta,\gamma^\phi) = (1 + \sum_{i=1}^{w_1-1} \alpha^{\theta k_i})(1 + \sum_{j=1}^{w_2-1} \gamma^{\phi\ell_j}) .$$

Thus, $\hat{v}(\beta^{\rho(\theta,\phi)}) = 0$ for $\theta \in S_1$ and $\phi = 0,1,\ldots,n_2-1$; and for $\phi \in S_2$ and $\theta = 0,1,\ldots,n_1-1$. According to [13] $\hat{v}(x)$ is a code polynomial of V_n. Hence $d_{odd} \leq d_{1odd}\, d_{2odd}$ and $d_{even} \leq \min(d_{1even}\, d_2, d_1\, d_{2even})$.

Q.E.D.

Example 2: As an example of application of Theorem 2 let us consider the (105,44) binary cyclic product code of the (7,4) and the (15,11) binary cyclic codes. In this example $d_{1odd} = 3$, $d_{1even} = 4$, $d_{2odd} = 3$ and $d_{2even} = 4$. Thus, by Theorem 2 $d_{odd} = 9$ and $d_{even} = 12$. The BCH bound gives $d_{odd} \geq 7$ and $d_{even} \geq 10$.

In order to avoid proving special cases of the following theorems, we define the following three quantities to be infinity: the minimum distance of the (n,0) code, the minimum weight of even-weight code vectors of the binary cyclic (n,1) code and the minimum weight of odd-weight code vectors of the binary cyclic codes which have 1 as roots of their generator polynomial.

The binary cyclic product code of V_{n_1} and V_{n_2}, where V_{n_1} is the (n_1,n_1) binary cyclic code will be called the one-dimensional product code of V_{n_2}. A lower bound on the minimum distance of a subcode of a one-dimensional product code can now be derived.

Let V_n be a subcode of the one-dimensional product code of V_{n_2}, generated by g(x) such that $g(1) \neq 0$. Let $\bar{J}_0 = \{\theta | g(\beta^{\rho(\theta,0)}) = 0\}$, $J_0 = \{\phi | g(\beta^{\rho(0,\phi)}) = 0\}$ and $S_2 = \{\phi | g(\beta^{\rho(\theta,\phi)}) = 0$ for $\theta = 0,1,\ldots,n_1-1\}$. According to [13], V_{n_2} is generated by $g_2(x) = \prod_{\phi \in S_2} (x+\gamma^{\phi})$. Now we define V_{n_1} to be the binary cyclic code of length n_1 generated by $g_1(x) = \prod_{\theta\varepsilon\bar{J}_0} (x+\alpha^\theta)$* and $V_{n_2}^{(0)}$ to be the binary cyclic code generated by $g_2^{(0)} = \prod_{\phi\varepsilon J_0} (x+\gamma^\phi)$. Finally we let $d_{2odd}^{(0)}$, $d_{2even}^{(0)}$ to be the minimum weight of odd-weight and of even-weight code vectors of $V_{n_2}^{(0)}$, respectively. Now we are in the position to prove the following theorem:

<u>Theorem 3</u>: $d_{odd} \geq \max(d_{1odd}\, d_{2odd},\, d_{2odd}^{(0)})$ and

$d_{even} \geq \min(d_{2even}^{(0)},\, 2d_{2even},\, d_{1even}\, d_{2odd})$.

<u>Proof</u>: Let v(x) be a nonzero code polynomial of V_n. Thus

$$v(\beta^{\rho(\theta,\phi)}) = \sum_{i=0}^{n_1-1} \bar{V}_i(\gamma^\phi)\alpha^{i\theta} = 0$$

for $\phi \varepsilon S_2$ and $\theta = 0,1,\ldots,n_1-1$. So, by Lemma 2 $\bar{V}_i(\gamma^\phi) = 0$ for $\phi \varepsilon S_2$. Hence, $\bar{V}_i(z)$ is a code polynomial of V_{n_2} [13]. Let

$$v_1(y) = \sum_{i=0}^{n_1-1} \bar{V}_i(1)y^i \quad .$$

We note that $v_1(y)$ is a code polynomial of V_{n_1}. If v(x) has odd weight, then, similar to the proof of Theorem 2, we obtain $d_{odd} \geq d_{1odd}\, d_{2odd}$. By [14, Theorem 3] $d_{odd} \geq d_{2odd}^{(0)}$. Hence $d_{odd} \geq \max(d_{1odd}\, d_{2odd},\, d_{2odd}^{(0)})$. If v(x) has even weight, then we

*If $\bar{J}_0$ is empty, then $g_1(x) = 1$.

consider two cases. $\bar{V}_i(1) \neq 0$ for some i, $0 \leq i < n_1$ and $\bar{V}_i(1) = 0$ for $i = 0,1,\ldots,n_1-1$. If $\bar{V}_i(1) \neq 0$ for some i, $0 \leq i < n_1$, then as in the proof of Theorem 2, we obtain $d_{even} \geq d_{1even}\, d_{2odd}$. Similarly, if $\bar{V}_i(1) = 0$ for $i = 0,1,\ldots,n_1-1$ then $x^{n_1} + 1$ divides $v(x)$. Thus, by [13] $v(x)$ is a code polynomial of the binary cyclic one-dimensional product code of $V_{n_2}^{(E)}$, where $V_{n_2}^{(E)}$ is the binary cyclic code of length n_2 generated by $(x+1)g_2(x)$, and $g_2(x)$ is the generator of V_{n_2}. For this $v(x)$ we can also write

$$v(\beta^{\rho(0,\phi)}) = v(\gamma^{\phi}) = \sum_{j=0}^{n_2-1} V_j(1)\gamma^{j\phi} = 0 \text{ for}$$

$\phi \in J_0 \cup \{0\}$. Let us define

$$v_2(z) = \sum_{j=0}^{n_2-1} V_j(1) z^j .$$

Thus, $v_2(z)$ is code polynomial of even weight of $V_{n_2}^{(0)}$. Now if $V_j(1) \neq 0$ for some j, $0 \leq j < n_2$, then $d_{even} \geq d_{2even}^{(0)}$. If $V_j(1) = 0$ for $j = 0,1,\ldots,n_2-1$, then $x^{n_2} + 1$ divides $v(x)$ and, by [13], $v(x)$ is a code polynomial of the binary cyclic product code of V'_{n_1}, the binary cyclic code of length n_1 generated by $g'_1(x) = (x+1)$, and $V_{n_2}^{(E)}$, the binary cyclic code of length n_2 generated by $(x+1)g_2(x)$. Thus $d_{even} \geq 2d_{2even}$. Hence

$$d_{even} \geq \min(d_{2even}^{(0)},\, 2d_{2even},\, d_{1even}\, d_{2odd}) .$$

Q.E.D.

<u>Example 3</u>: As an application of Theorem 3 let us consider the (21,7) binary cyclic code generated by $g(x) = m_1(x)m_3(x)m_7(x)m_9(x)$.

For this case $n_1 = 3$, $n_2 = 7$, $\bar{J}_0 = \{1,2\}$, $J_0 = \{1,2,3,4,5,6\}$ and $S_2 = \{1,2,4\}$. Thus, V_{n_2} is a (7,4) binary cyclic code, $V_{n_2}^{(0)}$ is the (7,1) binary cyclic code. Since $d_{1odd} = 3$, $d_{1even} = \infty$, $d_{2odd} = 3$, $d_{2even} = 4$, $d_{2odd}^{(0)} = 7$ and $d_{2\ even}^{(0)} = \infty$, by Theorem 3 $d_{odd} \geq 9$ and $d_{even} \geq 8$. The BCH bound gives $d_{odd} \geq 5$ and $d_{even} \geq 6$.

Now we will investigate the weight structure of a class of binary cyclic codes which will be called the class of binary cyclic quasi-product codes. These codes are defined in the following manner: consider the binary cyclic product code of V_{n_1}, with $d_1 \geq 2$ and $g_1(1) \neq 0$, and V_{n_2}, with $d_2 \geq 2$ and $g_2(1) \neq 0$, generated by $g(x)$, such that $d_1 d_2 > 4$. Let $\bar{g}(x) = GCD(g(x), (x^{n_1}+1)(x^{n_2}+1))$. The binary cyclic code of length n generated by $g'(x) = (g(x)/\bar{g}(x))$ is defined to be the binary cyclic quasi-product code of V_{n_1} and V_{n_2}. That is, if $S_1 = \{\theta | g(\beta^{\rho(\theta,\phi)}) = 0 \text{ for } \phi = 0,1,\ldots,n_2-1\}$ and $S_2 = \{\phi | g(\beta^{\rho(\theta,\phi)}) = 0 \text{ for } \theta = 0,1,\ldots,n_1-1\}$, then $g'(\beta^{\rho(\theta,\phi)}) = 0$ for $\theta \in S_1$ and $\phi = 1,2,\ldots,n_2-1$, and $g'(\beta^{\rho(\theta,\phi)}) = 0$ for $\phi \in S_2$ and $\theta = 1,2,\ldots,n_1-1$.

We are now in the position to prove the following theorem.

<u>Theorem 4</u>: Let V_n be the binary cyclic quasi-product code of V_{n_1} and V_{n_2}. Then

$$d_{odd} = \min(n_1, n_2, d_{1odd}\, d_{2odd})$$

and

$$d_{even} = \min(2n_1, 2n_2, d_{1even} d_2, d_1 d_{2even}, n_2 + (d_{1odd}-2) d_{2odd}, n_1 + (d_{2odd}-2) \times d_{1odd}) .$$

Proof: Let

$$v(x) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a_{\rho(i,j)} x^{\rho(i,j)}$$

be a nonzero code polynomial of V_n. Hence

$$v(\beta^{\rho(\theta,\phi)}) = \sum_{j=0}^{n_2-1} V_j(\alpha^\theta)\gamma^{j\phi}, \text{ where } V_j(y) = \sum_{i=0}^{n_1-1} a_{\rho(i,j)} y^i .$$

Since $v(\beta^{\rho(\theta,0)})$, $\theta \varepsilon S_1$, can be zero or nonzero and since $v(\beta^{\rho(0,\phi)})$, $\phi \varepsilon S_2$, can be zero or nonzero, we must inspect several cases.

Case 1. In this case we consider the possibility of having $v(\beta^{\rho(\theta,0)}) = 0$ for $\theta \varepsilon S_1$ and $v(\beta^{\rho(0,\phi)}) = 0$ for $\phi \varepsilon S_2$. Hence, $v(\beta^{\rho(\theta,\phi)}) = 0$ for $\theta \varepsilon S_1$ and $\phi = 0,1,\ldots,n_2-1$ and $v(\beta^{\rho(\theta,\phi)}) = 0$ for $\phi \varepsilon S_2$ and $\theta = 0,1,\ldots,n_1-1$. This implies that v(x) is a code polynomial of the binary cyclic product code of V_{n_1} and V_{n_2} [13]. Thus, by Theorem 2, $d_{odd} = d_{1odd}\, d_{2odd}$ and $d_{even} = \min(d_{1even}\, d_2, d_1\, d_{2even})$.

Case 2. In this case we consider the possibility of having $v(\beta^{\rho(\theta,0)}) \neq 0$ for $\theta \varepsilon S_1$ and $v(\beta^{\rho(0,\phi)}) = 0$ for $\phi \varepsilon S_2$. Hence, $v(\beta^{\rho(\theta,\phi)}) = 0$ for $\phi \varepsilon S_2$ and $\theta = 0,1,\ldots,n_1-1$. Let us define

$$v_2^{(\theta)}(z) = \sum_{j=0}^{n_2-1} V_j(\alpha^\theta) z^j .$$

Thus, $v_2^{(\theta)}(\gamma^\phi) = 0$ for $\theta \varepsilon S_1$ and $\phi = 1,2,\ldots,n_2-1$. This implies that for $\theta \varepsilon S_1$, $v_2^{(\theta)}(z)$ is divisible by $z^{n_2-1} + z^{n_2-2} +\ldots+ z+1$. Hence, for $\theta \varepsilon S_1$, $v_2^{(\theta)}(z) = V_j(\alpha^\theta)\ (\sum_{j=0}^{n_2-1} z^j)$. Since

$v_2^{(\theta)}(1) = v(\beta^{\rho(\theta,0)}) \neq 0$ for $\theta \in S_1$ we can conclude that

$$V_0(\alpha^\theta) = V_1(\alpha^\theta) = \ldots = V_{n_2-1}(\alpha^\theta) \neq 0 \tag{1}$$

for $\theta \in S_1$. So, the Hamming weight of $V_j(y)$, $w(V_j(y))$, is at least one for $j = 0,1,\ldots,n_2-1$. Hence $w(v(x)) \geq n_2$, which implies that $d_{odd} \geq n_2$ and $d_{even} \geq n_2+1$. Now let us obtain a better bound for d_{even}, for this we assume that $v(x)$ has even weight. Thus $w(v(x)) \geq n_2+1$. Furthermore let us assume that $v(x)$ is a code polynomial such that there exists at least one j, $0 \leq j < n_2$, satisfying $w(V_j(y)) = 1$. Because of the cyclic property we can, without loss of generality, assume that $V_0(y) = 1$. Thus, by Equation 1

$$V_0(\alpha^\theta) = V_1(\alpha^\theta) = \ldots = V_{n_2-1}(\alpha^\theta) = 1$$

for $\theta \in S_1$. Now based on the code polynomial $v(x)$ we construct the following polynomial:

$$v'(x) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a'_{\rho(i,j)} x^{\rho(i,j)}$$

where $a'_{\rho(i,j)} = a_{\rho(i,j)}$ for $i = 1,2,\ldots,n_1-1$ and $j = 0,1,\ldots,n_2-1$ $a'_{\rho(0,j)} = a_{\rho(0,j)} + 1$ for $j = 0,1,\ldots,n_2-1$. Associated with the polynomial $v'(x)$, polynomials $V'(y,z)$, $V'_j(y)$ and $\bar{V}'_i(z)$ are defined as follows:

$$V'(y,z) = \sum_{j=0}^{n_2-1} V'_j(y) z^j = \sum_{i=0}^{n_1-1} \bar{V}'_i(z) y^i$$

where $V'_j(y) = \sum_{i=0}^{n_1-1} a'_{\rho(i,j)} y^i$ and $\bar{V}'_i(z) = \sum_{j=0}^{n_2-1} a'_{\rho(i,j)} z^j$.

Thus

$$V'(y,z) = \sum_{j=0}^{n_2-1} (V_j(y)+1) z^j$$

and $v'(\beta^{\rho(\theta,\phi)}) = V'(\alpha^{\theta},\gamma^{\phi})$. This implies that

$$V'(\alpha^{\theta},\gamma^{\phi}) = \sum_{j=0}^{n_2-1} (V_j(\alpha^{\theta})+1)\gamma^{j\phi} .$$

Hence, $v'(\beta^{\rho(\theta,\phi)}) = 0$ for $\theta \in S_1$ and $\phi = 0,1,\ldots,n_2-1$. In addition

$$V'(\alpha^{\theta},\gamma^{\phi}) = \sum_{j=0}^{n_2-1} V_j(\alpha^{\theta})\gamma^{j\phi} + \sum_{j=0}^{n_2-1} \gamma^{j\phi} = \sum_{i=0}^{n_1-1} \bar{V}_i(\gamma^{\phi})\alpha^{i\theta} + \frac{\gamma^{n_2\phi}+1}{\gamma^{\phi}+1} .$$

Thus for $\phi \neq 0$ we have

$$v'(\beta^{\rho(\theta,\phi)}) = \sum_{i=0}^{n_1-1} \bar{V}_i(\gamma^{\phi})\alpha^{i\theta}.$$

Now, since $v(\beta^{\rho(\theta,\phi)}) = 0$ for $\phi \in S_2$ and $\theta = 0,1,\ldots,n_1-1$, by Lemma 2, $\bar{V}_i(\gamma^{\phi}) = 0$ for $\phi \in S_2$ and $i = 0,1,\ldots,n_1-1$. Hence, since $0 \notin S_2$ because $g_2(1) \neq 0$, we can conclude that $v'(\beta^{\rho(\theta,\phi)}) = 0$ for $\phi \in S_2$ and $\theta = 0,1,\ldots,n_1-1$. By [13] $v'(x)$ is a code polynomial of the binary cyclic product code of V_{n_1} and V_{n_2}. $v'(x)$ has odd weight because $v(x)$ has even weight. Now we investigate the $w(v'(x))$. Similar to the proof of Theorem 2 we can conclude that $V_j'(y)$ is a code polynomial of V_{n_1} for $j = 0,1,\ldots,n_2-1$ and that

$v_2'(z) = \sum_{j=0}^{n_2-1} V_j'(1)z^j$ is a code polynomial of V_{n_2}. Since $v'(x)$ has odd weight, there exists at least one j, $0 \leq j < n_2$, such that $V_j'(1) \neq 0$. This implies that we must have $V_{j_\ell}'(1) \neq 0$ for $\ell = 1,2,\ldots,r$, with $d_{2odd} \leq r \leq n_2$ and r odd. Let us assume that $V_{j_\ell}'(1) = 0$, with $V_{j_\ell}'(y) \neq 0$, for $\ell = r+1, r+2,\ldots,r+s$, with

$r \leq r + s \leq n_2$. Since $V_j'(y)$ is a code polynomial of V_{n_1}, $w(v'(x)) \geq r\, d_{1odd} + s\, d_{1even}$. Since $v(x) = v'(x) + 1 + x^{n_1} + x^{2n_1} + \ldots + x^{(n_2-1)n_1}$, then, for a given $w(v'(x))$, the minimum weight of $v(x)$ is going to be achieved when $w(\bar{V}_0'(z))$ is maximum. $w(\bar{V}_0'(z))$ is maximum when for each $V_j'(y) \not\equiv 0$ we have $a'_{\rho(0,j)} = 1$. Now the number of j such that $V_j'(y) \not\equiv 0$ is r+s. Thus
$w(v(x)) \geq r(d_{1odd}-1) + s(d_{1even}-1) + n_2 - (r+s) =$
$= r(d_{1odd}-2) + s(d_{1even}-2) + n_2$. Since $d_{1odd} \geq 3$, $d_{1even} \geq 2$, $r \geq d_{2odd}$ and $s \geq 0$, the minimum is achieved for $r = d_{2odd}$ and $s = 0$. Thus for this case we have shown that $d_{odd} \geq n_2$ and $d_{even} \geq \min(n_2 + (d_{1odd}-2)\, d_{2odd}, 2n_2)$. Now we will show the existence of v(x) with Hamming weights n_2, $2n_2$ and $n_2 + d_{2odd}(d_{1odd}-2)$. At first consider $\hat{v}(x) = 1 + x^{n_1} + x^{2n_1} + \ldots + x^{(n_2-1)n_1}$. Let us show that $\hat{v}(x)$ is a code polynomial of V_n of weight n_2. Now $\hat{v}(\beta^{\rho(\theta,\phi)}) = \frac{\gamma^{\phi n}+1}{\gamma^{\phi n_1}+1}$. Since $GCD(n_1,n_2) = 1$ and $0 \leq \phi < n_2$, $\gamma^{\phi n_1}+1 = 0$ if and only if $\phi = 0$. Thus, $\hat{v}(\beta^{\rho(\theta,\phi)}) = 0$ for $\theta = 0,1,\ldots,n_1-1$ and $\phi = 1,2,\ldots,n_2-1$ which implies that $\hat{v}(x)$ is a code polynomial of V_n. Now we consider the following polynomial of weight $2n_2$: $\hat{\text{v}}(x) = (1+x^{n_1} + \ldots + x^{(n_2-1)n_1})(1+x)$. By a similar procedure we can show that $\hat{\text{v}}(x)$ is a code polynomial of V_n. To prove the existence of a code polynomial of weight $n_2+(d_{1odd}-2)d_{2odd}$ we will show that if $w(v_1(x)) = w_1$, where $v_1(x)$ is a nonzero code polynomial of V_{n_1}, and $w(v_2(x)) = w_2$, where $v_2(x)$ is a nonzero code

polynomial of V_{n_2}, then there is a code polynomial of V_n with weight $n_2 + (w_1-2)w_2$. Let

$$v_1(x) = 1 + \sum_{i=1}^{w_1-1} x^{k_i},\ 0 < k_i < n_1$$

$$v_2(x) = 1 + \sum_{j=1}^{w_2-1} x^{\ell_j},\ 0 < \ell_j < n_2,$$

$M_1 = \{0,k_1,k_2,\ldots,k_{w_1-1}\}$ and $M_2 = \{0,\ell_1,\ell_2,\ldots,\ell_{w_2-1}\}$. Now we construct the following polynomial.

$$\hat{v}(x) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a_{\rho(i,j)} x^{\rho(i,j)} + \sum_{k=0}^{n_2-1} x^{kn_1}$$

such that $a_{\rho(i,j)} = 1$ if $i \varepsilon M_1$ and $j \varepsilon M_2$ otherwise $a_{\rho(i,j)} = 0$. Hence $w(\hat{v}(x)) = n_2 + (w_1-2)w_2$. Now

$$\hat{v}(\beta^{\rho(\theta,\phi)}) = \tilde{v}(\beta^{\rho(\theta,\phi)}) + \frac{\gamma^{\phi n}+1}{\gamma^{\phi n_1}+1},\text{ where } \tilde{v}(x) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a_{\rho(i,j)} x^{\rho(i,j)}.$$

As shown in the proof of Theorem 2 we can conclude that $\tilde{v}(\beta^{\rho(\theta,\phi)}) = 0$ for $\theta \varepsilon S_1$ and $\phi = 0,1,\ldots,n_2-1$; and for $\phi \varepsilon S_2$ and $\theta = 0,1,\ldots,n_1-1$. We also know that $\frac{\gamma^{\phi n}+1}{\gamma^{\phi n_1}+1} = 0$ for $\phi = 1,2,\ldots,n_2-1$. Thus, since $0 \not\varepsilon S_2$, we can conclude that $\hat{v}(\beta^{\rho(\theta,\phi)}) = 0$ for $\theta \varepsilon S_1$ and $\phi = 1,2,\ldots,n_2-1$; and $\hat{v}(\beta^{\rho(\theta,\phi)}) = 0$ for $\phi \varepsilon S_2$ and $\theta = 0,1,\ldots,n_1-1$. Thus $\hat{v}(x)$ is a code polynomial of V_n. We have shown for this case that $d_{odd} = n_2$ and $d_{even} = \min(2n_2,\ n_2 + (d_{1odd}-2)d_{2odd})$.

Case 3. In this case we consider the possibility of having $v(\beta^{\rho(\theta,0)}) = 0$ for $\theta \in S_{11}$ and $v(\beta^{\rho(\theta,0)}) \neq 0$ for $\theta \in S_{12}$, where S_{11} and S_{12} form a partition of S_1. By the same argument used in the analysis of the previous two cases we can conclude that $V_j(\alpha^\theta) = 0$ for $\theta \in S_{11}$ and $j = 0,1,\ldots,n_2-1$ and $V_0(\alpha^\theta) = V_1(\alpha^\theta) = \ldots = V_{n_2-1}(\alpha^\theta) \neq 0$ for $\theta \in S_{12}$. Hence $w(v(x)) \geq 2n_2$.

Case 4. In this case we consider the possibility of having $v(\beta^{\rho(\theta,0)}) = 0$ for $\theta \in S_1$ and $v(\beta^{\rho(0,\phi)}) \neq 0$ for $\phi \in S_2$. As proved in Case 2 we can show that $d_{odd} = n_1$ and $d_{even} = \min(2n_1, n_1 + (d_{2odd}-2)d_{1odd})$.

Case 5. In this case we consider the possibility of having $v(\beta^{\rho(0,\phi)}) = 0$ for $\phi \in S_{21}$ and $v(\beta^{\rho(0,\phi)}) \neq 0$ for $\phi \in S_{22}$, where S_{21} and S_{22} form a partition of S_2. As proved in Case 3 we can show that $w(v(x)) \geq 2n_1$.

Case 6. At last we consider the possibility of having $v(\beta^{\rho(\theta,0)}) \neq 0$ for $\theta \in S_1$ and $v(\beta^{\rho(0,\phi)}) \neq 0$ for $\phi \in S_2$. As proved in Case 2 we can show that

$$V_0(\alpha^\theta) = V_1(\alpha^\theta) = \ldots = V_{n_2-1}(\alpha^\theta) \neq 0 \qquad (2)$$

for $\theta \in S_1$, and

$$\bar{V}_0(\gamma^\phi) = \bar{V}_1(\gamma^\phi) = \ldots = \bar{V}_{n_1-1}(\gamma^\phi) \neq 0 \qquad (3)$$

for $\phi \in S_2$. Hence, $w(v(x)) \geq \max(n_1,n_2)$, which implies that $d_{odd} \geq \max(n_1,n_2)$ and $d_{even} \geq \max(n_1,n_2)+1$. Now let us obtain a better bound for d_{even}, for this we assume that $v(x)$ is a code polynomial of even weight such that there exists at least one j,

$0 \le j < n_2$, satisfying $w(V_j(y)) = 1$; and also there exists at least one i, $0 \le i < n_1$, satisfying $w(\bar{V}_i(z)) = 1$. Because of the cyclic property we can, without loss of generality assume that $V_0(y) = 1$. Thus, by Equation 2

$$V_0(\alpha^\theta) = V_1(\alpha^\theta) = \ldots = V_{n_2-1}(\alpha^\theta) = 1 \tag{4}$$

for $\theta \in S_1$ and by Equation 3

$$\bar{V}_0(\gamma^\phi) = \bar{V}_1(\gamma^\phi) = \ldots = \bar{V}_{n_1-1}(\gamma^\phi) = \gamma^{\phi j_2},\ 0 \le j_2 < n_2, \tag{5}$$

for $\phi \in S_2$. Now, based on the code polynomial v(x) we construct the following polynomial

$$v'(x) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a'_{\rho(i,j)} x^{\rho(i,j)}$$

where $a'_{\rho(0,j)} = a_{\rho(0,j)} + 1$ for $j = 0,1,\ldots,j_2-1,\ j_2+1,\ldots,n_2-1$; $a'_{\rho(i,j_2)} = a_{\rho(i,j_2)} + 1$ for $i = 1,2,\ldots,n_1-1$; $a'_{\rho(0,j_2)} = a_{\rho(0,j_2)}$ and $a'_{\rho(i,j)} = a_{\rho(i,j)}$ for $i = 1,2,\ldots,n_1-1$ and $j = 0,1,\ldots,j_2-1$, $j_2 + 1,\ldots,n_2 - 1$. Associated with the polynomial $v'(x)$, polynomials $V'(y,z)$, $V'_j(y)$ and $\bar{V}'_i(z)$ are defined as follows:

$$V'(y,z) = \sum_{j=0}^{n_2-1} V'_j(y) z^j = \sum_{i=0}^{n_1-1} \bar{V}'_i(z) y^i$$

where $V'_j(y) = \sum_{i=0}^{n_1-1} a'_{\rho(i,j)} y^i$ and $\bar{V}'_i(z) = \sum_{j=0}^{n_2-1} a'_{\rho(i,j)} z^j$.

Thus,

$$v'(\beta^{\rho(\theta,\phi)}) = V'(\alpha^\theta, \gamma^\phi)$$

and

$$V'(y,z) = \sum_{\substack{j=0\\ j\neq j_2}}^{n_2-1} (V_j(y)+1)z^j + (V_{j_2}(y)+y+y^2+\ldots+y^{n_1-1})z^{j_2}$$

$$= \sum_{i=1}^{n_1-1} (\bar{V}_1(z)+z^{j_2})y^i + (\bar{V}_0(z)+1+z+\ldots+z^{j_2-1}+z^{j_2+1}+\ldots+z^{n_2-1}) .$$

Hence,

$$v'(\beta^{\rho(\theta,\phi)}) = \sum_{\substack{j=0\\ j\neq j_2}}^{n_2-1} (V_j(\alpha^\theta)+1)\gamma^{j\phi}(V_{j_2}(\alpha^\theta)+\alpha^\theta+\alpha^{2\theta}+\ldots+\alpha^{(n_1-1)\theta})\gamma^{\phi j_2} .$$

But for $\theta \neq 0$ $\alpha^\theta + \alpha^{2\theta} + \ldots + \alpha^{(n_1-1)\theta} = 1$, which implies

$v'(\beta^{\rho(\theta,\phi)}) = \sum_{j=0}^{n_2-1} (V_j(\alpha^\theta)+1)\gamma^{j\phi}$ for $\theta \neq 0$. Since $0 \notin S_1$ because $g_1(1) \neq 0$, we conclude, by Equation 4, that $v'(\beta^{\rho(\theta,\phi)}) = 0$ for $\theta \in S_1$ and $\phi = 0,1,\ldots,n_2-1$. We also know that

$$v'(\beta^{\rho(\theta,\phi)}) = \sum_{i=1}^{n_1-1} (\bar{V}_i(\gamma^\phi) + \gamma^{\phi j_2})\alpha^{i\theta} +$$

$$(\bar{V}_0(\gamma^\phi)+1+\gamma^\phi+\ldots+\gamma^{(j_2-1)\phi}+\gamma^{(j_2+1)\phi}+\ldots+\gamma^{(n_2-1)\phi}) .$$

Thus, by a similar procedure we can show that $v'(\beta^{\rho(\theta,\phi)}) = 0$ for $\phi \in S_2$ and $\theta = 0,1,\ldots,n_1-1$. So, by [13] $v'(x)$ is a code polynomial of the binary product code of V_{n_1} and V_{n_2}. $v'(x)$ has even weight because $v(x)$ has even weight and $v(x) = v'(x) + \sum_{\substack{j=0\\ j\neq j_2}}^{n_2-1} x^{\rho(0,j)} + \sum_{i=1}^{n_1-1} x^{\rho(i,j_2)}$. If $v'(x) \equiv 0$, then $w(v(x)) = n_1 + n_2 - 2$.

If $v'(x) \not\equiv 0$, then we must consider two cases: $a'_{\rho(0,j_2)} = 0$ and $a'_{\rho(0,j_2)} = 1$. At first let us assume $a'_{\rho(0,j_2)} = 0$. Now if $w(\bar{V}'_0(z)) = w(V'_{j_2}(y)) = 0$, then $w(v(x)) \geq n_1+n_2-2+d_1d_2 > n_1+n_2-2$. If $w(\bar{V}'_0(z)) = 0$ and $w(V'_{j_2}(y)) = w_1$, then there exists i_k, $0 < i_k < n_1$, $k = 1,2,\ldots,w_1$, such that $w(\bar{V}'_{i_k}(z)) \geq d_2$. Thus, $w(v(x)) \geq n_2-1+w_1(d_2-1)+n_1-1-w_1 \geq n_1+n_2-2+d_1(d_2-2) \geq n_1+n_2-2$. Similarly, if $w(\bar{V}'_0(z)) = w_2$ and $w(V'_{j_2}(y)) = 0$, then $w(v(x)) \geq n_1+n_2-2+d_2(d_1-2) \geq n_1+n_2-2$. If $w(\bar{V}'_0(z)) = w_2$ and $w(v'_{j_2}(y)) = w_1$, then there exists i_k, $0 < i_k < n_1$, $k = 1,2,\ldots,w_1$, such that $w(\bar{V}'_{i_k}(z)) \geq d_2$ and also there exists j_ℓ, $0 \leq j_\ell < n_2$, $\ell = 1,3,4,\ldots,w_2+1$, such that $w(V'_{j_\ell}(y)) \geq d_1$. Thus, $w(v'(x)) \geq w_1d_2+w_2+(w_2-(d_2-1))(d_1-1) = w_1d_2+w_2d_1-(d_2-1)(d_1-1)$. Hence $w(v(x)) \geq n_1+n_2-2+w_1(d_2-2)+w_2(d_1-2)-(d_2-1)(d_1-1) \geq n_1+n_2-2+d_1(d_2-2)+d_2(d_1-2)-(d_2-1)(d_1-1) = n_1+n_2-2+(d_2-1)(d_1-1)-2 \geq n_1+n_2-2, (d_1d_2 > 4)$. At last we assume $a'_{\rho(0,j_2)} = 1$. Thus, we have only to inspect the case $w(\bar{V}'_0(z)) = w_2$ and $w(V'_{j_2}(y)) = w_1$. So, $w(v'(x)) \geq w_1d_2+(w_2-d_2)d_1 = w_1d_2+w_2d_1-d_2d_1$. Hence, $w(v(x)) \geq n_1+n_2-2+w_1(d_2-2)+w_2(d_1-2)-d_2d_1+4 \geq n_1+n_2-2+d_1(d_2-2)+d_2(d_1-2)-d_2d_1+4 = n_1+n_2-2+(d_1-2)(d_2-2) \geq n_1+n_2-2$. Since $n_1+n_2-2 \geq \min(2n_1,2n_2)$, we can conclude that for Case 6 $d_{even} \geq \min(2n_1,2n_2)$. This completes the proof of Theorem 4.

Q.E.D.

Example 4: As an application of Theorem 4 let us consider the

(119,47) binary quasi-product code generated by $g(x) = m_1(x)m_{11}(x)m_{13}(x)$. In this case $n_1 = 7$, $n_2 = 17$, $S_1 = \{1,2,4\}$ and $S_2 = \{1,2,4,8,9,13,15,16\}$. Hence, V_{n_1} is the (7,4) binary code with $d_{1odd} = 3$ and $d_{1even} = 4$; and V_{n_2} is the (17,9) binary code with $d_{2odd} = 5$ and $d_{2even} = 6$. Thus by Theorem 4, $d_{odd} = 7$ and $d_{even} = 14$. The BCH bound gives $d_{odd} \geq 7$ and $d_{even} \geq 10$.

Now we will investigate the weight structure of another class of binary cyclic codes which will be called the class of binary cyclic semi-quasi-product codes. These codes are defined in the following manner: consider the binary cyclic product code of V_{n_1}, with $g_1(1) \neq 0$, and V_{n_2}, with $d_2 \geq 2$, generated by $g(x)$. Let $\bar{g}(x) = GCD(g(x),(x^{n_2}+1))$. The binary cyclic code of length n generated by $g'(x) = (g(x)/\bar{g}(x))$ is defined to be the binary cyclic semi-quasi-product code of V_{n_1} and V_{n_2}. That is, if $S_1 = \{\theta | g(\beta^{\rho(\theta,\phi)}) = 0$ for $\phi = 0,1,\ldots,n_2-1\}$ and $S_2 = \{\phi | g(\beta^{\rho(\theta,\phi)}) = 0$ for $\theta = 0,1,\ldots,n_1-1\}$, then $g'(\beta^{\rho(\theta,\phi)}) = 0$ for $\theta \in S_1$ and $\phi = 0,1,\ldots,n_2-1$ and $g'(\beta^{\rho(\theta,\phi)}) = 0$ for $\phi \in S_2$ and $\theta = 1,2,\ldots,n_1-1$.

We are now in the position to prove the following theorem:

<u>Theorem 5</u>: Let V_n be the binary cyclic semi-quasi-product code of V_{n_1} and V_{n_2}. Then

$$d_{odd} = \min(n_1, d_{1odd}\, d_{2odd})$$

and

$$d_{even} = \min(2n_1, d_1 d_{2even}, d_{1even} d_2, n_1 + (d_{2odd}-2)d_{1odd})$$

Proof: Let

$$v(x) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a_{\rho(i,j)} x^{\rho(i,j)}$$

be a nonzero code polynomial of V_n. Since $v(\beta^{\rho(0,\phi)})$, $\phi \varepsilon S_2$, can be zero or nonzero, we must inspect 3 cases.

Case 1. In this case we consider the possibility of having $v(\beta^{\rho(0,\phi)}) = 0$ for $\phi \varepsilon S_2$. As proved in Case 1 of Theorem 4 we can conclude that $d_{odd} = d_{1odd}\, d_{2odd}$ and $d_{even} = \min(d_{1even} d_2, d_1 d_{2even})$.

Case 2. In this case we consider the possibility of having $v(\beta^{\rho(0,\phi)}) = 0$ for $\phi \varepsilon S_{21}$ and $v(\beta^{\rho(0,\phi)}) \neq 0$ for $\phi \varepsilon S_{22}$, where S_{21} and S_{22} are a partition of S_2. As proved in Case 3 of Theorem 4 we can conclude that $w(v(x)) \geq 2n_1$.

Case 3. In this case we consider the possibility of having $v(\beta^{\rho(0,\phi)}) \neq 0$ for $\phi \varepsilon S_2$. As proved in Case 2 of Theorem 4 we can conclude that $d_{odd} = n_1$ and $d_{even} = \min(2n_1, n_1 + (d_{2odd}-2) d_{1odd})$.

Q.E.D.

Let V_n be the binary cyclic semi-quasi-product code of V_{n_1} and V_{n_2}. If V_{n_1} is the (n_1, n_1) binary cyclic code we will call V_n the one-dimensional quasi-product code of V_{n_2}. The minimum distance of this class of codes is specified by the following corollary.

Corollary 1: Let V_n be the one-dimensional quasi-product code of V_{n_2}. Then

$$d_{odd} = \min(n_1,\ d_{2odd})$$

and

$$d_{even} = \min(2n_1, d_{2even}, n_1+d_{2odd}-2).$$

Example 5: As an application of Theorem 5 let us consider the (119,39) binary semi-quasi-product code generated by $g(x) = m_1(x)m_{11}(x)m_{13}(x)m_{21}(x)$. In this case $n_1 = 17$, $n_2 = 7$, $S_1 = \{1,2,4,8,9,13,15,16\}$ and $S_2 = \{1,2,4\}$. Hence, V_{n_1} is the (17,9) binary cyclic code, with $d_{1odd} = 5$ and $d_{1even} = 6$; and V_{n_2} is the (7,4) binary cyclic code, with $d_{2odd} = 3$ and $d_{2even} = 4$. Thus by Theorem 5, $d_{odd} = 15$ and $d_{even} = 18$. The BCH bound gives $d_{odd} \geq 13$ and $d_{even} \geq 14$.

At last we will derive a lower bound on the minimum distance of a subcode of a one-dimensional quasi-product code of V_{n_2}. Let V_n be a subcode of the one-dimensional quasi-product code of V_{n_2}, generated by $g(x)$ such that $g(1) \neq 0$. Let $\bar{J}_0 = \{\theta | g(\beta^{\rho(\theta,0)}) = 0\}$, $J_0 = \{\phi | g(\beta^{\rho(0,\phi)}) = 0\}$, $S_2 = \{\phi | g(\beta^{\rho(\theta,\phi)}) = 0$ for $\theta = 1,2,\ldots,n_1-1\}$, $N_2 = S_2 \cap J_0$ and $P_2 = S_2 \cup J_0$. Thus, by the definition of V_n, V_{n_2} is generated by $g_2(x) = \prod_{\phi\varepsilon S_2} (x+\gamma^{\phi})$. We define V_{n_1} to be the binary cyclic code of length n_1 generated by $g_1(x) = \prod_{\theta\varepsilon\bar{J}_0} (x+\alpha^{\theta})$*; $V_{n_2}^{(0)}$ to be the binary cyclic code of length n_2 generated by $g_2^{(0)}(x) = \prod_{\phi\varepsilon J_0} (x+\gamma^{\phi})$**;

*If $\bar{J}_0$ is empty, then $g_1(x) = 1$.

**If J_0 is empty, then $g_2^{(0)}(x) = 1$.

V'_{n_2} to be the binary cyclic code of length n_2 generated by $g'_2(x) = \prod_{\phi \varepsilon N_2} (x+\gamma^{\phi})$,* and V''_{n_2} to be the binary cyclic code of length n_2 generated by $g''_2(x) = \prod_{\phi \varepsilon P_2} (x+\gamma^{\phi})$. $d^{(0)}_{2odd}$ is defined as before. At last we let d'_{2odd} (d''_{2odd}), d'_{2even} (d''_{2even}) be the minimum weight of odd-weight, even-weight code vectors of V'_{n_2} (V''_{n_2}), respectively. Now we are in the position to prove the following theorem.

Theorem 6: Let $\bar{d}_{odd} = \max(d_{1odd}\, d_{2odd},\ d''_{2odd})$ and $\bar{d}_{even} = \min(d''_{2even},\ 2d_{2even},\ d_{1even}\, d_{2odd})$. If $d'_{2odd} > d'_{2even}$ then $d_{odd} \geq \min(\bar{d}_{odd},\ \max(n_1 d'_{2even} + (d'_{2odd} - d'_{2even})\, d_{1odd},\ d^{(0)}_{2odd}))$ and $d_{even} \geq \min(\bar{d}_{even},\ n_1 d'_{2even})$. If $d'_{2odd} < d'_{2even}$, then $d_{odd} \geq \min(\bar{d}_{odd},\ \max(n_1 d'_{2odd},\ d^{(0)}_{2odd}))$; $d_{even} \geq \min(\bar{d}_{even},\ n_1 d'_{2odd} + (d'_{2even} - d'_{2odd})\, d_{1odd})$ for N_2 nonempty and $d_{even} \geq \min(\bar{d}_{even}, 2n_1, n_1 + (d_{2odd}-2) d_{1odd})$ for N_2 empty.

Proof: Let $v(x)$ be a nonzero code polynomial of V_n. Thus

$$v(\beta^{\rho(\theta,\phi)}) = \sum_{i=0}^{n_1-1} \bar{V}_i(\gamma^{\phi})\alpha^{i\theta} = 0$$

for $\phi \varepsilon S_2$ and $\theta = 1,2,\ldots,n_1-1$. Since $v(\beta^{\rho(0,\phi)})$, $\phi \varepsilon S_2$, can be zero or nonzero we must inspect the following cases:

Case 1. In this case we consider the possibility of having $v(\beta^{\rho(0,\phi)}) = 0$ for $\phi \varepsilon S_2$. As proved in Theorem 3 we can conclude that $d_{odd} \geq \max(d_{1odd}\, d_{2odd},\ d''_{2odd})$ and $d_{even} \geq \min(d''_{2even},\ 2d_{2even},\ d_{1even}\, d_{2odd})$.

*If N_2 is empty, then $g'_2(x) = 1$.

Case 2. In this case we consider the possibility of having $v(\beta^{\rho(0,\phi)}) \neq 0$ for $\phi \in S_2'$, where $S_2' = S_2 - N_2$. Let

$$v_1^{(\phi)}(y) = \sum_{i=0}^{n_1-1} \bar{V}_i(\gamma^\phi)y^i .$$

Thus, $v_1^{(\phi)}(y) = 0$ for $\phi \in S_2$ and $\theta = 1,2,\ldots,n_1-1$. Hence $\bar{V}_0(\gamma^\phi) = \bar{V}_1(\gamma^\phi) = \ldots = \bar{V}_{n_1-1}(\gamma^\phi) \neq 0$ for $\phi \in S_2'$ and by Lemma 2 $\bar{V}_i(\gamma^\phi) = 0$ for $\phi \in N_2$, that is, $\bar{V}_i(z)$ is a nonzero code polynomial of V_{n_2}', $i = 0,1,\ldots,n_1-1$. We notice that if $w(v(x))$ is odd, then $v_1^{(0)}(y)$ has odd weight and if $w(v(x))$ is even, then $w(v_1^{(0)}(y))$ is even. Thus, if $\bar{V}_0(z) = \bar{V}_1(z) = \ldots = \bar{V}_{n_1-1}(z)$, then $d_{odd} \geq n_1 d_{2odd}'$ and $d_{even} \geq n_1 d_{2even}'$. If not all $\bar{V}_i(z)$,

$i = 0,1,\ldots,n_1-1$, are equal, then $d_{odd} \geq w_{1odd}\, d_{2odd}' + (n_1 - w_{1odd}) \times d_{2even}'$ and $d_{even} \geq w_{1even}\, d_{2odd}' + (n_1 - w_{1even})\, d_{2even}'$, where w_{1odd}, w_{1even} is the weight of an odd-weight, even-weight code word of V_{n_1}, respectively. Hence, $d_{odd} \geq n_1 d_{2even}' + (d_{2odd}' - d_{2even}') \times w_{1odd}$. If $d_{2odd}' > d_{2even}'$, then $d_{odd} \geq n_1 d_{2even}' + (d_{2odd}' - d_{2even}') \times d_{1odd}$. If $d_{2odd}' < d_{2even}'$, then $d_{odd} \geq n_1 d_{2odd}'$. For the even-weight code polynomials we obtain $d_{even} \geq n_1 d_{2even}' + (d_{2odd}' - d_{2even}')\, w_{1even}$. If $d_{2odd}' > d_{2even}'$, then $d_{even} \geq n_1 d_{2even}'$. If $d_{2odd}' < d_{2even}'$, then $d_{even} \geq n_1 d_{2even}' + (d_{2odd}' - d_{2even}') \times (n_1 - d_{1odd}) = n_1 d_{2odd}' + (d_{2even}' - d_{2odd}')\, d_{1odd}$. For this case we can conclude that if $d_{2odd}' > d_{2even}'$, then $d_{odd} \geq \max(n_1 d_{2even}' + (d_{2odd}' - d_{2even}')\, d_{1odd},\, d_{2odd}^{(0)})$ and $d_{even} \geq n_1 d_{2even}'$. Now if $d_{2odd}' < d_{2even}'$, then $d_{odd} \geq \max(n_1 d_{2odd}',\, d_{2odd}^{(0)})$ and $d_{even} \geq n_1 d_{2odd}' + (d_{2even}' - d_{2odd}')\, d_{1odd}$. These bounds are valid for N_2 empty or N_2 nonempty. However when N_2 is empty we can obtain a better bound for d_{even} as follows: assume we have some i, $0 \leq i < n_1$, such that $w(\bar{V}_i(z)) = 1$, without loss of generality we assume $\bar{V}_0(z) = 1$. Thus, $\bar{V}_i(z) + 1$ is a code polynomial of V_{n_2}, $i = 0,1,\ldots,n_1-1$. Since $w(v(x)) > n_1$, there exists at least one i, $0 < i < n_1$, such that $w(V_i(z)+1) \neq 0$. Remembering that $v_1^{(0)}(y) \not\equiv 0$ and has even weight we can conclude that

$w(v(x)) \geq w_{1even} + (n_1-w_{1even})(d_{2odd}-1) =$

$= n_1(d_{2odd}-1) - w_{1even}(d_{2odd}-2) \geq n_1(d_{2odd}-1) - (n_1-d_{1odd})(d_{2odd}-2) =$

$= n_1 + (d_{2odd}-2)d_{1odd}$. Thus, $d_{even} \geq \min(2n_1, n_1 + (d_{2odd}-2)d_{1odd})$.

Case 3. In this case we consider the possibility of having $v(\beta^{\rho(0,\phi)}) \neq 0$ for $\phi \in S'_{21}$ and $v(\beta^{\rho(0,\phi)}) = 0$ for $\phi \in S'_{22}$, where S'_{21} and S'_{22} are a partition of S'_2. In this case $\bar{V}_0(\gamma^{\phi}) = \bar{V}_1(\gamma^{\phi}) = \ldots = \bar{V}_{n_1-1}(\gamma^{\phi}) \neq 0$ for $\phi \in S'_{21}$ and $\bar{V}_i(\gamma^{\phi}) = 0$ for $\phi \in N_2 \cup S'_{22}$. Thus, $w(v(x))$ is lower bounded by the bounds found in the analyses of the last case.

Q.E.D.

Example 6: As an application of Theorem 6 we consider the (105,46) binary cyclic code generated by

$g(x) = m_1(x)m_3(x)m_7(x)m_9(x)m_{15}(x)m_{17}(x)m_{49}(x)$. In this case

$n_1 = 7$, $n_2 = 15$, $\bar{J}_0 = \{1,2,4\}$, $J_0 = \{1,2,4,7,8,11,13,14\}$,

$S_2 = \{1,2,3,4,6,8,9,12\}$, $N_2 = \{1,2,4,8\}$,

$P_2 = \{1,2,3,4,6,7,8,9,11,12,13,14\}$. Thus

$d_{2odd} = 5$, $d_{2even} = 6$, $d_{2odd}^{(0)} = 3$, $d_{2even}^{(0)} = 6$, $d'_{2odd} = 3$, $d'_{even} = 4$,

$d''_{2odd} = 5$ and $d''_{2even} = 10$. By Theorem 6, $d_{odd} \geq 15$ and $d_{even} \geq 10$.

The BCH bound gives $d_{odd} \geq 7$ and $d_{even} \geq 8$.

In the next section we present numerical results obtained from the application of the theorems proved in this section.

IV. Numerical Results

In Table I we give numerical results obtained from the application of Theorem 1, Theorem 3 and Theorem 6. Numerical results obtained from the application of Theorem 2, Theorem 4, Theorem 5 and Corollary 1 are given in Table II. The symbols for the tables are the following:

n = code length

k = number of information digits

roots = the powers of β that specify the generator polynomial

d_{0odd} = BCH lower bound on the minimum distance of odd-weight code words

d_{0even} = BCH lower bound on the minimum distance of even-weight code words

d_{odd} = actual minimum weight of odd-weight code words

d_{even} = actual minimum weight of even-weight code words

T - a = by Theorem a

C - a = by Corollary a

Table I

n	k	ROOTS	$d_{0\,even}=$	$d_{0\,odd}=$	$d_{even}\geq$	$d_{odd}\geq$	REMARKS
21	10	(1,7,9)	4*	5	4*	9	T-3
21	9	(1,3,9)	6*	5	6*	7*	T-3
21	7	(1,3,7,9)	6	5	8*	9*	T-3
33	13	(1,3)	10*	5	10*	11	T-1 and [10, T-2]
35	17	(1,5,15)	6*	5	6*	7	T-3
35	16	(1,7,15)	4*	5	4*	15	T-3
35	15	(0,1,7,5)	6	-	8*	-	T-6
35	13	(1,5,7,15)	6	7	8*	15*	T-3
39	27	(1)	4	3*	6*	3*	T-1
39	15	(1,3)	8	7	10*	13*	T-1 and [10, T-2]
45	31	(3,5,21)	4*	3	4*	5	T-6
45	27	(3,5,9,21)	4*	3	4*	5	T-6
45	14	(0,1,7,9,15)	8	-	10*	-	T-6
45	13	(1,5,7,15)	6*	7	6*	9	T-3
45	9	(1,5,7,9,15)	10	9	12*	15	T-3
51	27	(1,3,9)	6	5	8*	17	T-1 and [10, T-2]
51	25	(1,9,17,19)	6*	7	6*	15	T-3
51	19	(1,3,9,19)	10*	7	10*	17	T-3
51	17	(1,3,9,17,19)	10	7	12*	15	T-3
55	35	(1)	4	5*	6	5*	T-1
55	25	(1,5)	8	7	8	11*	T-1 and [10, T-2]
57	21	(1,3)	10	7	14*	19	T-1 and [10, T-2]
63	45	(3,7,15)	4*	3	4*	7	T-6
63	43	(1,3,7,21)	6*	5	6*	9	T-1 and [10, T-2]
63	42	(3,7,15,27)	4*	3	4*	7	T-6
63	39	(1,9,11,23,27)	6*	5	6*	7	T-1 and [10, T-2]
63	39	(3,7,9,15,27)	4*	3	4*	7	T-6
63	37	(1,11,15,21,23)	4*	5	4*	7	T-6
63	36	(1,5,9,11,23)	6*	5	6*	7	T-1

*The bound gives the actual weight [12].

Table I (cont.)

n	k	ROOTS	$d_{0even} =$	$d_{0odd} =$	$d_{even} \geq$	$d_{odd} \geq$	REMARKS
63	36	(1,3,9,11,23)	6*	5	6*	7	T-1
63	36	(1,11,15,23,27)	6*	5	6*	7	T-6
63	34	(1,11,15,21,23,27)	6*	7	6*	9	T-6
63	33	(1,7,9,11,23,27)	6*	5	6*	7	T-1 and [10, T-2]
63	33	(1,7,11,15,23)	4*	5	4*	9	T-6
63	31	(1,7,9,11,21,23,27)	6	7	8*	9	T-1 and [10, T-2]
63	31	(1,5,11,15,21,23)	10*	7	10*	9*	T-1
63	30	(1,7,11,15,23,27)	6	5	8*	9	T-1
63	28	(1,7,9,11,15,21,23)	4*	5	4*	27	T-3
63	28	(1,7,11,15,21,23,27)	6	7	8*	9	T-6
63	27	(1,3,7,11,15,23)	6	5	8*	9	T-1
63	25	(1,7,9,11,15,21,23,27)	6	7	8*	27	T-3
63	24	(1,3,7,11,15,23,27)	6	5	8*	9	T-1
63	18	(1,5,7,9,11,13,23,31)	6*	7	6*	9	T-3
63	16	(1,5,7,9,11,13,21,23,31)	10	9*	12*	9*	T-3
63	15	(1,5,7,9,11,13,23,27,31)	6*	7	6*	21	T-3
63	13	(1,5,7,9,11,13,21,23,27,31)	10	9	12*	21	T-3
65	41	(1,5)	6	7	6	13	T-1 and [10, T-2]
65	29	(1,5,7)	8	9	10	13	T-1 and [10, T-2]
69	34	(1,3,23)	6	7	8	21	T-3
69	25	(1,3,15)	8	7	14	23	T-3
69	23	(1,3,15,23)	10	9	16	21	T-3
105	46	(1,3,7,9,15,17,49)	8	7	10	15	T-6

*The bound gives the actual weight [12].

Table II

n	k	ROOTS	$d_{0even}=$	$d_{0odd}=$	$d_{even}=$	$d_{odd}=$	REMARKS
15	7	(1,7)	6	3	6	3	T-4
15	5	(1,5,7)	6	3	6	3	T-2
21	15	(1)	4	3	4	3	C-1
21	12	(1,9)	4	3	4	3	T-2
21	9	(1,5)	6	3	6	3	T-4
21	7	(1,5,7)	6	3	6	3	T-2
33	13	(1,5)	6	3	6	3	T-4
33	11	(1,5,11)	6	3	6	3	T-2
35	23	(1)	4	3	4	3	C-1
35	20	(1,15)	4	3	4	3	T-2
35	11	(1,3)	10	5	10	5	T-4
35	7	(1,3,7)	10	5	10	5	T-2
39	15	(1,7)	6	3	6	3	T-4
39	13	(1,7,13)	6	3	6	3	T-2
45	21	(1,7)	6	3	6	3	C-1
45	15	(1,5,7)	6	3	6	3	T-2
45	13	(1,3,7,21)	10	5	10	5	T-4
45	9	(1,3,7,9,21)	10	5	10	5	T-2
45	7	(1,3,7,9,15,21)	10	11	10	15	T-2
51	35	(1,19)	6	3	6	3	C-1
51	27	(1,9,19)	6	5	6	5	T-2
51	19	(1,5,11,19)	6	3	6	3	T-4
51	17	(1,5,11,17,19)	6	3	6	3	T-2
51	11	(1,3,5,11,19)	18	9	18	15	T-5
51	9	(1,3,5,11,17,19)	18	13	18	15	T-2
55	15	(1,3)	10	5	10	5	T-4
55	11	(1,3,11)	10	5	10	5	T-2
57	21	(1,5)	6	5	6	5	T-4

Table II (cont.)

n	k	ROOTS	$d_{0even}=$	$d_{0odd}=$	$d_{even}=$	$d_{odd}=$	REMARKS
57	19	(1,5,19)	6	3	6	3	T-2
63	43	(3,7,15,21)	4	3	4	9	T-5
63	39	(1,11,15,23)	4	3	4	3	C-1
63	36	(1,9,11,15,23)	4	3	4	3	T-2
63	33	(1,9,11,15,23,27)	6	5	6	7	T-5
63	33	(1,3,11,15,23)	6	5	6	7	T-4
63	31	(1,3,11,15,21,23)	6	7	6	9	T-5
63	31	(1,7,11,15,21,23)	4	5	4	9	T-5
63	30	(1,3,9,11,15,23)	6	5	6	7	T-5
63	28	(1,3,9,11,15,21,23)	6	7	6	9	T-2
63	27	(1,3,9,11,15,23,27)	6	5	6	7	T-5
63	27	(1,5,11,13,23,31)	6	3	6	3	C-1
63	25	(1,3,7,11,15,21,23)	6	7	8	9	T-5
69	47	(1)	4	3	6	3	C-1
69	36	(1,3)	6	5	8	7	T-2
69	45	(1,23)	4	3	6	3	C-1
69	25	(1,3,15)	8	7	14	23	T-5
69	14	(1,3,5)	18	15	24	21	T-5
77	47	(1)	4	3	4	3	C-1
77	44	(1,11)	4	3	4	3	T-2
77	41	(1,11,33)	6	5	6	7	T-5
77	37	(1,7)	4	5	4	11	C-1
85	53	(1,9,13,21)	6	5	6	5	C-1
85	45	(1,9,13,15,21)	6	5	6	5	T-2
85	49	(1,9,13,17,21)	6	5	6	5	C-1
85	37	(1,5,9,13,15,21)	6	7	6	17	T-5
105	63	(1,9,11,25)	4	3	4	3	C-1
105	57	(1,3,9,17)	6	5	6	5	C-1

Table II (cont.)

n	k	ROOTS	$d_{0even}=$	$d_{0odd}=$	$d_{even}=$	$d_{odd}=$	REMARKS
105	51	(1,9,11,17,25)	10	7	10	7	T-4
105	49	(1,7,9,11,21,25,35,49)	4	5	4	15	C-1
105	48	(1,9,11,15,17,25)	10	7	10	7	T-4
105	47	(1,9,11,17,25,49)	10	7	12	9	T-5
105	45	(1,5,9,11,17,25)	10	7	10	7	T-4
105	45	(1,9,11,15,17,25,45)	10	7	12	7	T-5
105	45	(1,3,5,9,17,25)	8	7	8	7	C-1
105	45	(1,7,9,11,25,35,49)	4	5	4	15	C-1
105	44	(1,9,11,15,17,25,49)	10	7	12	9	T-2
105	42	(1,5,9,11,15,17,25)	10	7	10	7	T-5
105	39	(1,3,9,11,17,25)	12	7	14	7	T-4
105	39	(1,5,9,11,17,25,35,49)	10	9	12	9	T-5
105	36	(1,3,9,11,15,17,25)	12	7	14	7	T-5
105	36	(1,5,9,11,15,17,25,35,49)	10	9	12	9	T-2
105	33	(1,3,5,9,11,17,25)	14	7	14	7	T-4
105	31	(1,3,9,11,17,21,25,49)	12	11	18	15	T-5
105	28	(1,3,9,11,15,17,21,25,49)	12	11	18	15	T-2
119	95	(1)	4	3	4	3	C-1
119	89	(1,7,21)	4	5	4	17	C-1
119	71	(1,13)	6	5	6	5	C-1
119	65	(1,13,17,51)	6	7	6	7	C-1
119	47	(1,11,13)	10	7	14	7	T-4
119	44	(1,11,13,51)	10	7	14	7	T-5
119	41	(1,11,13,17,51)	10	7	14	7	T-5
119	39	(1,11,13,21)	14	13	18	15	T-5
119	31	(1,7,11,13,21)	14	13	20	17	T-5

V. Conclusions

By exploiting the minimum distance relationship between codes of related lengths, the actual minimum distances of some classes of binary cyclic codes of composite length has been obtained. For other classes we were able to obtain new lower bounds on the minimum distance. These new lower bounds are useful in obtaining better estimates on the minimum distance of many new cyclic codes. The simplicity of the application of the theorems is apparent from the examples. In the examples of Table II the BCH bound gives a good estimate on the minimum distance.

References

[1] Burton, H.O. and E.J. Weldon, Jr., "Cyclic Product Codes", IEEE Trans. on Information Theory, Vol. IT-11, pp. 433-440, July 1965.

[2] Abramson, N., "Encoding and Decoding Cyclic Code Groups", Dept. of Elec. Engr., University of Hawaii, Honolulu, Technical Report, February 1967.

[3] Assmus, E.F. and H.F. Mattson, Jr., "Some Cyclic Codes of Block Length 3p", in Summary Scientific Report, Sec. 3, Sylvania Electronic Systems, Applied Research Lab., Needham, Mass., July 1963.

[4] Assmus, E.F. and H.F. Mattson, Jr., "Some (3p,p) Codes," Information Processing 68, North-Holland Publishing Company, Amsterdam, 1969.

[5] Goethals, J.M., "Factorization of Cyclic Codes", IEEE Trans. on Information Theory, Vol. IT-13, pp. 242-246, April 1967.

[6] Kasami, T., "Some Lower Bounds on the Minimum Weight of Cyclic Codes of Composite Length", IEEE Trans. on Information Theory, Vol. IT-14, pp. 814-818, November 1968.

[7] Mattson, H.F., Jr., and G. Solomon, "A New Treatment of Bose-Chaudhuri Codes", SIAM, Vol. 9, pp. 654-669, December 1961.

[8] Peterson, W.W. and E.J. Weldon, Jr., "Error-Correcting Codes, 2nd Edition", The MIT Press, 1972.

[9] Elias, P., "Error-Free Coding", IRE Trans. Information Theory, Vol. PGIT-4, pp. 29-37, September 1954.

[10] Hartmann, C.R.P. and K.K. Tzeng, "On Some Classes of Cyclic Codes of Composite Length", IEEE Trans. on Information Theory, Vol. IT-19, pp. 820-823, November 1973.

[11] Hartmann, C.R.P. and K.K. Tzeng, "Generalizations of the BCH Bound", Information and Control, Vol. 20, pp. 489-498, June 1972.

[12] Chen, C.L., "Computer Results on the Minimum Distance of Some Binary Cyclic Codes", IEEE Trans. on Information Theory, Vol. IT-16, pp. 359-360, May 1970.

[13] Lin, S. and E.J. Weldon, "Further Results on Cyclic Product Codes", IEEE Trans. on Information Theory, Vol. IT-16, pp. 452-459, July 1970.

[14] Hartmann, C.R.P., K.K. Tzeng and R.T. Chien, "Some Results on the Minimum Distance Structure of Cyclic Codes", IEEE Trans. on Information Theory, Vol. IT-18, pp. 402-409, May 1972.

Acknowledgment

The assistance of Mrs. Ruth Turnpaugh in the typing of the manuscript is gratefully acknowledged.