References

[1] T. Kasami and S. Lin, "Coding for a multiple-access channel," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 129–137, Mar. 1976.

[2] ——, "Bounds on the achievable rates of block coding for a memoryless multiple-access channel," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 187–197, Mar. 1978.

[3] ——, "Decoding of linear δ-decodable codes for a multiple-access channel," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 633–635, Sept. 1978.

[4] J. B. Anderson, "Theorems for superposable codes with applications to multiple-access communication," submitted to *IEEE Trans. Inform. Theory*.

[5] S. C. Chang, "Coding for a T-user channel," Ph.D. dissertation, Dep. Elec. Eng., Univ. of Hawaii, Honolulu, 1977.

[6] E. J. Weldon, Jr., "Coding for a multiple-access channel," *Inform. Contr.*, vol. 36, pp. 256–274, Mar. 1978.

[7] R. Ahlswede, "Multi-Way communications channels," *2nd Int. Symp. Information Transmission*, USSR, 1971.

[8] H. H. J. Liao, "Multiple-Access channels," Ph.D. dissertation, Dep. Elec. Eng., Univ. of Hawaii, Honolulu, 1972.

[9] D. Slepian and J. K. Wolf, "A coding theorem for multiple-access channels," *Bell Syst. Tech. J.*, vol. 51, pp. 1037–1076, 1973.

[10] G. D. Forney, Jr., "Convolutional codes I: Algebraic structure," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 720–738, Nov. 1970.

[11] J. L. Massey and M. K. Sain, "Inverses of linear sequential circuits," *IEEE Trans. Comput.*, vol. C-17, pp. 330–337, Apr. 1968.

[12] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 260–269, Apr. 1967.

[13] P. R. Chevillat, personal communication, May 1977.

[14] R. R. Olson, "Note on feedforward inverses for linear sequential circuits," *IEEE Trans. Comput.*, vol. C-19, pp. 1216–1221, Dec. 1970.

On the Weight Distribution of Binary Linear Codes

MARK G. KARPOVSKY

***Abstract*—Let V be a binary linear (n,k)-code defined by a check matrix H with columns $h_1,\cdots,h_n$, and let $h(x)=1$ if $x\in\{h_1,\cdots,h_n\}$, and $h(x)=0$ if $x\notin\{h_1,\cdots,h_n\}$. A combinatorial argument relates the Walsh transform of $h(x)$ with the weight distribution $A(i)$ of the code V for small $i\,(i<7)$. This leads to another proof of the Pless ith power moment identities for $i<7$. This relation also provides a simple method for computing the weight distribution $A(i)$ for small i. The implementation of this method requires at most $(n-k+1)2^{n-k}$ additions and subtractions, $5\cdot 2^{n-k}$ multiplications, and 2^{n-k} memory cells. The method may be very effective if there is an analytic expression for the characteristic Boolean function $h(x)$. This situation will be illustrated by several examples.**

I. Introduction

Suppose that the binary linear (n,k)-code V is defined by its $(n-k)\times n$ check matrix H with columns $h_1,\cdots,h_n$, so that $x\in V$ if and only if $Hx=0$. Our code has a minimum distance at least d if $h_{r_1}\oplus\cdots\oplus h_{r_{d-1}}\neq 0$ for every $1\leqslant r_1<\cdots<r_{d-1}\leqslant n$, where the symbol $\oplus$ stands for componentwise addition mod 2 of binary vectors. Here we assume $d>2$, and so $h_r\neq 0$, and $h_r\neq h_j$ for $r\neq j$.

We denote by $A(i)$ the number of code vectors of weight i which belong to our code ($A(0)=1$, $A(1)=0$, $A(2)=0$). The problem of determining $A(i)$ has been the subject of intensive study (see [1]–[6]).

Manuscript received January 27, 1978; revised April 17, 1978.

The author was with the Computer Science Division, Department of Mathematics, Tel-Aviv University, Tel-Aviv, Israel. He is now with the Computer Science Department, School of Advanced Technology, State University of New York at Binghamton, Binghamton, NY 13850.

Let $h(x)$ be the characteristic function for the set $\{h_1,\cdots,h_n\}$, i.e.,

$$h(x)=\begin{cases}1, & x\in\{h_1,\cdots,h_n\},\\ 0, & x\notin\{h_1,\cdots,h_n\}.\end{cases}$$

Then $h(x)$ is a Boolean function of $n-k$ arguments $x^{(1)},\cdots,x^{(n-k)}$. The Walsh transform $\hat{h}(\omega)$ of $h(x)$ may be defined by the formula

$$\hat{h}(\omega)=\sum_x h(x)w_\omega(x), \tag{1}$$

where $\omega=(\omega^{(1)},\cdots,\omega^{(n-k)})$ is any binary vector with $n-k$ components and

$$w_\omega(x)=(-1)^{\sum_{r=1}^{n-k}x^{(r)}\omega^{(r)}}. \tag{2}$$

All the classical properties of the Fourier transform, such as linearity, translation of arguments, the convolution theorem, the theorems of Plancherel, Poisson, Wiener and Khinchin, etc., apply to the Walsh transform [7].

In this paper we shall establish the connections between the Walsh transform $\hat{h}(\omega)$, as defined in (1), and the weight enumerators $A(i)$ $(i<7)$ by using combinatorial arguments. This will provide us with another proof of the Pless ith power moment identities [3] for $i<7$ and with a method for computing the weight enumerators $A(i)$ for small i $(i=3, 4, 5, 6)$. These $A(i)$ are very important if we are trying to estimate the error-detecting or error-correcting capability of a code with a small code distance when channel errors are independent.

For an arbitrary binary linear (n,k)-code this method needs at most $(n-k+1)2^{n-k}$ additions and subtractions, $5\cdot 2^{n-k}$ multiplications, and 2^{n-k} memory cells. Since the complexity of computations depends only on $n-k$, we may use this method for the important practical case when n and k are large but $n-k$ is comparatively small. This method may be very effective also if we have an analytic expression for the characteristic Boolean function $h(x)$. This situation will be illustrated by several examples in Section IV.

II. Weight Distribution of Binary Linear Codes

Let V be a binary linear (n,k)-code defined by its check matrix H with columns $h_1,\cdots,h_n$, and let C_i be the number of i-tuples of (not necessarily distinct) binary vectors from $\{h_1,\cdots,h_n\}$ such that for every i-tuple $(h_{r_1},\cdots,h_{r_i})$ we have

1) $h_{r_1}\oplus\cdots\oplus h_{r_i}=0$, and
2) there exist $\alpha,\beta\in\{1,\cdots,i\}$ such that $h_{r_\alpha}=h_{r_\beta}$ and $\alpha\neq\beta$. (Note that any rearrangement of an i-tuple counts as a different i-tuple.)

Theorem 1: For any binary (n,k)-code with check matrix $H=(h_1,\cdots,h_n)$, the weight enumerator is given by

$$A(i)=\frac{1}{i!}\Big(2^{-(n-k)}\sum_\omega \hat{h}^i(\omega)-C_i\Big), \qquad \text{for } i=3,\cdots,n, \tag{3}$$

where $\hat{h}^i(\omega)$ is the ith power of $\hat{h}(\omega)$.

Proof: Let S_i be the number of i-tuples $(h_{r_1},\cdots,h_{r_i})$ of not necessarily distinct vectors such that

$$\bigoplus_{j=1}^{i} h_{r_j}=0.$$

Then, by definition of $A(i)$ and C_i, we have

$$A(i)=\frac{1}{i!}(S_i-C_i). \tag{4}$$

0018-9448/79/0100-0105$00.75

Since, from (2),

$$W_\omega(x)W_\omega(y)=W_\omega(x\oplus y)$$

and

$$\sum_\omega W_\omega(x)=\begin{cases}2^{n-k}, & x=0\\ 0, & x\neq 0\end{cases}$$

we have from (1)

$$\hat{h}^i(\omega)=\sum_{x_1,\cdots,x_i} h(x_1)\cdots h(x_i)W_\omega(x_1\oplus\cdots\oplus x_i)$$

and

$$\sum_\omega \hat{h}^i(\omega)=2^{n-k}\sum_{x_1\oplus\cdots\oplus x_i=0} h(x_1)\cdots h(x_i). \tag{5}$$

By definitions of $h(x)$ and S_i it follows from (5) that

$$S_i=2^{-(n-k)}\sum_\omega \hat{h}^i(\omega), \tag{6}$$

and from (4) and (6) we obtain (3). This completes the proof.

We note that in order to compute $\hat{h}(\omega)$ it is expedient to use the algorithm of the fast Walsh transform. In this case the computation of $\hat{h}(\omega)$ requires only $(n-k)2^{n-k}$ additions and subtractions and 2^{n-k} memory cells [7], [8].

III. Computation of $A(3)$, $A(4)$, $A(5)$, $A(6)$ and Connection with the Pless–MacWilliams Identities

It follows from Theorem 1 that the problem of determining the weight distribution may be reduced to the computation of C_i. We shall now show that for small i ($i=3$, 4, 5, 6) this computation may be carried out by simple combinatorial methods.

Corollary 1: For any linear (n,k)-code with check matrix $H=(h_1,\cdots,h_n)$ and with minimum distance $d>2$,

$$A(3)=\frac{1}{6}2^{-(n-k)}\sum_\omega \hat{h}^3(\omega), \tag{7}$$

$$A(4)=\frac{1}{24}\left(2^{-(n-k)}\sum_\omega \hat{h}^4(\omega)-n(3n-2)\right), \tag{8}$$

$$A(5)=\frac{1}{120}\left(2^{-(n-k)}\sum_\omega \hat{h}^5(\omega)-60A(3)(n-2)\right), \tag{9}$$

$$A(6)=\frac{1}{720}\left(2^{-(n-k)}\sum_\omega \hat{h}^6(\omega)-(n+15n(n-1)^2+120A(4)(3n-8))\right). \tag{10}$$

Proof: Let $f(d)$ be the number of distinct components in a vector $d=(d_1,\cdots,d_i)$, where $d_1,\cdots,d_i\in\{h_1,\cdots,h_n\}$, and define $D_r(i)$ by

$$D_r(i)=\left\{d=(d_1,\cdots,d_i)\,\Big|\,\bigoplus_{j=1}^{i} d_j=0;\ d_1,\cdots,d_i\in\{h_1,\cdots,h_n\};\ f(d)=r\right\},\quad r=1,\cdots,i. \tag{11}$$

Then, by definition of C_i and S_i, we have

$$S_i=\sum_{r=1}^{i}|D_r(i)|\qquad C_i=\sum_{r=1}^{i-1}|D_r(i)| \tag{12}$$

where $|D_r(i)|$ is the cardinality of $D_r(i)$.

1) If $i=3$, then since $h_r\neq 0$, $h_r\neq h_j$ ($r\neq j$; $r,j=1,\cdots,n$), we have

$$|D_1(3)|=0,\qquad |D_2(3)|=0,\quad\text{and}\quad C_3=0.$$

2) If $i=4$, then

$$|D_1(4)|=n,\qquad |D_2(4)|=\frac{1}{2}\binom{4}{2}n(n-1),$$

$$|D_3(4)|=0,\qquad\text{and } C_4=n(3n-2).$$

3) For $i=5$ we have

$$|D_1(5)|=0,\qquad |D_2(5)|=0,\qquad |D_3(5)|=\binom{5}{3}A(3)\cdot 3!,$$

$$|D_4(5)|=\binom{5}{3}A(3)3!(n-3),\quad\text{and}\quad C_5=60A(3)(n-2).$$

4) For $i=6$ we have

$$|D_1(6)|=n,\qquad |D_2(6)|=\binom{6}{2}n(n-1),$$

$$|D_3(6)|=\binom{6}{2}n(n-1)(n-2),$$

$$|D_4(6)|=\frac{1}{3}\binom{6}{4}\cdot 4!4A(4)=120A(4)\cdot 4,$$

$$|D_5(6)|=\binom{6}{4}4!A(4)(n-4)=120A(4)(3n-12),\quad\text{and}$$

$$C_6=|D_1(6)|+\cdots+|D_5(6)|=n+15n(n-1)^2+120A(4)(3n-8).$$

Expressions (7)–(10) may now be obtained from (4) and (6), completing the proof.

If the all-ones vector belongs to our (n,k)-code, then

$$A(i)=A(n-i),\qquad \sum_{i=0}^{n}A(i)=2^k,$$

and by (7)–(10) we may immediately obtain the weight distribution $\{A(i)\}$ ($i=0,\cdots,n$) for every $n<16$.

Next we shall discuss the connections between Theorem 1, Corollary 1, and the classical Pless–MacWilliams identities [2], [3].

Let $B(i)$ denote the number of vectors of weight i in the dual code, and let the Pless rth power moment identity [3] ($r=0,1,\cdots$) be expressed as follows:

$$\sum_{i=0}^{n} i^rB(i)=Q_r(0)+\sum_{i=3}^{r}A(i)Q_r(i). \tag{13}$$

Moreover, let

$$C_r=S_r-r!A(r). \tag{14}$$

Then we shall show that for $r<7$ $Q_r(i)$ may be generated by $Q_0(i),\cdots,Q_{r-1}(i)$, and C_r. Thus the Pless power moment identities (13) for $r<7$ may be obtained recursively from (7)–(10). Alternatively, it will be seen that expressions for C_r may be obtained from the Pless–MacWilliams identities. This computation of C_r, however, becomes cumbersome for $r>5$.

We note that $\hat{h}(\omega)$, as given in (1), is equal to $n-2\,wt\,(\omega H)$, where $wt(x)$ denotes the weight of the vector x, and ωH is the vector of length n obtained by multiplying the parity check matrix H by the row vector ω (thus ωH belongs to the dual code). It follows that S_i, as defined in (6), is equal to

$$S_i=2^{-(n-k)}\sum_{j=0}^{n}B(j)(n-2j)^i. \tag{15}$$

Thus we have from (13)–(15),

$$C_r+r!A(r)=2^{-(n-k)}\sum_{i=0}^{n}B(i)\sum_{t=0}^{r}(-1)^tn^{r-t}2^t\binom{r}{t}i^t$$

$$=2^{-(n-k)}\sum_{t=0}^{r-1}(-1)^tn^{r-t}2^t\binom{r}{t}\cdot\left(Q_t(0)+\sum_{i=3}^{t}A(i)Q_t(i)\right)$$

$$+2^{-(n-k)+r}(-1)^r\sum_{i=0}^{n}i^rB(i),$$

and

$$\sum_{i=0}^{n} i^r B(i) = (-1)^r 2^{n-k-r} C_r + \sum_{t=0}^{r-1} (-1)^{t-r+1} 2^{t-r} n^{r-t} \binom{r}{t} \cdot \left(Q_t(0) + \sum_{i=3}^{t} A(i) Q_t(i) \right) + (-1)^r r! 2^{n-k-r} A(r). \tag{16}$$

For any (n,k)-code, it follows from (6), (1), (2), $h(0,\cdots,0)=0$, and the Parseval theorem for the Walsh transform, that

$$S_0 = 1, \quad S_1 = 0, \quad S_2 = n, \tag{17}$$

and, since $A(0)=1$ and $A(1)=A(2)=0$, we conclude from (6)–(10), (14), and (17), that

$$C_0 = C_1 = 0, \quad C_2 = n, \quad C_3 = 0,$$
$$C_4 = n(3n-2), \quad C_5 = 60A(3)(n-2),$$
$$C_6 = n + 15n(n-1)^2 + 120A(4)(3n-8). \tag{18}$$

The Pless rth power moment identities for $r=0,1,\cdots,6$ follow now immediately from (16) and (18). Alternatively, we have by the MacWilliams identities

$$A(i) = 2^{-(n-k)} \sum_{j=0}^{n} B(j) P_i(j), \tag{19}$$

where $P_i(j)$ is a (Krawtchouk) polynomial of degree i in the variable j. Thus (15) and (19) imply that

$$A(i) = \frac{1}{i!} \left(S_i - 2^{-(n-k)} \sum_{j=0}^{n} B(j) \left((n-2j)^i - i! P_i(j) \right) \right). \tag{20}$$

For the Krawtchouk polynomial

$$P_i(j) = \sum_{S=0}^{i} (-1)^s \binom{j}{s} \binom{n-j}{i-s} = \sum_{t=0}^{i} P_{i,t} j^t,$$

we have

$$P_{i,i} = (-1)^i (i!)^{-1} 2^i$$

and

$$P_{i,i-1} = (-1)^{i-1} ((i-1)!)^{-1} n 2^{i-1}$$

and the degree of the polynomial $(n-2j)^i - i! P_i(j)$ is at most $i-2$. Consequently we may obtain formulas (7)–(10) from (20) by the Pless rth power moment identities for $r=0,\cdots,4$.

We note also that Corollary 1 generates necessary and sufficient conditions that the given (n,k)-code V be double- or triple-error-correcting.

Corollary 2: Let V be a linear (n,k)-code with distance $d(V)$ and with check matrix $H=(h_1,\cdots,h_n)$. Then 1) $d(V) \geqslant 5$ if and only if

$$S_0 = 1, \quad S_1 = 0, \quad S_2 = n, \quad S_3 = 0, \quad S_5 = n(3n-2); \tag{21}$$

and 2) $d(V) \geqslant 7$ if and only if (21) is satisfied and

$$S_5 = 0, \quad S_6 = n + 15n(n-1)^2, \tag{22}$$

where S_i is the ith power-symmetric function of $\hat{h}(\omega)$, defined by (6). The proof of Corollary 2 follows immediately from (7)–(10) and (17).

For any function $f(x^{(1)},\cdots,x^{(n-k)})$ of binary arguments, the convolution theorem for the Walsh transform [7] states that $\hat{f}*\hat{f} = 2^{n-k}\hat{f}$ (where $(f*f)(x) = \Sigma_\tau f(\tau) f(x \oplus \tau)$) if and only if f is a Boolean function. Thus, for example, Corollary 2 implies that for the construction of an (n,k)-code V with $d(V) \geqslant 7$ it is sufficient to find $\hat{h}(\omega)$ for all ω such that $\hat{h}*\hat{h} = 2^{n-k}\hat{h}$ and the power symmetric functions S_i $(i=0,\cdots,6)$ satisfy (21) and (22).

It should be pointed out that if we use the fast Walsh transform to compute $\hat{h}(\omega)$, then the computation of $A(i)$ $(i=3, 4, 5, 6)$ using (7)–(10) requires at most $(n-k+1)2^{n-k}$ additions and subtractions, $5 \cdot 2^{n-k}$ multiplications, and 2^{n-k} memory cells. This method of computation of $A(i)$ $(i=3, 4, 5, 6)$ may be simpler for codes with a small distance than the well-known alternative of first computing the weight distribution $\{B(j)\}$ $(j=0,\cdots,n)$ of the dual code and then applying the MacWilliams identities (19). Indeed, the computation of $wt(\omega H)$ for all ω requires at least $n \cdot 2^{n-k}$ additions and, moreover, the computation of $A(i)$ $(i=3, 4, 5, 6)$ from $B(j)$ $(j=3,\cdots,n)$ further requires at least $4n$ multiplications and $4n$ additions. We note also that if we have an analytic expression for the characteristic Boolean function $h(x)=h(x^{(1)},\cdots,x^{(n-k)})$ of our code, then sometimes we may find $\hat{h}(\omega)$ and $A(i)$ $(i=3, 4, 5, 6)$ immediately (without application of the algorithm of the fast Walsh transform). This situation will be illustrated by several examples in the next section. Tables of $\hat{h}(\omega)$ for a large number of classes of Boolean functions $h(x)$ may be found in the monograph [7].

IV. EXAMPLES

Example 1: As the first example we consider the well-known Hamming (n,k)-codes with code distance $d=3$, $n=2^\alpha-1$, and $k=2^\alpha-\alpha-1$. For these codes

$$h(x) = \begin{cases} 0, & x=0 \\ 1, & x \neq 0, \end{cases} \qquad \hat{h}(\omega) = \begin{cases} 2^{n-k}-1, & \omega=0 \\ -1, & \omega \neq 0, \end{cases}$$

and $\Sigma_\omega \hat{h}^i(\omega) = (2^{n-k}-1)^i + (-1)^i(2^{n-k}-1)$. By (7)–(10) we have

$$A(3) = \frac{1}{3!} n(n-1), \tag{23}$$

$$A(4) = \frac{1}{4!} n(n^2-4n+3), \tag{24}$$

$$A(5) = \frac{1}{5!} n(n^3-11n^2+31n-21), \tag{25}$$

$$A(6) = \frac{1}{6!} n(n^4-16n^3+86n^2-176n+105). \tag{26}$$

Example 2: We consider extended Hamming (n,k)-codes with $n=2^\alpha$, $k=2^\alpha-\alpha-1$. The check matrix

$$H = \begin{bmatrix} 0 & & & \\ 0 & & & \\ \vdots & & H' & \\ 0 & & & \\ 1 & 1 & \cdots & 1 \end{bmatrix}$$

of this code may be obtained by adding a row of ones to the check matrix H' of the Hamming $(2^\alpha-1, 2^\alpha-\alpha-1)$-code. It is evident that for these codes $A(2i+1)=0$, for all i.

The characteristic function $h(x)$ is defined by the formula $h(x^{(1)},\cdots,x^{(n-k)}) = x^{(1)}$. Thus

$$\hat{h}(\omega) = \hat{h}(\omega^{(1)},\cdots,\omega^{(n)}) = \begin{cases} n, & \omega=(0,\cdots,0) \\ -n, & \omega=(1,0,\cdots,0) \\ 0, & \text{otherwise}, \end{cases}$$

$$\sum_\omega \hat{h}^i(\omega) = (1+(-1)^i)n^i,$$

and by (8) and (10) we have

$$A(4)=\frac{1}{4!}n(n^2-3n+2), \tag{27}$$

$$A(6)=\frac{1}{6!}n(n^4-15n^3+70n^2-120n+64). \tag{28}$$

We note that formulas (23)–(26) and (27) and (28) correspond to the more general and well-known results about weight distribution of Hamming codes and extended Hamming codes (see [1]).

Example 3: Consider the (n,k)-codes with $n=2^\alpha-2^{\alpha-t}$, $k=2^\alpha-2^{\alpha-t}-\alpha$ $(t=2,\cdots,\alpha)$, and $d=3$, obtained by deleting from the check matrix for the $(2^\alpha-1, 2^\alpha-\alpha-1)$-Hamming code all columns $h_j=(h_j^{(1)},\cdots,h_j^{n-k})$ for which $h_j^{(1)}=h_j^{(2)}=\cdots=h_j^{(t)}=0$ $(j=1,\cdots,2^{\alpha-t}-1)$. Thus we have

$$h(x)=\bigvee_{i=1}^{t} x^{(i)},$$

where the symbol V stands for logical summation, and [7]

$$\hat{h}(\omega)=\begin{cases} n, & \omega=(0,\cdots,0);\\ -2^{n-k-t}, & \omega^{(t+1)}=\cdots=\omega^{(n-k)}=0 \text{ and } \omega\neq(0,\cdots,0);\\ 0, & \text{otherwise.}\end{cases}$$

Hence

$$\sum_\omega \hat{h}^i(\omega)=n^i+(2^t-1)(-1)^i 2^{i(n-k-t)},$$

and by (7)–(10) we have

$$A(3)=\frac{1}{3!}n(n-2^{n-k-t}), \tag{29}$$

$$A(4)=\frac{1}{4!}n(2^{2(n-k)}-3n(2^{n-k-t}+1)+2), \tag{30}$$

$$A(5)=\frac{1}{5!}n(n-2^{n-k-t})(n^2+2^{2(n-k-t)}-10n+20), \tag{31}$$

$$\begin{aligned}A(6)=\frac{1}{6!}n\big(&n^4-2^{n-k-t}n^3+2^{2(n-k-t)}n^2-2^{3(n-k-t)}n\\ &+2^{4(n-k-t)}-5(3n-8)\\ &\cdot(2^{2(n-k)}-3n(2^{n-k-t}+1)+2)-15(n-1)^2-1\big).\end{aligned} \tag{32}$$

Example 4: Consider the (n,k)-codes with $n=2^{\alpha-1}(2^\alpha-1)$, $k=2^{\alpha-1}(2^\alpha-1)-2\alpha$, and $d=3$, generated by "nonrepetitive quadratic forms over GF(2)" through

$$h(x^{(1)},\cdots,x^{(2\alpha)})=\bigoplus_{i,t=1}^{2\alpha} x^{(i)}x^{(t)}, \tag{33}$$

in which each of the arguments $x^{(s)}$ $(s=1,\cdots,2\alpha)$ appears exactly once. For the nonrepetitive quadratic form (33) we have [7]

$$\hat{h}(\omega)=\begin{cases} 2^{\alpha-1}(2^\alpha-1), & \omega=(0,\cdots,0),\\ 2^{\alpha-1}, & h(\omega)=1,\\ -2^{\alpha-1}, & h(\omega)=0,\ \omega\neq(0,\cdots,0).\end{cases}$$

Hence

$$\sum_\omega \hat{h}^i(\omega)=2^{i(\alpha-1)}((2^\alpha-1)^i+2^{\alpha-1}(2^\alpha-1)+(-1)^i 2^{\alpha-1}(2^\alpha+1)),$$

and by (7)–(10) we have

$$A(3)=\frac{1}{3!}2^{2\alpha-2}(2^\alpha-1)(2^{\alpha-1}-1), \tag{34}$$

$$A(4)=\frac{1}{4!}2^{\alpha-1}(2^\alpha-1)(2^{4\alpha-3}-3\cdot2^{3\alpha-3}-2^{2\alpha}+3\cdot2^{\alpha-1}+2), \tag{35}$$

$$\begin{aligned}A(5)=\frac{1}{5!}&2^{2\alpha-2}(2^\alpha-1)(2^{\alpha-1}-1)\\ &\cdot(2^{4\alpha-2}-2^{3\alpha-1}-9\cdot2^{2\alpha-1}+10\cdot2^{\alpha-1}+20),\end{aligned} \tag{36}$$

$$\begin{aligned}A(6)=\frac{1}{6!}&(2^{4\alpha-6}(2^\alpha-1)((2^\alpha-1)^5+2^\alpha+1)\\ &-(n+15n(n-1)^2+120A(4)(3n-8))).\end{aligned} \tag{37}$$

V. Generalization to Nonbinary Codes

The results of the previous sections may be easily generalized to the case of linear codes over GF(q), where q is a prime. To this end we need only make two changes in the basic definitions. First, we replace the check matrix H with columns $h_1,\cdots,h_n$ by the "extended check matrix" with columns h_1, $2h_1,\cdots,(q-1)\cdot h_1,\cdots,h_n$, $2h_n,\cdots,(q-1)h_n$. (All the multiplications are carried out in GF(q).) Second, we replace the Walsh functions $w_\omega(x)$ by the characters $\chi_\omega(x)$ of the group of q-ary vectors (Chrestenson functions [7])

$$\chi_\omega(x)=\exp\left(\frac{2\pi}{q}i\sum_{r=1}^{n-k}x^{(r)}\omega^{(r)}\right),$$

where $x^{(r)}$, $\omega^{(r)}\in\{0,\cdots,q-1\}$, and $i=\sqrt{-1}$. Theorem 1 may now be modified to yield

$$A(r)=\frac{1}{r!}\Big(q^{-(n-k)}\sum_\omega \hat{h}^r(\omega)-C_r\Big), \qquad r=3,\cdots,n;$$

but in this case, C_r depends on q.

To compute $\hat{h}(\omega)$, it is expedient to use the algorithm of the corresponding fast Fourier transform [7], [8], which requires only $(n-k)\,q^{n-k}$ operations and q^{n-k} memory cells. The computation of C_r for small r may be carried out by the method described in the proof of Corollary 1. Thus we have, for example, for ternary (n,k)-codes

$$A(3)=\frac{1}{6}\Big(3^{-(n-k)}\sum_\omega \hat{h}^3(\omega)-2n\Big),$$

$$A(4)=\frac{1}{24}\Big(3^{-(n-k)}\sum_\omega \hat{h}^4(\omega)-12n^2+6n-36A(3)\Big),$$

$$\begin{aligned}A(5)=\frac{1}{120}\Big(&3^{-(n-k)}\sum_\omega \hat{h}^5(\omega)-40n^2+30n\\ &-30A(3)(4n-3)-240A(4)\Big).\end{aligned}$$

We note also that, analogous to the binary case, the Pless rth power moment identities may be obtained if we know C_r for the given q and, alternatively, the expressions for C_r follow from the Pless–MacWilliams identities for linear codes over GF(q).

Acknowledgment

The author would like to thank one of the referees for helpful suggestions concerning the connection between Corollary 1 and the Pless–MacWilliams identities.

References

[1] W. W. Peterson and E. J. Weldon, Jr., *Error Correcting Codes*, 2nd ed. Cambridge: MIT, 1972.

[2] F. J. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell Syst. Tech. J.*, vol. 42, pp. 79–94, 1963.

[3] V. Pless, "Power moment identities on weight distributions in error correcting codes," *Inform. Contr.*, vol. 6, pp. 147–152, 1963.

[4] F. J. MacWilliams, C. L. Mallows, and N. J. A. Sloane, "Generalizations of Gleason's theorem on weight enumerators of self-dual codes," *IEEE Trans. Inform. Theory*, IT-18, pp. 794–805, Nov. 1972.

[5] C. L. Mallows and N. J. A. Sloane, "An upper bound for self-dual codes," *Inform. Contr.*, vol. 22, pp. 188–200, 1973.
[6] G. Cohen, P. Godlewski, and S. Perrine, "Sur les idempotents des codes," *C. R. Acad. Sci.*, vol. 284, Feb. 28, 1977.
[7] M. G. Karpovsky, *Finite Orthogonal Series in the Design of Digital Devices*. New York: Wiley and Jerusalem IUP, 1976.
[8] K. C. Andrews and K. L. Caspari, "A generalized technique for spectral analysis," *IEEE Trans. Comput.*, vol. C-19, pp. 16–25, Jan. 1970.

On a (21,11,6) Binary Code

TAKEO KANAI AND YASUO SUGIYAMA, MEMBER, IEEE

***Abstract*—It is shown that the (21,11,6) binary linear code obtained from BCH codes and a single parity check code by construction *X* is equivalent to a difference-set cyclic code.**

Let us consider construction X which has been proposed by Sloane, Reddy, and Chen [1]. This scheme provides a new code by combining three codes. When applied to BCH codes, the parity check matrix H of the new code is given by

$$H=\begin{array}{|c|c|}\hline H_1 & 0 \\ \hline H_2 & H_3 \\ \hline 0 & H_4 \\ \hline\end{array}$$

where

$\begin{bmatrix} H_1 \\ H_2 \end{bmatrix}$ parity check matrix of BCH code $C_1(n_1, \log_2 M_1, d_1)$,

H_1 parity check matrix of BCH code $C_2(n_1, \log_2 bM_1, d_2)$,

$\begin{bmatrix} H_3 \\ H_4 \end{bmatrix}$ nonsingular matrix,

H_4 parity check matrix of $C_3(n_3, \log_2 b, \Delta)$,

H parity check matrix of the new code $C_4(n_1+n_3, \log_2 bM_1, \min[d_1, d_2+\Delta])$.

We use this result without proof. Let the code C_1 be a (16, 7, 6) extended BCH code which is majority-logic decodable [2], let C_2 be a (16, 11, 4) extended BCH (or Hamming) code, and let C_3 be a (5, 4, 2) single parity check code. The parity check matrix H of the (21, 11, 6) code C_4 obtained from codes C_1, C_2, and C_3 using construction X is given by

$$H=\begin{array}{|c|c|}\hline 1 & 0 \\ \hline \alpha_i & 0 \\ \hline \alpha_i^3 & A \\ \hline 0 & 1 \\ \hline\end{array}$$

Manuscript received February 3, 1978. This paper was presented at the National Conference of the Institute of Electronics and Communication Engineers of Japan, March 31, 1978.

The authors are with Communication Research and Development, Mitsubishi Electric Corp., 80-Nakano, Minamishimizu, Amagasaki City, Hyogo, 661, Japan.

$$H=\begin{bmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&&&&& \\
&&&1&&&1&1&&1&&1&1&1&1&&&&&& \\
&&1&&&1&1&&1&&1&1&1&1&&&&&&& \\
&1&&&1&1&&1&&1&1&1&1&&&&&&&& \\
1&&&&1&&&1&1&&1&&1&1&1&&&&&& \\
&1&1&1&1&&1&1&1&1&&1&1&1&1&&&1&1&1&1 \\
&&1&&1&&&1&&1&&&1&&1&&&&1&&1 \\
&&&1&1&&&&1&1&&&&1&1&&&&&1&1 \\
1&&&&1&1&&&&1&1&&&&1&&1&&&&1 \\
&&&&&&&&&&&&&&&&1&1&1&1&1
\end{bmatrix}$$

Fig. 1. Parity check matrix of (21, 11, 6) majority-logic decodable code obtained by construction X.

where $\alpha_1, \alpha_2, \cdots, \alpha_{16}$ are distinct elements from $GF(2^4)$. The 4×5 submatrix A satisfies the restriction that any four of its columns are linearly independent.

We define the following symbols:

- e_i ith error bit,
- S_i 5×21 composite parity check matrix which is orthogonal on e_i,
- S_i' 5×16 submatrix of S_i,
- S_i'' 5×5 submatrix of S_i,
- P_i 5×10 matrix which generates S_i from H.

With this notation we have the relations

$$S_i=[S_i' S_i'']$$

and

$$S_i=P_iH.$$

As each S_i' is a composite parity check matrix for the code C_1, S_i' is orthogonal on e_i for $i=1,2,\cdots,16$. Therefore, C_4 is also one-step majority-logic decodable if the weight of each column in S_i'' is one or less for all i, $i=1,2,\cdots,11$. An example of the parity check matrix is shown in Fig. 1.

Furthermore, this code is seen to be equivalent to the (21, 11, 6) difference-set cyclic code by applying the following permutation of columns from C_4 to the difference set cyclic code [2]:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 \\ 1 & 3 & 21 & 8 & 15 & 7 & 16 & 9 & 13 & 11 & 10 & 18 & 5 & 17 & 4 & 6 & 20 & 2 & 19 & 14 & 12 \end{bmatrix}$$

One of the reviewers has pointed out that this result can be generalized in terms of PG codes and EG codes [3], [4]. A PG code can be shortened to obtain an EG code. This fact was stated without a formal proof in [3].

Acknowledgment

The authors wish to thank Professor Kasahara for his fruitful discussions. The authors are also grateful to reviewers for their helpful suggestions, and especially to one of the reviewers for a significant comment.

References

[1] N. J. A. Sloane, S. M. Reddy, and C. L. Chen, "New binary codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 503–510, July 1972.
[2] S. Lin, *An Introduction to Error-Correcting Codes*. Englewood Cliffs, NJ: Prentice-Hall, 1970.
[3] C. L. Chen, "On shortened finite geometry codes," *Inform. Contr.*, vol. 20, pp. 216–221, Apr. 1972.
[4] W. T. Warren and C. L. Chen, "On efficient majority logic decodable codes," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 737–745, Nov. 1976.