Coordinated Science Laboratory

UNIVERSITY OF ILLINOIS – URBANA, ILLINOIS

WEIGHT DISTRIBUTIONS OF BOSE-CHAUDHURI-HOCQUENGHEM CODES

Tadao Kasami

REPORT R-317 AUGUST, 1966

This work was supported in part by the Joint Services Electronics Program (U.S. Army, U.S. Navy, and U.S. Air Force) under Contract DA 28 043 AMC 00073(E); and in part by the National Science Foundation under Grant NSF GK-690, and in part by the Air Force Cambridge Research Laboratories under Contract AF 19(628)4379.

WEIGHT DISTRIBUTIONS OF BOSE-CHAUDHURI-HOCQUENGHEM CODES

Tadao Kasami*

Abstract

Several techniques useful for finding weight distributions of the binary Bose-Chaudhuri-Hocquenghem codes (the BCH codes) of length 2^m-1 and some other cyclic codes are presented. By using (1) a relation between the BCH codes and the Reed-Muller codes, (2) the invariant property of the BCH codes (extended by the addition of an overall parity check) under a doubly transitive group of permutations on digit positions and (3) the power moment identities, explicit weight distribution formulas are derived for $(2^{m-1}-2^{m/2-j}-1)$-BCH codes with $j = 0$ and 1, $(2^{m-1}-2^{(m-1)/2+j}-1)$-BCH codes with $0 \leq j \leq 2$, the dual codes of double-error-correcting BCH codes, the dual codes of triple-error-correcting BCH codes, and some other class of cyclic codes. Here, for odd d, a d-BCH code is a BCH code of length 2^m-1 which has $\beta,\beta^2,\ldots,\beta^{d-1}$ but not β^d as roots of its generator polynomial, where β is a primitive element of $GF(2^m)$.

* On leave from Osaka University, Osaka, Japan.

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

1. INTRODUCTION

The weight distribution problem of a code is to find the number of code vectors of each weight in the code. The weight distribution is one of the important properties of the structure of a code and gives the complete information on the probability of an undetected error when the code is used for error detection only.

To the author's knowledge, explicit formulas of weight distribution have been known only for the Hamming codes [1] and the Reed-Solomon codes [2]. The weight distributions of all cyclic codes of length 31 were computed by Prange [3] and a number of weight distributions for BCH codes and their dual codes of length 63 to 1023 found by digital computation have been tabulated by Peterson [4].

In this paper, several methods useful for finding the weight distributions of binary Bose-Chaudhuri-Hocquenghem codes [5] (BCH codes) of length 2^m-1 are presented. Explicit weight distribution formulas for several classes of BCH codes and some other cyclic codes are derived.

Let C be a binary linear code of length n and let k denote the number of information digits. Let a_j denote the number of vectors of weight j in C and b_j denote the number of vectors of weight j in the dual code of C. A series of identities by which each a_j can be calculated from the b_j's has been given by MacWilliams [6]. Thus it is enough to consider the case where $k \leq n-k$. The following power moment identities have been derived from MacWilliams identities by Pless [7].

$$\sum_{j=0}^{n} j^{\ell} a_j = \sum_{j=0}^{n} (-1)^j b_j \left(\sum_{\nu=0}^{\ell} \nu ! G_{\ell}^{\nu} 2^{k-\nu} \binom{n-j}{n-\nu} \right), \qquad (1)$$

where G_{ℓ}^{ν} is a Stirling number of the second kind [8].

Simple formulas for even j

$$j a_j = (n+1-j)\, a_{n+1-j} \qquad (2)$$

$$j b_j = (n+1-j)\, b_{n+1-j} \qquad (3)$$

have been proved to hold for the BCH codes of length 2^m-1 by Prange and Peterson [4] as a simple consequence of the fact that it is possible to extend these codes by adding one more check digit in such a way that the extended code is invariant under a doubly transitive group of permutations on the components of a code vector.

For odd d, by a d-BCH code is meant a binary BCH code of length 2^m-1 which has $\beta, \beta^2, \ldots, \beta^{d-1}$ but not β^d as roots of its generator polynomial, where β is a primitive element of $GF(2^m)$. For even d, let a d-BCH code be a code consisting of the code vectors of even weight in a (d-1)-BCH code. A t-error-correcting BCH code [5] is a (2t+1)-BCH code.

A cyclic code of length 2^m-1 can be derived from the ν-th order Reed-Muller code of length 2^m [9] by deleting the first component of each code vector and permuting the remaining components suitably. The resulting code will be called the ν-th order modified Reed-Muller code. This code has been proved to be a subcode of a $(2^{m-\nu}-1)$-BCH code [10]. It is shown in section 3 that the possible values of weights of code vectors of the second order Reed-Muller code are very sparse. By using this fact as well as the power moment identities and the invariant property, explicit weight distribution formulas are obtained for the following subcodes of the second order modified Reed-Muller code: the dual code of every double-error-correcting

BCH code, the dual code of triple-error-correcting BCH code for any odd $m \geq 5$ and several even m's, $(2^{m-1} - 2^{m/2-1})$-BCH codes for even $m \geq 4$, $(2^{m-1} - 2^{m/2})$-BCH codes for even $m \geq 4$, $(2^{m-1} - 2^{(m-1)/2})$-BCH codes for odd $m \geq 3$, $(2^{m-1} - 2^{(m+1)/2})$-BCH codes for odd $m \geq 5$, $(2^{m-1} - 2^{(m+3)/2})$-BCH codes for odd $m \geq 11$ and some other classes of cyclic codes.

2. INVARIANT PROPERTIES

Let $n = 2^m-1$. The extended code of C is the code with an overall parity check added to C as the first digit. The first component in a code vector is numbered 0, and for $i > 1$ the i-th component is numbered α^{i-2}, where α is a primitive element of $GF(2^m)$. Let v be a vector of the extended code. For $a(\neq 0)$ and b in $GF(2^m)$, permute the component of v in position X to position $aX + b$. Then, the resulting vector will be denoted by $\pi_{ab}v$. If the extended code of C is invariant under doubly transitive group of permutations $\pi = \{\pi_{ab} \mid a\neq 0, b \in GF(2^m)\}$, then C is a cyclic code by definition. Peterson [4] proved that the extended codes of (2t+1)-BCH codes are invariant under permutation group π.

Let i be a positive integer less than 2^m. Then i can be expressed in binary form:

$$i = \sum_{j=0}^{m-1} \delta_j \, 2^j.$$

Let $I(i)$ denote the set of all nonzero integers i' such that

$$i' = \sum_{j=0}^{m-1} \delta'_j \, 2^j,$$

where $0 \leq \delta'_j \leq \delta_j$ for $0 \leq j < m$.

<u>Theorem 1</u> [10]: Let C be a cyclic code of length 2^m-1 generated by polynomial $g(X)$. The extended code of C is invariant under permutation group π if and only if (1) $g(1) \neq 0$ and (2), for every root α^i of $g(X)$,

$$g(\alpha^{i'}) = 0 \qquad \text{for } i' \text{ in } I(i).$$

Let C_o be a cyclic code of length 2^m-1 generated by $g(X) = (X^{2^m-1}-1)/(h_o(X)\ldots h_p(X))$, where $h_o(X) = X-1$, $h_i(X)$ is an irreducible polynomial of degree m_i and $h_i(\alpha^{j_i}) = 0$ $(0 \leq i \leq p)$. Suppose that $g(X)$ satisfies the condition of Theorem 1. Let $v(X)$ be the polynomial representation [1] of a code vector of C_o. If $g(\alpha^j) = 0$, then $v(\alpha^j) = 0$. Obviously, $v(\alpha^{j_i}) \in GF(2^{m_i})$ $(0 \leq i \leq p)$. Conversely, for any set of β_i in $GF(2^{m_i})$ $(0 \leq i \leq p)$, there exists a unique code vector* $v(\beta_o, \ldots, \beta_p : X)$ in C_o such that $v(\beta_o, \ldots, \beta_p : \alpha^{j_i}) = \beta_i$ $(0 \leq i \leq p)$. (Mattson and Solomon [11]) Let $\bar{v}(\beta_o, \ldots, \beta_p)$ denote the vector with an overall parity added to code vector $v(\beta_o, \ldots \beta_p : X)$ as the first component. $\bar{v}(\beta_o, \ldots, \beta_p)$ is a vector of the extended code C_{ex} of C_o. Let $X_1, \ldots, X_w$ be the location numbers of nonzero components of $\bar{v}(\beta_o, \ldots, \beta_p)$. By definition, w is an even integer and

$$\sum_{f=1}^{w} X_f^{j_i} = v(\beta_o, \ldots, \beta_p : \alpha^{j_i}) = \beta_i, \ (1 \leq i \leq p).$$

If $g(\alpha^{\ell}) = 0$, then

$$\sum_{f=1}^{w} X_f^{\ell} = 0. \tag{4}$$

Otherwise, $h_q(\alpha^{\ell}) = 0$ for some q and, consequently, $\ell \equiv j_q 2^{\nu} \pmod{2^m - 1}$ for some $0 \leq \nu < m_q$. Hence,

$$\sum_{f=1}^{w} X_f^{\ell} = \beta_q^{2^{\nu}} \tag{5}$$

For any $a(\neq 0)$ and b in $GF(2^m)$, there exists $\bar{v}(\beta'_o, \ldots, \beta'_p)$ in C_{ex} such that

$$\bar{v}(\beta'_o, \ldots, \beta'_p) = \pi_{ab}\, \bar{v}(\beta_o, \ldots, \beta_p).$$

By definition,

$$\beta'_i = \sum_{f=1}^{w} (aX_f + b)^{j_i}, \ (1 \leq i \leq p). \tag{6}$$

If

$$j = 2^{\sigma_1} + 2^{\sigma_2} + \ldots + 2^{\sigma_t} \quad (0 \leq \sigma_1 < \sigma_2 \ \ldots \ \sigma_t < m),$$

$$(aX_f + b)^j = (a^{2^{\sigma_1}} X_f^{2^{\sigma_1}} + b^{2^{\sigma_1}}) \ldots (a^{2^{\sigma_t}} X_f^{2^{\sigma_t}} + b^{2^{\sigma_t}})$$

$$= \sum_{\ell \in I(j)} a^{\ell} X_f^{\ell}\, b^{j-\ell}. \tag{7}$$

---

*Vector $v(X)$ means the vector represented by polynomial $v(X)$.

It follows from (4) through (7) that

$$\beta_i' = \sum_{q=1}^{p} \sum_{\nu \in E_{iq}} a^{j_q 2^\nu} \beta_q^{2^\nu} b^{j_i - j_q 2^\nu}, \quad (1 \leq i \leq p) \tag{8}$$

where E_{iq} is the set of integer ν's such that the remainder of $j_q 2^\nu/(2^m-1)$ is in $I(j_i)$ and that $0 \leq \nu < m_q$.

Lemma 2: Assume that, for given β_i and β_i' in $GF(2^{m_i})$ $(1 \leq i \leq p)$, there are $a(\neq 0)$ and b in $GF(2^m)$ which satisfy (8). Then, if the weight of $v(0, \beta_1, \ldots, \beta_p: X)$ is w, the weight of $v(0, \beta_1', \ldots, \beta_p': X)$ is either w or $n + 1 - w$.

Proof: It follows from the assumption that there exists β_o' in GF(2) such that $\bar{v}(\beta_o', \ldots, \beta_p') = \pi_{ab}\bar{v}(0, \beta_1, \ldots, \beta_p)$. Obviously, the weights of $\bar{v}(0, \beta_1, \ldots, \beta_p)$ and $\bar{v}(\beta_o', \ldots, \beta_p')$ are equal to w. If $\beta_o' = 0$, the weight of $v(0, \beta_1', \ldots, \beta_p': X)$ is w. If $\beta_o' = 1$, the weight of $v(1, \beta_1', \ldots, \beta_p': X)$ is w-1 by definition. C_o contains all-one vector $e(X) = 1 + X + \ldots + X^{2^m-2}$. Since $e(\alpha^j) = \sum_{f=0}^{2^m-2} \alpha^{jf} = 0$ $(0 < j < 2^m-1)$, $v(0, \beta_1', \ldots, \beta_p': X) = v(1, \beta_1', \ldots, \beta_p': X) + e(X)$. Therefore, the weight of $v(0, \beta_1', \ldots, \beta_p': X)$ is $n + 1 - w$.

Q.E.D.

Since C_o contains all-one vector $e = (1, \ldots, 1)$,

$$a_{n-j} = a_j, \text{ for any } j.$$

Consequently, it is enough to consider code C consisting of all the code vectors of even weight in C_o. In code C, $\beta_o = 0$. Since symmetry property (2) holds for C_o by Prange Theorem [3,4], it also holds for C. Hence, it is sufficient to find $a_j + a_{n+1-j}$ for even j $(0 < j \leq (n+1)/2)$. Thus the following power moments are convenient.

$$I_\ell = \sum_{j \neq 0} (j - [(n+1)/2])^\ell \, a_j,$$

where [x] denotes the integer part of x.

If n is odd and $b_1 = b_2 = 0$, then

$$I_2 = 2^{k-2} (n+1) - 2^{-2}(n+1)^2, \tag{9}$$

$$I_4 = 2^{k-4} [3(n+1)^2 - 2(n+1)] - 2^{-4} (n+1)^4 + 3 \cdot 2^{k-1} (b_3+b_4) \tag{10}$$

If n is odd and $b_i = 0$ $(1 \leq i \leq 4)$,

$$I_6 = 15 \cdot 2^{k-6} [(n+1)^3 - 2(n+1)^2] + 2^{k-2} (n+1)$$

$$- 2^{-6} (n+1)^6 + 6! \, 2^{k-6} (b_5+b_6) \tag{11}$$

The proof of (9), (10) and (11) is given in Appendix 1.

3. MODIFIED REED-MULLER CODES

Let V_j denote a j-dimensional vector space over GF(2) and x_i $(1 \leq i \leq m)$ be a variable over GF(2). For $1 \leq \nu \leq m$, let P_ν be the set of polynomials over GF(2) of variables $x_1, \ldots, x_m$ of degree ν or less. For $0 \leq j < 2^m-1$, let

$$\alpha^j = \sum_{i=0}^{m-1} v_{ji}\alpha^i, \ v_{ji} \in GF(2).$$

For $f(x_1, \ldots, x_m) \in P_\nu$, let v(f) denote a vector in V_{2^m} of which the first component is $f(0, \ldots, 0)$ and the j-th component $(j > 1)$ is $f(v_{j-20}, v_{j-21}, \ldots, v_{j-2\,m-1})$. Then the ν-th order Reed-Muller code of length 2^m is the set of vectors $\{v(f) | f \in P_\nu\}$.* Delete the first component of each vector of the ν-th order Reed-Muller code of length 2^m. Then the resulting set of vectors in V_{2^m-1} will be called the ν-th order modified Reed-Muller code. Let

$$y_j = u_{jo} + \sum_{i=1}^{m} u_{ji}\, x_i \in P_1 \quad (1 \leq j \leq m)$$

If vectors $(u_{j1}, u_{j2}, \ldots, u_{jm})$ $(1 \leq j \leq \ell)$ are linearly independent, $y_1, \ldots, y_\ell$ will be said to be independent. For $f(x_1, \ldots, x_m) \in P_\nu$, there is f' in P_ν such that $f(y_1, \ldots, y_m) = f'(x_1, \ldots, x_m)$. Therefore, if v(f) is a code vector of the ν-th order Reed-Muller code, then v(f') is also a code vector. It follows from this fact that a modified Reed-Muller code is cyclic [10]. Let w(j) denote the number of ones in the binary expression of j.

<u>Theorem 3</u> [10]: Let g(X) be the generator polynomial of the ν-th order modified Reed-Muller code of length 2^m-1. Then α^j is a root of g(X)

---

*The order of the digit positions is different from the original one [1,9].

if and only if $0 < w(j) < m-\nu$.

This theorem implies that the ν-th order modified Reed-Muller code is a subcode of a $(2^{m-\nu}-1)$-BCH code.

For polynomial $f(x_1,\ldots, x_m)$, let $|f|_m$ denote the number of m-tuple $(v_1,\ldots, v_m)$'s such that

$$f(v_1,\ldots, v_m) = 1.$$

By definition, $|f|_m$ is the weight of vector $v(f)$. If y_j's $(1 \leq j \leq m)$ in P_1 are independent and $f'(x_1,\ldots, x_m) = f(y_1,\ldots, y_m)$, then

$$|f'|_m = |f|_m. \tag{12}$$

This follows from the fact that $y_j = u_{jo} + \sum_{i=1}^{m} u_{ji}\, x_i$ $(1 \leq j \leq m)$ defines a one-to-one mapping from V_m onto itself.

<u>Lemma 4</u>: Assume that (1) $m \geq 2$, (2) $f(x_1,\ldots, x_m) \in P_2$, (3) f does not depend on x_i $(i < i_o \leq m)$ but on x_{i_o}. Then there exist independent $y_j^{(i)}$'s $(1 \leq i \leq t;\ 1 \leq j \leq \ell_i)$ in P_1 such that

(1) $y_1^{(1)} = x_{i_o}$

(2) $f(x_1,\ldots, x_m) = u_o + \sum_{i=1}^{t} \left(\sum_{j=1}^{\ell_i -1} y_j^{(i)}\, y_{j+1}^{(i)} + u_i\, y_{\ell_i}^{(i)} \right)$,

where $u_i \in GF(2)$ $(0 \leq i \leq t)$.

<u>Proof</u>: If $m = 2$, it is easy to check that this lemma holds. Suppose that this lemma holds for $2 \leq m < m'$. Consider the case of $m = m'$. Let

$$f(x_1,\ldots, x_m) = F_o(x_2,\ldots, x_m) + x_1\, F_1(x_2,\ldots, x_m), \tag{13}$$

where $F_o \in P_2$ and $F_1 \in P_1$. If $F_1 = 1$,

$$f(x_1,\ldots, x_m) = x_1 + F_o(x_2,\ldots, x_m).$$

Then apply the induction hypothesis to $F_o(x_2, \dots, x_m)$. Suppose that F_1 is not a constant. Since x_1 and $F_1(x_2, \dots, x_m)$ are independent, there exist independent $y_1, \dots, y_m$ such that

(1) $y_1 = x_1$,

(2) $y_2 = F_1(x_2, \dots, x_m)$,

and (3) $y_2, \dots, y_m$ are polynomials of $x_2, \dots, x_m$ of the first degree. Then it follows from (13) that

$$f(x_1, \dots, x_m) = y_1 y_2 + f'(y_2, \dots, y_m),$$

where $f'(y_2, \dots, y_m) = F_o(x_2, \dots, x_m)$. Now apply the induction hypothesis to $f'(y_2, \dots, y_m)$. Q.E.D.

Let $G_o(\ell)$ and $G_1(\ell)$ be defined by the following:

$$G_o(\ell) = |x_1x_2 + x_2x_3 + \dots + x_{\ell-1}x_\ell|_\ell, \quad \ell \geq 2$$

$$G_o(1) = 0,$$

$$G_1(\ell) = |x_1x_2 + x_2x_3 + \dots + x_{\ell-1}x_\ell + x_\ell|_\ell, \quad \ell \geq 1.$$

Note that

$$|f(x_1, \dots, x_m)|_m = |f(x_1, \dots, x_{m-1}, 0)|_{m-1} + |f(x_1, \dots, x_{m-1}, 1)|_{m-1} \tag{14}$$

$$|1 + f(x_1, \dots, x_m)|_m = 2^m - |f(x_1, \dots, x_m)|_m \tag{15}$$

It is easy to check that, for $\ell \geq 2$,

$$\begin{aligned} G_o(\ell) &= |x_1x_2 + \dots + x_{\ell-2}x_{\ell-1}|_{\ell-1} + |x_1x_2 + \dots + x_{\ell-2}x_{\ell-1} + x_{\ell-1}|_{\ell-1} \\ &= G_o(\ell-1) + G_1(\ell-1) \end{aligned} \tag{16}$$

$$G_1(\ell) = |x_1x_2 + \ldots + x_{\ell-2}\,x_{\ell-1}|_{\ell-1} + |x_1x_2 + \ldots + x_{\ell-2}x_{\ell-1} + x_{\ell-1} + 1|_{\ell-1}$$

$$= G_o(\ell-1) + 2^{\ell-1} - G_1(\ell-1) \tag{17}$$

By (16) and (17), for $\ell \geq 3$

$$G_o(\ell) = G_o(\ell-2) + G_1(\ell-2) + G_o(\ell-2) + 2^{\ell-2} - G_1(\ell-2)$$

$$= 2G_o(\ell-2) + 2^{\ell-2}$$

$$G_1(\ell) = G_o(\ell-2) + G_1(\ell-2) + 2^{\ell-1} - (G_o(\ell-2) + 2^{\ell-2} - G_1(\ell-2))$$

$$= 2G_1(\ell-2) + 2^{\ell-2}$$

Hence,

$$2^{\ell-1} - G_i(\ell) = 2(2^{\ell-3} - G_i(\ell-2)), \quad i = 0, 1 \tag{18}$$

On the other hand, it is easy to check that

$$G_i(2) = 1 = 2-1, \quad i = 0, 1$$

$$G_o(1) = 0,$$

$$G_1(1) = 1.$$

Therefore, it follows from (18) that, for even $\ell \geq 2$,

$$G_o(\ell) = G_1(\ell) = 2^{\ell-1} - 2^{\ell/2-1} \tag{19}$$

and that, for odd $\ell \geq 1$,

$$G_o(\ell) = 2^{\ell-1} - 2^{(\ell-1)/2}, \tag{20}$$

$$G_1(\ell) = 2^{\ell-1}. \tag{21}$$

<u>Lemma 5</u>: Suppose that $m \geq 2$ and $f(x_1, \ldots, x_m) \in P_2$. Then $|f|_m$ is of the form:

$$2^{m-1} + \varepsilon 2^{\ell},$$

where $m/2-1 \leq \ell \leq m-1$ and ε is either 0, 1 or -1.

<u>Proof</u>: If $m = 2$, this lemma is obvious. Assume that this lemma holds for $2 \leq m < m'$ and consider the case of $m = m'$. By Lemma 4, there exist independent $y_1, \ldots, y_m$ in P_1 such that, for some $h (1 \leq h \leq m)$,

$$f(x_1, \ldots, x_m) = f_o(y_1, \ldots, y_h) + f_1(y_{h+1}, \ldots, y_m),$$

$$f_o(y_1, \ldots, y_h) = y_1 y_2 + y_2 y_3 + \ldots + y_{h-1}\, y_h + u y_h,$$

where $u \in GF(2)$ and, if $h = m$, f_1 is a constant. If $h = m$, this lemma follows from (15), (19), (20) and (21). Otherwise, it follows from the induction hypothesis that

$$|f_o|_h = 2^{h-1} + \mathcal{E}_o 2^{\ell_o}, \tag{22}$$

$$|f_1|_{m-h} = 2^{m-h-1} + \mathcal{E}_1 2^{\ell_1}, \tag{23}$$

where $\mathcal{E}_i$ $(i = 0, 1)$ is either 0, 1 or -1 and

$$h/2 - 1 \leq \ell_o \leq h-1 \tag{24}$$

$$(m-h)/2 - 1 \leq \ell_1 \leq (m-h) - 1. \tag{25}$$

It is easy to check that

$$|f|_m = |f_o|_h \,(2^{m-h} - |f_1|_{m-h}) + |f_1|_{m-h}\,(2^h - |f_o|_m).$$

By (22) and (23),

$$\begin{aligned} |f|_m &= (2^{h-1} + \mathcal{E}_o 2^{\ell_o})(2^{m-h-1} - \mathcal{E}_1 2^{\ell_1}) + (2^{h-1} - \mathcal{E}_o 2^{\ell_o})(2^{m-h-1} + \mathcal{E}_1 2^{\ell_1}) \\ &= 2^{m-h-1} - \mathcal{E}_o \mathcal{E}_1 2^{\ell_o + \ell_1 + 1} \end{aligned}$$

By (24) and (25),

$$m/2 - 1 \leq \ell_o + \ell_1 + 1 \leq m-1.$$

Since $\mathcal{E}_o \mathcal{E}_1$ is either 0, 1 or -1, the lemma holds. Q.E.D.

The following theorem follows from the definition of Reed-Muller codes and Lemma 5.

Theorem 6: The weight of a code vector of the second order Reed-Muller code of length 2^m is of the form:

$$2^{m-1} + \mathcal{E}\, 2^{\ell},$$

where $m/2 - 1 \leq \ell \leq m-1$ and $\mathcal{E}$ is either 0, 1 or -1.

4. SUBCODES OF THE SECOND-ORDER MODIFIED REED-MULLER CODES

In what follows, the weight distributions of subcodes of the second order modified Reed-Muller code will be considered.

Lemma 7: A cyclic code C with overall parity check is a subcode of the second order modified Reed-Muller code of length 2^m-1, if and only if the generator g(X) is of the form:

$$g(X) = (X^{2^m-1} - 1) / (h_1(X)\dots h_p(X)),$$

where $h_1(X), \dots, h_p(X)$ are different irreducible polynomials and there are integers μ_i $(1 \leq i \leq p)$ such that

$$0 \leq \mu_1 < \mu_2 < \dots < \mu_p \leq m/2,$$

$$h_i(\alpha^{-2^{\mu_i}-1}) = 0.$$

Proof: It follows from Theorem 3 that if $h_i(\alpha^j) = 0$ $(0 < j < 2^m-1)$, then $m-2 \leq w(j) < m$. Hence, $j = 2^m - 1 - j'$, where $1 \leq w(j') \leq 2$. If $w(j') = 1$, let $\mu_i = 0$. Q.E.D.

If $\mu_1 = 0$, the extended code of C is invariant under permutation group π by Theorem 1 and, consequently, the symmetry properties (2) and (3) hold for C. If $\mu_i = m/2$, the degree of $h_i(X)$ is m/2. Otherwise, the degree of $h_i(X)$ is m. (Refer to [12].) Hence, if $\mu_p = m/2$, then $k = (2p-1)m/2$, and otherwise $k = pm$.

Theorem 8: Suppose that code C satisfies the condition of Lemma 7 and that $p \geq 2$. If $\mu_1 = 0$, let $\mu = \mu_2$. Otherwise, let $\mu = \mu_1$. Then the weight of a nonzero code vector of C is of the form:

$$2^{m-1} + \varepsilon\, 2^{\ell},$$

where $m/2-1 \leq \ell \leq m-1-\mu$ and ε is either 0, 1 or -1.

Proof: Let C_o be the cyclic code of length 2^m-1 generated by $g(X)/(X-1)$. Then C is the set of the code vectors of even weight in C_o. It is easy to check that, for $1 \leq \mu_i \leq m/2$, $2^{m-1} - 2^{m-1-\mu_i}-1$ is the smallest among the positive exponents of the roots of $h_i(X)$. Hence, the minimum distance of C_o is at least $2^{m-1} - 2^{m-1-\mu} - 1$ by the BCH bound [5]. Since C_o contains all-one vector e, there is no code vector of weight j with $2^{m-1} + 2^{m-1-\mu} \leq j < 2^m - 1$. Thus, this theorem follows from Theorem 6 and Lemma 7. Q.E.D.

For $0 \leq i \leq [(m-1)/2]$, let

$$\bar{a}_i = a_{2^{m-1}-2^{[(m-1)/2]+i}} + a_{2^{m-1}+2^{[(m-1)/2]+i}} \tag{26}$$

From Theorem 8, it follows that, for even ℓ,

$$I_\ell = \sum_{i=0}^{[m/2]-\mu} 2^{\ell[(m-1)/2]+\ell i}\,\bar{a}_i \tag{27}$$

Lemma 9: Let $m \geq 3$. If $\mu_1 = 0$, $\mu_i = [m/2] - p+i$ $(2 \leq i \leq p)$ and $[m/2] - [m/3] + 2 \geq p$, then code C is a $(2^{m-1} - 2^{m-[m/2]+p-3})$-BCH code.

Proof: For $0 < j < 2^m-1$, let j_{min} denote the smallest exponent of the roots of the minimum polynomial of α^j. If $g(\alpha^j) = 0$ and $w(j) \leq m-3$, then $j_{min} \leq 2^m-1 - (2^{m-1} + 2^{m-[m/3]-1} + 2^{[m/3]-1})$.

Hence,

$$j_{min} < 2^{m-1} - 2^{m-[m/3]-1} - 1 \leq 2^{m-1} - 2^{m-[m/2]+p-3} - 1.$$

If $g(\alpha^j) = 0$ and $w(j) = m-2$, then

$$j_{min} \leq 2^m - 1 -(2^{m-1} + 2^{m-1-[m/2]+p-1}) < 2^{m-1} - 2^{m-[m/2]+p-3} -1.$$

On the other hand, if $g(\alpha^j) \neq 0$,

$$j_{min} \geq 2^m-1 -(2^{m-1}+2^{m-[m/2]+p-3}) = 2^{m-1} - 2^{m-[m/2]+p-3}-1.$$

Thus, this lemma follows from the definition of $(2^{m-1}-2^{m-[m/2]+p-3})$-BCH codes. Q.E.D.

It is easy to check that $b_1 + b_2 = 0$, if and only if the exponent of $g(X)$ is equal to 2^m-1. Hereafter, this condition will be assumed. Let $(\ell_1, \ldots, \ell_f)$ denote the greatest common divisor of $\ell_1, \ldots$ and ℓ_f.

Lemma 10: Let $\mu_1 = 0$. Then $b_3 + b_4 \neq 0$, if and only if $(m, \mu_2, \ldots, \mu_p) > 1$.

Proof: From (3)

$$4\, b_4 = (2^m-4)\, b_{2^m-4}.$$

Since the dual code of C contains all-one vector $(1, \ldots, 1)$,

$$b_{2^m-1-3} = b_3.$$

Hence, $b_3 + b_4 \neq 0$ if and only if $b_3 \neq 0$. Assume that α^{j_1}, α^{j_2} and α^{j_3} are the location numbers of non-zero components of a code vector of weight 3 in C. Then,

$$\alpha^{j_1} + \alpha^{j_2} = \alpha^{j_3}, \tag{28}$$

$$\alpha^{j_1(2^{\mu_i}+1)} + \alpha^{j_2(2^{\mu_i}+1)} = \alpha^{j_3(2^{\mu_i}+1)}, \quad (1 < i \leq p) \tag{29}$$

From (28),

$$\alpha^{j_3(2^{\mu_i}+1)} = (\alpha^{j_1} + \alpha^{j_2})^{2^{\mu_i}+1}$$

$$= \alpha^{j_1(2^{\mu_i}+1)} + \alpha^{j_1 2^{\mu_i}} \alpha^{j_2} + \alpha^{j_1} \alpha^{j_2 2^{\mu_i}} + \alpha^{j_2(2^{\mu_i}+1)} \tag{30}$$

By subtracting (29) from (30),

$$\alpha^{j_1 2^{\mu_i}} \alpha^{j_2} + \alpha^{j_1} \alpha^{j_2 2^{\mu_i}} = 0,$$

$$\alpha^{(j_1-j_2)(2^{\mu_i}-1)} = 1.$$

Thus, for $1 < i \leq p$,

$$(j_1-j_2)(2^{\mu_i}-1) \equiv 0 \pmod{2^m-1}.$$

Since $j_1-j_2 \not\equiv 0 \pmod{2^m-1}$, the "only if part" of the lemma follows. The converse can be proved similarly. Q.E.D.

5. WEIGHT DISTRIBUTION FORMULAS

Several cases will be considered in detail.

(a) $p = 2$ and $\mu_1 = 0$.

If $\mu_2 = m/2$, then $k = 3m/2$, and otherwise, $k = 2m$. For examples, $(2^{m-1} - 2^{m-[m/2]-1})$-BCH codes and the duals of double-error-correcting BCH codes belong to this case. Since the order of permutation group π is $2^m(2^m-1)$ and the number of code vectors is 2^{2m} or $2^{3m/2}$, Lemma 2 is very useful. By using Lemma 2 and power moment identities (9) and (10), the weight distribution formula is derived for any μ_2.

<u>Theorem 11</u>: Let $p = 2$ and $\mu_1 = 0$.

(1) If $(m, \mu_2) = (m, 2\mu_2) = c$, then

$$a_{2^{m-1} \pm 2^{(m+c)/2-1}} = (2^{m-c-1} \mp a^{(m-c)/2-1})(2^m-1),$$

$$a_{2^{m-1}} = (2^m - 2^{m-c} + 1)(2^m - 1),$$

$$a_j = 0, \quad \text{for other nonzero } j.$$

(2) If $2(m, \mu_2) = (m, 2\mu_2) = c$ and $c \neq m$, then

$$a_{2^{m-1} \pm 2^{(m+c)/2-1}} = 2^{(m-c)/2-1}(2^{(m-c)/2} \mp 1)(2^m-1)/(2^{c/2}+1),$$

$$a_{2^{m-1} \pm 2^{m/2-1}} = 2^{(m+c)/2-1}(2^{m/2} \mp 1)(2^m-1)/(2^{c/2}+1),$$

$$a_{2^{m-1}} = ((2^{c/2}-1)\, 2^{m-c} + 1)(2^m - 1),$$

$$a_j = 0, \quad \text{for other nonzero } j.$$

(3) If $2(m, \mu_2) = (m, 2\mu_2) = m$, then

$$a_{2^{m-1} \pm 2^{m/2-1}} = (2^{m-1} \mp 2^{m/2-1})(2^{m/2}-1),$$

$$a_{2^{m-1}} = 2^m-1,$$

$$a_j = 0, \quad \text{for other nonzero } j.$$

The proof is given in [12].

The following theorem is due to Pless [7].

Theorem 12: If only u a_j's are unknown, and $b_1, b_2, \ldots, b_{u-1}$ are known, then a unique solution to (1) exists.

(b) m = odd and k = 2m.

Theorem 13: Let C be any binary linear code for which $b_1 = b_2 = 0$, $n = 2^m - 1$ and $k = 2m$, where m is an odd integer.

(i) Let j_o denote the smallest j such that

$$a_j + a_{2^m-j} \neq 0 \quad 0 < j < 2^{m-1}.$$

Then,

$$j_o \leq 2^{m-1} - 2^{(m-1)/2}.$$

If j_o is identical with the upperbound $2^{m-1} - 2^{(m-1)/2}$, the weight distribution is the same as the weight distribution of the dual code of a double-error-correcting BCH code:

$$a_{2^{m-1} \pm 2^{(m-1)/2}} = (2^{m-2} \mp 2^{(m-3)/2})(2^m-1),$$

$$a_{2^{m-1}} = (2^{m-1} + 1)(2^m-1),$$

$$a_j = 0, \text{ for other nonzero } j.$$

(ii) If C is a subcode of the second order modified Reed-Muller code for which $b_3 = b_4 = 0$, C has the weight distribution mentioned above.

Proof: By (9) and (10),

$$I_2 = 2^{2m-2}(2^m - 1),$$

$$I_4 = 2^{3m-3}(2^m - 1) + 3\cdot 2^{2m-1}(b_3 + b_4)$$

Thus,

$$I_4 - 2^{m-1} I_2 = \sum_{j_o \leq j < 2^{m-1}} (2^{m-1} - j)^2 \left[(2^{m-1} - j)^2 - 2^{m-1}\right](a_j + a_{2^m - j})$$

$$= 3\cdot 2^{2m-1}(b_3 + b_4). \tag{31}$$

Hence,

$$(2^{m-1} - j_o)^2 \geq 2^{m-1} \tag{32}$$

If $j_o = 2^{m-1} - 2^{(m-1)/2}$, it follows from (31) that for $j_o < j < 2^{m-1}$,

$$a_j + a_{2^m - j} = 0$$

and that

$$b_3 + b_4 = 0.$$

Since only $a_{2^{m-1} \pm 2^{(m-1)/2}}$ and $a_{2^{m-1}}$ are unknown, part (i) follows from Theorem 12. The weight distribution of the dual code of a double-error-correcting BCH code is given by letting $\mu_2 = 1$ in Theorem 11 (1).

Consider part (ii). By Theorem 8, for $2^{m-1} - 2^{(m-1)/2} < j < 2^{m-1}$,

$$a_j + a_{2^m - j} = 0.$$

Since $b_3 + b_4 = 0$, for $j \neq 0$, $2^{m-1} \pm 2^{(m-1)/2}$ and 2^{m-1},

$$a_j + a_{2^m - j} = 0.$$

Thus part (ii) follows from Theorem 12. Q.E.D.

The results in cases (a) and (b) can be applied to the cross-correlation problem of two maximum length sequences [12, 13].

(c) $(2^{m-1} - 2^{m/2})$-BCH codes for even $m \geq 4$.

Let $p = 3$, $\mu_1 = 0$, $\mu_2 = m/2-1$ and $\mu_3 = m/2$. Then $k = 5m/2$. Lemma 9 shows that this code is a $(2^{m-1} - 2^{m/2})$-BCH code. Therefore,

$$\bar{a}_i = 0 \quad (i \geq 2). \tag{33}$$

Since $m/2-1$ is relatively prime to $m/2$, it follows from Lemma 10 that

$$b_3 + b_4 = 0.$$

By (9) and (10),

$$I_2 = 2^{2m-2} (2^{3m/2} - 1),$$

$$I_4 = 2^{7m/2-4} (2^{m/2} - 1)(3 \cdot 2^{m/2} + 2).$$

By solving (27) for $\ell = 2$ and 4,

$$\bar{a}_o = 2^m (2^{m/2} - 1)(2^m + 2^{m/2+1} + 4)/3,$$

$$\bar{a}_1 = 2^{m+2} (2^{m/2+1} - 1)(2^m - 1)/3.$$

By using (2), the following theorem is obtained.

<u>Theorem 14</u>: For even $m \geq 4$, a $(2^{m-1} - 2^{m/2})$-BCH code has the following weight distribution:

$$a_{2^{m-1} \pm 2^{m/2}} = 2^{m/2-2} (2^{m/2-1} \mp 1)(2^{m/2+1} - 1)(2^m - 1)/3$$

$$a_{2^{m-1} \pm 2^{m/2-1}} = 2^{m/2-1} (2^{m/2} \mp 1)(2^{m/2} - 1)(2^m + 2^{m/2+1} + 4)/3,$$

$$a_{2^{m-1}} = (2^{m/2} - 1)(2^{2m-1} + 2^{3m/2-2} - 2^{m-2} + 2^{m/2} + 1),$$

$$a_j = 0 \text{ for other nonzero } j.$$

(d) $p = 3$ and $m = \text{odd} \geq 5$.

In this case, $k = 3m$. By (9), (10) and (11),

$$I_2 = 2^{2m-2} (2^{2m} - 1), \tag{34}$$

$$I_4 = 3 \cdot 2^{4m-4} (2^m-1), \tag{35}$$

$$I_6 = 2^{4m-5}(7 \cdot 2^m-8)(2^m-1) + 6!\ 2^{3m-6}(b_5 + b_6). \tag{36}$$

(d1) Assume that $b_i = 0$ $(1 \leq i \leq 6)$. The dual code of a triple-error-correcting BCH code is this case.

By (27),

$$2^{m-1}\ \bar{a}_o + 2^{m-1} \sum_{i=1} 2^{2i}\ \bar{a}_i = 2^{2m-2}\ (2^{2m}-1) \tag{37}$$

$$2^{2(m-1)}\ \bar{a}_o + 2^{2(m-1)} \sum_{i=1} 2^{4i}\ \bar{a}_i = (3 \cdot 2^{4m-4})(2^m-1) \tag{38}$$

$$2^{3(m-1)}\ \bar{a}_o + 2^{3(m-1)} \sum_{i=1} 2^{6i}\ \bar{a}_i = 2^{4m-5}(7 \cdot 2^m-8)(2^m-1) \tag{39}$$

By subtracting 2^{m-1} times of (37) from (38),

$$2^{2(m-1)} \sum_{i=1} 2^{2i}(2^{2i}-1)\ \bar{a}_i = 2^{3m-3}\ (2^m-1)(2^{m-1}-1). \tag{40}$$

By subtracting 2^{m-1} times of (38) from (39),

$$2^{3(m-1)} \sum_{i=1} 2^{4i}\ (2^{2i}-1)\ \bar{a}_i = 2^{4m-2}\ (2^m-1)(2^{m-1}-1) \tag{41}$$

By subtracting 2^{m+1} times of (40) from (41),

$$\sum_{i=1} (2^{4i} - 2^{2i+2})(2^{2i}-1)\ \bar{a}_i = 0$$

Since $(2^{4i} - 2^{2i+2})(2^{2i}-1) > 0$ for $i > 1$,

$$\bar{a}_i = 0, \quad (i > 1). \tag{42}$$

From (37) and (38),

$$\bar{a}_o = 2^{m-1}\ (2^m - 1)(5\cdot 2^{m-1} + 4)/3,$$

$$\bar{a}_1 = a^{m-3}\ (2^m - 1)(2^{m-1} - 1)/3.$$

Since equation (2) holds for the dual code of a triple-error-correcting BCH code, it follows from equation (42) and Theorem 12 that equation (2) holds for other cases. Hence the weight distribution can be calculated easily.

(d2) Now consider the case where $a_j + a_{2^m - j} = 0$ for $0 < j < 2^{m-1} - 2^{(m+1)/2}$ and $b_i = 0$ for $1 \leq i \leq 4$. For example, let $\mu_1 = 0$, $\mu_2 = (m-3)/2$ and $\mu_3 = (m-1)/2$. Lemma 9 shows that this code is a $(2^{m-1} - 2^{(m+1)/2})$-BCH code. Since $(m-1)/2$ is relatively prime to m, it follows from Lemma 10 that $b_i = 0$ for $1 \leq i \leq 4$.

Theorem 12 and equation (42) imply that the weight distribution for case (d2) is the same as the one for case (d1). Consequently, for $1 \leq i \leq 6$,

$$b_i = 0.$$

Thus the following theorem holds.

<u>Theorem 15</u>: Let m be an odd integer greater than 4.

(i) A $(2^{m-1} - 2^{(m+1)/2})$-BCH code and the dual code of a triple-error-correcting BCH code have the following weight distribution:

$$a_{2^{m-1} \pm 2^{(m+1)/2}} = 2^{(m-5)/2}(2^{(m-3)/2} \mp 1)(2^m - 1)(2^{m-1} - 1)/3,$$

$$a_{2^{m-1} \pm 2^{(m-1)/2}} = 2^{(m-3)/2}(2^{(m-1)/2} \mp 1)(2^m - 1)(5\cdot 2^{m-1} + 4)/3,$$

$$a_{2^{m-1}} = (2^m - 1)(9\cdot 2^{2m-4} + 3\cdot 2^{m-3} + 1),$$

$$a_j = 0, \quad \text{for other nonzero } j.$$

(ii) These weight distribution formulas hold also for every subcode with $k = 3m$ of the second order modified Reed-Muller code that satisfies one of the following conditions:

(1) $b_i = 0$ for $1 \leq i \leq 6$.

(2) $a_j + a_{2^m - j} = 0$ for $0 < j < 2^{m-1} - 2^{(m+1)/2}$

and $b_i = 0$ for $1 \leq i \leq 4$.

(e) $(2^{m-1} - 2^{(m+3)/2})$-BCH codes for odd $m \geq 11$.

Let $p = 4$, $\mu_1 = 0$, $\mu_2 = (m-5)/2$, $\mu_3 = (m-3)/2$ and $\mu_4 = (m-1)/2$. Then $k = 4m$. From Theorem 8, $\bar{a}_i = 0$ $(i > 3)$. Lemma 9 shows that, for $m \geq 11$, this code is a $(2^{m-1} - 2^{(m+3)/2})$-BCH code. The dual code is a subcode of the dual code of a $(2^{m-1} - 2^{(m+1)/2})$-BCH code, which has minimum weight 7 by Theorem 15. Consequently,

$$b_i = 0 \quad (1 \leq i \leq 6).$$

By solving (27) for $\ell = 2$, 4 and 6 and using symmetry property (2), the following theorem is obtained.

<u>Theorem 16</u>: (i) For odd $m \geq 7$, let $p = 4$, $\mu_i = 0$, $\mu_2 = (m-5)/2$, $\mu_3 = (m-3)/2$ and $\mu_4 = (m-1)/2$. Then,

$$a_{2^{m-1} \pm 2^{(m-1)/2}} = (2^{m-1} \mp 2^{(m-1)/2})(151 \cdot 2^{2m-3} + 25 \cdot 2^m + 2^5)$$
$$(2^m - 1)/45,$$

$$a_{2^{m-1} \pm 2^{(m+1)/2}} = (2^{m-2} \mp 2^{(m-1)/2})(23 \cdot 2^{m-5} + 1)(2^{m-1} - 1)$$
$$(2^m - 1)/9,$$

$$a_{2^{m-1} \pm 2^{(m+3)/2}} = (2^{m-6} \mp 2^{(m-7)/2})(2^{m-3}-1)(2^{m-1}-1)$$

$$(2^m-1)/45,$$

$$a_{2^{m-1}} = 2^{4m} - 1 - \sum_{j \neq 0,\ 2^{m-1}} a_j,$$

$$a_j = 0, \quad \text{for other nonzero } j.$$

(ii) For $m \geq 11$, the code in (i) is a $(2^{m-1}-2^{(m+3)/2})$-BCH code.

(f) The dual codes of triple-error-correcting BCH codes for even $m \geq 6$.

Let $\mu_1 = 0$, $\mu_2 = 1$, and $\mu_3 = 2$. Then $k = 3m$. It is easy to check that this code is the dual code of a triple-error-correcting BCH code. Hence, $b_i = 0$ $(1 \leq i \leq 6)$. From (27), (34), (35) and (36),

$$2^{m-2}\,\bar{a}_o + 2^m\,\bar{a}_1 + 2^{m-2} \sum_{i\geq 2} 2^{2i}\,\bar{a}_i = 2^{2m-2}(2^{2m}-1), \tag{43}$$

$$2^{2m-4}\,\bar{a}_o + 2^{2m}\,\bar{a}_1 + 2^{2m-4} \sum_{i\geq 2} 2^{4i}\,\bar{a}_i = 3\cdot 2^{4m-4}(2^m-1), \tag{44}$$

$$2^{3m-6}\,\bar{a}_o + 2^{3m}\,\bar{a}_1 + 2^{3m-6} \sum_{i\geq 2} 2^{6i}\,\bar{a}_i = 2^{4m-5}(7\cdot 2^m-8)(2^m-1) \tag{45}$$

By eliminating $\bar{a}_o$ and $\bar{a}_1$,

$$\bar{a}_2 + 28\bar{a}_3 + \sum_{i\geq 4} c_i\bar{a}_i = 2^{m-4}(2^{m-2}-1)(2^m-1)/15,$$

where $c_i > 28$.

On the other hand, it can be shown that, for $j \geq 3$, $\bar{a}_j$ is divisible by $2^{m-4}(2^m-1)$. The proof is given in Appendix 2. Hence, it is easy to check that, for $6 \leq m \leq 10$, $\bar{a}_i = 0$ $(i \geq 3)$. Consequently, the weight distributions of the dual codes of triple-error-correcting BCH codes for m = 6, 8 and 10 can easily be found by solving equations (43), (44) and (45) and using symmetry property (2).

APPENDIX 1

The Proof of (9), (10) and (11)

Assume that code C has no code vector with odd weight. Add all-ones vector (1,..., 1) to the basis of C, and let C' denote the resulting code with k+1 information digits. Add an overall parity check to C' and denote the resulting code of length n+1 by C". Let a'_j (or a''_j) denote the number of code vectors of weight j of code C' (or C") and let b" denote the number of code vectors of weight j of the dual of code C". Then, for even j

$$a'_j = a'_{n-j} = a_j,$$

$$a''_j = a'_j + a'_{j-1} = a_j + a_{n+1-j}, \quad j \neq 0. \tag{A1}$$

It is easy to check that for odd j

$$b''_j = 0 \tag{A2}$$

and that for even $j \neq 0$

$$b''_j = b_j + b_{j-1} \tag{A3}$$

By identity (1),

$$\sum_{j=0}^{n+1} j^{\ell} a''_j = \sum_{h=0}^{n+1} (-1)^h \, b''_h \left(\sum_{\nu=0}^{\ell} \nu! \, G_{\ell}^{\nu} \, 2^{k+1-\nu} \binom{n+1-h}{n+1-\nu} \right), \tag{A4}$$

where G_{ℓ}^{ν} is a Stirling number of the second kind and $\binom{n+1-h}{n+1-\nu} = 0$ for $h > \nu$. By (A1) through (A4),

$$I_p = 2^{-1} \sum_{j=0}^{n+1} (j - (n+1)/2)^p\, a''_j - (n+1)^p\, 2^{-p}$$

$$= 2^{-1} \sum_{\ell=0}^{p} (-1)^{p-\ell} \binom{p}{\ell} (n+1)^{p-\ell}\, 2^{-p+\ell} \sum_{h=0}^{p} (-1)^h\, b''_h \sum_{\nu=0}^{\ell} \nu!$$

$$G_\ell^\nu\, 2^{k+1-\nu} \binom{n+1-h}{n+1-\nu} - (n+1)^p\, 2^{-p}$$

$$= 2^{k-p} \sum_{h=0}^{p} (-1)^h\, b''_h\, J_{ph} - (n+1)^p\, 2^{-p},$$

$$= 2^{k-p} \sum_{h=0}^{p/2} (b_{2h} + b_{2h-1})\, J_{p2h} - (n+1)^p\, 2^{-p}, \text{ for even } p, \qquad (A5)$$

where

$$J_{ph} = \sum_{\ell=0}^{p} (-1)^{p-\ell} \binom{p}{\ell} (n+1)^{p-\ell}\, 2^\ell \sum_{\nu=0}^{\ell} \nu!\, G_\ell^\nu\, 2^{-\nu} \binom{n+1-h}{n+1-\nu}.$$

By using formula

$$(n+1)n \ldots (n-\nu+2) = \sum_{f=1}^{\nu} S_\nu^f\, (n+1)^f,$$

where S_ν^f is a Stirling number of the first kind [8], we have

$$J_{po} = \sum_{\ell=0}^{p} (-1)^{p-\ell} \binom{p}{\ell} (n+1)^{p-\ell}\, 2^\ell \sum_{\nu=0}^{\ell} G_\ell^\nu\, 2^{-\nu} \sum_{f=0}^{\nu} S_\nu^f\, (n+1)^f.$$

By noting that $S_\nu^f = 0$ for $f > \nu$ and $G_\ell^\nu = 0$ for $\nu > \ell$,

$$J_{po} = \sum_{q=0}^{p} (n+1)^{p-q} \sum_{\ell=0}^{p} (-1)^\ell \binom{p}{\ell} 2^\ell \sum_{\nu=0} 2^{-\nu}\, G_\ell^\nu\, S_\nu^{\ell-q}$$

$$= \sum_{q=0}^{p} (n+1)^{p-q} \sum_{i=0}^{p} 2^i \sum_{\ell=0}^{q} (-1)^\ell \binom{p}{\ell} G_\ell^{\ell-i}\, S_{\ell-i}^{\ell-q} \qquad (A6)$$

Since $G_\ell^\ell = 1$, we have

$$J_{pp} = p! \qquad (A7)$$

By (A5), (A6), (A7) and a straightforward but tedious calculation, equations (9), (10) and (11) can be derived. Code C has been assumed to have no code vector with odd weight. However, it follows from identity (1) that the form of I_p depends on only n and k. Therefore, (9), (10) and (11) hold for the general case.

APPENDIX 2

The notations in section 2 will be used. Let $p = 3$, $j_1 = 2^m-1-3$, $j_2 = 2^m-1-5$ and $j_3 = 2^m-1-1$. It is easy to check that (1) E_{iq} ($i \neq q$, $i = 1,2$) is empty, (2) $E_{ii} = \{1\}$ ($1 \leq i \leq 3$) and (3) $E_{31} = \{0, m-1\}$ and $E_{32} = \{0, m-2\}$. From (8) it follows that

$$\beta_1' = a^{-3}\beta_1$$

$$\beta_2' = a^{-5}\beta_2$$

$$\beta_3' = a^{-3}\beta_1 b^2 + a^{-3\cdot 2^{m-1}} \beta_1^{2^{m-1}} b^{2^{m-1}}$$

$$+a^{-5} \beta_2 b^4 + a^{-5\cdot 2^{m-2}} \beta_2^{2^{m-2}} b^{2^{m-2}} + a^{-1}\beta_3$$

Let $Z = b^{2^{m-2}}$ and

$$f(Z) = a^{-5} \beta_2 Z^{2^4} + a^{-3} \beta_1 Z^{2^2} + a^{-3\cdot 2^{m-1}} \beta_1^{2^{m-1}} Z^2$$

$$+a^{-5\cdot 2^{m-2}} \beta_2^{2^{m-2}} Z.$$

If β_1 or β_2 is not equal to zero, the zeros of $f(Z)$ form a σ-dimensional subspace of $GF(2^m)$, where $1 \leq \sigma \leq 4$. Thus, for fixed a, β_1, β_2, and β_3, the number of elements of $\{\beta_3' \mid \beta_3' = f(Z) + a^{-1}\beta_3,\ Z = b^{2^{m-2}},\ b \in GF(2^m)\}$ is ~~divisi~~ble by 2^{m-4}. Now, suppose that $v(0, \beta_1, \beta_2, \beta_3{:}X)$ has weight j with $2^{m/2+2} \leq |j - 2^{m-1}| < 2^{m-1}$. If β_1 or β_2 is equal to zero, $v(0,\beta_1, \beta_2, \beta_3{:}X)$ is a code vector of a code considered in case (a) and the weight of nonzero vector $v(0, \beta_1, \beta_2, \beta_3{:}X)$ is greater than $2^{m-1} - 2^{m/2+2} - 1$ and smaller than $2^{m-1} + 2^{m/2+2} - 1$. Hence, β_1 and β_2 can not be zero.

Let ℓ be a positive integer such that

$$3\ell \equiv 5\ell \equiv 0 \pmod{2^m-1}.$$

Then,

$$2\ell \equiv 0 \pmod{2^m-1}.$$

Hence, ℓ must be a multiple of 2^m-1. Thus the number of pairs $\{(\beta_1', \beta_2') \mid \beta_1' = a^{-3}\beta_1,\ \beta_2' = a^{-5}\beta_2,\ a \neq 0,\ a \in GF(2^m)\}$ is equal to 2^m-1. Consequently, it follows from Lemma 2 that $a_j + a_{2^m-j}$ is divisible by $2^{m-4}(2^m-1)$.

Acknowledgment

The author is grateful to Professor W. W. Peterson for many valuable suggestions and to Professors R. T. Chien and J. S. Lin for their helpful discussions.

References

[1] Peterson, W. W. (1961). Error Correcting Codes. John and Wiley, New York.

[2] Mattson, H. F. (1965). Research program to extend the theory of weight distribution and related problems for cyclic error-correcting codes. Applied Research Lab., Sylvania Electronic Lab., Waltham, Massachusetts.

[3] Prange, E. Unpublished paper.

[4] Peterson, W. W. (1965). On the weight structure and symmetry of BCH codes. Report of University of Hawaii, Contract No. AF19(628)-4379, No. 1.

[5] Bose, R. C., and Ray-Chaudhuri, D. K. (1960). On a class of error-correcting binary group codes. Inf. and Control, 3 68-79.

[6] MacWilliams, F. J. (1962). A theorem on the distribution of weights in a systematic code. Bell System Tech. J. 42 79-94.

[7] Pless, V. (1963). Power moment identities on weight distributions in error correcting codes. Inf. and Control, 6 147-152.

[8] Jordan, C. (1950). Calculus of Finite Differences. 2nd ed. Chelsea, New York.

[9] Muller, D. E. (1954). Application of Boolean algebra to switching circuit design and to error detection. IRE Trans. EC-3 6-12.

[10] Kasami, T. and Lin, J. S. (1966). Some invariant properties of Reed-Muller codes and their application. Report of University of Hawaii, Contract No. AF19(628)-4379, No. 6.

[11] Mattson, H. F. and Solomon, G. (1961). A new treatment of Bose-Chaudhuri codes. J. Soc. Indust. Appl. Math. 9 654-669.

[12] Kasami, T. (1966). Weight distribution formula for some class of cyclic codes. Report of Coordinated Science Lab., University of Illinois, R-285.

[13] Gold, R. and Kopitzka, E. (1965). Study of correlation properties of binary sequences. Report of Magnavox Research Lab. Vol. 1-5.

Distribution list as of May 1, 1966

1 Dr. Edward M. Reilley
Asst. Director (Research)
Ofc. of Defense Res. & Engrg.
Department of Defense
Washington, D. C. 20301

1 Office of Deputy Director
(Research and Information Rm 3D1037)
Department of Defense
The Pentagon
Washington, D. C. 20301

1 Director
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Director for Materials Sciences
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Headquarters
Defense Communications Agency (333)
The Pentagon
Washington, D. C. 20305

20 Defense Documentation Center
Attn: TISIA
Cameron Station, Building 5
Alexandria, Virginia 22314

1 Director
National Security Agency
Attn: Librarian C-332
Fort George G. Meade, Maryland 20755

1 Weapons Systems Evaluation Group
Attn: Col. Finis G. Johnson
Department of Defense
Washington, D. C. 20305

1 National Security Agency
Attn: R4-James Tippet
Office of Research
Fort George G. Meade, Maryland 20755

1 Central Intelligence Agency
Attn: OCR/DD Publications
Washington, D. C. 20505

1 AFRSTE
Hqs. USAF
Room 1D-429, The Pentagon
Washington, D. C. 20330

1 AUL3T-9663
Maxwell Air Force Base, Alabama 36112

1 AFFTC (FTBPP-2)
Technical Library
Edwards AFB, California 93523

1 Space Systems Division
Air Force Systems Command
Los Angeles Air Force Station
Los Angeles, California 90045
Attn: SSSD

1 SSD(SSTRT/Lt. Starbuck)
AFUPO
Los Angeles, California 90045

1 Det. #6, OAR (LOOAR)
Air Force Unit Post Office
Los Angeles, California 90045

1 Systems Engineering Group (RTD)
Technical Information Reference Branch
Attn. SEPIR
Directorate of Engineering Standards
& Technical Information
Wright-Patterson AFB, Ohio 45433

1 ARL (ARIY)
Wright-Patterson AFB, Ohio 45433

1 AFAL (AVT)
Wright-Patterson AFB, Ohio 45433

1 AFAL (AVTE/R. D. Larson)
Wright-Patterson AFB, Ohio 45433

1 Office of Research Analyses
Attn: Technical Library Branch
Holloman AFB, New Mexico 88330

2 Commanding General
Attn: STEWS-WS-VT
White Sands Missile Range
New Mexico 88002

1 RADC (EMLAL-I)
Griffiss AFB, New York 13442
Attn: Documents Library

1 Academy Library (DFSLB)
U. S. Air Force Academy
Colorado 80840

1 FJSRL
USAF Academy, Colorado 80840

1 APGC (PGBPS-12)
Eglin AFB, Florida 32542

1 AFETR Technical Library
(ETV, MU-135)
Patrick AFB, Florida 32925

1 AFETR (ETLLG-I)
STINFO Officer (for Library)
Patrick AFB, Florida 32925

1 AFCRL (CRMXLR)
AFCRL Research Library, Stop 29
L. G. Hanscom Field
Bedford, Massachusetts 01731

2 ESD (ESTI)
L. G. Hanscom Field
Bedford, Massachusetts 01731

1 AEDC (ARO, INC)
Attn: Library/Documents
Arnold AFS, Tennessee 37389

2 European Office of Aerospace Research
Shell Building
47 Rue Cantersteen
Brussels, Belgium

5 Lt. Col. E. P. Gaines, Jr.
Chief, Electronics Division
Directorate of Engineering Sciences
Air Force Office of Scientific Research
Washington, D. C. 20333

1 U. S. Army Research Office
Attn. Physical Sciences Division
3045 Columbia Pike
Arlington, Virginia 22204

1 Research Plans Office
U. S. Army Research Office
3045 Columbia Pike
Arlington, Virginia 22204

1 Commanding General
U. S. Army Materiel Command
Attn: AMCRD-RS-PE-E
Washington, D. C. 20315

1 Commanding General
U. S. Army Strategic Communications Command
Washington, D. C. 20315

1 Commanding Officer
U. S. Army Materials Research Agency
Watertown Arsenal
Watertown, Massachusetts 02172

1 Commanding Officer
U. S. Army Ballistics Research Laboratory
Attn: V. W. Richards
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commandant
U. S. Army Air Defense School
Attn: Missile Sciences Division C&S Dept.
P. O. Box 9390
Fort Bliss, Texas 79916

1 Commanding General
U. S. Army Missile Command
Attn: Technical Library
Redstone Arsenal, Alabama 35809

1 Commanding General
Frankford Arsenal
Attn: SMUFA-L6000 (Dr. Sidney Ross)
Philadelphia, Pennsylvania 19137

1 U. S. Army Munitions Command
Attn: Technical Information Branch
Picatinney Arsenal
Dover, New Jersey 07801

1 Commanding Officer
Harry Diamond Laboratories
Attn: Mr. Berthold Altman
Connecticut Avenue & Van Ness Street N. W.
Washington, D. C. 20438

1 Commanding Officer
U. S. Army Security Agency
Arlington Hall
Arlington, Virginia 22212

1 Commanding Officer
U. S. Army Limited War Laboratory
Attn: Technical Director
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commanding Officer
Human Engineering Laboratories
Aberdeen Proving Ground, Maryland 21005

1 Director
U. S. Army Engineer Geodesy, Intelligence
and Mapping
Research and Development Agency
Fort Belvoir, Virginia 22060

1 Commandant
U. S. Army Command and General Staff College
Attn: Secretary
Fort Leavenworth, Kansas 66270

1 Dr. H. Robl, Deputy Chief Scientist
U. S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

1 Commanding Officer
U. S. Army Research Office (Durham)
Attn: CRD-AA-IP (Richard O. Ulsh)
Box CM, Duke Station
Durham, North Carolina 27706

1 Superintendent
U. S. Army Military Academy
West Point, New York 10996

1 The Walter Reed Institute of Research
Walter Reed Medical Center
Washington, D. C. 20012

1 Commanding Officer
U. S. Army Electronics R&D Activity
Fort Huachuca, Arizona 85163

1 Commanding Officer
U. S. Army Engineer R&D Laboratory
Attn: STINFO Branch
Fort Belvoir, Virginia 22060

1 Commanding Officer
U. S. Army Electronics R&D Activity
White Sands Missile Range, New Mexico 88002

1 Dr. S. Benedict Levin, Director
Institute for Exploratory Research
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703

1 Director
Institute for Exploratory Research
U. S. Army Electronics Command
Attn: Mr. Robert O. Parker, Executive
Secretary, JSTAC (AMSEL-XL-D)
Fort Monmouth, New Jersey 07703

1 Commanding General
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Attn: AMSEL-SC
RD-D
RD-G
RD-GF
RD-MAF-I
RD-MAT
XL-D
XL-E
XL-C
XL-S
HL-D
HL-L
HL-J
HL-P
HL-O
HL-R
NL-D
NL-A
NL-P
NL-R
NL-S
KL-D
KL-E
KL-S
KL-T
VL-D
WL-D

3 Chief of Naval Research
Department of the Navy
Washington, D. C. 20360
Attn: Code 427

4 Chief, Bureau of Ships
Department of the Navy
Washington, D. C. 20360

3 Chief, Bureau of Weapons
Department of the Navy
Washington, D. C. 20360

2 Commanding Officer
Office of Naval Research Branch Office
Box 39, Navy No. 100 F.P.O.
New York, New York 09510

3 Commanding Officer
Office of Naval Research Branch Office
219 South Dearborn Street
Chicago, Illinois 60604

1 Commanding Officer
Office of Naval Research Branch Office
1030 East Green Street
Pasadena, California

1 Commanding Officer
Office of Naval Research Branch Office
207 West 24th Street
New York, New York 10011

Distribution list as of May 1, 1966 (cont'd.)

1 Commanding Officer
Office of Naval Research Branch Office
495 Summer Street
Boston, Massachusetts 02210

8 Director, Naval Research Laboratory
Technical Information Officer
Washington, D. C.
Attn: Code 2000

1 Commander
Naval Air Development and Material Center
Johnsville, Pennsylvania 18974

2 Librarian
U. S. Naval Electronics Laboratory
San Diego, California 95152

1 Commanding Officer and Director
U. S. Naval Underwater Sound Laboratory
Fort Trumbull
New London, Connecticut 06840

1 Librarian
U. S. Navy Post Graduate School
Monterey, California

1 Commander
U. S. Naval Air Missile Test Center
Point Magu, California

1 Director
U. S. Naval Observatory
Washington, D. C.

2 Chief of Naval Operations
OP-07
Washington, D. C.

1 Director, U. S. Naval Security Group
Attn: G43
3801 Nebraska Avenue
Washington, D. C.

2 Commanding Officer
Naval Ordnance Laboratory
White Oak, Maryland

1 Commanding Officer
Naval Ordnance Laboratory
Corona, California

1 Commanding Officer
Naval Ordnance Test Station
China Lake, California

1 Commanding Officer
Naval Avionics Facility
Indianapolis, Indiana

1 Commanding Officer
Naval Training Device Center
Orlando, Florida

1 U. S. Naval Weapons Laboratory
Dahlgren, Virginia

1 Weapons Systems Test Division
Naval Air Test Center
Patuxtent River, Maryland
Attn: Library

1 Mr. Charles F. Yost
Special Assistant to the Director of Research
National Aeronautics and Space Administration
Washington, D. C. 20546

1 Dr. H. Harrison, Code RRE
Chief, Electrophysics Branch
National Aeronautics and Space Administration
Washington, D. C. 20546

1 Goddard Space Flight Center
National Aeronautics and Space Administration
Attn: Library, Documents Section Code 252
Greenbelt, Maryland 20771

1 NASA Lewis Research Center
Attn: Library
21000 Brookpark Road
Cleveland, Ohio 44135

1 National Science Foundation
Attn: Dr. John R. Lehmann
Division of Engineering
1800 G Street, N. W.
Washington, D. C. 20550

1 U. S. Atomic Energy Commission
Division of Technical Information Extension
P. O. Box 62
Oak Ridge, Tennessee 37831

1 Los Alamos Scientific Laboratory
Attn: Reports Library
P. O. Box 1663
Los Alamos, New Mexico 87544

2 NASA Scientific & Technical Information Facility
Attn: Acquisitions Branch (S/AK/DL)
P. O. Box 33
College Park, Maryland 20740

1 Director
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

1 Polytechnic Institute of Brooklyn
55 Johnson Street
Brooklyn, New York 11201
Attn: Mr. Jerome Fox
Research Coordinator

1 Director
Columbia Radiation Laboratory
Columbia University
538 West 120th Street
New York, New York 10027

1 Director
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois 61801

1 Director
Stanford Electronics Laboratories
Stanford University
Stanford, California

1 Director
Electronics Research Laboratory
University of California
Berkeley 4, California

1 Director
Electronic Sciences Laboratory
University of Southern California
Los Angeles, California 90007

1 Professor A. A. Dougal, Director
Laboratories for Electronics and
Related Sciences Research
University of Texas
Austin, Texas 78712

1 Division of Engineering and Applied Physics
210 Pierce Hall
Harvard University
Cambridge, Massachusetts 02138

1 Aerospace Corporation
P. O. Box 95085
Los Angeles, California 90045
Attn: Library Acquisitions Group

1 Professor Nicholas George
California Institute of Technology
Pasadena, California

1 Aeronautics Library
Graduate Aeronautical Laboratories
California Institute of Technology
1201 E. California Boulevard
Pasadena, California 91109

1 Director, USAF Project RAND
Via: Air Force Liaison Office
The RAND Corporation
1700 Main Street
Santa Monica, California 90406
Attn: Library

1 The Johns Hopkins University
Applied Physics Laboratory
8621 Georgia Avenue
Silver Spring, Maryland
Attn: Boris W. Kuvshinoff
Document Librarian

1 Hunt Library
Carnegie Institute of Technology
Schenley Park
Pittsburgh, Pennsylvania 15213

1 Dr. Leo Young
Stanford Research Institute
Menlo Park, California

1 Mr. Henry L. Bachmann
Assistant Chief Engineer
Wheeler Laboratories
122 Cuttermill Road
Great Neck, New York

1 University of Liege
Electronic Department
Mathmatics Institute
15, Avenue Des Tilleuls
Val-Benoit, Liege
Belgium

1 School of Engineering Sciences
Arizona State University
Tempe, Arizona

1 University of California at Los Angeles
Department of Engineering
Los Angeles, California

1 California Institute of Technology
Pasadena, California
Attn: Documents Library

1 University of California
Santa Barbara, California
Attn: Library

1 Carnegie Institute of Technology
Electrical Engineering Department
Pittsburgh, Pennsylvania

1 University of Michigan
Electrical Engineering Department
Ann Arbor, Michigan

1 New York University
College of Engineering
New York, New York

1 Syracuse University
Department of Electrical Engineering
Syracuse, New York

1 Yale University
Engineering Department
New Haven, Connecticut

1 Airborne Instruments Laboratory
Deerpark, New York

1 Bendix Pacific Division
11600 Sherman Way
North Hollywood, California

1 General Electric Company
Research Laboratories
Schenectady, New York

1 Lockheed Aircraft Corporation
P. O. Box 504
Sunnyvale, California

1 Raytheon Company
Bedford, Massachusetts
Attn: Librarian

Security Classification

DOCUMENT CONTROL DATA R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) University of Illinois Coordinated Science Laboratory Urbana, Illinois 61801	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP

3. REPORT TITLE

Weight Distribution of Bose-Chaudhuri-Hocquenghem Codes

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

5. AUTHOR(S) (Last name, first name, initial)

Kasami, Tadao

6. REPORT DATE August, 1966	7a TOTAL NO. OF PAGES 32	7b. NO. OF REFS. 13

8a. CONTRACT OR GRANT NO. b. PROJECT NO. DA 28 043 AMC 00073(E) 20014501B31F c. Also in part: National Science d. Foundation NSF GK-690 and Air Force AF 19(628)4379	9a. ORIGINATOR'S REPORT NUMBER(S) R-317 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. AVAILABILITY/LIMITATION NOTICES

Distribution of this report is unlimited

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY Joint Services Electronics Program thru U.S. Army Electronics Command Fort Monmouth, New Jersey 07703

13. ABSTRACT

Several techniques useful for finding weight distributions of the binary Bose-Chaudhuri-Hocquenghem codes (the BCH codes) of length 2^m-1 and some other cyclic codes are presented. By using (1) a relation between the BCH codes and the Reed-Muller codes, (2) the invariant property of the BCH codes (extended by the addition of an overall parity check) under a doubly transitive group of permutations on digit positions and (3) the power moment identities, explicit weight distribution formulas are derived for $(2^{m-1}-2^{m/2-j}-1)$-BCH codes with $j = 0$ and 1, $(2^{m-1}-2^{(m-1)/2+j}-1)$-BCH codes with $0 \leq j \leq 2$, the dual codes of double-error-correcting BCH codes, and some other class of cyclic codes. Here. for odd d, a d-BCH code is a BCH code of length 2 -1 which has $\beta,\beta^2,\ldots,\beta^{d-1}$ but not β^d as roots of its generator polynomial, where β is a primitive element of $GF(2^m)$.

DD FORM 1473 1 JAN 64

Security Classification

Security Classification

KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Weight Distribution Formula						
Bose-Chaudhuri-Hocquenghem Codes						
Reed-Muller Codes						

INSTRUCTIONS

1. ORIGINATING ACTIVITY: Enter the name and address of the contractor, subcontractor, grantee, Department of Defense activity or other organization (corporate author) issuing the report.

2a. REPORT SECURITY CLASSIFICATION: Enter the overall security classification of the report. Indicate whether "Restricted Data" is included. Marking is to be in accordance with appropriate security regulations.

2b. GROUP: Automatic downgrading is specified in DoD Directive 5200.10 and Armed Forces Industrial Manual. Enter the group number. Also, when applicable, show that optional markings have been used for Group 3 and Group 4 as authorized.

3. REPORT TITLE: Enter the complete report title in all capital letters. Titles in all cases should be unclassified. If a meaningful title cannot be selected without classification, show title classification in all capitals in parenthesis immediately following the title.

4. DESCRIPTIVE NOTES: If appropriate, enter the type of report, e.g., interim, progress, summary, annual, or final. Give the inclusive dates when a specific reporting period is covered.

5. AUTHOR(S): Enter the name(s) of author(s) as shown on or in the report. Enter last name, first name, middle initial. If military, show rank and branch of service. The name of the principal author is an absolute minimum requirement.

6. REPORT DATE: Enter the date of the report as day, month, year; or month, year. If more than one date appears on the report, use date of publication.

7a. TOTAL NUMBER OF PAGES: The total page count should follow normal pagination procedures, i.e., enter the number of pages containing information.

7b. NUMBER OF REFERENCES: Enter the total number of references cited in the report.

8a. CONTRACT OR GRANT NUMBER: If appropriate, enter the applicable number of the contract or grant under which the report was written.

8b, 8c, & 8d. PROJECT NUMBER: Enter the appropriate military department identification, such as project number, subproject number, system numbers, task number, etc.

9a. ORIGINATOR'S REPORT NUMBER(S): Enter the official report number by which the document will be identified and controlled by the originating activity. This number must be unique to this report.

9b. OTHER REPORT NUMBER(S): If the report has been assigned any other report numbers (either by the originator or by the sponsor), also enter this number(s).

10. AVAILABILITY/LIMITATION NOTICES: Enter any limitations on further dissemination of the report, other than those imposed by security classification, using standard statements such as:

(1) "Qualified requesters may obtain copies of this report from DDC."

(2) "Foreign announcement and dissemination of this report by DDC is not authorized."

(3) "U. S. Government agencies may obtain copies of this report directly from DDC. Other qualified DDC users shall request through
______________________________."

(4) "U. S. military agencies may obtain copies of this report directly from DDC. Other qualified users shall request through
______________________________."

(5) "All distribution of this report is controlled. Qualified DDC users shall request through
______________________________."

If the report has been furnished to the Office of Technical Services, Department of Commerce, for sale to the public, indicate this fact and enter the price, if known.

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING MILITARY ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring (paying for) the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document indicative of the report, even though it may also appear elsewhere in the body of the technical report. If additional space is required, a continuation sheet shall be attached.

It is highly desirable that the abstract of classified reports be unclassified. Each paragraph of the abstract shall end with an indication of the military security classification of the information in the paragraph, represented as (TS), (S), (C), or (U).

There is no limitation on the length of the abstract. However, the suggested length is from 150 to 225 words.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a report and may be used as index entries for cataloging the report. Key words must be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location, may be used as key words but will be followed by an indication of technical context. The assignment of links, roles, and weights is optional.

DD FORM 1 JAN 64 1473

Security Classification