Nonlinear Codes Defined by Quadratic Forms over GF(2)

JEAN-MARIE GOETHALS

MBLE Research Laboratory, Brussels, Belgium

An investigation is made of the family of codes which are supercodes of the first-order and subcodes of the second-order Reed-Muller codes. These codes are in a one-to-one correspondence with subsets of alternating bilinear forms and it is shown how their distance enumerators can be obtained. A nice duality relation is defined on the set of linear codes in this family which relates their weight enumerators. The best codes of this family are defined and constructed, most of which are new nonlinear codes. The main part of the paper is devoted to a proof of the properties of the “dual” families of nonlinear codes which were announced in a letter by Goethals (1974).

1. INTRODUCTION

The first- and second-order Reed-Muller codes are described by the sets \( \mathcal{L} \) and \( \mathcal{Q} \) of all linear and quadratic forms, respectively, on a vector space \( V \) over the binary field. As shown by Cameron and Seidel (1973), there is a natural indexing of the cosets of \( \mathcal{Q} \) in \( \mathcal{L} \) by the elements of the set \( \mathcal{B} \) of all bilinear forms on \( V \). In this paper, we shall mainly be concerned with the family of codes that are supercodes of the first-order and subcodes of the second-order Reed-Muller codes. These codes are in one-one correspondence with the subsets \( Y \subseteq \mathcal{B} \) which were studied by Delsarte and Goethals (1975), as we show in Section 2. In Section 3, we shall use their results to obtain a useful description of the codes in the above family. In particular, we show that there exists, among the linear codes of this family, a nice “duality relation” which relates their weight enumerators by an identity similar to that of MacWilliams (1963). In Section 4, by use of the results of Delsarte and Goethals (1975), we describe a construction of the best codes in this family, which we call \( r \)-optimal: for a given length \( 2^m - 1 \) and minimum distance \( 2^{m-1} - 2^{m-1-r} \), they are the codes with the largest cardinality. For \( m \) odd, these codes were already discovered by Berlekamp (1970); for \( m \) even, they are nonlinear and all are new, except for the codes discovered by Kerdock (1972) which are \( (m/2) \)-optimal codes in this family. A nice feature about the Kerdock...
codes is that their distance enumerator is related to that of the nonlinear codes discovered by Preparata (1968) by the MacWilliams identity, (cf. MacWilliams et al., 1972). A similar property holds for the infinite family of pairs of nonlinear codes $C, C'$, described by Goethals (1974), where $C'$ is obtained from a $(m/2 - 1)$-optimal code and $C$ with minimum distance 8 contains four times as many codevectors as the extended BCH code of the same length and minimum distance. The main part of this paper, Section 5, is devoted to a proof of the properties of these codes which were announced in a letter by Goethals (1974). Finally, in Section 6, we show how easily the weight enumerators of some cyclic subcodes of the second-order Reed-Muller codes can be derived by our methods. These weight enumerators were already obtained by Kasami (1969) and Kerdock et al. (1974), but we feel that our approach was worth mentioning.

2. QUADRATIC FORMS AND SECOND-ORDER REED--MULLER CODES

The geometric nature of Reed-Muller codes is now widely known (cf. Peterson and Weldon, 1972). Here, we shall give an account of these codes, starting from purely geometrical concepts. Let $V = V(m, 2)$ be an $m$-dimensional vector space over the field $\mathbb{F} = GF(2)$, $(m \geq 2)$. A linear form on $V$ is a function $L$ from $V$ to $\mathbb{F}$ satisfying

$$L \left( \sum a_i \xi_i \right) = \sum a_i L(\xi_i), \quad \forall a_i \in \mathbb{F}, \quad \forall \xi_i \in V.$$ 

The set $\mathcal{L}$ of all linear forms on $V$, usually called the dual space of $V$, is itself an $m$-dimensional vector space over $\mathbb{F}$. A bilinear form on $V$ is a function $B(\cdot, \cdot)$ from $V \times V$ to $\mathbb{F}$ satisfying

$$B \left( \sum a_i \xi_i, \sum b_j \eta_j \right) = \sum \sum a_i b_j B(\xi_i, \eta_j), \quad \forall a_i, b_j \in \mathbb{F}, \quad \forall \xi_i, \eta_j \in V.$$ 

Hence, a bilinear form on $V$ is uniquely defined by its matrix of order $m$,

$$B = [b_{i,j} = B(\delta_i, \delta_j)], \quad (1)$$

with respect to any fixed basis $(\delta_1, \delta_2, \ldots, \delta_m)$ of $V$. The bilinear form $B(\cdot, \cdot)$ is alternating if

$$B(\xi, \xi) = 0, \quad \forall \xi \in V, \quad (2)$$
from which the additional property
\[ B(\xi, \eta) + B(\eta, \xi) = 0 \] (3)
follows, as a consequence of \( B(\xi + \eta, \xi + \eta) = 0 \). From (2) and (3), we conclude that the matrix (1) of an alternating bilinear form satisfies
\[ b_{i,i} = 0, \quad b_{i,j} + b_{j,i} = 0, \quad 1 \leq i, j \leq m, \] (4)
i.e., \( B \) is skew-symmetric. Clearly, the set \( \mathcal{B} \) of all alternating bilinear forms on \( V \) is an \( \binom{m}{2} \)-dimensional vector space over \( F \). A \textit{quadratic form} on \( V \) is a function \( Q \) from \( V \) to \( F \) with the properties:

(i) \( Q(0) = 0 \), where 0 is the zero vector;

(ii) the function \( B = \phi(Q) : V \times V \rightarrow F \) defined by
\[ B(\xi, \eta) = Q(\xi + \eta) + Q(\xi) + Q(\eta), \quad \forall \xi, \eta \in V, \] (5)
is bilinear.

Note that \( B \) defined by (5) is the zero bilinear form \( B_0 \) iff \( Q \) is a linear form, and that, for any quadratic form \( Q \), it satisfies \( B(\xi, \xi) = 0, \forall \xi \in V \); hence, it is alternating.

Let \( \mathcal{Q} \) denote the set of all quadratic forms on \( V \), and let \( \phi \) be the linear function from \( \mathcal{Q} \) to \( \mathcal{B} \) which maps the quadratic form \( Q \) on the bilinear form (5). Clearly, \( \phi \) is a vector space homomorphism with kernel \( \text{Ker}(\phi) = \mathcal{L} \), the set of linear forms on \( V \). Hence, \( \mathcal{B} \) is isomorphic to \( \mathcal{Q}/\mathcal{L} \), and \( \mathcal{Q} \) has dimension \( m + \binom{m}{2} \) as a vector space over \( F \). Moreover, the map \( \phi \) identifies every coset of \( \mathcal{L} \) in \( \mathcal{Q} \) with a given alternating bilinear form (5).

For an integer \( n \), a \textit{binary code of length} \( n \) is a subset \( C \), with \( |C| \geq 2 \), of the vector space \( F^n \) of all (ordered) \( n \)-tuples over \( F \). A binary code is said to be a \textit{linear} \((n, k)\) \textit{code} if it is a \( k \)-dimensional subspace of \( F^n \). For any \( u, v \in F^n \), the \textit{weight} of \( u \), denoted by \( w(u) \), is the number of nonzero components in \( u \), and the \textit{distance} \( d(u, v) \) between \( u \) and \( v \) is the number of components in which they differ, that is, we have \( d(u, v) = w(u - v) \). We shall use the notations \( V^* = V \setminus \{0\} \) for the set of nonzero elements of \( V \), and \( F^{V^*} \) for the vector space of \((2^m - 1)\)-tuples with components in \( F \) indexed by the elements of \( V^* \), that is, for any nonzero \( \xi \in V \), and any \( u \in F^{V^*} \), \( u(\xi) \) will denote the \( \xi \)th component of \( u \). Let \( \text{RM}(m, 1) \) and \( \text{RM}(m, 2) \) denote the sets

\[
\text{RM}(m, 1) = \{ u \in F^{V^*} | u(\xi) = L(\xi), \forall \xi \in V^*; L \in \mathcal{L} \},
\]
\[
\text{RM}(m, 2) = \{ u \in F^{V^*} | u(\xi) = Q(\xi), \forall \xi \in V^*; Q \in \mathcal{Q} \}.
\]
From the above discussion, it clearly appears that the following proposition holds true.

**Proposition 1.** The set $RM(m, 1)$ is a linear $(2^m - 1, m)$ code, and $RM(m, 2)$ is a linear $(2^m - 1, (2^m - 1)/2)$ code over $\mathbb{F}$. Moreover, $RM(m, 1)$ is a subcode of $RM(m, 2)$, and every coset of $RM(m, 1)$ in $RM(m, 2)$ is identified with a given alternating bilinear form $B \in \mathcal{B}$.

The linear codes $RM(m, 1)$ and $RM(m, 2)$ are known as the **shortened Reed–Muller codes** of the first and second order, respectively (cf. Berlekamp, 1968, p. 362). The shortened $r$th-order Reed–Muller code $RM(m, r)$ is obtained similarly from the set of all functions $f : V \to \mathbb{F}$ of degree $r$ or less satisfying $f(0) = 0$. The corresponding Reed–Muller codes of length $2^m$ are obtained from the codes $RM(m, r)$ by annexing the all-one vector of length $2^m$ to their generating set (cf. Berlekamp, 1968, p. 336). For an alternative description of these codes, we refer the reader to Peterson and Weldon (1972, p. 125).

For a given alternating bilinear form $B \in \mathcal{B}$, let $\mathcal{Q}(B)$ and $C(B)$ denote the cosets attached to $B$ of $\mathcal{M}$ in $\mathcal{S}$ and of $RM(m, 1)$ in $RM(m, 2)$, respectively, that is

$$\mathcal{Q}(B) = \{ Q \in \mathcal{M} | \phi(Q) = B \},$$

$$C(B) = \{ u \in \mathbb{F}^V \times \mathbb{F}^V | u(\xi) = Q(\xi), \forall \xi \in V^*; Q \in \mathcal{Q}(B) \}.$$  

In particular, for the zero bilinear form $B_0$, we have $C(B_0) = RM(m, 1)$. In this paper, we shall mainly be concerned with binary codes consisting of a union of cosets $C(B)$ of $RM(m, 1)$ in $RM(m, 2)$, for a given subset $Y$ of $\mathcal{B}$. Clearly, the distribution of distances in the code

$$C(Y) = \bigcup_{B \in Y} C(B)$$

is obtained from the distribution of weights in the cosets $C(B - B')$, $B, B' \in Y$. As we shall see in Proposition 2 below, the distribution of weights in any coset $C(B)$ only depends on the rank $\text{rk}(B)$ of the form $B \in \mathcal{B}$. The rank $\text{rk}(B)$ of a bilinear form $B$ can be defined to be the rank over $\mathbb{F}$ of its matrix (1) with respect to any fixed basis of $V$. Thus, the rank of an alternating bilinear form necessarily is an even number; cf. (4). The distribution of weights in a code $C$ is characterized by the formal polynomial,

$$W_C(z) = \sum_{u \in C} z^{w(u)},$$

where $w(u)$ denotes the weight of the vector $u$. For a given subset $Y$ of $\mathcal{B}$, the distribution of distances in the code $C(Y)$ is characterized by the formal polynomial

$$W_{C(Y)}(z) = \sum_{B \in Y} W_B(z),$$

where $W_B(z)$ is the weight distribution of the code $C(B)$. 

The distribution of weights in a code $C$ is characterized by the formal polynomial,
called the **weight enumerator** of $C$, where, apparently, the coefficient of $z^i$ in its expansion equals the number of vectors of weight $i$ in $C$.

**Proposition 2.** The weight enumerator of any coset $C(B)$ of $RM(m, 1)$ in $RM(m, 2)$ is uniquely determined from the rank $rk(B)$ of the bilinear form $B$. For $rk(B) = 2r$, the nonzero coefficients $A_i$ in the expansion $\sum A_i z^i$ of the weight enumerator (9) of $C = C(B)$ are as indicated in Table I.

**TABLE I**

Weight Distribution of $C(B)$, with $rk(B) = 2r$

<table>
<thead>
<tr>
<th>$i$</th>
<th>$A_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^{m-1} - 2^{m-1-r}$</td>
<td>$2^{r-1}(2^r + 1)$</td>
</tr>
<tr>
<td>$2^{m-1}$</td>
<td>$2^m - 2^{2r}$</td>
</tr>
<tr>
<td>$2^{m-1} + 2^{m-1-r}$</td>
<td>$2^{r-1}(2^r - 1)$</td>
</tr>
</tbody>
</table>

The above result is a consequence of the fact that any quadratic form $Q \in \mathcal{Q}(B)$ with $rk(B) = 2r$ has $2^m - i$ zeros in $V$, where $i$ is one of the numbers appearing in Table I, and that the number of distinct $Q \in \mathcal{Q}(B)$ with $2^m - i$ zeros in $V$ is given by $A_i$ as indicated in Table I. We obtain, in particular, from Proposition 2, the well-known result that the linear code $RM(m, 1) = C(B_0)$ contains, in addition to the all-zero vector, exactly $2^m - 1$ vectors of weight $2^{m-1}$. For more details concerning quadratic and bilinear forms over GF(2), we refer to Cameron and Seidel (1973).

In the next section, we shall investigate the structure of the set of cosets $C(B)$ and show how the results of Delsarte and Goethals (1975) can be used to obtain the distribution of distances in the codes $C(Y)$ of type (8).

### 3. The Association Scheme on the Cosets of $RM(m, 1)$ in $RM(m, 2)$

#### 3.1. It was shown by Delsarte and Goethals (1975) that the set $\mathcal{B}$ of alternating bilinear forms on an $m$-dimensional vector space $V$ over a finite field GF($q$) has the structure of an association scheme with $N = \lfloor m/2 \rfloor$ classes (in the sense of Bose and Shimamoto (1952)) with respect to the $N + 1$ relations

$$\theta_k = \{(B, B') \in \mathcal{B}^2 | \text{rk}(B - B') = 2k\}, \quad 0 \leq k \leq N.$$  

1 For a real number $x$, we denote by $[x]$ its integral part, that is, the largest integer not exceeding $x$.  

643/31/1-4
Clearly, in our case \((q = 2)\), since the minimum weight \(w_m(C)\) of the code \(C = C(B - B')\) is equal to \(2^{m-1} - 2^{m-1-k}\) iff \(\text{rk}(B - B') = 2k\) holds (cf. Proposition 2), it follows that the set \(\{C(B) \mid B \in \mathcal{B}\}\) of coset codes has the same isomorphic structure with respect to the relations
\[(C(B), C(B')) \in \theta_k' \iff \min d(u, v) = 2^{m-1} - 2^{m-1-k}, \quad u \in C(B), \quad v \in C(B').\]

For \(k = 0, 1, \ldots, N\), let \(D_k\) be the \((1,0)\)-incidence matrix of the relation \(\theta_k\). We quote from Delsarte and Goethals (1975) the following theorem, where we use the notation \(\left[\begin{array}{c} n \\ k \end{array}\right]\) for the quaternary Gaussian coefficients defined by
\[
\left[\begin{array}{c} n \\ 0 \end{array}\right] = 1, \quad \left[\begin{array}{c} n \\ k \end{array}\right] = \prod_{i=0}^{k-1} \frac{(4^n - 4^i)}{(4^k - 4^i)}, \quad k \geq 1,
\]
for all nonnegative integers \(k\) (cf. Goldman and Rota, 1970).

**Theorem 3.** (i) The \(N + 1\) matrices \(D_k\) generate over the real field an \((N + 1)\)-dimensional linear associative and commutative algebra of square matrices of order \(c^N = 2^{m(m-1)/2}\).

(ii) The \(i\)th eigenvalue of \(D_k\) is given by \(P_k(i)\) for \(i = 0, 1, \ldots, N\), where
\[
P_k(x) = \sum_{j=0}^{k} (-1)^{k-j} 4^{(k-j) \left[\frac{N-j}{2} \right] \left[\frac{N-x}{j} \right]} c^j.
\] (10)

The function \(P_k(x)\) defined by (10) is a polynomial of degree \(k\) in the variable \(z = 4^{-x}\). For these, the name of generalized Krawtchouk polynomials was proposed by Delsarte and Goethals (1975), who showed that the orthogonality relation
\[
\sum_{k=0}^{N} P_k(k) P_k(j) = \delta_{i,j} c^N
\] (11)
holds, which shows that the square matrix \(P\) of order \(N + 1\),
\[
P = \left[\begin{array}{ccc} p_{i,j} = P_k(i) ; 0 \leq i, j \leq N \end{array}\right]
\] (12)
satisfies \(P^2 = c^N I\).

**3.2.** Now let \(Y\) be any nonempty subset of \(\mathcal{B}\), and let us define the \(\theta\)-enumerator of \(Y\) to be the formal polynomial
\[
R_Y(z) = \left| Y \right|^{-1} \sum_{B \in Y} \sum_{B' \in Y} z^{(1/2)\text{rk}(B - B')}.
\] (13)
Thus, the coefficient $a_r$ of $z^r$ in its expansion $R_r(z) = \sum a_r z^r$ is equal, up to the constant factor $|Y|^{-1}$, to the number of pairs $(B, B') \in Y^2$ belonging to the $r$th relation $\theta_r$. We quote that, for these coefficients, we have

$$a_0 = 1, \quad \text{and} \quad a_0 + a_1 + \cdots + a_N = |Y|.$$ 

Let us define the dual $\theta$-enumerator of $Y$ to be the polynomial $R'_\theta(z) = \sum b_k z^k$ with coefficients $b_k$ obtained from those of $R_\theta(z) = \sum a_i z^i$, by the linear transformation

$$b_k = |Y|^{-1} \sum_{i=0}^{N} a_i P_k(i), \quad k = 0, 1, ..., N,$$  \hspace{1cm} (14)

with matrix (12). For a subspace $Y$ of the vector space $\mathcal{V}$, let $Y^\perp$ denote its orthogonal complement. The next two theorems were mentioned in Delsarte and Goethals (1975) as an application of more general results due to Delsarte (1973a).

**Theorem 4.** The dual $\theta$-enumerator of any subset $Y \subseteq \mathcal{V}$ has nonnegative coefficients.

**Theorem 5.** The $\theta$-enumerators of a subspace $Y \subseteq \mathcal{V}$ and of its orthogonal complement $X = Y^\perp$ are dual of each other, that is, we have

$$R_X(z) = R'_\theta(z), \quad R_\theta(z) = R'_X(z).$$

The reader will have noticed the analogy between the above concepts and the MacWilliams identities (cf. (MacWilliams, 1963)), relating the weight enumerators of a pair of dual codes. Let us mention an interesting consequence of Theorem 5. Let $Y$ be a $t$-dimensional subspace of the vector space $\mathcal{V}$, and let $X = Y^\perp$ be its orthogonal complement, that is, a subspace of dimension $(n \choose 2) - t$ over $\mathbb{F}$. It should be clear, from (7) and (8), that $C(Y)$ and $C(X)$ are binary linear $(2^m - 1, m + t)$ and $(2^{m-1}, m + (m \choose 1) - t)$ codes, respectively. Let $R_\theta(z) = \sum a_i z^i$ and $R_X(z) = \sum b_k z^k$ denote the $\theta$-enumerators of $Y$ and $X$, respectively. By Theorem 5, their coefficients are related as in (14). We shall show that this implies a relation between the weight enumerators of $C(Y)$ and $C(X)$. Let us denote by $W_\theta(z)$ the weight enumerator

---

2 By the orthogonal complement of a subspace $X$ in a vector space $V$, we mean the maximal subspace of $V$ orthogonal to $X$.

3 In coding terminology, the dual $C^\perp$ of a linear $(n, k)$ code $C$ is its orthogonal complement, that is, a linear $(n, n - k)$ code.
\[ W_r(z) = \sum A_i z^i \] with the coefficients \( A_i \) of Table I, that is, the weight enumerator of any coset code \( C(B) \) with \( \text{rk}(B) = 2r \). Since \( Y \) and \( X \) are linear subspaces of \( \mathcal{B} \), it should be clear from the definition (13) that the coefficients \( a_r, b_r \), in their respective \( \theta \)-enumerators are equal to the number of forms \( B \) of rank \( 2r \) in \( Y \), and \( X \), respectively. Then, it follows from Proposition 2 that the weight enumerators of \( C(Y), C(X) \), are given by
\[ W_{C(Y)}(z) = \sum_{i=0}^{N} a_i W_i(z), \quad W_{C(X)}(z) = \sum_{k=0}^{N} b_k W_k(z), \] respectively, where the coefficients \( a_i, b_k \) are related as in (14).

More generally, for an arbitrary subset \( Y \subseteq \mathcal{B} \), the polynomial \( W_{C(Y)}(z) \) defined by (15) with the coefficients \( a_i \) of the \( \theta \)-enumerator of \( Y \), is the distance enumerator of the code \( C = C(Y) \), that is, the formal polynomial
\[ D_{C}(z) = \frac{1}{|C|} \sum_{u \in C} z^{d(u,v)}. \] This clearly appears from the results of Section 2. Note that, for a linear code \( C \), its distance enumerator (16) is identical to its weight enumerator (9); the same property holds true for a distance-invariant code (that is, a code having the property that, for every \( i \), the number of codevectors at distance \( i \) from a given codevector \( u \) is the same for every codevector \( u \)), provided that it contains the all-zero vector. In conclusion, we have shown that the following proposition holds true.

**Proposition 6.**

(i) For any subset \( Y \subseteq \mathcal{B} \), the distance enumerator of the code \( C(Y) \) is uniquely determined from the \( \theta \)-enumerator of \( Y \);

(ii) For a pair of complementary orthogonal subspaces \( Y, X = Y^\perp \subseteq \mathcal{B} \), the weight enumerators (15) of the linear codes \( C(Y), C(X) \) are related by (14).

**Remark.** Note that the coefficients \( a_i, b_k \) appearing in the expressions (15) are uniquely determined from their expansions \( W(z) = x_i z^i \), due to the special form of the weight enumerators \( W_r(z) \) defined by the coefficients of Table I.

**Example 1.** The dual code of the BCH (63, 51) binary code with minimum distance 5 (cf. (Berlekamp, 1968)), is a linear (63, 12) code containing \( \text{RM}(6, 1) \) and contained in \( \text{RM}(6, 2) \); it contains 210 vectors of weight 24, 1512 vectors of weight 28, and no vectors of weight 16. This provides enough information to obtain the coefficients
\[ a_0 = 1, \quad a_1 = 0, \quad a_2 = 21, \quad a_3 = 42, \]
of the \( \theta \)-enumerator of the subset \( Y \subseteq \mathcal{B} \) to which this code corresponds. We then obtain by (14), for the orthogonal complement \( Y^\perp \) of dimension 9,

\[
b_0 = 1, \quad b_1 = 0, \quad b_2 = 315, \quad b_3 = 196,
\]

from which the weight enumerator of the linear \((63, 15)\) code \( C(Y^\perp) \) can be obtained by (15), that is,

\[
W(z) = (1 + 63z^2) + 315(10z^{34} + 48z^{32} + 6z^{40}) + 196(36z^{28} + 28z^{36}).
\]

3.3. Let \( Y \) be any subset of \( \mathcal{B} \) with the property that

\[
\forall B, B' \in Y, \quad B \neq B', \quad \text{rk}(B - B') \geq 2r \tag{17}
\]

holds. Then, it follows from Proposition 2 that the distance between any two distinct codevectors in the code \( C(Y) \) defined by (8) satisfies

\[
d(u, v) \geq 2^{m-1} - 2^{m-1-r}. \tag{18}
\]

On the other hand, we clearly have

\[
| C(Y) | = 2^m | Y |.
\]

Hence, the problem of finding the best codes \( C(Y) \) (that is, of the largest cardinality) for a given minimum distance (18), reduces to the problem of finding subsets \( Y \subseteq \mathcal{B} \) of the largest cardinality for which property (17) holds. Such subsets \( Y \) were studied by Delsarte and Goethals (1975), who called them \((m, r)\)-sets of alternating bilinear forms. They obtained, in particular, the following theorems.

**Theorem 7.** (i) The cardinality of any \((m, r)\)-set \( Y \) is bounded by

\[
| Y | \leq c^{N-r+1}, \quad N = \lfloor m/2 \rfloor, \quad c = 2^{(m^2)/N}.\tag{19}
\]

(ii) In case of equality, the \( \theta \)-enumerator \( \sum a_i z^i \) of \( Y \) is uniquely determined by

\[
a_{N-i} = \sum_{j-i}^{N-r} (-1)^{j-i} 4^{(j-i)} \frac{j!}{i! \frac{j!}{j!}} (e^{N-r+1-j} - 1), \tag{20}
\]

for \( i = 0, 1, \ldots, N - r \), and \( Y \) is called a maximal \((m, r)\)-set.

**Theorem 8.** For \( 1 < r \leq N \), a subspace \( Y \subseteq \mathcal{B} \) is a maximal \((m, r)\)-set iff its orthogonal complement \( Y^\perp \) is a maximal \((m, N - r + 2)\)-set.

A code \( C(Y) \) with minimum distance (18) will be called \( r \)-optimal if the corresponding \( Y \subseteq \mathcal{B} \) is a maximal \((m, r)\)-set. It follows from Theorem 7 and
TABLE II
θ-Enumerators of Maximal (m, r)-Sets

<table>
<thead>
<tr>
<th>m</th>
<th>r</th>
<th>a_0</th>
<th>a_1</th>
<th>a_2</th>
<th>a_3</th>
<th>a_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>35</td>
<td>28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>31</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>31 × 5</td>
<td>31 × 28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td></td>
<td>31</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>31 × 21</td>
<td>31 × 12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>31 × 21</td>
<td>31 × 588</td>
<td>31 × 448</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td>127</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>127 × 21</td>
<td>127 × 108</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>127 × 21</td>
<td>127 × 2604</td>
<td>127 × 13888</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td>127</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>127 × 85</td>
<td>127 × 44</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>127 × 357</td>
<td>127 × 9180</td>
<td>127 × 6976</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>127 × 85</td>
<td>127 × 44268</td>
<td>127 × 1180480</td>
<td>127 × 888832</td>
</tr>
</tbody>
</table>

Proposition 6 that the distance enumerator of an r-optimal code is uniquely determined from r. The reader will find in Table II the coefficients (24) of the θ-enumerators of maximal (m, r)-sets in the first few cases, from which the distance enumerators of the r-optimal codes can be obtained (cf. (15)) by use of Table I. In the next section, we shall describe the constructions of the r-optimal codes which are obtained from the maximal (m, r)-sets of Delsarte and Goethals (1975).

4. OPTIMAL SUBCODES OF RM(M, 2)

In this section, we shall describe a construction for the r-optimal codes defined in Section 3.3. The cases m odd, m even, are treated separately.

4.1. The Odd-Dimensional Case: m = 2t + 1. In this case, we have (cf. (19)) N = t, c = 2^m. Hence, we may take GF(c) as m-dimensional vector space V over F. Let Tr denote the trace from GF(c) to F, that is,

\[ \text{Tr}(\xi) = \sum_{i=0}^{2t} \xi^{2^i}, \quad \forall \xi \in V = \text{GF}(c). \]
For any \( \eta \in V \), a linear form \( L_\eta \) on \( V \) is defined by
\[
L_\eta(\xi) = \text{Tr}(\xi \eta), \quad \forall \xi \in V.
\]
The map \( \eta \rightarrow L_\eta \) sets up a vector space isomorphism between \( V \) and its dual space \( V^* \).

Let \( \omega \) be a primitive element in \( \text{GF}(c) \); any nonzero \( \xi \in V \) can be identified with some power \( \xi = \omega^i \), say, of the primitive element \( \omega \). We shall adopt the numbers \( i, \quad 0 \leq i \leq 2^m - 2 \), as indexing set for the elements of \( V^* \). Accordingly, the components of the vectors \( u \) in the coset codes \( C(B) \) (cf. (7)) will be numbered \( u_0, u_1, \ldots, u_{M-1} \) with \( M = 2^m - 1 \), and we shall identify \( u \) with the polynomial
\[
u(x) = u_0 + u_1 x + \cdots + u_{M-1} x^{M-1}
\]
in the algebra \( \mathbb{F}[x]/(x^M - 1) \). This notation makes it clear that the first-order shortened Reed-Muller code
\[
RM(m, 1) = \{u(x) \mid u_0 = L_\omega(\omega^i), \quad 0 \leq i \leq M - 1; \quad n \in V\}
\]
is invariant under the cyclic permutation induced by \( \eta \rightarrow \omega \eta \) on the elements of \( V^* \). Hence (cf. Berlekamp (1968), \( RM(m, 1) \) is a cyclic code, that is, an ideal in \( \mathbb{F}[x]/(x^M - 1) \). A similar property holds for all shortened Reed-Muller codes, in particular for \( RM(m, 2) \). The code \( RM(m, 1) \) is the ideal generated by
\[
(x^M - 1)/m_1(x),
\]
where we denote by \( m_1(x) \) the minimal polynomial of \( \omega^{-i} \); similarly, \( RM(m, 2) \) is the ideal generated by
\[
(x^M - 1)/m_1(x) \prod_{i=1}^{t} m_{1+2i}(x).
\]
For more details, we refer the reader to Peterson and Weldon (1972).

For elements \( \gamma_i \in \text{GF}(c) \), let \( Q(\xi) \) be defined by
\[
Q(\xi) = \sum_{i=0}^{t} \text{Tr}(\gamma_i \xi^{2^i+2^i}), \quad \forall \xi \in \text{GF}(c).
\]
Clearly, we have \( Q(0) = 0 \), and it is easily verified that the function \( B = \phi(Q) \) defined by (5), that is,
\[
B(\xi, \eta) = \sum_{i=1}^{t} \text{Tr}(\gamma_i (\xi \eta^{2^i} + \xi^{2^i} \eta)), \quad \forall \xi, \eta \in V,
\]
is a bilinear form on $V$. Hence, $Q(\xi)$ is a quadratic form on $V$, and every quadratic form on $V$ can be given the form (21). Note that (22) can be given the form

$$B(\xi, \eta) = \text{Tr}(\xi L_B(\eta)), \quad \forall \xi, \eta \in V,$$

with

$$L_B(\eta) = \sum_{i=1}^{t} \gamma_i \eta^{2i} + (\gamma_i \eta)^{2^{t+1} - 1}, \quad \forall \eta \in \text{GF}(q),$$

where $L_B : V \to V$ is an endomorphism of $V$ with kernel denoted by $\text{Ker}(L_B)$. Clearly, we have, since $\text{Tr}$ is a nonsingular linear map $V \to F$,

$$\text{rk}(B) + \dim_F \text{Ker}(L_B) = \dim_F V = 2t + 1.$$ (25)

For an integer $r, 1 < r \leq t$, let $E_r$ be the set of endomorphisms (24) with $\gamma_1 = \gamma_2 = \cdots = \gamma_{r-1} = 0$, and let $Y_r$ be the set of alternating bilinear forms $B$ defined by (23) for $L_B \in E_r$. The following theorem was obtained by Delsarte and Goethals (1975).

**Theorem 9.** The linear subspace $Y_r \subseteq \mathcal{B}$ is a maximal $(2t + 1, r)$-set.

It follows from Theorems 8 and 9 that the orthogonal complement of $Y_r$ in $\mathcal{B}$ is a maximal $(2t + 1, t + 2 - r)$-set. With respect to the inner product

$$\langle B, B' \rangle = \text{Tr} \left( \sum \gamma_i \gamma_i' \right),$$

(cf. (24)), this orthogonal complement $Y_r^\perp$ is the set of forms (23) with $\gamma_r = \gamma_{r+1} = \cdots = \gamma_t = 0$ in (24). From the above discussion, it follows that the following proposition holds true.

**Proposition 10.** The code $C(Y_r)$ is an $r$-optimal linear code of length $2^{2t+1} - 1$ and dimension $(t - r + 2)(2t + 1)$ over $F$; the code $C(Y_r^\perp)$ is a $(t + 2 - r)$-optimal linear code of dimension $r(2t + 1)$ over $F$. They are described by the set of quadratic forms (21) where $\gamma_1 = \gamma_2 = \cdots = \gamma_{r-1} = 0$ for $C(Y_r)$, and $\gamma_r = \gamma_{r+1} = \cdots = \gamma_t = 0$ for $C(Y_r^\perp)$.

The reader familiar with coding theory will easily recognize in $C(Y_r)$ the cyclic code with parity check polynomial

$$m_1(x) \prod_{i=r}^{t} m_{1+2r}(x),$$
and, in $C(Y_r^⊥)$, the one with parity check polynomial

$$m_1(x) \prod_{i=1}^{r-1} m_{1+2^i}(x).$$

These codes were studied by Berlekamp (1970) who obtained the explicit form of their weight enumerators, which, by Proposition 6 and Theorem 7, depends only on $r$.

4.2. The Even-Dimensional Case: $m = 2t + 2$. Here, we have (cf. (19)) $N = t + 1$, $c = 2^{m-1}$, and we shall take the Kronecker product $GF(c) \times GF(2)$ as $m$-dimensional vector space $V$, that is, we represent $V$ as the set of pairs $(\xi, x)$ with $\xi \in GF(c)$ and $x \in GF(2)$. By means of the trivial isomorphism $(\xi, 0) \equiv \xi$, we shall identify $GF(c)$ with the $(m - 1)$-dimensional subspace $U$ of $V$,

$$U = \{(\xi, x) \in V \mid x = 0\}.$$

By means of the trace $Tr$ from $GF(c)$ to $F$, defined as in Section 4.1, any quadratic form $Q$ on $V$ can be given the form

$$Q(\xi, x) = Q'(\xi) + x(a + Tr(\gamma \xi)), \quad \forall (\xi, x) \in V,$$

where $a \in F$, $\gamma \in GF(c)$, and $Q'(\xi)$ is a quadratic form on $U \equiv GF(c)$ of the type (21). Then, for the corresponding bilinear form $B = \phi(Q)$, we have, $\forall (\xi, x), (\eta, y) \in V$,

$$B((\xi, x), (\eta, y)) = B'(\xi, \eta) + Tr(\gamma(\xi y + \eta x)),$$

where $B' = \phi(Q')$ is a bilinear form on $U$ defined by

$$B'(\xi, \eta) = Tr(\xi L_{B'}(\eta)), \quad \forall \xi, \eta \in GF(c),$$

with $L_{B'} \in End(U)$. Let $\text{Im}(L_{B'})$ denote the image subspace of $U$ by the endomorphism $L_{B'}$. It was shown by Delsarte and Goethals (1975) that, between the ranks of the forms (27) and (28), there exists the relation:

$$\text{rk}(B) = \text{rk}(B') \quad \text{if} \quad \gamma \in \text{Im}(L_{B'}),$$

$$\text{rk}(B') + 2, \quad \text{otherwise.} \quad (29)$$

For any $\gamma \in GF(c)$, let $B_\gamma \in \mathcal{B}$ be defined as follows:

$$B_\gamma((\xi, x), (\eta, y)) = Tr(\gamma^2 \xi \eta) + Tr(\gamma \xi) Tr(\eta) + Tr(\gamma(\xi y + \eta x)).$$
for all \((\xi, x), (\eta, y) \in V\). The following theorem was proved by Delsarte and Goethals (1975).

**Theorem 11.** The set \(K = \{B, \beta \in \mathcal{B} : \gamma \in GF(c)\}\) is a maximal \((2t + 2, t + 1)\)-set.

The codes \(C(K)\) defined, for all integers \(t \geq 1\), by the sets \(K\) of Theorem 11, were found by Nordstrom and Robinson (1967) for \(t = 1\), and by Kerdock (1972) for \(t > 1\). We shall call \(K\) the **Kerdock set** of alternating bilinear forms on \(V\). Note that \(K\) is not a linear space. Actually, it can be shown that no maximal \((2t + 2, t + 1)\)-set can be linear. The argument is essentially the following: Assume \(Y\) is a subspace of \(\mathcal{B}\) which is a maximal \((2t + 2, t + 1)\)-set; then, \(C(Y)\) is an optimal linear code with the same parameters as the corresponding Kerdock code, and its dual code \(C'(Y)\) has the same parameters as the Preparata code (Preparata, 1968) of the same length (cf. (MacWilliams et al., 1972)); however, no code with the latter parameters can be linear (cf. (Goethals and Snover, 1972)); this shows that \(Y\), whence \(C(Y)\) cannot be linear.

Maximal \((2t + 2, r)\)-sets with \(r \leq t\) were constructed by Delsarte and Goethals (1975) as follows. Let \(X_r\) be the set of alternating bilinear forms \(B'\) on \(U \equiv GF(c)\) defined as in (28), with their last \(r - 1\) components \(\gamma_i\) equal to zero in (24); that is, for any \(B' \in X_r\) defined by (28), we have, with \(\gamma_i \in GF(c), 1 \leq i \leq t - r + 1,\)

\[
L_{B'}(\eta) = \sum_{i=1}^{t-r+1} \gamma_i \eta^{2^i} + (\gamma_i \eta)^{2^{t+1-r}}, \quad \forall \eta \in GF(c).
\]

Note that \(X_r\) can be viewed as the orthogonal complement of \(Y_{t-r+2}\) (cf. Theorem 9), from which it follows that \(X_r\) is a maximal linear \((2t + 1, r)\)-set on \(U \equiv GF(c)\). The following theorem presents the construction announced hereabove (cf. (Delsarte and Goethals, 1975)).

**Theorem 12.** For \(1 \leq r \leq t\), the set

\[
Z_r = \{B \in \mathcal{B} : B = B' + B_\gamma; B' \in X_r, B_\gamma \in K\}
\]

is a maximal \((2t + 2, r)\)-set on \(V\).

The \(r\)-optimal codes \(C(Z_r)\) thus obtained for \(r \geq 1\) all are new, and all are nonlinear since \(K\) is. The case \(r = t\) is particularly interesting as we shall see in Section 5. We first give below more details concerning the construction of these codes.
4.3. The $r$-Optimal Codes $C(Z_r)$

Note that $Z_r$ defined by (30) can be viewed as a union of the $2^{2t+1}$ cosets

$$Z_r(\gamma) = \{B \in Z_r | B = B' + B_r; B' \in X_r\},$$

with coset leaders $B_r \in K$, of the linear set $Z_r(0) \equiv X_r$. Accordingly, the code $C(Z_r)$ is a union of $2^{2t+1}$ cosets $C_r = C(Z_r(\gamma))$ of the linear code $C_0 = C(Z_r(0))$ which we call the kernel. Any vector $u \in C_0$ is described by a quadratic form $Q$, with

$$Q(\xi, x) = \sum_{i=0}^{t-r+1} \text{Tr}(\gamma \xi^{i+2^i}) + ax, \quad \forall (\xi, x) \in V. \quad (31)$$

For any quadratic form $Q$ on $V$, the corresponding vector $u = u(Q)$ will be described by the triple

$$u(Q) = (u_L(x); u_R(x); u_\infty), \quad (32)$$

where $u_L(x), u_R(x)$ are the polynomials in $\mathbb{F}[x]/(x^M - 1)$, $M = 2^{2t+1} - 1$, defined by

$$u_L(x) = \sum_{i=0}^{M-1} Q(\omega^i, 0)x^i,$$

$$u_R(x) = \sum_{i=0}^{M-1} Q(\omega^i, 1)x^i,$$

for a primitive element $\omega \in GF(c)$, and

$$u_\infty = Q(0, 1) \in \mathbb{F}.$$ 

Hence, for any $u \in C_0$, $u_L(x)$ and $u_R(x)$ defined as above, with $Q$ of the form (31), belong to the cyclic codes of length $M$ with parity check polynomials $m(x)$ and $(1 + x)m(x)$, respectively, where

$$m(x) = m_1(x) \prod_{i=1}^{t-r+1} m_{1+2^i}(x)$$

(cf. Section 4.1). In addition, we observe that we have $u_\infty = u_R(1)$. We choose as coset leader for $C_r$ the vector $v = v(Q_r)$ described by the quadratic form $Q_r \in \mathcal{Q}(B_r)$ defined by

$$Q_r(\xi, x) = \sum_{i=1}^{t} \text{Tr}((y \xi)^{i+2^i}) + x \text{Tr}(y \xi), \quad \forall (\xi, x) \in V.$$
For any $\gamma \neq 0, \gamma = \omega^{-i}$, say, we may write
\[ v(Q,\gamma) = (x^i\epsilon(x); x^i(\epsilon(x) + \epsilon_1(x)); 0), \]
(33)
where
\[ \epsilon(x) = \sum_{i=0}^{M-1} x^i \sum_{k=1}^t \text{Tr}(\omega^{i(1+x^k)}), \]
and
\[ \epsilon_1(x) = \sum_{i=0}^{M-1} x^i \text{Tr}(\omega^i), \]
are idempotents in $\mathbb{F}[x]/(x^M - 1)$ (cf. (MacWilliams, 1965)). Hence, the code $C = \cup C_r$ is completely described in terms of cyclic codes of length $M$.

For $r = t + 1$, we obtain a shortened version of the code described by Kerdock (1972), which consists of $\text{RM}(2t+2,1)$ and its $2^{2t+1} - 1$ cosets with coset leaders (33). For $r = t \geq 2$, we obtain a shortened version of the code described by Goethals (1974). In both cases, codes with the “dual” parameters do exist; for $r = t + 1$, they are the codes discovered by Preparata (1968), and for $r = t$, they were described by Goethals (1974). By a pair of codes with “dual” parameters, we mean two codes $C, C'$ of the same length $n$, say, with respective distance enumerators $D_C(z), D_C'(z)$ (cf. (16)), satisfying the MacWilliams identity
\[ D_C'(z) = |C|^{-1}(1+z)^n D_C((1-z)/(1+z)), \]
(34)
first proved to hold for a linear code $C$ and its dual $C' = C^\perp$ (cf. (MacWilliams, 1963)). The distance enumerators of the Preparata codes were first obtained in “dual” form (34) by Goethals and Snover (1972). In the next section, we shall give a description and a proof of the properties of the “dual” families of codes discovered by Goethals (1974).

5. Two Dual Families of Nonlinear Codes

In this section, we shall prove the results announced in Goethals (1974). We first recall these results.

5.1. Description of the Codes

For all block lengths $n = 2^{2t+2}, t \geq 2$, two nonlinear codes $C, C'$ are defined, which are called dual as their distance enumerators satisfy the
MacWilliams identity (34). Both consist of a union of $2^{2t+1}$ cosets of a linear code, called the kernel, and are described by pairs of vectors in extended cyclic codes of length $M + 1 = 2^{2t+1}$. More precisely, any vector $u \in C$ or $C'$ is described as follows,

$$u = (u_L(x); u_L(1); u_R(x); u_R(1)),$$

(35)

by a pair of polynomials $u_L(x), u_R(x) \in \mathbb{F}[x]/(x^M - 1)$, and their overall parity checks $u_L(1), u_R(1) \in \mathbb{F}$. As in Section 4, we use the notations: $\omega$ for a primitive element in $\mathbb{GF}(c)$, $c = 2^{2t+1}$, and $m_i(x)$ for the minimal polynomial of $\omega^{-i}$; in addition, we use $e_i(x)$ to denote the unique idempotent of the irreducible ideal generated by $(x^M - 1)/m_i(x)$, that is the unique polynomial satisfying

$$e_i(\omega^{-j}) = 1, \quad e_i(\omega^j) = 0 \quad \forall j \neq -2^k(\text{mod } M), \quad 0 \leq k \leq 2t.$$

Note that $e_d(x)$ and $e_i(x) + 1$ are generating idempotents for the ideals generated by $(x^M - 1)/m_i(x)$ and $m_i(x)$, respectively (cf. (MacWilliams, 1965)). We now proceed to give a description of the codes $C$, called primal, and $C'$, called dual.

5.1.1. The Primal Code $C$. The kernel $\text{Ker } C$ consists of all vectors of the form (35) with $u_L(x)$ belonging to the cyclic code generated by $m_i(x)$ and $a(x) = u_L(x) + u_R(x)$ belonging to the cyclic code generated by

$$m(x) = m_i(x) m_{i+2t-1} m_{i+2}(x).$$

Hence, $\text{Ker } C$ is a linear code of length $2^{2t+2}$ and dimension $2^{2t+2} - 4(2t + 1) - 2$. The coset leaders are $v_0 = 0$ and the $2^{2t+1} - 1$ vectors

$$v_j = (x^j; 1; x^j e_i(x); 0), \quad 1 \leq j \leq M.$$

(36)

Thus, the code

$$C = \bigcup_{j=0}^{M} \{ \text{Ker } C + v_j \}$$

(37)

contains $|C| = 2^k$ vectors, where $k = 2^{2t+2} - 6t - 5$. We shall show that the minimum distance of $C$,

$$d(C) := \min d(u, v), \quad u, v \in C, \quad u \neq v,$$

(38)

satisfies $d(C) = 8$. 

5.1.2. The Dual Code $C'$. The kernel $\text{Ker } C'$ consists of all vectors of the form (35) with
\begin{align*}
u_L(x) &= a_0 \varphi(x) + a_1 x^i \epsilon_1(x) + a_2 x^j \epsilon_2(x), \\
u_R(x) &= b_0 \varphi(x) + a_1 x^i \epsilon_1(x) + a_2 x^j \epsilon_2(x),
\end{align*}
where $a_i, b_i \in F$ and $i, j \in \{0, 1, \ldots, M - 1\}$. It is a linear code of dimension $4t + 4$. The coset leaders are $\mathbf{u}_0 = \mathbf{0}$ and the $2^{st+1} - 1$ vectors
\begin{equation}
\mathbf{u}_j = (x^i \epsilon(x); 0; x^j (\epsilon(x) + \epsilon_1(x)); 0), \quad 1 \leq j \leq M,
\end{equation}
where
\begin{equation}
\epsilon(x) = \sum_{k=1}^{t} \epsilon_{1+2^k}(x).
\end{equation}
Hence, the code
\begin{equation}
C' = \bigcup_{j=0}^{M} \{\text{Ker } C' + \mathbf{u}_j\}
\end{equation}
contains $|C'| = 2^{st+5}$ vectors.

Note that, for an integer $r$, $1 \leq r < M$, relatively prime to $M$, the idempotent $\epsilon_r(x)$ is the polynomial
\begin{equation}
\epsilon_r(x) = \sum_{i=0}^{M-1} x^i \text{Tr}(\omega^{ri}),
\end{equation}
where $\text{Tr}$ denotes, as in Section 4, the trace from $\text{GF}(c)$ to $\text{GF}(2)$. Hence, the polynomials $\epsilon(x)$ and $\epsilon_1(x)$ appearing in (33) and (40) are actually the same.

Let $\gamma_0, \gamma_1 \in \text{GF}(c)$ be defined by
\begin{equation}
\gamma_0 = a_1 \omega^{-i_1}, \quad \gamma_1 = a_2 \omega^{-i_2},
\end{equation}
and $Q(\eta, y), \forall \eta \in \text{GF}(c), \forall y \in F$, by
\begin{equation}
Q(\eta, y) = a_0 + \text{Tr}(\gamma_0 \eta + \gamma_1 \eta^2) + (a_0 + b_0) y.
\end{equation}
Then, it clearly appears from (39) and (42) that we have
\begin{align*}
u_L(x) &= \sum_{i=0}^{M-1} Q(\omega^i, 0)x^i, \quad \nu_L(1) = a_0, \\
u_R(x) &= \sum_{i=0}^{M-1} Q(\omega^i, 1)x^i, \quad \nu_R(1) = b_0.
\end{align*}
This shows that the code of length $2^{2t+2} - 1$ obtained from the set of vectors
\[ \{u \in C' \mid u_t(1) = 0; \text{(cf. (35))}\}, \]
by deleting their component $u_t(1) = a_0 = 0$, is identical to the code $C(Z_t)$ described in Section 4.3. In other words, $C(Z_t)$ is obtained by shortening $C'$; conversely, $C'$ is obtained by lengthening $C(Z_t)$ (cf. Berlekamp, 1968, p. 336). It then follows from Proposition 6 and Theorem 7 that the distance enumerator $D_{C'}(z)$ of $C'$ is uniquely determined. We give in Table III the nonzero coefficients $D_i$ appearing in its expansion $\sum D_i z^i$.

**Table III**

Coefficients of the Distance-Enumerator of the Code $C'$ of Length $2^{2t+2}$

<table>
<thead>
<tr>
<th>$i$</th>
<th>$D_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 or $2^{t+2}$</td>
<td>1</td>
</tr>
<tr>
<td>$2^{t+1}$ ± $2^{t+1}$</td>
<td>$2^{t}(2^{t+1} - 1)(2^{t+2} - 1)/3$</td>
</tr>
<tr>
<td>$2^{t+1}$ ± $2^t$</td>
<td>$2^{t+1}(2^{t+1} + 1)(2^{t+1} + 4)/3$</td>
</tr>
<tr>
<td>$2^{t+1}$</td>
<td>$2(2^{t+2} - 1)(2^{t+1} - 2^t + 1)$</td>
</tr>
</tbody>
</table>

5.2. Proofs

This section is essentially devoted to a proof of the following theorem and to its consequences.

**Theorem 13.** The distance enumerators of the codes $C$, $C'$ described in Section 5.1 are related by the MacWilliams identity (34).

5.2.1. Preliminaries. For any two vectors $u, v \in F^n$, let $(u, v) = \sum u_i v_i$ denote their inner product. For any $u \in F^n$, the map $\chi_u : F^n \to \mathbb{Q}$ defined by
\[
\chi_u(v) = (-1)^{(u,v)}, \quad \forall v \in F^n,
\]
(43)
is a character of the additive group of $F^n$.

For any subset $X \subseteq F^n$, we define
\[
\chi_u(X) = \sum_{v \in X} \chi_u(v).
\]
(44)

**Lemma 13.1.** For any $u \in F^n$ of weight $w(u) = j$, we have
\[
\sum_{v \in F^n} \chi_u(v) z^{w(v)} = (1 - z)j(1 + z)^{n-j}.
\]
(45)
Proof. From the definition (43), we obtain
\[ \sum_{v \in \mathbb{F}^n} \chi_u(v) z^{w(v)} = \prod_{i=1}^{n} \left( \sum_{v_i=0}^{1} (-1)^{u_i} v_i z^{v_i} \right). \]
Clearly, the summation on the right-hand side is equal to \((1 - z)\) if \(u_i = 1\),
or to \((1 + z)\) if \(u_i = 0\). This proves the lemma.

Let \(K_i(j)\) denote the coefficient of \(z^j\) in (45), and let \(X_i\) be the set
\[ X_i := \{ v \in \mathbb{F}^n \mid w(v) = i \}. \]
By comparing the coefficients of \(z^j\) on both members of (45), we obtain, by use of (44),
\[ K_i(j) = \sum_{k} (-1)^k \binom{j}{k} \binom{n-j}{i-k} = \chi_u(X_i), \quad \forall u \in X_i. \tag{46} \]
The following lemma can be obtained from the results of MacWilliams et al. (1972).

**Lemma 13.2.** For a binary code \(C\) of length \(n\), let \(D_C(z) = \sum A_j z^j\) be the expansion of its distance enumerator (16), and let the rational numbers \(B_i\) be defined by
\[ B_i = |C|^{-1} \sum_{u \in X_i} |\chi_u(C)|^2, \quad 0 \leq i \leq n. \tag{47} \]
Then, the following (MacWilliams) identity holds:
\[ \sum_{i=0}^{n} B_i z^i = |C|^{-1} \sum_{j=0}^{n} A_j (1 - z)^j (1 + z)^{n-j}. \tag{48} \]

Note that, for a linear code \(C\), we have
\[ \chi_u(C) = |C|, \quad \text{if } u \in C^\perp, \]
\[ = 0, \quad \text{otherwise}, \tag{49} \]
by definition of the dual code \(C^\perp\). In that case, \(B_i\) defined by (4) equals the number of vectors of weight \(i\) in \(C^\perp\), and (48) merely is the MacWilliams identity (34). For more details concerning the MacWilliams identity for nonlinear codes, we refer to MacWilliams et al. (1972). We quote, for future use, that the coefficients \(A_j, B_i\) in (48) are related by
\[ B_i = |C|^{-1} \sum_{j=0}^{n} A_j K_i(j). \tag{50} \]
5.2.2. Proof. We shall prove Theorem 13 by showing that the numbers $B_i$ defined by (47) for the code $C$ described in Section 5.1.1, are identical to the numbers $D_i$ appearing in Table III. We shall use, for the inner product of vectors $u, v$ of length $M$ described by polynomials

$$u(x) = \sum u_i x^i, \quad v(x) = \sum v_i x^i \in \mathbb{F}[x]/(x^M - 1),$$

the definition

$$(u(x), v(x)) = u_0 v_0 + \sum_{i=1}^{M-1} u_i v_{M-i},$$

which clearly is permutation-equivalent to the usual one. With this definition, we have

$$u(x), v(x) = 0 \quad \text{for} \quad i = 0, 1, \ldots, M - 1, \quad \text{iff}$$

$$u(x) v(x) \equiv 0 \pmod{x^M - 1},$$

as it clearly appears from the identity

$$\sum_{i=0}^{M-1} (u(x), x^{-i}v(x)) y^i \equiv u(y) v(y) \pmod{x^M - 1}. \quad (51)$$

It is then a simple matter to verify that the dual code $(\text{Ker} C)^\perp$ of the linear code Ker $C$ consists of all vectors of the form (35) with

$$u_L(x) = a_0 e_0(x) + a_1 x^i e_1(x) + a_2 x^s e_1(x) + a_3 x^s e_3(r),$$

$$u_R(x) = u_L(x) + a_2 e_0(r) + b x^i e_1(x), \quad (52)$$

where, for convenience, we have written $r$ and $s$ for $1 + 2^{i-1}$ and $1 + 2^i$, respectively, and where

$$a_i, b \in \mathbb{F}; \quad i_1, i_2, i_3, j \in \{0, 1, \ldots, M - 1\}.$$

**Lemma 13.3.** (i) $\forall u \notin (\text{Ker} C)^\perp, \chi_u(C) = 0$,

(ii) $\forall u \in (\text{Ker} C)^\perp, \text{we have}$

$$|C|^{-1} \chi_u(C) = (M + 1)^{-1} \left\{ 1 + \sum_{i=1}^M \chi_u(v_i) \right\},$$

where the $v_i$ are the coset leaders (36).

**Proof.** By decomposing the summation

$$\chi_u(C) = \sum_{v \in C} \chi_u(v)$$

643/31/1-5
according to the decomposition (37) of $C$ into cosets of $\text{Ker } C$, we readily obtain

$$
\chi_u(C) = \chi_u(\text{Ker } C) \left\{ 1 + \sum_{j=1}^{M} \chi_u(v_j) \right\}.
$$

Then, by use of (49) which holds for the linear code $\text{Ker } C$, the lemma easily follows.

Let, for any $u \in (\text{Ker } C)^\perp$, the polynomial $v(x) \in \mathbb{F}[x]/(x^M - 1)$ be defined by

$$
v(x) = (u, v_0) + \sum_{j=1}^{M-1} (u, v_j)x^{M-j}.
$$

Then, with $u$ defined by (35) and (52), we obtain, by use of (51),

$$
v(x) = b\gamma x^0 + a_2x^1 + a_3x^2 + a_4x^3,
$$

and, by Lemma 13.3(ii),

$$
|C|^{-1}\chi_u(C) = 1 - 2(w(v)/(M + 1)),
$$

where $w(v)$ denotes the weight of the vector of length $M$ defined by (53). Let $\alpha_1, \alpha_2, \alpha_3$ and $\gamma \in \text{GF}(c)$ be defined by

$$
\alpha_1 = a_1\omega^{-i_1}, \quad \alpha_2 = a_2\omega^{-i_2}, \quad \alpha_3 = a_3\omega^{-i_3}, \quad \gamma = b\omega^{-j}.
$$

Then, $v(x)$ can be expressed as

$$
v(x) = \sum_{i=0}^{M-1} Q'(\omega^i)x^i,
$$

where $Q'$ is the quadratic form on $\text{GF}(c)$ defined by

$$
Q'(\xi) = \text{Tr}(\gamma\xi + \alpha_2\xi^2 + \alpha_3\xi^3), \quad \forall \xi \in \text{GF}(c).
$$

This shows (cf. 21)) that $v(x)$ belongs to the $(t - 1)$-optimal code $C(Y_{t-1})$ described in Proposition 10. It follows that any $v(x)$ defined by (53) has weight

$$
w(v) \in \{ 0, 2^{2t}, 2^{2t} \pm 2^t, 2^{2t} \pm 2^{t+1} \},
$$

and thus, by (54), we have, for any $u \in (\text{Ker } C)^\perp$,

$$
|C|^{-2} |\chi_u(C)|^2 = 1, 0, 2^{-2t} \text{ or } 2^{-(2t-2)},
$$

(56)
according to the weight of \( v(x) \). It remains to be shown that the sum, extended over all vectors \( u \) of weight \( i \) in \((\text{Ker} \ C)^{\perp}\), of the contributions (56) to (47) is given by \( D_i \) for any \( i \) appearing in Table III, and is zero otherwise.

The subset of vectors \( u \in (\text{Ker} \ C)^{\perp} \) defined by \( a_2 = a_3 = b = 0 \) in (52) is the first-order Reed–Muller code of length \( 2^{2t+2} \) and dimension \( 2t + 3 \), to be denoted by \( \text{RM} \). It contains \( 2(2^{2t+1} - 1) \) vectors of weight \( 2^{2t+1} \), one vector of weight \( 2^{2t+2} \), and the all-zero vector. Each coset of \( \text{RM} \) in \((\text{Ker} \ C)^{\perp}\) is characterized by a given vector (53). Clearly, for all \( u \) in a given coset, the character (54) has the same value. It should be clear from the results of the previous sections that each such coset is in a one–one correspondence with a bilinear form \( B \) on the vector space \( V = \text{GF}(c) \times \text{GF}(2) \), and that the weight enumerator of that coset is uniquely determined from the rank of \( B \). Hence, the problem reduces to finding the rank of the form \( B \) attached to a coset characterized by a given vector (53). We shall take as coset leader, for the coset characterized by (53), the vector \( u \) defined by \( a_2 = a_1 = a_4 = 0 \) in (52), for which we have \( u_R(x) = v(x) \) defined by the quadratic form (55), and \( u_L(x) \) defined similarly by the quadratic form

\[
Q''(\xi) = \text{Tr}(\alpha_2\xi^r + \alpha_8\xi^s), \quad \forall \xi \in \text{GF}(c). \tag{57}
\]

Clearly, the two forms (55) and (57) belong to the same bilinear form (5) on \( \text{GF}(c) \).

**Lemma 13.4.** The set of vectors described by the polynomials

\[
u_L(x) = \sum_{i=0}^{M-1} Q''(\omega^i)x^i;
\]

with \( Q'' \) defined by (57) for all \( \alpha_2, \alpha_8 \in \text{GF}(c) \), is a linear \( (M, 4t + 2) \) cyclic code \( D \) with weight enumerator \( W(z) = \sum A_jz^j \) defined by the coefficients \( A_j \) appearing in Table IV.

**Table IV**

<table>
<thead>
<tr>
<th>( j )</th>
<th>( A_j )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( 2^{2t} - 2^t )</td>
<td>( (2^{2t+1} - 1)(2^{2t-1} + 2^{t-1}) )</td>
</tr>
<tr>
<td>( 2^{2t} )</td>
<td>( (2^{2t+1} - 1)(2^{2t} + 1) )</td>
</tr>
<tr>
<td>( 2^{2t} + 2^t )</td>
<td>( (2^{2t+1} - 1)(2^{2t-1} - 2^{t-1}) )</td>
</tr>
</tbody>
</table>
Proof. From the equivalent expression

\[ u_L(x) = a_2 x^{2t} e(x) + a_3 x^{2t} e_3(x) \]

of any \( u_L(x) \) defined by (57), it clearly appears that \( D \) is the direct sum of the irreducible ideals generated by \( e(x) \) and \( e_3(x) \), and hence, a linear \((M, 4t + 2)\) cyclic code. On the other hand, apparently, \( D \) is a subcode of the \((t - 1)\)-optimal code \( C(Y_{t-1}) \) described by the quadratic forms (55). Hence, any nonzero \( u_L(x) \in D \) has weight \( 2^{2t}, 2^{2t} \pm 2^t \) or \( 2^{2t} \pm 2^{t+1} \). We shall show that the minimum (nonzero) weight in its dual code \( D^\perp \), generated by \( m_2(x) m_3(x) \), is at least equal to 5. For, assume \( D^\perp \) contains a vector \( v(x) \) of weight 2, \( v(x) = x^t + x^j + x^k + x^l \), say, and let \( \langle S \rangle \) be the linear subcode generated by the elements of \( S = \{ \omega^{-1}, \omega^{-j}, \omega^{-k}, \omega^{-l} \} \) over \( F \). Then, the polynomial

\[ \sigma(y) = \prod_{\xi \in \langle S \rangle} (y - \xi), \]

having as zeros the elements of \( \langle S \rangle \), is a linearized polynomial of the form

\[ \sigma(y) = \sum_{i=0}^{4} \sigma_i y^{2^i}, \]

of degree at most equal to 16 (cf. (Berlekamp, 1968)). Let \( \sigma_i \) be the first non-zero coefficient in \( \sigma(y) \), and let us consider the sum

\[ \sum_{\xi \in S} \xi \sigma_i 2^{t-2-i}(\xi) = \sigma_i 2^{t-2-i} \sum_{\xi \in S} \xi 2^{t-2-i} + \cdots = 0, \quad (58) \]

which obviously is zero by definition of \( \sigma(y) \). Since \( v(x) \) belongs to \( D^\perp \), we have \( v(\omega^{-t}) = v(\omega^{-5}) = 0 \), that is, with \( S_v \) defined by

\[ S_v = \sum_{\xi \in S} \xi^{1+2^v}, \]

we have

\[ S_{t+2} = S_{t+1} = 0, \quad S_{t+1} = S_{t+1} = 0. \]

Now, from (58), we deduce, since \( \sigma_i \neq 0 \),

\[ S_{t+3} = S_{t+2} = 0. \]

By induction, we obtain \( S_v = 0 \) for all \( v \geq 0 \). Hence, \( v(x) \) satisfies \( v(\omega^{-1}) = v(\omega^{-5}) = v(\omega^{-5}) = 0 \), and by the BCH argument (cf. (Bose and Ray-Chaudhuri, 1960)), it should have weight at least equal to 7, which contradicts
our assumption. The cases \( w(v) \leq 3 \) are treated similarly. This shows that \( D^\perp \) has minimum weight \( \geq 5 \). Now, by the MacWilliams identities (50) relating the coefficients \( B_i \) and \( A_j \) of the weight enumerators \( \sum B_i z^i \) of \( D^\perp \) and \( \sum A_j z^j \) of \( D \), we easily obtain, from

\[
B_0 = 1, \quad B_1 = B_2 = B_3 = B_4 = 0,
\]

the coefficients \( A_j \), since \( A_0 = 1 \) by definition, and \( A_j \neq 0 \) for \( j > 1 \) only if \( j \) is one of the five possible weights in \( D \). As it turns out, there are only three nonzero \( A_j \), \( j > 1 \), as given in Table IV. This proves the lemma.

Note that \( D \) can be viewed as a complete set of representatives for the cosets of \( \text{RM}(2t + 1, 1) \) in the \((t - 1)\)-optimal code \( C(Y_{t-1}) \), as it clearly appears by comparison of the quadratic forms (55) and (57). To any coset with leader \( u_L(x) \) defined by (57) is attached a bilinear form \( B' \) on \( \text{GF}(c) \), with \( \text{rk}(B') = 2t \) or \( 2t - 2 \), \( \forall B' \neq 0 \). On the other hand, the coset of \( \text{RM} \) in \((\text{Ker } C)^\perp \) with leader

\[
u = (u_L(x); 0; u_R(x); 0), \tag{59}
\]

where \( u_R(x) \) and \( u_L(x) \) are defined by the quadratic forms (55) and (57), respectively, is attached to a bilinear form \( B \) on \( \text{GF}(c) \times \text{GF}(2) \) related to \( B' \) as in (27). Hence, from (29), we deduce \( \text{rk}(B) = 2t + 2 \), \( 2t \) or \( 2t - 2 \), \( \forall B \neq 0 \). We now observe that, according to Proposition 2 and Theorem 7:

(i) For any \( u_L(x) \in D \) of weight \( 2^{2t} \pm 2^t \), we have \( \text{rk}(B') = 2t \), whence \( u_R(x) \) has weight \( w(u_R) = w(v) = 2^{2t} \) or \( 2^{2t} \pm 2^t \) in (59) (cf. Table I);

(ii) since \( C(Y_{t-1}) \) is \((t - 1)\)-optimal, the \( \theta \)-enumerator of \( Y_{t-1} = \{B'\} \) is known:

\[
a_0 = 1, \quad a_{t-1} = (2^{2t+1} - 1)(2^{2t} - 1)/3, \quad a_t = (2^{2t+1} - 1)(52^{2t} + 4)/3.
\]

Hence, we deduce from Lemma 13.4 that, among the vectors \( u_L(x) \) of weight \( 2^{2t} \) in \( D \), there are exactly:

(iii) \( (2^{2t+1} - 1)(2^{2t} - 1)/3 \) vectors which correspond to a form \( B' \) of rank \( 2t - 2 \), and for which we have, accordingly, \( w(u_R) = w(v) = 2^{2t} \) or \( 2^{2t} \pm 2^{t-1} \) in (59);

(iv) \( (2^{2t-1} - 1)(2^{2t-1} + 4)/3 \) vectors which correspond to forms \( B' \) of rank \( 2t \), for which we have \( w(u_R) = w(v) = 2^{2t} \) or \( 2^{2t} \pm 2^t \) in (59).

These observations provide enough information to obtain by use of Proposition 2 the distribution of weights among the coset leaders (59). We observe that only the weights \( w(u_L) + w(u_R) = 2^{2t+1}, 2^{2t+1} \pm 2^t, \) and \( 2^{2t+1} \pm 2^t \)
occur. For any \( \mathbf{u} \) of weight \( 2^{t+1} \pm 2^{t+1} \) or \( 2^{t+1} \pm 2^t \), the rank of the form \( B \) attached to its coset is \( 2t \) or \( 2t + 2 \), respectively. For any \( \mathbf{u} \) of weight \( 2^{t+1} \) with \( w(\mathbf{u}_L) = w(\mathbf{u}_R) = w(v) = 2^t \), the rank of \( B \) is not determined, but the character \((54)\) is equal to zero. For any \( \mathbf{u} \) of weight \( 2^{t+1} \) with \( w(\mathbf{u}_L) = 2^t \pm 2^t \), \( w(\mathbf{u}_R) = 2^t \mp 2^t \), we have \( \text{rk}(B) \geq \text{rk}(B') = 2t \); hence, \( \text{rk}(B) = 2t \), since no vector \( \mathbf{u} \) of weight \( 2^{t+1} \) can occur in a coset \( C(B) \) of rank \( 2t + 2 \) (cf. Table I). Hence, for all \( v(x) = u_R(x) \) for which the character \((54)\) is nonzero, the rank \( \text{rk}(B) \) of its coset, whence the weight enumerator of that coset, is uniquely determined. Now, by straightforward calculations, we readily obtain the values of the numbers \( B_i \) defined by \((47)\). These satisfy \( B_i = D_i \) for the values of \( i \) appearing in Table III, and \( B_i = 0 \) otherwise. This proves Theorem 13.

5.2.3. Consequences. For an arbitrary binary code \( C \) of length \( n \), let the numbers \( B_i \) be defined as in \((47)\), let \( N(C) \) be the set of integers

\[
N(C) = \{ i \mid 1 \leq i \leq n, B_i \neq 0 \},
\]

and let \( d'(C) \) denote the smallest integer \( i \in N(C) \). Similarly, for the numbers \( A_j \) appearing in the expansion \( A_j z^j \) of the distance enumerator \((16)\) of \( C \), let be the set of integers

\[
M(C) = \{ j \mid 1 \leq j \leq n, A_j \neq 0 \},
\]

and let \( d(C) \) be defined as in \((38)\), that is, \( d(C) \) is the smallest integer \( j \in M(C) \). The parameters

\[
d(C), d'(C), s(C) = |M(C)|, s'(C) = |N(C)|,
\]

were called by Delsarte (1973b) minimum distance, dual distance, number of distances, and external distance, respectively. By Lemma 13.2, all these numbers can be obtained from the distance enumerator \( D_C(z) = \sum A_j z^j \), or from its MacWilliams transform \( \sum B_i z^i \), as the identity \((48)\) can be reversed to

\[
\sum A_j z^j = 2^{-n} \sum |C| B_i (1 - z)^i (1 + z)^{n-i},
\]

by the transformation \( z \to (1 - z)/(1 + z) \). For a pair of codes \( C, C' \) satisfying the MacWilliams identity \((34)\) (in particular for a linear code and its dual), we clearly have

\[
d(C') = d'(C), \quad s(C') = s'(C).
\]
Theorem 14. The parameters (60) the codes $C$, $C'$ satisfy:

\begin{align*}
  s'(C) &= s(C') = 6, & d'(C) &= d(C') = 2^{2t+1} - 2^{t+1}, \\
  d(C) &= d'(C') = 8. 
\end{align*}

Proof. From Table III, it clearly appears that $s(C')$ and $d(C')$ satisfy (62). By Theorem 13, we obtain $s'(C) = s(C')$ and $d'(C) = d(C')$; then by straightforward verifications, we obtain, by use of (61), $A_1 = A_2 = \cdots = A_7 = 0$, and

$$A_8 = 2^{2t-1}(2^{2t+2} - 1)(2^{2t+1} - 1)(2^t - 1)(2^{2t+3} - 17)/315,$$

for the coefficients of the distance enumerator of $C$, which shows that $d(C) = d'(C') = 8$ and proves the theorem.

The importance of the four parameters (60) of a code was stressed by Delsarte (1973b). He obtained, in particular, some theorems proving the existence of $t$-designs in a code $C$ for which $d(C) > s'(C)$ holds. We recall that a $t$-design $S_t^k(t, k, n)$ consists of a collection of $k$-subsets of an $n$-set having the property that every $t$-subset is properly contained in precisely $\lambda$ of the $k$-subsets. From the results of Delsarte (1973b), it follows that $C$ is distance-invariant and yields 2-designs. However, it can be shown that these 2-designs actually are 3-designs. In particular, the set of codevectors of weight 8 in $C$ produces the 3-design $S_3(3, 8, 2^{2t+2})$ with $\lambda = (2^t - 1)(2^{2t+3} - 17)/15$.

Similar properties hold for the code $C'$.

Let $C_p$ be the code of length $2^{2t+3} - 1$ obtained from $C$ by deleting the component $u_L(1)$ from every vector $u \in C$ (cf. (35)), and let $C'_s = C(Z_t)$ be the shortened code of the same length obtained from $C'$ as indicated in Section 5.1.2. Then, it can be shown, by use of the above properties of $C$, $C'$, that the following theorem, stated without proof, holds.

Theorem 15. The codes $C_p$, $C'_s$ of length $2^{2t+2} - 1$ are both distance-invariant, their distance enumerators are related by the MacWilliams identity, and their parameters (60) satisfy

$$s'(C_p) = s(C'_p) = 5, \quad d(C_p) = d'(C'_p) = 7.$$

Remarks. (i) The code $C_p$ contains as many vectors as $C$, that is,

$$|C_p| = 2^k, \quad \text{with} \quad k = 2^{2t+3} - 6t - 5,$$

which is four times as many as in the BCH code of the same length and distance.
(ii) It is perhaps worth noting that $C_p$ is a uniformly packed code in the sense of Goethals and van Tilborg (1975).

(iii) Note that the distance enumerators $D'(z) = \sum D_i' z^i$ of $C_s'$, and $D(z) = \sum D_i z^i$ of $C$, are related by

$$D_i' = D_i(2^{2t+2} - i)/2^{2t+2}$$

for all $i$. Hence, $D'(z)$ is easily obtained from Table III. It can also be obtained from the $\theta$-enumerator of $Z_t$, since $C_s' = C(Z_t)$.

6. SOME SUBCODES OF RM$(m, 2)$

In this section, we shall investigate the class of cyclic codes of length $n = 2^m - 1$ with parity check polynomial of the form

$$h(x) = m_s(x) m_s(x),$$

with $s = 2^i + 1$ for some integer $i$, $1 \leq i \leq m/2$, and where $m_s(x)$ denotes the minimal polynomial of $\omega^{-i}$ for a primitive element $\omega \in GF(2^m)$. In particular, we shall show how the results of Kasami (1969) and Kerdock et al. (1974) on their weight enumerators can be easily derived by our methods.

Let $T$ denote the trace from $GF(2^m)$ to $GF(2)$, and, for $m$ even, let $T'$ be the trace from $GF(2^{m/2})$ to $GF(2)$. Then any $v(x)$ in the code with parity check polynomial (64) is of the form

$$v(x) = \sum_{i=0}^{n-1} Q(\omega^i) x^i$$

where $Q$ is a quadratic form on $V = GF(2^m)$ defined by

$$Q(\xi) = T(\alpha \xi + \beta \xi^s), \quad \forall \xi \in V,$$

for some $\alpha, \beta \in V$ if $s \neq 1 + 2^{m/2}$, or by

$$Q(\xi) = T(\alpha \xi) + T'(\beta \xi^s), \quad \forall \xi \in V,$$

for $\alpha \in GF(2^m), \beta \in GF(2^{m/2})$ if $m$ is even and $s = 1 + 2^{m/2}$. The bilinear form (5) defined by (66) is uniquely defined by $\beta$ as follows:

$$B(\xi, \eta) = T(\eta L_\beta(\xi)), \quad L_\beta(\xi) = \beta \xi^{2^i} + (\beta \xi)^{2m-i}, \quad \forall \xi, \eta \in V.$$
Similarly, for the bilinear form defined by (67), we have

\[ B(\xi, \eta) = T'(\eta L_B(\xi)), \quad L_B(\xi) = \beta_\xi \xi^{m/2}, \quad \forall \xi, \eta \in V. \]  

(69)

We recall (cf. (25)) that there exists, between the rank \( \text{rk}(B) \) of the bilinear form \( B \) and the dimension of the kernel \( \text{Ker}(L_B) \) of the linear map \( L_B: V \to V \), the relation

\[ \text{rk}(B) + \dim \text{Ker}(L_B) = m. \]  

(70)

Clearly, for any nonzero \( \beta \in GF(2^{m/2}) \), we have, in (69), \( \text{Ker}(L_B) = \{0\} \), whence \( \text{rk}(B) = m \). Hence, for \( m \) even, the set of alternating bilinear forms on \( V \) defined by (69) for all \( \beta \in GF(2^{m/2}) \) is a linear \((m, m/2)\)-set (cf. Section 3).

Clearly, its \( \theta \)-enumerator is the polynomial \( 1 + (2^{m/2} - 1)\xi^{m/2} \), from which we easily obtain (cf. Proposition 6) the weight enumerator of the \((2^m - 1, 3m/2)\) cyclic code defined by all quadratic forms (67), by

\[ W(z) = W_0(z) + (2^{m/2} - 1)W_{m/2}(z), \]

with \( W_0(x) \) defined by Table I.

Let us now consider the case \( s \neq 1 + 2^{m/2} \), and let \( \gamma \) be defined by \( \gamma = \beta^{2^m - i}, \forall \beta \in GF(2^m) \). Then, \( L_B(\xi) \) in (68) can be expressed by

\[ L_B(\xi) = (L_B'(\xi))^{2^i}, \quad L_B'(\xi) = \gamma \xi (\xi^{2^m - 2i} + \gamma^{2^i - 1}), \quad \forall \xi \in V. \]  

(71)

For \( \gamma \neq 0 \), let \( \gamma \) be expressed as the \( j \)th power \( \omega^j \) of a primitive element, and let \( d \) and \( t \) be defined by

\[ d = \gcd(m, 2i), \quad t = \gcd(2^m - 1, 2^i + 1). \]  

(72)

**Lemma 16.** The dimension of the kernel in \( V = GF(2^m) \) of the linear map \( L_B \) defined by (71) for a nonzero \( \gamma = \omega^j \in V \), is given by

\[ \dim \text{Ker}(L_B) = d \quad \text{if} \quad j \equiv 0 \text{ (mod } t), \]

\[ = 0, \quad \text{otherwise.} \]

**Proof.** Apparently, we have \( \text{Ker}(L_B) = \text{Ker}(L_B') \), and for \( \gamma = \omega^j \), a nonzero element \( \omega^\nu \in V \) is a zero of \( L_B' \) iff the congruence

\[ \nu(2^{m-2i} - 1) \equiv j(2^i - 1)(\text{mod } 2^m - 1) \]  

(73)

admits a solution \( \nu \). We observe that we have

\[ \gcd(2^m - 1, 2^{m-2i} - 1) = \gcd(2^m - 1, 2^i - 1) = 2^d - 1 \]
with \( d \) defined by (72). Hence, the congruence (73) admits \( 2^d - 1 \) or no solutions \( \nu \) according as \( j(2^r - 1) \) is divisible by \( 2^d - 1 \) or not, that is, according as \( j \) is congruent to zero mod \( t \) or not, with \( t \) defined by (72). This proves the lemma.

**Corollary 17.** The \( \theta \)-enumerator \( \sum a_\nu z^\nu \) of the set of alternating bilinear forms defined by (68) for all \( \beta \in \text{GF}(2^m) \), has the following nonzero coefficients, where \( d \) and \( t \) are defined by (72),

\[
a_0 = 1, \quad a_{(m-d)/2} = (2^m - 1)/t, \quad a_m/2 = (2^m - 1)(t - 1)/t.
\]

**Proof.** For \( \beta = 0 \), we have \( \text{rk}(B) = 0 \), and for any nonzero \( \beta = \gamma^2 \), \( \gamma = \omega^j \), we have by Lemma 16 and (70), \( \text{rk}(B) = m - d \) or \( m \), according as \( j \equiv 0 \pmod{t} \) or \( j \not\equiv 0 \pmod{t} \). This proves the corollary.

**Remark.** Note that, for \( m \) odd, we have \( t = 1 \) and \( d \) odd (cf. (72)), whence all the nonzero bilinear forms have the same rank \( m - d \equiv 0 \pmod{2} \).

From Proposition 6 it follows that the weight enumerator \( W(z) \) of the linear \( (2^m - 1, 2m) \) cyclic code, consisting of the vectors (65) defined by all quadratic forms (66), is uniquely determined by

\[
W(z) = \sum a_r W_r(z) \tag{74}
\]

with \( W_r(z) \) defined by Table I and \( a_r \) given as in Corollary 17. These weight enumerators were already obtained by Kasami (1969) in all cases, and by Kerdock et al. (1974) in the case when \( m \) is odd. We feel, however, that our way of obtaining it was worth mentioning, especially since, by Proposition 6(ii), we may obtain the weight enumerators of some other codes by the duality relation (14), as illustrated in Example 1. We give below another example.

**Example 2.** For \( m = 8 \) and \( s = 3 \) or 9, we have \( t = 3 \), \( d = 2 \). Hence, by Corollary 17, we obtain \( a_0 = 1, \ a_3 = 85, \ a_4 = 170 \), from which the weight enumerator of the corresponding \( (255, 16) \) code can be obtained by (74). By the duality relation (14), we obtain \( b_0 = 1, \ b_1 = 0, \ b_2 \neq 0 \) in the dual \( \theta \)-enumerator, thus showing the existence of a linear \( (255, 28) \) code with minimum weight \( 2^7 - 2^6 = 96 \). Note that the 2-optimal code \( C(Z_2) \) of the same length and minimum distance, which is nonlinear, contains \( 2^{29} \) vectors (cf. Section 4.3), and that the shortened BCH code of the same length and distance has dimension 28.
ACKNOWLEDGMENTS

The author would like to state that he found in a manuscript (to appear as a chapter in a forthcoming book) by MacWilliams and Sloane (1973) the basic idea of the proof of Theorem 13.

Thanks are also due to N. Patterson and J. J. Seidel for some discussions on the subject of this paper, and to P. Delsarte for his helpful remarks.

RECEIVED: February 21, 1975

REFERENCES


