function obtained by taking w to be the Fourier spectrum is optimal in some sense. (Perhaps the reader will sense a challenge in this.)

Finally, we remark that the above threshold decoding technique is generally applicable to all linear codes over $GF(p)$ (whether block, cyclic, convolutional, or whatever) in the sense that any syndrome decoding function can be implemented using the threshold scheme of (1) and (2). In the general case, $\hat{e}_{i0}(s)$ in (1) and (2) is simply the decoded estimate of the error digit under consideration that would be made by the decoding function to be realized. In general, a different estimator matrix B and weight vector w would be required for the error component of each information digit in the block being decoded. For cyclic codes and $R = 1/b$ convolutional codes, however, one B and one w suffice for all decoding decisions.

References

[1] L. D. Rudolph, "Threshold decoding of cyclic codes," *IEEE Trans. Information Theory*, vol. IT-15, pp. 414–418, May 1969.

[2] J. L. Massey, *Threshold Decoding.* Cambridge, Mass.: M.I.T. Press, 1963.

[3] A. D. Wyner and R. B. Ash, "Analysis of recurrent codes," *IEEE Trans. Information Theory,* vol. IT-9, pp. 143–156, July 1963.

[4] ——, "On the equivalence of two convolution code definitions," *IEEE Trans. Information Theory* (Correspondence), vol. IT-11, pp. 600–602, October 1965.

[5] J. P. Robinson, "Error propagation and definite decoding of convolutional codes," *IEEE Trans. Information Theory,* vol. IT-14, pp. 121–128, January 1968.

[6] W. W. Peterson, *Error-Correcting Codes.* Cambridge, Mass.: M.I.T. Press, 1961.

[7] J. J. Bussgang, "Some properties of binary convolutional code generators," *IEEE Trans. Information Theory,* vol. IT-11, pp. 90–100, January 1965.

[8] L. Rudolph, P. Blackwell, and D. Shurtleff, "Data processing using distributed parameter techniques," Syracuse University Res. Corp., Syracuse, N. Y., Repts. 1, 2, F on Contract (ECOM) DAAB07-67-C-0223, 1968.

Weight Enumerator for Second-Order Reed–Muller Codes

NEIL J. A. SLOANE, MEMBER, IEEE, AND ELWYN R. BERLEKAMP, MEMBER, IEEE

***Abstract*—In this paper, we establish the following result.**

***Theorem*: A_i, the number of codewords of weight i in the second-order binary Reed–Muller code of length 2^m, is given by $A_i = 0$ unless $i = 2^{m-1}$ or $2^{m-1} \pm 2^{m-1-j}$, for some j, $0 \leq j \leq [m/2]$, $A_0 = A_{2^m} = 1$, and**

$$A_{2^{m-1} \pm 2^{m-1-j}} = 2^{j(j+1)} \left\{ \frac{(2^m - 1)(2^{m-1} - 1)}{4 - 1} \right\} \cdot \left\{ \frac{(2^{m-2} - 1)(2^{m-3} - 1)}{4^2 - 1} \right\} \cdots \cdot \left\{ \frac{(2^{m-2j+2} - 1)(2^{m-2j+1} - 1)}{4^j - 1} \right\}, \qquad 1 \leq j \leq [m/2]$$

$$A_{2^{m-1}} = 2\left\{ 2^{m(m+1)/2} - \sum_{j=0}^{[m/2]} A_{2^{m-1} - 2^{m-1-j}} \right\}.$$

Introduction

As SHOWN by Berlekamp ([1], sec. 15.3), the rth-order Reed–Muller (RM) code of length 2^m contains 2^k codewords, where $k = \sum_{i=0}^{r} \binom{m}{i}$. If a codeword is written as $\vec{C} = [C_\infty, C_0, C_1, C_2, \cdots, C_{2^m-2}]$, its coefficients may be evaluated by

$$C_i = F(X_{1,i}, X_{2,i}, \cdots, X_{m,i}),$$

where $F(\cdot, \cdot, \cdots, \cdot)$ is an m-variate binary polynomial, of degree at most r, and the binary elements $X_{1,i}$, $X_{2,i}$, $\cdots$, $X_{m,i}$ are obtained from the equation

$$\alpha^i = \sum_{i=1}^{m} X_{i,i} \alpha^{i-1},$$

where α is a fixed primitive element of $GF(2^m)$, and α^∞ is conventionally defined by the equation $\alpha^\infty = 0$. Each of the 2^k codewords corresponds to a different polynomial F.

It is well known that the minimum distance of the rth-order RM code of length 2^m is given by $d = 2^{m-r}$ and that the number of codewords of that weight is given by

$$A_d = \frac{2^m(2^m - 2^0)(2^m - 2^1)(2^m - 2^2) \cdots (2^m - 2^{\mu-1})}{2^\mu(2^\mu - 2^0)(2^\mu - 2^1)(2^\mu - 2^2) \cdots (2^\mu - 2^{\mu-1})}$$

where $\mu = m - r$. Berlekamp and Sloane [2] have shown that all possible weights between d and $2d$ are of the form $2d - 2^i$.

In the special case $r = 2$, a theorem of McEliece [5] guarantees that every weight is divisible by $2^{[(m-1)/2]}$, thus, the only weights between 0 and $2d = 2^{m-1}$ must be of the form $2^{m-1} - 2^i$, $[(m-1)/2] \leq i < m - 1$. Since the code contains the all-one codeword of weight 2^m, the only

Mansucript received October 6, 1969.

The authors are with the Bell Telephone Laboratories, Inc., Murray Hill, N. J. 07974.

weights between 2^{m-1} and 2^m must be of the form $2^{m-1} + 2^i$, $[(m-1)/2] \leq i < m-1$. This result was first obtained by Kasami [4] using other arguments.

In this paper, we obtain a formula for the number of second-order RM codewords for each weight between d and $2d$. Using this result, Kasami and Tokura have recently obtained a formula for the number of rth-order RM codewords of each weight between d and $2d$.

After reading a preprint of this paper, McEliece [5] has presented a simpler proof of our main result, starting from results by Dickson ([3], secs. 99, 199–204). McEliece's proof also considers nonbinary codes. Since most coding theorists are not familiar with Dickson's investigations of orthogonal groups, we present our own derivation of the weight enumerator of the second-order RM code. This proof is longer than the one given by McEliece, but it requires substantially less background.

Weight Enumerator for the Second-Order Reed–Muller Code

Since each codeword in the second-order RM code corresponds to a polynomial of degree at most 2 in m variables, it may be represented as

$$F(\vec{X}) = \sum_{i>j} F_{i,j}X_iX_j + \sum_i F_{i,i}X_i + G, \qquad (1)$$

where each of the 2^k codewords corresponds to a different choice of the $k = \binom{m}{2} + m + 1$ binary elements, $F_{i,j}$, $F_{i,i}$, and G. Since the X_i are binary variables, $X_i^2 = X_i$, and we may write

$$F(\vec{X}) + G = \sum_{i \geq j} F_{i,j}X_iX_j.$$

Thus, $F(\vec{X}) + G$ is a quadratic form, which may be written as

$$[X_1X_2, \cdots, X_m]\begin{bmatrix} F_{1,1} & 0 & 0 & \cdots & 0 \\ F_{2,1} & F_{2,2} & 0 & \cdots & 0 \\ F_{3,1} & F_{3,2} & F_{3,3} & \cdots & 0 \\ \vdots & \vdots & & & \vdots \\ F_{m,1} & F_{m,2} & F_{m,3} & \cdots & F_{m,m} \end{bmatrix}\begin{bmatrix} X_1 \\ X_2 \\ \vdots \\ \vdots \\ X_m \end{bmatrix}.$$

As done by Berlekamp ([1], ch. 16) we now show that an arbitrary binary quadratic form may be reduced to one of a few special types by appropriate invertible affine transformations of the form $X_i \rightarrow Y_i$, where

$$Y_i = \sum_j B_{i,j}X_j + B_i.$$

In the special case of linear transformations, each $B_i = 0$. Since the transformation is invertible, each vector $\vec{X} = (X_1, X_2, \cdots, X_m)$ corresponds to one and only one vector $\vec{Y} = (Y_1, Y_2, \cdots, Y_m)$, and hence, the weight of the codeword corresponding to the transformed quadratic form is equal to the weight of the codeword corresponding to the original quadratic form.

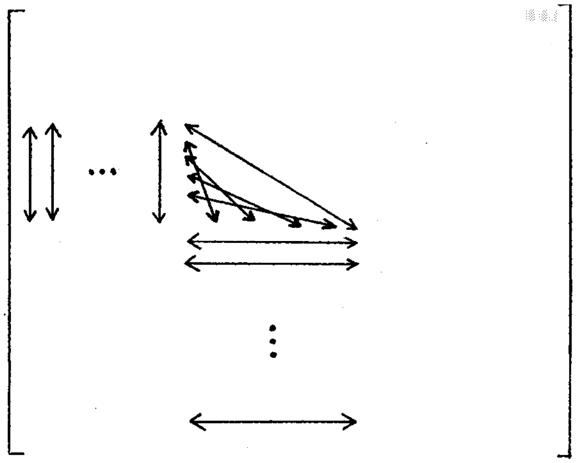
We now review the two elementary linear transformations of quadratic forms:

1) Exchange i and j, i.e., let $Y_i = X_j$, $Y_j = X_i$, $Y_k = X_k$ for $k \neq i, j$, where $i < j$. This transforms the matrix of the quadratic form as follows.

$$\begin{bmatrix} F_{1,1} & & & & & & & \\ \cdots & & & & & & & \\ F_{i,1} & F_{i,2} & \cdots & F_{i,i} & & & & \\ & & & F_{i+1,i} & & & & \\ & & & \vdots & & & & \\ F_{j,1} & F_{j,2} & \cdots & F_{j,i} & \cdots & F_{j,j} & & \\ & & & F_{j+1,i} & & F_{j+1,j} & & \\ & & & \vdots & & \vdots & & \\ F_{m,1} & F_{m,2} & \cdots & F_{m,i} & \cdots & F_{m,j} & \cdots & F_{m,m} \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} F_{1,1} & & & & & & & \\ \cdots & & & & & & & \\ F_{j,1} & F_{j,2} & \cdots & F_{j,j} & & & & \\ & & & F_{j,i+1} & & & & \\ & & & \vdots & & & & \\ F_{i,1} & F_{i,2} & \cdots & F_{j,i} & \cdots & F_{i,i} & & \\ & & & F_{j+1,i} & & F_{j+1,i} & & \\ & & & \vdots & & \vdots & & \\ F_{m,1} & F_{m,2} & \cdots & F_{m,j} & \cdots & F_{m,i} & \cdots & F_{m,m} \end{bmatrix}.$$

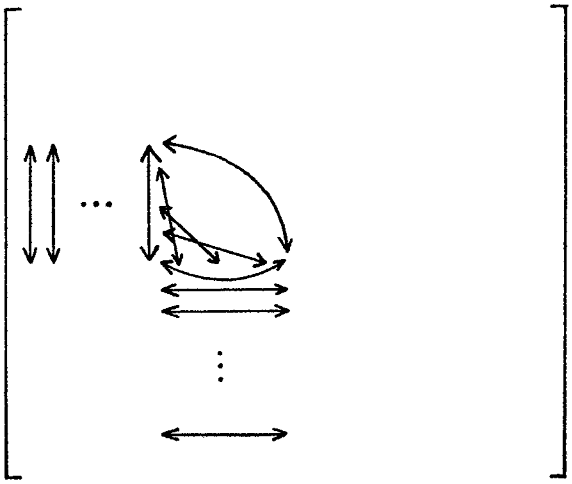
In other words, the elements of the matrix are permuted according to the arrows in the following diagram.



2) Add row-column i into row-column j, i.e., replace X_j by $Y_i + Y_j$, X_B by Y_B for $k \neq j$, where $i < j$. This transforms the matrix as follows.

$$F \rightarrow \begin{bmatrix}
F_{1,1} & & & & & \\
\cdots & & & & & \\
F_{i,1} & F_{i,2} & \cdots F_{i,i} & & & \\
 & & F_{i+1,i} & & & \\
\vdots & & \vdots & & & \\
F_{i,1} + F_{j,1} & F_{i,2} + F_{j,2} & \cdots F_{j,i} & F_{i+1,i} + F_{j,i+1} \cdots & \xi & \\
 & & F_{j+1,i} & & F_{j+1,i} + F_{j+1,j} & \\
\vdots & & \vdots & & \vdots & \\
F_{m,1} & & F_{m,i} & & F_{m,i} + F_{m,j} & \cdots F_{m,m}
\end{bmatrix},$$

where $\xi = F_{i,i} + F_{j,j} + F_{i,j}$. Thus, elements of the matrix are added according to the arrows in the following diagram.



In order to enumerate the number of binary quadratic forms that may be transformed into each of the elementary forms, we reduce a randomly chosen binary quadratic form.

For notational convenience, we let $a, b, c, \cdots$, denote arbitrary binary variables, and we use the symbol $\frac{1}{2}$ for entries that are independent, randomly distributed, binary variables, which may be either 0 or 1 with probability $\frac{1}{2}$.

Lemma 1

$$\begin{bmatrix}
0 & & & & & \bigcirc & \\
1 & 0 & & & & & \\
a & b & c & & & & \\
d & e & f & g & & & \\
h & i & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & & \\
j & k & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \\
\ell & m & \frac{1}{2} & & & & \\
\vdots & \vdots & \vdots & & & & \\
n & p & \frac{1}{2} & & & & \frac{1}{2}
\end{bmatrix}
\rightarrow
\begin{bmatrix}
0 & & & & & \bigcirc & \\
1 & 0 & & & & & \\
0 & 0 & x & & & & \\
0 & 0 & y & z & & & \\
0 & 0 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & & \\
0 & 0 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \\
\cdots & & & & & & \\
 & & & & & & \\
0 & 0 & \frac{1}{2} & & & & \frac{1}{2}
\end{bmatrix}$$

where $x = c + ab$, $y = f + db + ae$, $z = g + de$.

Proof: With * denoting scalar multiplication of a row column,

$$\begin{bmatrix}
0 & & & & \\
1 & 0 & & & \\
a & b & c & & \\
d & e & f & g & \\
h & i & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\
\vdots & & & &
\end{bmatrix}
\xrightarrow{\substack{\text{add } a*2 \\ \text{into } 3}}
\begin{bmatrix}
0 & & & & \\
1 & 0 & & & \\
0 & b & c + ab & & \\
d & e & f + ae & g & \\
h & i & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\
\vdots & & & &
\end{bmatrix}$$

$$\xrightarrow{\substack{\text{add } b*1 \\ \text{into } 3}}
\begin{bmatrix}
0 & & & & \\
1 & 0 & & & \\
0 & 0 & x & & \\
d & e & y & g & \\
h & i & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\
\vdots & & & &
\end{bmatrix}
\xrightarrow{\substack{\text{add } d*2 \\ \text{into } 4}}
\begin{bmatrix}
0 & & & & \\
1 & 0 & & & \\
0 & 0 & x & & \\
0 & e & y & z & \\
h & i & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\
\vdots & & & &
\end{bmatrix}$$

$$\xrightarrow{\substack{\text{add } e*1 \\ \text{into } 4}}
\begin{bmatrix}
0 & & & & \\
1 & 0 & & & \\
0 & 0 & x & & \\
0 & 0 & y & z & \\
h & i & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\
\vdots & & & &
\end{bmatrix}
\xrightarrow{\substack{\text{add } h*2 \\ \text{into } 5}} \cdots .$$

Q.E.D.

We now reexamine the reduction of an arbitrary quadratic form via linear transformations, according to Dickson's theorem ([1], theorem 16.35). A flow chart of this reduction is shown in Fig. 1. Initially, we start with a random triangular matrix of the form

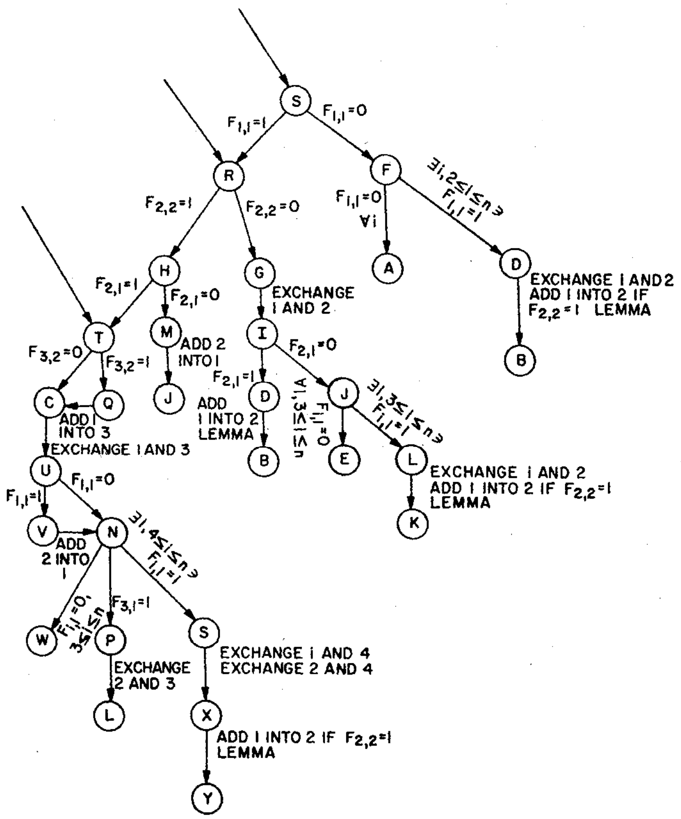


Fig. 1. Flowchart reduction of random quadratic form in n variables.

$$\mathcal{S} = \begin{bmatrix} \frac{1}{2} & 0 & 0 & & \\ \frac{1}{2} & \frac{1}{2} & 0 & & \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & & \\ \vdots & & & \ddots & \\ \frac{1}{2} & & & & \frac{1}{2} \end{bmatrix}.$$

At nonterminal states of the flow chart, we have a matrix that has one of several forms such as

$$\mathcal{J} = \begin{bmatrix} 1 & & & & & \\ 1 & 1 & & & & \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & & & \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & & \\ \vdots & & & & \ddots & \\ \frac{1}{2} & & & & & \frac{1}{2} \end{bmatrix},$$

or

$$\mathcal{R} = \begin{bmatrix} 1 & & & & \\ \frac{1}{2} & \frac{1}{2} & & & \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & & \\ \vdots & & & \ddots & \\ \frac{1}{2} & & & & \frac{1}{2} \end{bmatrix},$$

or others that can be found easily from the flow chart.

After working our way through the flow chart, we terminate with a matrix having one of the simpler forms, $\mathcal{A}$, $\mathcal{B}$, $\mathcal{E}$, $\mathcal{K}$, $\mathcal{W}$, $\mathcal{Y}$. We illustrate by giving $\mathcal{A}$ and $\mathcal{B}$, the other forms can again be found easily from the flow chart

$$\mathcal{A} = \begin{bmatrix} 0 & & & & \\ 0 & \frac{1}{2} & & & \\ 0 & \frac{1}{2} & \frac{1}{2} & & \\ \vdots & & & \ddots & \\ 0 & \frac{1}{2} & \frac{1}{2} & & \frac{1}{2} \end{bmatrix}$$

$$\mathcal{B} = \begin{bmatrix} 0 & & & & & \\ 1 & 0 & & & & \\ 0 & 0 & \frac{1}{2} & & & \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} & & \\ \vdots & & & & \ddots & \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} & & \frac{1}{2} \end{bmatrix}.$$

Each terminal matrix has one or two initial columns simplified, plus a submatrix having one of the forms $\mathcal{R}$, $\mathcal{S}$, or $\mathcal{J}$. It can be seen that $\mathcal{A}, \mathcal{B}$ contain $\mathcal{S}$ as a submatrix, $\mathcal{E}$, $\mathcal{K}$ contain $\mathcal{R}$, and $\mathcal{W}$, $\mathcal{Y}$ contain $\mathcal{J}$.

If we reenter the flow chart at the appropriate entry, we may simplify the remaining submatrix and continue to do so until we eventually terminate with a reduced $m \times m$ matrix that is a permutation of the following form.

$$\begin{array}{c} \uparrow \\ j \\ 2 \times 2 \\ \text{matrices} \\ \downarrow \end{array} \left[\begin{array}{cccccccc} \begin{bmatrix} 0 & \\ 1 & 0 \end{bmatrix} & & & & & & & \\ 0 \quad 0 & \begin{bmatrix} 0 & \\ 1 & 0 \end{bmatrix} & & & & & & \\ & & \ddots & & & & & \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & & \begin{bmatrix} 0 & \\ 1 & 0 \end{bmatrix} & & & & \\ & & & & 0_{0_0} & & & \\ & & & & & \ddots & & \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \begin{matrix} 000 \\ 000 \end{matrix} & \begin{matrix} \cdots \\ \cdots \end{matrix} & [\mathfrak{z}] & \end{array}\right]$$

where j is some integer $\le m/2$, and

$$\mathfrak{z} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \qquad [1],$$

or the empty matrix. We define the order of the reduced matrix as

$$\text{order} = \begin{cases} j & \mathfrak{Z} \text{ is empty} \\ j + \frac{1}{3} & \mathfrak{Z} = [1] \\ j + \frac{2}{3} & \mathfrak{Z} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \end{cases}$$

We now let $R_{m,i}$, $S_{m,i}$, and $T_{m,i}$ be the probability that a random $m \times m$ matrix of the form of $\mathcal{R}$, $\mathcal{S}$, or $\mathcal{T}$ is equivalent (under an invertible linear transformation of variables) to a reduced matrix of order i. From the transition probabilities shown in Fig. 2 (an abbreviation of Fig. 1) we derive the recurrences

$$S_{m,j} = \tfrac{1}{2}R_{m,j} + 2^{-m}S_{m-1,j} + (\tfrac{1}{2} - 2^{-m})S_{m-2,j-1}, \quad (2)$$

$$R_{m,j} = 2^{-(m-1)}R_{m-1,j} + (\tfrac{1}{2} - 2^{-(m-1)})R_{m-2,j-1} + \tfrac{1}{4}S_{m-2,j-1} + \tfrac{1}{4}T_{m,j}, \quad (3)$$

$$T_{m,j} = \tfrac{1}{2}R_{m-2,j-1} + (\tfrac{1}{2} - 2^{-(m-2)})T_{m-2,j-1} + 2^{-(m-2)}T_{m-1,j}, \quad (4)$$

and the initial conditions

$$S_{m,j} = R_{m,j} = T_{m,j} = 0 \qquad \text{if } m \leq 0 \qquad \text{or } j \leq 0$$
$$S_{0,0} = R_{1,1/3} = T_{2,2/3} = 1.$$

A simpler recurrence may be obtained by allowing invertible affine transformations as well as invertible linear transformations. By invoking the binary identity

$$X_1^2 + X_1X_2 + X_2^2 = X_1 + X_1X_2 + X_2 = (1 + X_1)(1 + X_2) + 1,$$

followed by the application of Lemma 1, we may transform a matrix of the form $\mathcal{T}$ to a matrix of the form $\mathcal{R}$. We may ignore the fact that this transformation changes the constant term G in (1) to $1 + G$, since for a random codeword both G and $1 + G$ are each 0 or 1 with probability $\frac{1}{2}$.

Let $R'_{m,i}$, $S'_{m,i}$, and $T'_{m,i}$ be the probability that a random $m \times m$ matrix of the form of R, S, or T is equivalent (under an invertible affine transformation of variables) to a reduced matrix of order i, where i is an integer or an integer $+ \frac{1}{3}$. Then $R'_{m,i}$, $S'_{m,i}$, and $T'_{m,i}$ satisfy (2) and (3) with everything primed, but (4) may be replaced by

$$T'_{m,j} = S'_{m-2,j-1}. \quad (4')$$

To convert probabilities to integers, we set

$$\begin{aligned} s_{m,j} &= 2^{(m+1)m/2}S_{m,j} \\ r_{m,j} &= 2^{(m+1)m/2-1}R_{m,j} \quad (5) \\ t_{m,j} &= 2^{(m+1)m/2-3}T_{m,j}. \end{aligned}$$

Inserting (5) into (2′), (3′), and (4′) and using (4′) to eliminate t gives

$$s_{m,j} = r_{m,j} + s_{m-1,j} + (2^{2m-2} - 2^{2m-1})s_{m-2,j-1}. \quad (6)$$

$$r_{m,j} = 2r_{m-1,j} + (2^{2m-2} - 2^{m})r_{m-2,j-1} + 2^{2m-3}s_{m-2,j-1}. \quad (7)$$

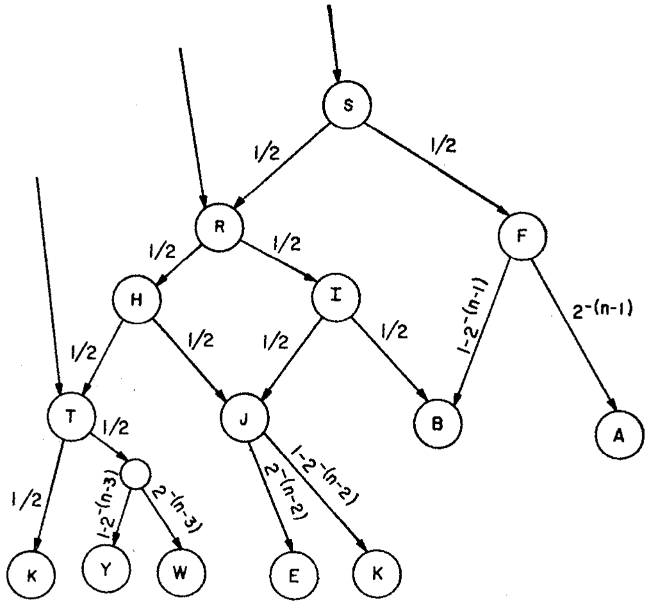


Fig. 2. Abbreviation of Fig. 1, showing probabilities.

Using (6) to eliminate r from (7) gives the basic recursion

$$s_{m,j} = 3s_{m-1,j} - 2s_{m-2,j} + (5.2^{2m-3} - 3.2^{m-1})s_{m-2,j-1} - 3(2^{2m-3} - 2^{m-1})s_{m-3,j-1} - (2^{2m-2} - 2^{m}) \cdot (2^{2m-6} - 2^{m-3})s_{m-4,j-2} \qquad m \geq 3, \quad (8)$$

with initial conditions

$$s_{0,0} = s_{1,0} = 1;\ s_{m,j} = 0 \qquad \text{if } m < 0 \qquad \text{or } j < 0$$
$$\text{or if} \quad m = 0 \text{ or } 1 \qquad \text{and } j \neq 0.$$

Since the matrices whose order is an integer $+ \frac{1}{3}$ correspond to codewords of weight 2^{m-1}, we need only consider $s_{m,j}$ for integral values of j. In view of Berlekamp's results ([1], p. 416, sec. 16.3), it is clear that $s_{m,j}$ is equal to $A_{2^{m-1}-2^{m-1-j}}$, the number of codewords of weight $2^{m-1} - 2^{m-1-j}$ (or $2^{m-1} + 2^{m-1-j}$) in the second-order RM code of length 2^m.

For fixed j, (8) is of the form

$$s_{m,j} - 3s_{m-1,j} + 2s_{m-2,j} = f_m. \quad (9)$$

If f_m is the impulse function ($f_0 = 1$, $f_m = 0$ for $m \neq 0$), then the solution of (9) is given by (still for j fixed)

$$s_{m,j} = (2^{m+1} - 1) \quad m \geq 0; \qquad s_{m,j} = 0 \quad m < 0.$$

For arbitrary f_m, the solution of (9) is given by

$$s_{m,j} = \sum_{k=0} (2^{m+1-k} - 1)f_k. \quad (10)$$

By repeatedly applying (9) and (10) to (8), we find that

$$s_{m,0} = 1$$

$$s_{m,1} = \frac{2^2(2^m - 1)(2^{m-1} - 1)}{3}$$

$$s_{m,2} = \frac{2^6(2^m - 1)(2^{m-1} - 1)(2^{m-2} - 1)(2^{m-3} - 1)}{45},$$

TABLE I

m	3	4			5				6					7						8						
factors	2	2	3	5	2	5	7	31	2	3	5	7	31	2	3	5	7	31	127	2	3	5	7	17	31	127
W																										
8	0	1	1	1	2	1	0	1	3	2	1	0	1	4	1	0	0	1	1	5	2	1	0	1	0	1
10		-			-				-					-						-						
12		-			6	0	1	1	7	2	0	2	1	8	1	0	2	1	1	9	2	1	1	1	1	1
14		-			-				14	2	1	0	1	15	2	1	0	1	1	16	2	2	0	1	1	1
16		0			1	0	0	2	2	1	3	1	2	3	1	1	0	1	1	4	1	0	0	1	1	1
18					-				14	1	0	2	1	15	1	0	2	1	1	16	1	1	1	1	1	1
20					6	0	1	1	7	4	0	1	1	8	0	1	1	1	1	9	1	2	1	1	1	1
22					-				16	2	0	1	1	17	1	0	0	1	1	18	1	1	0	1	1	1
24					2	1	0	1	3	1	0	1	1	4	1	1	1	1	1	5	1	1	0	1	1	1
26					-				16	2	0	1	1	17	1	0	1	1	1	18	3	1	2	1	1	1
28					-				8	0	1	2	1	9	0	0	0	1	1	10	0	1	0	1	1	1
30					-				15	2	0	2	1	16	1	1	2	1	1	17	2	0	0	1	1	1
32					0	0	0	0	1	4	0	1	0	2	1	0	1	0	1	3	2	2	0	1	0	1
34									15	2	0	2	1	16	2	1	1	1	1	17	1	1	1	1	1	1
36									8	0	1	2	1	9	0	0	1	1	1	10	0	0	0	2	1	1
38									16	2	0	1	1	17	0	1	1	1	1	18	1	1	0	2	0	1
40									3	1	0	1	1	4	1	1	2	1	1	5	0	0	1	1	1	1
42									16	2	0	1	1	17	1	0	1	1	1	18	1	2	0	1	1	1
44									7	4	0	1	1	8	1	1	2	1	1	9	2	1	0	1	1	1
46									14	1	0	2	1	15	0	0	1	1	1	16	4	0	1	1	1	1
48									2	1	3	1	2	3	1	1	1	1	1	4	2	1	1	1	1	1
50									14	2	1	0	1	15	1	0	0	1	1	16	2	1	0	1	1	1
52									7	2	0	2	1	8	1	0	1	1	1	9	1	1	1	0	1	1
54									-					18	1	1	1	1	1	19	2	1	1	1	1	1
56									3	2	1	0	1	4	0	0	0	1	1	5	1	0	0	1	1	1
58									-					18	2	0	0	1	1	19	0	1	0	1	1	1
60									-					10	1	0	2	1	1	11	1	0	1	1	1	1
62									-					17	1	0	1	1	1	18	3	1	1	1	1	1
64									0	0	0	0	0	1	0	1	0	0	1	2	0	1	0	1	0	1
66														17	1	0	1	1	1	18	0	0	0	1	1	1
68														10	1	0	2	1	1	11	4	1	1	0	0	1
70														18	2	0	0	1	1	19	1	0	0	1	1	1
72														4	0	0	0	1	1	5	1	1	1	1	1	1
74														18	1	1	1	1	1	19	1	1	0	1	1	1
76														8	1	0	1	1	1	9	1	0	1	1	1	1
78														15	1	0	0	1	1	16	1	3	0	1	1	2
80														3	1	1	1	1	1	4	2	0	0	1	1	1
82														15	0	0	1	1	1	16	1	1	1	1	1	1
84														8	1	1	2	1	1	9	0	1	0	1	1	1
86														17	1	0	1	1	1	18	2	0	1	0	1	1
88														4	1	1	2	1	1	5	1	1	0	1	1	1
90														17	0	1	1	1	1	18	1	0	1	1	1	1
92														9	0	0	1	1	1	10	1	1	0	1	1	1
94														16	2	1	1	1	1	17	0	1	0	1	1	1
96														2	1	0	1	0	1	3	5	0	1	1	0	1
98														16	1	1	2	1	1	17	3	2	0	1	0	1
100														9	0	0	0	1	1	10	1	0	0	2	1	1
102														17	1	0	1	1	1	18	1	1	3	0	1	1
104														4	1	1	1	1	1	5	3	1	1	1	1	1
106														17	1	0	0	1	1	18	2	0	1	1	1	1
108														8	011		1	1	1	9	0	3	0	1	1	1
110														15	1	0	2	1	1	16	2	0	1	1	1	1
112														3	1	1	0	1	1	4	0	1	0	1	1	2
114														15	2	1	0	1	1	16	2	1	0	1	1	1
116														8	1	0	2	1	1	9	2	1	0	1	1	1
118														-						20	0	1	1	1	1	1
120														4	1	0	0	1	1	5	0	0	1	0	1	1
122														-						20	3	1	1	1	1	1
124														-						12	2	2	1	1	1	1
126														-						19	2	3	0	1	1	1
128														0	0	0	0	0	0	1	2	1	0	1	0	0
130																				19	2	3	0	1	1	1

Cofactors

m	4	5	6	7	8 (In unstarred rows factors ≥ 3388817 omitted)
8	1	1	1	1	*
10	0	0	0	0	0
12	0	1	1	1	*
14	0	0	1	1	*
16	1	19	23	746129	293x169937*
18		0	23	743	60337*
20		1	23x181	379x33359	67
22		0	13x23	13^2x43x991	47
24		1	127x277x653	33989848801	
26		0	2239	499x685141	19
28		0	11x24967	25046126802457	19
30		0	1723	107x607x46643	1019
32		1	11^2x6374941	349x1478663625832409	23x71x139x229x523
34			1723	550584398867	23x107
36			11x24967	47x468154046769977	11x37
38			2239	23x47x1249x75811037	23x211
40			127x277x653	23x47x189658993969717	23x101
42			13x23	13x23x47x277125805459	89
44			23x181	23x47x203619085344607	
46			23	47x1293935656443 0083	47x53x353
48			23	571x856254555861352867	53
50			1	107770052339 38670609	53x1481
52			1	4462948050162745 78561	53x163
54			0	173602948413845831	11x53
56			1	53x988312592567871969 9901	
58			0	13x422524983444734279	733
60			0	11x1067854468450476 1019	
62			0	773846843940801 5059	13x173x307
64			1	70255883456633416018327673	53x1399
66				7738468439408015059	199

TABLE I (*cont.*)

Cofactors

m	4	5	6	7	8
w					(In starred rows, factors ≥ 3388817 omitted)
68				. . .	421
70					47×71
72					37×47
74					47×163×241
76					47
78					41×47
80					47×89
82					47×89
84					47×89×241
86					47×89×1559
88					47×89×409
90					47
92					13×47
94					73×647
96					73×607
98					53
100					13×53
102					13×53
104					53×163
106					23×563
108					23×71
110					37
112					241×1151
114					
116					47×359
118					
120					997
122					
124					109×173
126					
128					13
130					

which leads to the correct conjecture that

$$s_{m,j} = \frac{2^{j(j+1)}(2^m-1)(2^{m-1}-1)(2^{m-2}-1), \cdots, (2^{m-2j+1}-1)}{(2^2-1)(2^4-1), \cdots, (2^{2j}-1)}. \qquad (11)$$

In order to verify that (11) solves (8), let us define

$$D(n, r) \triangleq (2^n - 1)(2^{n-1} - 1) \cdots (2^{n-r} - 1) \qquad (12)$$

$$K_j \triangleq 2^{j(j+1)}\{(2^{2j} - 1)(2^{2j-2} - 1) \cdots (2^2 - 1)\}^{-1}, \qquad (13)$$

so that (11) becomes

$$s_{n,j} = K_j D(n, 2j - 1). \qquad (14)$$

Then

$$\Delta D(n, r) \triangleq D(n + 1, r) - D(n, r)$$
$$= 2^{n-r}(2^{r+1} - 1)\, D(n, r - 1) \qquad (15)$$

$$\Delta s_{n,j} \triangleq s_{n+1,j} - s_{n,j}$$
$$= K_j 2^{n-2j+1}(2^{2j} - 1)\, D(n, 2j - 2). \qquad (16)$$

and

$$D(n + 1, r + 1) = (2^{n+1} - 1)D(n, r) \qquad (17)$$

$$K_j/K_{j-1} = 2^{2j}/(2^{2j} - 1). \qquad (18)$$

Then (8) may be rewritten as

$$\Delta s_{n-1,j} - 2\, \Delta s_{n-2,j} = (4.2^{2n-3} - 3.2^{n-1}) \cdot \Delta s_{n-3,j-1}$$
$$+ 2^{2n-3}\{s_{n-2,j-1} + s_{n-3,j-1}\}$$
$$- (2^{2n-2} - 2^n)(2^{2n-6} - 2^{n-3})s_{n-4,j-2} \qquad (19)$$

and the verification is completed by using (14)–(18) to reduce both sides of (19) to

$$K_{j-1}D(n - 2, 2j - 3)2^{2n-2j}(2^{2j-1} - 1).$$

This proves the theorem stated in the abstract.

In order to obtain further data on the weight structure of Reed–Muller codes of orders > 2, Brillhart wrote a computer program to determine the weight enumerators for some of the duals of the second-order RM codes from our theorem and MacWilliams' theorem ([1], theorem 16.21). Brillhart's results, in factored form, are given in Table I. The reader will notice many patterns in these data, which he is invited to try to prove in general.

References

[1] E. R. Berlekamp, *Algebraic Coding Theory.* New York: McGraw-Hill, 1968.

[2] E. R. Berlekamp and N. J. A. Sloane, "Restrictions on weight distribution of Reed–Muller codes," *Inform. and Control,* vol. 14, pp. 442–456, May 1969.

[3] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory.* New York: Dover, 1958.

[4] T. Kasami, "Weight distribution of BCH codes," in *Proc. Conf. on Combinatorial Mathematics and Its Applications,* R. C. Bose and T. A. Dowling, Eds. Chapel Hill, N. C.: University of North Carolina Press, 1969, ch. 20.

[5] R. J. McEliece, "Linear recurring sequences over finite fields," Ph.D. dissertation, Dept. of Math., California Institute of Technology, Pasadena, 1967.

[6] R. J. McEliece, "Quadratic forms over finite fields and second-order Reed-Muller codes," Jet Propulsion Lab., California Institute of Technology, Pasadena, *Space Program Summary,* vol. 3, 37–58, pp. 28–33, 1969.