INFORMATION AND CONTROL 17, 485–500 (1970)

The Weight Enumerators for Certain Subcodes of the Second Order Binary Reed–Muller Codes

E. R. BERLEKAMP

Bell Telephone Laboratories, Inc., Murray Hill, New Jersey

In this paper we obtain formulas for the number of codewords of each weight in several classes of subcodes of the second order Reed–Muller codes. Our formulas are derived from the following results: (i) the weight enumerator of the second order RM code, as given by Berlekamp-Sloane (1970), (ii) the MacWilliams–Pless identities, (iii) a new result we present here (Theorem 1), (iv) the Carlitz–Uchiyama (1957) bound, and, (iv′) the BCH bound.

The class of codes whose weight enumerators are determined includes subclasses whose weight enumerators were previously found by Kasami (1967–69) and Berlekamp (1968a, b).

We begin with a new theorem which asserts that all sufficiently low weight codewords in certain supercodes of the $(m-3)$rd order Reed–Muller code must also lie in the $(m-3)$rd order Reed–Muller code.

THEOREM 1. *If $\mathscr{B}$ is an extended cyclic code of length 2^m, which is invariant under the translational group and whose generator polynomial's roots include α^k for all k in the set*

$$k = 1; \qquad 1 + 2, 1 + 2^2, 1 + 2^3, \ldots, 1 + 2^{t-1}$$

or if there exists an s such that the generator polynomial's roots include α^k for all k in the set

$$k = 1; \qquad 1 + 2^{s+1}, 1 + 2^{s+2}, 1 + 2^{s+3}, \ldots, 1 + 2^{s+2t-1},$$

and if $\mathbf{c} \in \mathscr{B}$ is a codeword of weight $\leqslant 2t$, then $\mathbf{c}$ is also a codeword in the $(m-3)$rd order Reed–Muller code of length 2^m.

Proof. Without loss of generality, we may assume that weight $(\mathbf{c}) = 2t$. Let $X_1, X_2, X_3, \ldots, X_{2t}$ be the elements in $GF(2^m)$ corresponding to the nonzero coordinates of $\mathbf{c}$. Since $\mathscr{B}$ and the Reed–Muller code are invariant

under the same transitive group of permutations of their coordinates, there is no loss of generality in assuming that $X_{2t} = 0$. We denote the power-sum symmetric functions of the X's by

$$S_\ell = \sum_{i=1}^{2t-1} X_i{}^\ell. \tag{1}$$

It is clear that $S_{2\ell} = S_\ell{}^2$ and that $S_{1+2^\ell} = (S_{1+2^{m-\ell}})^{2^\ell}$. If α^k is a root of the code's generator polynomial, then $S_k = 0$. The roots of the generator polynomial of the $(m-3)$rd order RM code include $\alpha^{2^i(2^j+1)}$ for all non-negative i and j. Hence, if $\mathbf{c} \in \mathscr{B}$ but $\mathbf{c}$ is not in the $(m-3)$rd order RM code, then there must exist a v $(v \geqslant t)$ such that for all i

$$\begin{aligned} S_{2^i} &= 0 \\ S_{2^i(1+2^j)} &= 0 \qquad \text{for} \quad j = \begin{cases} 1, 2, 3, \ldots, v-1 & \text{if} \quad v < 2t, \\ v - 2t + 1, v - 2t + 2, \ldots, v - 1 & \text{if} \quad v \geqslant 2t. \end{cases} \\ S_{2^i(1+2^v)} &\neq 0 \end{aligned} \tag{2}$$

To show that the assumption of Eq. (2) leads to a contradiction, we will show that S_{2^v+1} can be expressed as a linear combination of $S_{2^j(2^i+1)}$ for $i < v$. To this end, we introduce the locator polynomial

$$\sigma(z) = \prod_{i=1}^{2t-1} (1 - X_i z)$$

and its reciprocal,

$$f(z) = \tilde{\sigma}(z) = \prod_{i=1}^{2t-1} (z - X_i).$$

Now if $F(z) = \sum_n F_n z^n$ is some polynomial which is a multiple of $f(z)$, then $F(X_i) = 0$ for $1 \leqslant i < 2t$ and

$$\sum_{i=1}^{2t-1} \sum_n F_n X_i{}^n = \sum_n F_n \sum_{i=1}^{2t-1} X_i{}^n = \sum_n F_n S_n = 0.$$

In other words,

$$\text{if} \quad \sum_n F_n z^n \equiv 0 \bmod f(z) \qquad \text{then} \quad \sum_n F_n S_n = 0. \tag{3}$$

We now wish to obtain an appropriate polynomial $F(z)$. To do this, we first factor $f(z)$ into two factors, $f^{(1)}(z)$ and $f^{(2)}(z)$, defined by

$$f^{(1)}(z) = \prod_{i=1}^{t-1} (z - X_i),$$

$$f^{(2)}(z) = \prod_{i=t}^{2t-1} (z - X_i).$$

Of course, the only property we really need is that $\deg f^{(1)} = t - 1$ and $\deg f^{(2)} = t$; the labelling of the indices on the X_i makes no real difference.

We next compute the least linearized multiple of $f^{(1)}(z)$. Since there are only $t - 1$ distinct residue classes modulo $f^{(1)}(z)$, the residues of $z, z^2, z^{2^2}, z^{2^3}, \ldots, z^{2^{t-1}}$ cannot be linearly independent. We may therefore obtain a nontrivial relation of the form

$$L(z) = \sum_{i=0}^{t-1} L_i z^{2^i} \equiv 0 \bmod f^{(1)}(z)$$

which implies that $f^{(1)}(z) \mid L(z)$. If $L_0 = 0$, then $L(z)$ is a perfect square, and $f^{(1)}(z)$ must also divide its square root. Therefore, we may assume that $L_0 \neq 0$, and by appropriate normalization we may take $L_0 = 1$.

In a similar manner, we may compute a polynomial $K(z)$ which satisfies

$$K(z) = \sum_{i=0}^{t} K_i z^{2^i} \equiv 0 \bmod f^{(2)}(z).$$

In this case, however, we normalize in such a way as to make $K(z)$ monic. Instead of taking the square root, we square $K(z)$ as many times as necessary to bring the degree of $K(z)$ up to 2^v. We then have

$$f^{(2)}(z) \Big| \sum_{i=v-t}^{v} K_i z^{2^i}, \qquad K_v = 1.$$

We now have

$$f^{(1)}(z) f^{(2)}(z) \mid L(z)\, K(z)$$

or

$$L(z)\, K(z) \equiv 0 \bmod f(z).$$

Since

$$L(z)\, K(z) = \sum_{i=0}^{t-1} \sum_{j=v-t}^{v} L_i K_j z^{2^i + 2^j},$$

it follows from Eq. (3) that

$$0 = \sum_{i=0}^{t-1} \sum_{j=v-t}^{v} L_i K_j S_{2^i+2^j} . \tag{4}$$

The only subscripts of S which occur in this expression are of the form

$$2^i + 2^j = 2^{\min(i,j)}(1 + 2^{|i-j|}),$$

where $v + 1 - 2t \leqslant |i - j| \leqslant v$. The upper bound on $|i - j|$ is attained only when $j = v$, $i = 0$, and since $L_0 K_v = 1$, Eq. (4) contradicts Eq. (2). Q.E.D.

We shall now show that Theorem 1, in conjunction with previously known results, enables us to determine the weight enumerators for two sequences of codes which are supercodes of the first order Reed–Muller codes and subcodes of the second order Reed–Muller codes.

DEFINITIONS. Let $[x]$ be the greatest integer less than or equal to x. For $u = 1, 2, 3, \ldots, [m/2] + 1$, let $\mathscr{B}^{(u)}$ be the extended cyclic code of length 2^m whose generator polynomial is

$$g(x) = \prod_{i=0}^{u-1} M^{(1+2^i)}(x)$$

where $M^{(j)}(x)$ is the minimal polynomial of α^j and α is a primitive element in $GF(2^m)$. Let $\mathscr{D}^{(u)}$ be the extended cyclic code of length 2^m whose generator polynomial is

$$g(x) = M^{(1)}(x) \prod_{i=0}^{u-2} M^{(1+2^{[m/2]-i})}(x),$$

if m is odd, or

$$g(x) = M^{(1)}(x)\, M^{(1+2^{m/2})}(x) \prod_{i=0}^{u-1} M^{(1+2^{[m/2]-i})}(x),$$

if m is even. The duals of $\mathscr{B}^{(u)}$ and $\mathscr{D}^{(u)}$ will be denoted by $\mathscr{A}^{(u)}$ and $\mathscr{C}^{(u)}$ respectively.

Remarks. The dimension of $\mathscr{A}^{(u)}$ is $1 + um$ except when m is even and $u = [m/2] + 1$; in that case the dimension is $1 + m(m + 1)/2$. $\mathscr{B}^{(1)}$, $\mathscr{B}^{(2)}$, and $\mathscr{B}^{(3)}$ are extended 1-, 2-, and 3-error-correcting BCH codes. $\mathscr{A}^{([m/2]+1)}$ is the second order Reed–Muller code.

The dimension of $\mathscr{C}^{(u)}$ is $1 + um$ if m is odd, but it is $1 + (u + 1/2)m$ if m is even. When $u \leqslant \lfloor (m+1)/2 \rfloor - \lfloor m/3 \rfloor + 1$, $\mathscr{C}^{(u)}$ is a BCH code.

THEOREM 2. *The weight enumerators of* $\mathscr{A}^{(u)}$ *and* $\mathscr{B}^{(u)}$ *are uniquely determined by the following*:

(i) *the weight enumerator of the second order* RM *code* $\mathscr{A}^{(\lfloor m/2 \rfloor + 1)}$, *as given by Berlekamp–Sloane* (1970),

(ii) *the MacWilliams–Pless identities,*

(iii) *Theorem* 1,

(iv) *the Carlitz–Uchiyama* (1957) *bound.*

The weight enumerators of $\mathscr{C}^{(u)}$ *and* $\mathscr{D}^{(u)}$ *are uniquely determined by* (i), (ii), (iii) *above and*

(iv′) *the* BCH *bound.*

If m *is odd, the weight enumerators for* $\mathscr{C}^{(u)}$ *and* $\mathscr{D}^{(u)}$ *are identical to the weight enumerators for* $\mathscr{A}^{(u)}$ *and* $\mathscr{B}^{(u)}$, *respectively.*

Proof. Let $A_w^{(u)}$, $B_w^{(u)}$, $C_w^{(u)}$, and $D_w^{(u)}$ be the number of codewords of weight w in $\mathscr{A}^{(u)}$, $\mathscr{B}^{(u)}$, $\mathscr{C}^{(u)}$, and $\mathscr{D}^{(u)}$, respectively. An explicit, simplified formula for $A_w^{(\lfloor m/2 \rfloor + 1)}$ is given by Berlekamp–Sloane (1970). From this, the MacWilliams–Pless identities determine $B_w^{(\lfloor m/2 \rfloor + 1)}$. Theorem 1 then gives $B_w^{(u)} = B_w^{(\lfloor m/2 \rfloor + 1)}$ for $w = 0, 1, 2, \ldots, 2u$. If m is even, the roots of the generator polynomial of $\mathscr{D}^{(u)}$ include α^k for $k = 1$ and for all k of the form $k = 1 + 2^i$; $m/2 - (u-1) \leqslant i \leqslant m/2$. Since

$$(1 + 2^{m/2+j}) \equiv 2^{m/2+j}(1 + 2^{m/2-j}) \bmod 2^m - 1,$$

the generator polynomial's roots must also include α^k for all k of the form $k = 1 + 2^i$, $m/2 - (u-1) \leqslant i \leqslant m/2 + (u-1)$. Theorem 1 then gives $D_w^{(u)} = B_w^{(m/2+1)}$ for $w = 0, 1, 2, \ldots, 2u$. If m is odd, a similar application of Theorem 1 gives $D_w^{(u)} = B_w{}^{(\lfloor m/2 \rfloor + 1)}$ for $w = 0, 1, 2, \ldots, 2u - 2$.

One of the known properties of the known $A_w^{(\lfloor m/2 \rfloor + 1)}$, which was first discovered by Kasami (1967–1969), is that

$$\begin{gathered} A_w = 0 \text{ unless } w \text{ is of the form} \\ w = 2^{m-1} + \epsilon 2^{(m+i)/2-1}, \qquad (4) \\ \text{where } \epsilon = 0 \text{ or } \pm 1 \text{ and } i \equiv m \bmod 2. \end{gathered}$$

Since $\mathscr{A}^{(u)} \subset \mathscr{A}^{(\lfloor m/2 \rfloor + 1)}$, Eq. (4) also holds for $\mathscr{A}^{(u)}$. Since $\mathscr{C}^{(u)} \subset \mathscr{A}^{(\lfloor m/2 \rfloor + 1)}$, Eq. (4) also holds for $\mathscr{C}^{(u)}$.

Restated in the terminology of binary coding theory, the Carlitz–Uchiyama (1957) bound asserts that the minimum distance of the dual of the extended t-error-correcting binary BCH code of length 2^m is bounded by

$$d \geqslant 2^{m-1} - (t-1)\,2^{m/2}.$$

Since $\mathcal{C}^{(u)}$ is a subcode of the dual of the $1 + 2^{u-2}$-error-correcting BCH code, the Carlitz–Uchiyama bound guarantees that its distance is bounded by

$$d \geqslant 2^{m-1} - 2^{m/2+u-2}. \tag{5}$$

The BCH bound asserts that Eq. (5) is also valid for $\mathscr{C}^{(u)}$. Applying this bound to Eq. (4), we deduce that

$$\begin{aligned} &A_w^{(u)} = 0 \text{ unless } w = 0, N, N/2, \text{ or some number of the form} \\ &w = 2^{m-1} \pm 2^{(m+i)/2-1}, \\ &\text{where } i \equiv m \bmod 2 \text{ and } 0 \leqslant i \leqslant 2(u-1). \end{aligned} \tag{6}$$

Since $A_0^{(u)} = A_N^{(u)} = 1$, the number of w's for which A_w (or C_w) is unknown is only $2u - 1$ or $2u + 1$, depending on whether m is odd or even. In either case, the Pless identities give us sufficient equations relating these unknown $A_w^{(u)}$ (or $C_w^{(u)}$) to the $B_j^{(u)}$ (or $D_j^{(u)}$) with sufficiently low j to be known from Theorem 1, and the Pless identities are known to have a unique solution. If m is odd, the fact that $A_w^{(u)} = C_w^{(u)}$ follows from the fact that they are the solution to the same set of Pless identities. When m is even, the Pless identities for $A_w^{(u)}$ and $C_w^{(u)}$ differ because the dimensionality of the code enters into the Pless identities. Q.E.D.

We now procede to derive explicit formulas for these weight enumerators, following the methods described in the proof of Theorem 2. The answers are naturally expressed in terms of *Guassian binomial coefficients*, which are defined as follows: For any real y and any nonnegative integer j, let

$$\begin{bmatrix} y \\ j \end{bmatrix} = \begin{cases} 1 & \text{if } j = 0, \\ \dfrac{1 - x^{y+1-j}}{1 - x^j} \begin{bmatrix} y \\ j-1 \end{bmatrix} & \text{if } j > 0, \end{cases}$$

$$[j] = \begin{cases} 1 & \text{if } j = 0, \\ (1 - x^j)[j-1] & \text{if } j > 0. \end{cases}$$

This is the conventional definition of the Guassian binomial coefficients in terms of the indeterminate x. When dealing with subcodes of the second

order Reed–Muller code, however, we shall always assume that $x = 4$. Thus, in this paper,

$$\begin{bmatrix} y \\ j \end{bmatrix} = \prod_{i=1}^{j} \frac{(1 - 4^{y+1-i})}{(1 - 4^i)}.$$

The utility of this definition may be seen be examining the weight enumerator of the second order Reed–Muller code itself, which was determined by Berlekamp and Sloane (1970) to be

$$A_{2^{m-1}\pm 2^{m-1-j}} = 2^{j(j+1)} \left\{\frac{(2^m - 1)(2^{m-1} - 1)}{4 - 1}\right\} \times \left\{\frac{(2^{m-2} - 1)(2^{m-3} - 1)}{4^2 - 1}\right\}$$
$$\cdots \times \left\{\frac{(2^{m-2j+2} - 1)(2^{m-2j+1} - 1)}{4^j - 1}\right\}$$

with the side conditions that $A_0 = A_{2^m} = 1$, $A_i = 0$ unless $i = 2^{m-1}$ or some number of the form $2^{m-1} \pm 2^{m-1-j}$, and that once the rest of the weights are known, $A_{2^{m-1}}$ can then be easily determined from the formula $\sum_i A_i = 2^{\dim \mathscr{A}}$. Since these side conditions also apply to all subcodes of the second Reed–Muller code, we assume them throughout the rest of this paper. When the Berlekamp–Sloane formulas are rewritten in terms of the Guassian binomial coefficients with $x = 4$, they become

$$A_{2^{m-1}\pm 2^{m-1-j}} = 4^{\binom{j+1}{2}} (-1)^j \begin{bmatrix} m/2 \\ j \end{bmatrix} \begin{bmatrix} (m-1)/2 \\ j \end{bmatrix} [j].$$

The Guassian binomial coefficients also prove useful in expressing the weight enumerators of the subcodes $\mathscr{A}^{(u)}$ and $\mathscr{C}^{(u)}$. The results are stated in Theorem 3.

THEOREM 3. *If m is odd,*

$$A^{(u)}_{2^{m-1}-2^{(m-1)/2+j}} = C^{(u)}_{2^{m-1}-2^{(m-1)/2+j}} = \begin{bmatrix} (m-1)/2 \\ j \end{bmatrix} 2^{m-1-2j} Q^{(u)}_j$$

where for $j = u - 2, u - 3, \ldots, 1, 0$; $Q^{(u)}_j$ is recursively given by

$$Q^{(u)}_j = 2^{mu-mj-m} - 1 - \sum_{i=1}^{u-j-2} Q^{(u)}_{j+i} \begin{bmatrix} (m-1)/2 - j \\ i \end{bmatrix}.$$

(*If* $j = u - 2$, *the vacuous sum is taken as* 0.) *If* m *is even,*

$$A^{(u)}_{2^{m-1}-2^{m/2+j-1}} = \begin{bmatrix} m/2 \\ j \end{bmatrix} 2^{m-2j} P^{(u)}_j$$

where for $j = u - 1, u - 2, \ldots, 1, 0,$

$$P^{(u)}_j = 2^{mu-mj-m+j} - 1 - \sum_{i=1}^{u-j-1} P^{(u)}_{j+i} \begin{bmatrix} m/2 - j \\ i \end{bmatrix}$$

and

$$C^{(u)}_{2^{m-1}-2^{m/2+j-1}} = \begin{bmatrix} m/2 \\ j \end{bmatrix} 2^{m-2j} R^{(u)}_j$$

where for $j = u - 1, u - 2, \ldots, 1, 0,$

$$R^{(u)}_j = 2^{m/2+mu-mj-m+j} - 1 - \sum_{i=1}^{u-j-1} R^{(u)}_{j+i} \begin{bmatrix} m/2 - j \\ i \end{bmatrix}.$$

Remarks. Theorem 3 gives the minimum distance of $\mathcal{A}^{(u)}$ and $\mathcal{C}^{(u)}$ as $d = 2^{m-1} - 2^{(m-1)/2+u-2}$ for m odd or as $d = 2^{m-1} - 2^{m/2+u-2}$ for m even. The minimum distance of $\mathcal{C}^{(u)}$ is thus identical to the lower bound given by the BCH theorem. For even m, the minimum distance of $\mathcal{A}^{(u)}$ is identical to the Carlitz–Uchiyama lower bound. For odd m, the minimum distance of $\mathcal{A}^{(u)}$ is the minimum value consistent with both the Carlitz–Uchiyama lower bound and Kasami's weight restriction for all subcodes of the second order RM code. The number of codewords of minimum weight is

$$A^{(u)}_d = (2^m - 1)\, 2^{m+3-2u} \begin{bmatrix} (m-1)/2 \\ u - 2 \end{bmatrix} \qquad (m \text{ odd}),$$

$$A^{(u)}_d = (2^{u-1} - 1)\, 2^{m-2u+2} \begin{bmatrix} m/2 \\ u - 1 \end{bmatrix} \qquad (m \text{ odd}),$$

$$C^{(u)}_d = (2^{m/2+u-1} - 1)\, 2^{m-2u+2} \begin{bmatrix} m/2 \\ u - 1 \end{bmatrix} \qquad (m \text{ odd}).$$

The recursions given here for Q, P, and R are easiest to apply when u is small and m is large. In certain other cases, different recursions may be preferable. Indeed, when $u = (m+1)/2$, $\mathcal{A}^{(u)}$ is the full second order RM code and the recursion of Q has a simple solution. The formula for $R^{(m/2)}$ also has a simple solution for the same reason.

It is easily seen by induction that every Q is divisible by $2^m - 1$. For

some purposes, it may be preferable to alter the recursion in order to compute $Q/(2^m - 1)$ instead of Q.

The proof of Theorem 3 is based on three Lemmas:

LEMMA 1. *If either y or z is an integer, then*

$$\sum_j x^{\binom{j}{2}}(-1)^j \begin{bmatrix} y \\ j \end{bmatrix}\begin{bmatrix} z \\ j \end{bmatrix}[j] = x^{yz}.$$

Proof. Without loss of generality, we may assume that y is integral. If $y = 0$, then

$$\sum_j x^{\binom{j}{2}}(-1)^j \begin{bmatrix} 0 \\ j \end{bmatrix}\begin{bmatrix} z \\ j \end{bmatrix}[j] = x^0(-1)^0 \begin{bmatrix} 0 \\ 0 \end{bmatrix}\begin{bmatrix} z \\ 0 \end{bmatrix}[0] = 1.$$

We procede by induction on y. We compute

$$\begin{aligned}
\sum_j x^{\binom{j}{2}}(-1)^j \begin{bmatrix} y+1 \\ j \end{bmatrix}\begin{bmatrix} z \\ j \end{bmatrix}[j] &= \sum_j x^{\binom{j}{2}}(-1)^j \left\{\begin{bmatrix} y \\ j \end{bmatrix} x^j + \begin{bmatrix} y \\ j-1 \end{bmatrix}\right\}\begin{bmatrix} z \\ j \end{bmatrix}[j] \\
&= \sum_j x^{\binom{j+1}{2}}(-1)^j \begin{bmatrix} y \\ j \end{bmatrix}\begin{bmatrix} z \\ j \end{bmatrix}[j] \\
&\quad - \sum_j x^{\binom{j+1}{2}}(-1)^j \begin{bmatrix} y \\ j \end{bmatrix}\begin{bmatrix} z \\ j+1 \end{bmatrix}[j+1] \\
&= \sum_j x^{\binom{j+1}{2}}(-1)^j \begin{bmatrix} y \\ j \end{bmatrix}\begin{bmatrix} z \\ j \end{bmatrix}[j]\{1 - (1 - x^{z-j})\} \\
&= x^z \sum_j x^{\binom{j}{2}}(-1)^j \begin{bmatrix} y \\ j \end{bmatrix}\begin{bmatrix} z \\ j \end{bmatrix}[j] = x^{(y+1)z}.
\end{aligned}$$

Q.E.D.

LEMMA 2. *For integral y or z,*

$$\sum_j x^{\binom{j}{2}}(-1)^j \begin{bmatrix} y \\ j \end{bmatrix}\begin{bmatrix} z \\ j \end{bmatrix}[j]\begin{bmatrix} z-j \\ k \end{bmatrix} = \begin{bmatrix} z \\ k \end{bmatrix} x^{y(z-k)}.$$

Proof. Replace the z of Lemma 1 by $z - k$ to obtain

$$\sum_j x^{\binom{j}{2}}(-1)^j \begin{bmatrix} y \\ j \end{bmatrix}\begin{bmatrix} z-k \\ j \end{bmatrix}[j] = x^{y(z-k)}.$$

Multiplying both sides by $\begin{bmatrix} z \\ k \end{bmatrix}$ then yields Lemma 2, because

$$\begin{bmatrix} z-k \\ j \end{bmatrix} [j] \begin{bmatrix} z \\ k \end{bmatrix} [k] = \begin{bmatrix} z \\ j+k \end{bmatrix} [j+k] = \begin{bmatrix} z-j \\ k \end{bmatrix} [k] \begin{bmatrix} z \\ j \end{bmatrix} [j].$$

Q.E.D.

LEMMA 3. *Let*

$$a_i^{(u)} = 2^{-\dim \mathcal{A}^{(u)}} A_i^{(u)}$$

and let

$$\Delta_j^{(u)} = a^{(u)}_{2^{m-1}-2^{m-1-j}} - a^{(\lfloor m/2 \rfloor+1)}_{2^{m-1}-2^{m-1-j}}$$

where $\mathcal{A}^{(\lfloor m/2 \rfloor+1)}$ *denotes the full second order Reed–Muller code. Then if* ℓ, k, *and* r *are integers such that* $0 \leqslant k$, $1 \leqslant r$, *and* $k + r \leqslant u$, *then*

$$\sum_j 4^{-rj} \Delta_j^{(u)} \begin{bmatrix} \ell - j \\ k \end{bmatrix} = 0.$$

Proof. One form of the MacWilliams–Pless identities (p. 405 of Algebraic Coding Theory) gives, for any u,

$$\sum_{i=0}^{N} (N-2i)^r a_i^{(u)} = \sum_{j=0}^{r} B_j^{(u)} F_r^{(j)}(N)$$

for $r = 0, 1, 2, \ldots$, where

$$F_r^{(j)}(N) = \left[\frac{d^r}{dz^r} \cosh^{N-j} z \sinh^j z \right]_{z=0}.$$

Fortunately, we can eliminate $B_j^{(u)}$ and $F_r^{(j)}(N)$ from the Pless identities for $r \leqslant 2u$ by applying Theorem 1, which states that for $w = 0, 1, 2, \ldots, 2u$, $B_w^{(u)} = B_w^{(\lfloor m/2 \rfloor+1)}$. Therefore, if $r \leqslant 2u$,

$$\sum_{i=0}^{N} (N-2i)^r a_i^{(u)} = \sum_{i=0}^{N} (N-2i)^r a_i^{(\lfloor m/2 \rfloor+1)}.$$

Replacing r by $2r$, we conclude that for $0 \leqslant r \leqslant u$,

$$\sum_{i=0}^{N} (N-2i)^{2r} \{a_i^{(u)} - a_i^{(\lfloor m/2 \rfloor+1)}\} = 0.$$

Since $a_i^{(u)} = a_{N-i}^{(u)}$ for all i,

$$\sum_{i=0}^{N/2} (N - 2i)^{2r} \{a_i^{(u)} - a_i^{(\lfloor m/2 \rfloor + 1)}\} = 0.$$

If $1 \leqslant r \leqslant u$, then the summand vanishes for $i = N/2$ so

$$\sum_{i=0}^{N/2-1} (N - 2i)^{2r} \{a_i^{(u)} - a_i^{(\lfloor m/2 \rfloor + 1)}\} = 0.$$

Since $a_i^{(\lfloor m/2 \rfloor + 1)}$ and $a_i^{(u)}$ vanish for all i, $0 \leqslant i < N/2$, except those of the form $i = 2^{m-1} - 2^{m-1-j}$, we set $N - 2i = 2^{m-j}$ and multiply through by 2^{-mr} to obtain

$$\sum_j 4^{-jr} A_j^{(u)} = 0$$

for $r = 1, 2, \ldots, u$. This establishes the Lemma for $k = 0$. The proof for positive k follows immediately by induction, using the identity

$$\begin{bmatrix} \ell - j \\ k \end{bmatrix} = \frac{1 - 4^{l-j+1-k}}{1 - 4^k} \begin{bmatrix} \ell - j \\ k - 1 \end{bmatrix}. \qquad \text{Q.E.D.}$$

Proof of Theorem 3. With $x = 4$, we may apply Lemma 2 to the computation of certain sums involving the weights of the second order Reed–Muller code, whose weight distribution is given by Berlekamp–Sloane (1970). Setting $y = m/2$ and $z = (m - 1)/2$ gives, for any i,

$$\sum_j 4^{-j} A^{(\lfloor m/2 \rfloor + 1)}_{2^{m-1} - 2^{m-1-j}} \begin{bmatrix} (m-1)/2 - j \\ k \end{bmatrix} = \begin{bmatrix} (m-1)/2 \\ k \end{bmatrix} 2^{m((m-1)/2-k)}.$$

Alternatively, we may set $y = (m - 1)/2$ and $z = m/2$ to obtain

$$\sum_j 4 \; A^{(\lfloor m/2 \rfloor + 1)}_{2^{m-1} - 2^{m-1-j}} \begin{bmatrix} m/2 - j \\ k \end{bmatrix} = \begin{bmatrix} m/2 \\ k \end{bmatrix} 2^{(m-1)(m/2-k)}.$$

Since the dimension of $\mathcal{R}^{(\lfloor m/2 \rfloor + 1)}$ is $1 + m(m + 1)/2$, normalization of these two identities yields the single identity

$$\sum_j 4^{-j} a^{(\lfloor m/2 \rfloor + 1)}_{2^{m-1} - 2^{m-1-j}} \begin{bmatrix} \lceil m/2 \rceil - j \\ k \end{bmatrix} = \begin{bmatrix} \lfloor m/2 \rfloor \\ k \end{bmatrix} 2^{-1-mu}(1 + h(k, m, u))$$

where, in order to simplify subsequent expressions, we have introduced the definition

$$h(k, m, u) = \begin{cases} 2^{mu-mk-m} - 1 & \text{if } m \text{ odd,} \\ 2^{mu-mk-m+k} - 1 & \text{if } m \text{ even.} \end{cases}$$

Application of Lemma 3 with $r = 1$, $\ell = \lfloor m/2 \rfloor$ now yields

$$\sum_{j \geqslant 0} 4^{-j} a^{(u)}_{2^{m-1}-2^{m-1-j}} \begin{bmatrix} \lfloor m/2 \rfloor - j \\ k \end{bmatrix} = \begin{bmatrix} \lfloor m/2 \rfloor \\ k \end{bmatrix} 2^{-1-mu}(1 + h(k, m, u)).$$

Since the dimension of $\mathscr{A}^{(u)}$ is $1 + mu$ and $A^{(u)}_0 = 1$, we may unnormalize and then subtract $\left[{\lfloor m \rfloor 2 \rfloor \atop k}\right]$ from each side of this identity to obtain

$$\sum_{j>0} 4^{-j} A^{(u)}_{2^{m-1}-2^{m-1-j}} \begin{bmatrix} \lfloor m/2 \rfloor - j \\ k \end{bmatrix} = \begin{bmatrix} \lfloor m/2 \rfloor \\ k \end{bmatrix} h(k, m, u)$$

for $k = 0, 1, 2, \ldots, u - 1$.

Another definition at this point allows us to generalize the previous identity to include the codes $\mathscr{C}^{(u)}$ as well as $\mathscr{A}^{(u)}$. If m is odd, there is no problem because $C^{(u)}(z) = A^{(u)}(z)$ by Theorem 2. To include the case of even m, however, it is convenient to define $A^{(v)}(z)$ for half-integers v by the equation $A^{(v)}(z) = C^{(v-1/2)}(z)$. Since $A^{(v)}(1) = 2^{1+mv}$ remains valid for both integral and half-integral v, the previous identity still holds.

If v is integral, the Carlitz–Uchiyama bound asserts that $A^{(v)}_\ell = 0$ unless $\ell \geqslant 2^{m-1} - 2^{m/2+v-2}$. This allows us to boost the lower limit of the summation from $j > 0$ to $j \geqslant m/2 + 1 - v$. When v is half-integral, the BCH bound applied to $\mathscr{C}^{(v-1/2)}$ allows us to boost the lower limit of the summation to $j \geqslant m/2 + 1 - v$. In either case, upper limits on the summation may be obtained from the fact that $\left[{n \atop k}\right] = 0$ whenever n is integral and $n < k$. We thus obtain the identity

$$\sum_{j=\lfloor m/2 \rfloor + 1 - \lfloor v \rfloor}^{\lfloor m/2 \rfloor - k} 4^{-j} A^{(v)}_{2^{m-1}-2^{m-1-j}} \begin{bmatrix} \lfloor m/2 \rfloor - j \\ k \end{bmatrix} = \begin{bmatrix} \lfloor m/2 \rfloor \\ k \end{bmatrix} h(k, m, v)$$

for $k = 0, 1, 2, \ldots, \lfloor v \rfloor - 1$. Replacing j by $\lfloor m/2 \rfloor - j$ gives

$$\sum_{j=k}^{v-1} 4^{-\lfloor m/2 \rfloor + j} A^{(v)}_{2^{m-1}-2^{\lfloor (m-1)/2 \rfloor + j}} \frac{\begin{bmatrix} j \\ k \end{bmatrix}}{\begin{bmatrix} \lfloor m/2 \rfloor \\ k \end{bmatrix}} = h(k, m, v).$$

We next apply the identity

$$\frac{\begin{bmatrix} j \\ k \end{bmatrix}}{\begin{bmatrix} \lfloor m/2 \rfloor \\ k \end{bmatrix}} = \frac{[j][\lfloor m/2 \rfloor - k][\lfloor m/2 \rfloor - j]}{[j-k][\lfloor m/2 \rfloor][\lfloor m/2 \rfloor - j]} = \frac{\begin{bmatrix} \lfloor m/2 \rfloor - k \\ j - k \end{bmatrix}}{\begin{bmatrix} \lfloor m/2 \rfloor \\ j \end{bmatrix}}$$

and the substitution

$$A^{(v)}_{2^{m-1}-2^{\lfloor (m-1)/2 \rfloor + j}} = \begin{bmatrix} \lfloor m/2 \rfloor \\ j \end{bmatrix} 4^{\lfloor m/2 \rfloor - j} Q_j^{(v)}$$

to obtain

$$\sum_{j=k}^{\lfloor v \rfloor - 1} Q_j^{(v)} \begin{bmatrix} \lfloor m/2 \rfloor - k \\ j - k \end{bmatrix} = h(k, m, v).$$

Finally, setting $i = j - k$ gives

$$\sum_{i=0}^{\lfloor v \rfloor - k - 1} Q_{k+i}^{(v)} \begin{bmatrix} \lfloor m/2 \rfloor - k \\ i \end{bmatrix} = h(k, m, v) = \begin{cases} 2^{mv - mk - m} - 1 & \text{if } m \text{ odd,} \\ 2^{mv - mk - m + k} - 1 & \text{if } m \text{ even.} \end{cases}$$

For odd m, $h(k, m, v) = 0$ if $k = v - 1$, and this implies that $Q_{v-1}^{(v)} = 0$. This identity is then directly equivalent to Theorem 3. Q.E.D.

COROLLARY. *If $j \geqslant m/2 - 1$, then the extended primitive* BCH *code of length 2^m and designed distance $d = 2^{m-1} - 2^j$ has codewords of weight d.*

Proof. The extended BCH code contains the subcode $\mathscr{C}^{(j+2-\lfloor (m-1)/2 \rfloor)}$ and Theorem 3 shows that this subcode contains codewords of weight d. Q.E.D.

This corollary lends further support to the conjecture that the minimum distance of all long primitive BCH codes is, in a certain asymptotic sense, essentially equal to the Bose distance. More precisely, let $I(q, n, d)$ denote the number of information symbols in the q-ary BCH code of length n and designed distance d, and let $\check{I}(q, n, d)$ denote the maximum number of information symbols in any q-ary BCH code of length n and actual distance $\geqslant d$. Berlekamp (1968) has evaluated the singular function

$$s(u) = \lim_{m \to \infty} \frac{\log I(2, 2^m - 1, u2^m)}{m} \qquad \text{for} \quad 0 < u < 1/2,$$

and conjectured that $s(u) = \check{s}(u)$, which is defined as

$$\check{s}(u) = \limsup_{m\to\infty} \frac{\log \check{I}(2, 2^m - 1, u2^m)}{m}.$$

It was previously known that $s(u) = \check{s}(u)$ for various particular values of u, including 1/2, 1/4, 1/8, 1/16,..., and certain other sequences of $u \leqslant 1/4$. The corollary of this paper shows that $s(u) = \check{s}(u)$ for $u = 1/4, 3/8, 7/16, 15/31,\ldots$. Kasami and Tokura (1968) have shown that $\check{I}(2, 2^m - 1, d) > I(2, 2^m - 1, d)$ for various particular values of m and d starting with $m = 7$, $d = 31$, but the asymptotic conjecture that $\check{s}(u) = s(u)$ for all u, $0 < u < 1/2$, remains open.

Historical Remarks

Using a variety of special arguments instead of the Carlitz–Uchiyama bound and Theorem 1 of this paper, Kasami (1967–69) obtained the formulas for the enumerators of several of the codes considered here. For even m, he enumerated $\mathscr{C}^{(1)}$, $\mathscr{C}^{(2)}$, and $\mathscr{A}^{(2)}$, and he conjectured the correct enumerator for $\mathscr{A}^{(3)}$. For odd m, he enumerated $\mathscr{A}^{(2)}$, $\mathscr{A}^{(3)}$, $\mathscr{C}^{(2)}$, $\mathscr{C}^{(3)}$, and $\mathscr{C}^{(4)}$. By further special arguments, Berlekamp (1968a) obtained enumerators for $\mathscr{C}^{(5)}$ and $\mathscr{C}^{(6)}$, odd m. Later, Berlekamp (1968b) observed that the Carlitz–Uchiyama bound completed the proof of Kasami's conjectured enumerator for $\mathscr{A}^{(3)}$, m even. The formulas for all of these codes, and several other codes not in the classes considered in this paper, are given in Tables 16.3 and 16.4 of Berlekamp (1968a).

Further Problems

Although Theorem 3 solves the weight enumeration problem for certain infinite classes of codes, and the MacWilliams–Pless identities then give the weight enumerators of their dual codes *in principle*, there remains the practical problem of actually calculating the answers and simplifying the resulting expressions for the weight enumerators of the dual codes. Even the calculation of $B_w^{(\lfloor m/2\rfloor+1)}$ from the known $A_w^{(\lfloor m/2\rfloor+1)}$ proves difficult. The relevant Pless identities yield relatively cumbersome expressions which are not easy to simplify. However, it is known that in the dual of the second order RM code,

$$B_8 = \frac{N(N-1)(N-2)(N-4)}{8 \times 7 \times 6 \times 4}.$$

Using special arguments, Berlekamp–Sloane (1969) give

$$B_{10} = 0.$$

Kasami–Tokura (1970) give

$$B_{12} = \frac{2^{m+1}(2^m - 1)(2^{m-1} - 1) \cdots (2^{m-4} - 1)}{45},$$

$$B_{14} = \frac{2^{m+8} \prod_{i=0}^{5} (2^{m-i} - 1)}{7^2 \times 3^2},$$

but no expressions of comparable simplicity are known for B_w when $w \geqslant 16$.

There are also a number of intriguing questions of a more theoretical nature. Is there some geometric characterization of the minimum weight codewords in $\mathcal{A}^{(v)}$ and $\mathcal{C}^{(v)}$, similar to that obtained by Dowling (1969) for the minimum weight codewords in $\mathcal{A}^{(2)}$ and $\mathcal{C}^{(2)}$? If so, what? Are $\mathcal{A}^{(v)}$ and $\mathcal{C}^{(v)}$ isomorphic to each other under some unexpected permutation of the coordinates? If not, how do they differ? Are their automorphism groups the same? Are their distributions of coset leaders the same?

What are the weight enumerators for other interesting classes of subcodes of the second order Reed–Muller code?

How can Theorem 1 be generalized?[1] Specifically, for an arbitrary linear cyclic code, what is the linear cyclic subcode generated by the sufficiently low weight codewords of the original code? Table 16.1 suggests that for most short cyclic codes, the minimum weight codewords generate the entire code, but Theorem 1 exhibits cases in which all codewords of weight up to and including some number much larger than the minimum weight all lie in a much smaller subcode.

Acknowledgments

I am indebted to C. L. Mallows and J. Riordan, who suggested the use of Guassian binomial coefficients and showed me how to prove some identities needed in the proof of Theorem 3.

[1] The alert reader may notice that Theorem 2 implies that when m is odd and $s = (m - 1)/2 - t$, then the conclusion of Theorem 1 remains valid when k ranges over the set

$$k = 1; \quad 1 + 2^{s+1}, 1 + 2^{s+2}, \ldots, 1 + 2^{s+2t-2}.$$

There is no known way of obtaining this strengthened form of Theorem 1 for this special case directly.

Received: February 17, 1970; Revised: May 24, 1970

643/17/5-6*

Note added in proof. While this paper was in press, Kasami showed that these same formulas also give the weight enumerators for many more subcodes of the second Reed–Muller codes. Kasami's paper will appear in a forthcoming issue of Information and Control.

References

BERLEKAMP, E. R. (1968a), "Algebraic Coding Theory," McGraw-Hill, New York.

BERLEKAMP, E. R. (1968b), Weight enumeration theorems, *Proc. Sixth Allerton Conf. Circuit and Systems Theory*, pp. 161–170. Univ. of Illinois Press, Urbana, Ill.

BERLEKAMP, E. R., AND SLOANE, N. J. A. (1969), Restrictions on weight distribution of Reed–Muller codes, *Inform. Control* **14**, 442–456.

BERLEKAMP, E. R., AND SLOANE, N. J. A. (1970), The weight enumerator of second order Reed–Muller codes, *Proc. IEEE Trans. Inform. Th.* **IT-16**, 745-751.

CARLITZ, L., AND UCHIYAMA, S. (1957), Bounds for exponential sums, *Duke Math. J.* **24**, 37–41.

DOWLING, T. A. (1969), A class of cyclic codes, UNC Inst. of Stat. Mimeo Series No. 600.3. Univ. of North Carolina, Chapel Hill, N. C.

KASAMI, T. (1967–69), Weight distributions of Bose–Chaudhuri–Hocquenghem codes, in "Combinatorial Mathematics and Its Applications," R. C. Bose and T. A. Dowling, Eds., pp. 335–357.

KASAMI, T., AND TOKURA, N. (1969), Some remarks on BCH bounds and minimum weights of binary primitive BCH codes, *IEEE Trans. Inform. Th.* **IT-15**, 408–413.

KASAMI, T., AND TOKURA, N. (1970), On the weight structure of Reed–Muller codes, *IEEE Trans. Inform. Theory*, **IT-16**, 752-759.