ON THE ENUMERATION OF COSETS OF FIRST ORDER REED MULLER CODES

N. J. A. Sloane
Bell Telephone Laboratories, Incorporated
Murray Hill, New Jersey

and

R. J. Dick
School of Electrical Engineering
Cornell University, Ithaca, New York

(from Proceedings IEEE International Conference on Communication, Montreal June 1971, Vol 7.)

ABSTRACT

The aim of this paper is (i) to give a systematic method for enumerating the cosets of the shortened first order Reed Muller (RM) code and of the first order RM code, and (ii) to derive an approximation to the weight distribution of the coset leaders of the first order RM code which is simpler than Hobbs' approximation.

1. INTRODUCTION

As pointed out by Berlekamp[1] in a survey of unsolved problems in coding theory, little is known about the enumeration of the cosets of even the simplest families of error correcting codes. Slepian[2] and Fontaine and Peterson[3] obtained the weight distribution of the coset leaders of some optimum codes of length ≤ 29. Wolf[17] has considered cosets of BCH codes. An approximation to the coset distribution of a code was given by Hobbs[4]. For the first order Reed Muller (RM) code a simpler approximation which is asymptotically equivalent to Hobbs' is given in Section 3 below. This approximation is unimodal, rising to a maximum of

$\alpha_{h_1} = N^{-3/2} 2^N \sqrt{2 \log N}\ (1+\varepsilon)$ coset leaders of weight

$$h_1 = \tfrac{1}{2}[N - (1+\varepsilon)\sqrt{2N \log N}],$$

where ε denotes a number which approaches zero as the block length N approaches infinity.

Recently Berlekamp and Welch[5] have shown that the enumeration of cosets of the first order RM code is equivalent to the enumeration of Boolean functions under a certain group of transformations, and have thus obtained the cosets of the length 32 first order RM code.

In Section 2 we give a method (different from that of [5]) for the enumeration of cosets of the shortened first order RM (or binary simplex) code, the expurgated first order RM (or orthogonal) code and the first order RM (or biorthogonal) code. A basic idea is to associate with any binary n-tuple Y a single-error-correcting code called the structure code SC(Y). Cosets of the simplex code are then classified by the structure code of their coset leaders. Theorems 1 to 4 give the weight distribution of a coset and the number of cosets with this weight distribution, in terms of the weight distribution of the structure code of a coset leader. Theorem 5 contains a similar result for the weight distribution of a coset of the first order RM code. As an example these theorems are used to enumerate the cosets of the (15,4) simplex code and the (16,5) first order RM code (Tables 3, 4).

The enumeration of coset leaders permits calculation of the exact probability of error when maximum likelihood decoding is used[2]. Finally it should be mentioned that Hadamard matrices have recently been suggested for the coding of TV pictures[6,7,8] and optical spectra[9,10]. The detailed analysis of at least one of these schemes[8] requires knowledge of the weight distribution of the cosets of first order Reed Muller codes.

2. CLASSIFICATION OF COSETS IN TERMS OF SINGLE ERROR CORRECTING CODES

Definition of Codes[11]

$\mathcal{C}_s$, the shortened first order RM code (or binary simplex code) of length $n = 2^m - 1$ and dimension m, is generated by the rows of the $m \times (2^m-1)$ matrix whose columns are the binary representations of the numbers from 1 to $2^m - 1$. These columns will also be thought of as coordinate vectors for the corresponding positions of the codeword, and thus set up a one-one correspondence between these positions and the non-zero points of U, an m-dimensional vector space over GF(2). For example when $m = 3$, $n = 7$, the codewords of $\mathcal{C}_s$ can be taken as the rows of Table I. Rows 2-4 give the coordinate vectors of the positions of the codewords.

Table I. Codewords of Simplex Code of Length 7

0	0	0	0	0	0	0
0	0	0	1	1	1	1
0	1	1	0	0	1	1
1	0	1	0	1	0	1
0	1	1	1	1	0	0
1	0	1	1	0	1	0
1	1	0	0	1	1	0
1	1	0	1	0	0	1

$\mathcal{C}_o$, the expurgated first order RM code (or orthogonal code) is obtained by annexing an overall parity check to $\mathcal{C}_s$. $\mathcal{C}_b$, the first order RM code (or biorthogonal code) has as codewords those of $\mathcal{C}_o$ together with their complements.

The Structure Code of a Vector

Let Y be any binary n-typle, with 1's in positions $S_1, \ldots, S_e$ (say), where e = weight (Y). The set $S = \{S_1, \ldots, S_e\}$ is a subset of U, and the points in S will in general satisfy certain linear equations with binary coefficients, of the form $S_i + S_j + S_k + \ldots = 0$. These equations may be added to one another and themselves form a binary vector space. If these equations are represented by binary vectors of length e, the equations form a binary group code of length e, which will be called the structure code SC(Y). Since the points S_i are non-zero and distinct, equations of the form $S_i = 0$ or $S_i + S_j = 0$ cannot occur. Therefore SC(Y) is (at least) single-error-correcting.

An equivalent definition of SC(Y) is to puncture the simplex code $\mathcal{C}_s$ by deleting all positions of the codewords except those in S, i.e., where Y has 1's. Then SC(Y) is the dual code of this puncture code.

Define the rank (Y) to be the maximum number of linearly independent points in S. Every linearly independent constraint on S reduces its rank by 1, so

$$\text{rank } (Y) + \text{dimension of } SC(Y) = e \qquad (1)$$

Example. Let Y = 0111010, of weight $e = 4$. From Table I, Y has 1's in positions $S_1 = \begin{pmatrix}0\\1\\0\end{pmatrix}$, $S_2 = \begin{pmatrix}0\\1\\1\end{pmatrix}$,

$S_3 = \begin{pmatrix}1\\0\\0\end{pmatrix}$, $S_4 = \begin{pmatrix}1\\1\\0\end{pmatrix}$, satisfying the equations $0 = 0$, $S_1 + S_3 + S_4 = 0$; and so the structure code of Y is $SC(Y) = \{0000, 1011\}$. Y has rank 3 and the dimension of SC(Y) is 1, satisfying equation (1).

Classification of Cosets of the Simplex Code

Let us consider a fixed coset of $\mathfrak{C}_s$, and let Y be any vector in the coset, with 1's in positions $S_1, \ldots, S_e$, (say), where e = weight (Y). The vectors of the coset are obtained by complementing positions $S_1, \ldots, S_e$ in $\mathfrak{C}_s$. Thus each of the 2^m codewords in $\mathfrak{C}_s$ is changed in e places. Let us call this set of 2^m (not necessarily distinct) e-tuples before they are changed the cross-section of Y, or of $S_1, \ldots, S_e$. In other words, the vectors of the coset containing Y are obtained by complementing the cross-section of Y. By definition, the dot product of any vector in SC(Y) with any vector in the cross-section of Y is 0.

Lemma. The cross-section of Y consist of 2^{m-r} repetitions of the codewords of the dual code of the structure code SC(Y), where r = rank (Y). (Proof omitted.)

Weight Distribution of a Coset of the Simplex Code

Theorem 1. Let Y be any binary vector of length $n = 2^m - 1$, and weight e. Then that coset of the simplex code which contains Y has $1 + 2^{m-r}B_{N/4}$ vectors of weight e; $2^{m-r}B_i$ of weight $\frac{1}{2}N + e - 2i$ for $i \neq 0, N/4$; and $2^{m-r} - 1$ of weight $\frac{1}{2}N + e$; where r = rank (Y), $N = 2^m$, and $\{B_i\}$ is the weight distribution of the dual code of SC(Y).

Proof. By the lemma the weight distribution of the cross-section of Y is $\{B_i'\}$, where $B_i' = 2^{m-r}B_i$. If a vector in the cross-section has weight i, after complementing it has weight $e - i$, a gain of $e - 2i$. The theorem then follows using the fact that the simplex code has one codeword of weight 0 and $2^m - 1$ of weight 2^{m-1}.

Theorem 2. If Y and Y' are two vectors of equal weight in the same coset, then SC(Y) and SC(Y') have the same weight distribution.

Proof. From the MacWilliams identities[12] the weight distribution of SC(Y) is uniquely determined by that of its dual code. The theorem then follows from Theorem 1.

Taking Y to be a coset leader, we obtain

Theorem 3. The structure code SC(Y) of any coset leader Y of weight e is a single-error-correcting code of length e whose weight distribution uniquely determines the weight distribution of the coset containing Y, and conversely.

Enumeration of Cosets of the Simplex Code

By Theorem 3 we may define $\mathfrak{F}\{A_i\}$ to be the family of all cosets of the simplex code such that the weight distribution of SC(Y), Y any coset leader in the family, is a fixed weight distribution $\{A_i\}$. The weight distribution of any of these cosets is given in Theorem 1, where $\{B_i\}$ are the dual weights to $\{A_i\}$; and $\mathfrak{F}\{A_i\}$ includes all cosets with this weight distribution. The rank r of any coset leader of a coset in $\mathfrak{F}\{A_i\}$ is also constant.

The aim of this section is to calculate the number of cosets in $\mathfrak{F}\{A_i\}$, i.e., having this weight distribution.

Let $\mathfrak{C}_1, \ldots, \mathfrak{C}_v$ be all the non-equivalent codes with weight distribution $\{A_i\}$ (using equivalence in the usual sense of Peterson[13] p. 44). Let $\mathfrak{G}_i$ be the permutation group of $\mathfrak{C}_i$, i.e., the group of all permutations of the codeword positions that preserve the set of codewords, and let $G_i = |\mathfrak{G}_i|$.*

Theorem 4. The number of cosets in $\mathfrak{F}\{A_i\}$ is

$$\frac{(2^m-2^0)(2^m-2^1)\ldots(2^m-2^{r-1})}{1 + 2^{m-r}B_{2^{m-2}}} \sum_{i=1}^{v} \frac{1}{G_i} .$$

Proof. Let $\mathfrak{Y}_i = \{Y | SC(Y) = \mathfrak{C}_i\}$, $i = 1, \ldots, v$. Then the number of vectors in $\mathfrak{Y}_i$ is

$$|\mathfrak{Y}_i| = \frac{(2^m-2^0)(2^m-2^1)\ldots(2^m-2^{r-1})}{G_i} , \qquad (2)$$

from Burnside's theorem ([14] p. 150) and the fact that r non-zero independent points can be chosen from an m-dimensional binary vector space in $(2^m-2^0)(2^m-2^1)\ldots(2^m-2^{r-1})$ ways.

Then $\mathfrak{Y} = \mathfrak{Y}_1 \cup \ldots \cup \mathfrak{Y}_v$ contains all vectors Y such that the weight distribution of SC(Y) is $\{A_i\}$; these are exactly all the coset leaders of cosets in $\mathfrak{F}\{A_i\}$. Also

$$|\mathfrak{Y}| = \sum_{i=1}^{v} |\mathfrak{Y}_i| \qquad (3)$$

By Theorem 1 there are $1 + 2^{m-r}B_{2^{m-2}}$ leaders in each coset. Therefore the number of cosets is

$$\frac{|\mathfrak{Y}|}{1 + 2^{m-r}B_{2^{m-2}}} \qquad (4)$$

Equations (2-4) together prove the theorem.

Relation Between Cosets of $\mathfrak{C}_s$, $\mathfrak{C}_o$ and $\mathfrak{C}_b$

Since the all-1's vector is not in $\mathfrak{C}_s$ or $\mathfrak{C}_o$, it can be added to any coset with weights $w_1, w_2, \ldots$ to give a coset with the complementary weights $n - w_1$, $n - w_2$, ... Thus the cosets of $\mathfrak{C}_s$ and $\mathfrak{C}_o$ occur in complementary pairs (see for example Table III). The cosets of $\mathfrak{C}_o$ consist of those of $\mathfrak{C}_s$ (if the overall parity check is 0) together with the same weights shifted right by one (if the overall parity check is 1). Finally the cosets of $\mathfrak{C}_b$ are obtained from those of $\mathfrak{C}_o$ by adding together the weights of the complementary cosets (since the codewords of $\mathfrak{C}_b$ are obtained in that way). Using Theorem 1 we obtain the following result for the weight distribution of a coset of $\mathfrak{C}_b$.

Theorem 5. Let Y be a coset leader of weight e of the first order RM code of length $N = 2^m$. If Y has a 1 in its overall parity check position, let Y' be Y with this 1 changed to 0; otherwise let Y' = Y. Let r = rank (Y') and let $\{B_i\}$ be the weight distribution of the dual code to SC(Y'). Then the weight distribution of the coset containing Y is given by Table II.

Example. Cosets of $\mathfrak{C}_s$ and $\mathfrak{C}_b$ when m = 4.

We begin by finding the cosets of the simplex code of length 15 (see Table III). Using Theorems 1, 3 and

*If S is any set, |S| will denote the cardinality of S.

Table II. Weight Distribution of the Cosets of the First Order RM Code
(e is the weight of the coset leader.)

$0 < e < N/4$

Weight	e and N−e	$\frac{1}{2}N \pm e$	$\frac{1}{2}N - e + 2i,\ 0 < i < e$
Number	1	$2^{m-r}(1+B_e)-1$	$2^{m-r}(B_i+B_{e-i})$

$e = N/4$

Weight	N/4 and 3N/4	$2i + N/4,\ 0 < i < N/4$
Number	$2^{m-r}(1+B_{N/4})$	$2^{m-r}(B_i+B_{N/4 - i})$

$e > N/4$ (In this case $r = m$.)

Weight	e and N − e	$\frac{1}{2}N - e + 2i,\ e - N/4 < i < N/4$
Number	$1 + B_{N/4} + B_{e-N/4}$	$B_i + B_{e-i}$

Table III. Cosets of the Length 15 Simplex Code

The rows of the table give the weight distribution of the cosets.

	Weights																
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	SC(Y)
1	1								15								-
15		1						8		7							(0)
105			1				4		8		3						(00)
420				1		2		6		6		1					(000)
35				1				12				3					(000,111)
420					2		4		6		4						(0000)
28						6				10							(00000,11111)
28							10				6						
420						4		6		4		2					
35					3				12				1				
420					1		6		6		2		1				
105						3		8		4				1			
15							7		8						1		
1								15								1	

Table IV. Cosets of the Length 16 First Order Reed Muller Code

The rows of the table give the weight distribution of the cosets.

	Weights																
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1
1	1								30								1
16		1						15		15						1	
120			1				7		16		7				1		
560				1		3		12		12		3		1			
840					2		8		12		8		2				
35					4				24				4				
448						6		10		10		6					
28							16				16						

4 we list single-error-correcting codes of lengths 1, 2, 3, ... and obtain the weight distribution and multiplicity of the corresponding cosets. In this way the top half of Table III is rapidly obtained, containing 1024 cosets, half of the total number. The others are then obtained by complementing.

The cosets of the first order RM code of length 16 are then enumerated by the method of the previous section, and appear in Table IV.

3. NORMAL APPROXIMATION TO NUMBER OF COSET LEADERS

In this section a normal approximation, Equation (5) is obtained to α_h, the number of coset leaders of weight h in the biorthogonal code of length $N = 2^m$.

The weights $\{\alpha_h\}$ are the weights of the correctable errors when optimum decoding is used. If the codewords are represented by ±1's, that is, if 0's are changed to +1's and 1's to -1's, an optimum decoding of a received sequence of +1's is to take the dot product of the received sequence with each codeword of the orthogonal code and then to choose the codeword giving the largest magnitude of dot product. If that dot product is negative, complement the codeword chosen. (Decide ties in any way.)

The decoder decides that an error of weight h occurs, where $h = \frac{1}{2}(N - |\text{dot product chosen}|)$, because this is the number of places in which the received sequence and the decoded sequence differ.

If we now imagine that the code were used for transmission through a binary symmetric channel (sending ±1's) with crossover probability $\frac{1}{2}$, then the probability that the optimum decoder described above decides that an error of weight h has occurred is proportional to α_h, the number of cosets having minimum weight h.

The dot products which this decoder examines are orthogonal identically distributed Bernoulli random variables. They are not independent.

However, the normal distribution is an approximation of the Bernoulli distribution, and orthogonal normal random variables are independent. This suggests the following hypothetical experiment.

Suppose the optimum decoder were applied to N independent identically distributed normal random variables of mean 0 and variance 1. Then the probability density of $H = \frac{1}{2}(N - |\text{dot product chosen}|)$ in this experiment is an approximation to the weight distribution of the coset leaders.

Therefore let $X_1, \ldots, X_N$ be independent identically distributed normal variables with mean 0 and variance N, representing the dot product of the received vector with the codewords of the orthogonal code, and let $Z = \max_i |X_i|$. The density of Z is

$$f_Z(x) = 2\sqrt{N}\,\varphi\left(\frac{x}{\sqrt{N}}\right)\left[2\Phi\left(\frac{x}{\sqrt{N}}\right) - 1\right]^{N-1}$$

where φ and Φ are the normal density and distribution functions. Then the number of cosets of weight h ≈ (total number of cosets) $\text{PR}(|H-h| < \frac{1}{2})$

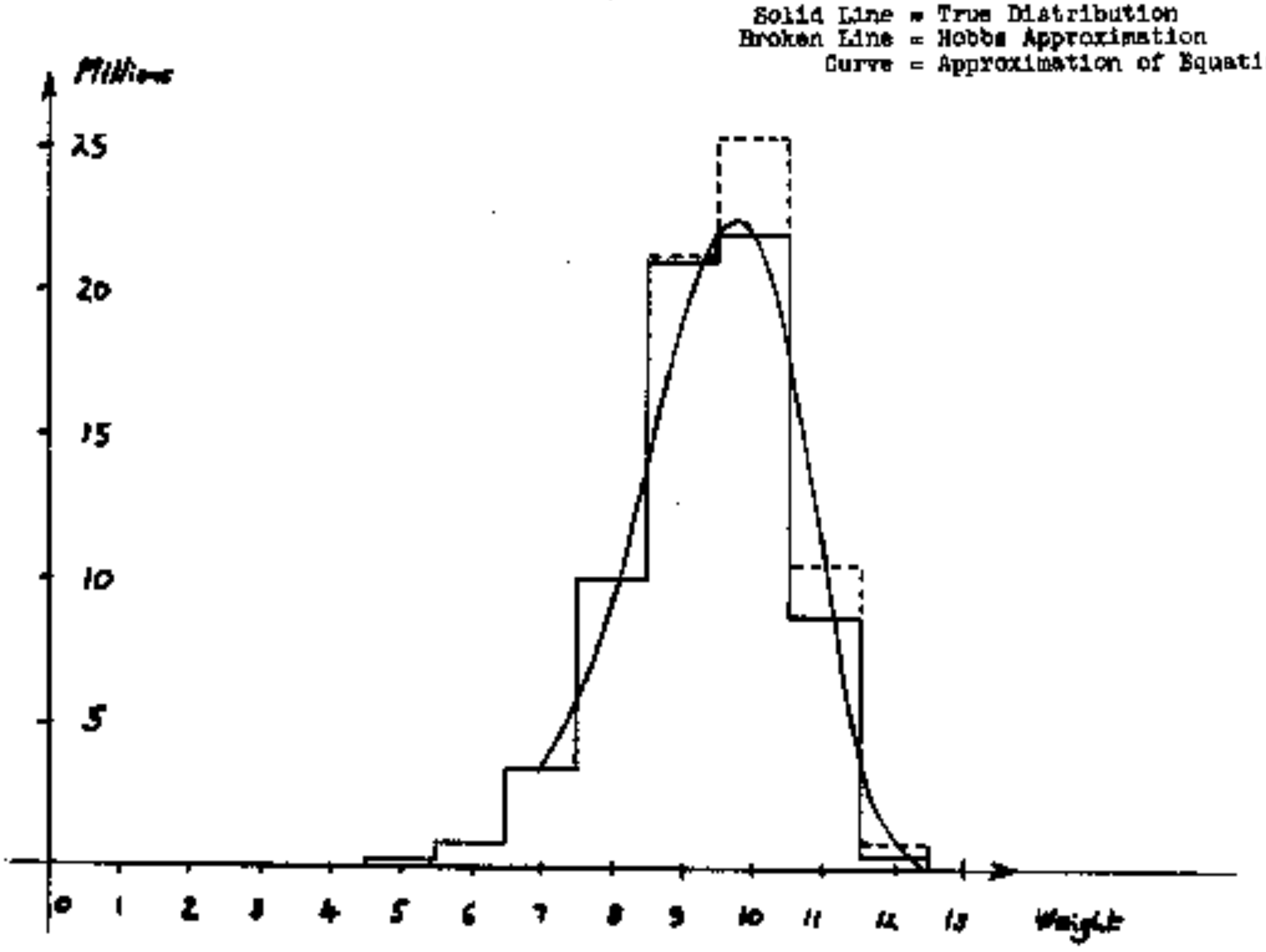
$$= \frac{2^N}{2N}\,\text{PR}[N-2h-1 < Z < N-2h+1] \approx \frac{2^N}{2N}\,2f_Z(N-2h).$$

We conclude that in the first order Reed Muller or biorthogonal code of length N, the number of coset leaders of weight h is approximately given by

$$\alpha_h \approx \frac{2^{N+1}}{\sqrt{N}}\,\varphi\left(\frac{N-2h}{\sqrt{N}}\right)\left[2\Phi\left(\frac{N-2h}{\sqrt{N}}\right) - 1\right]^{N-1} \qquad (5)$$

Figure 1

Weight Distribution of Coset Leaders of First Order RM Code of Length 32



A similar approximation can be written down for the orthogonal code.

Hobbs' approximation[4] for this code is

$$\alpha_h \approx \binom{N}{h}\left[1 - \binom{N}{h}^{-1} \sum_{r=\frac{N}{4}}^{h} \epsilon_r \binom{\frac{N}{2}}{r} \binom{\frac{N}{2}}{h-r}\right]^{2N-2}$$

where $\epsilon_r = \frac{1}{2}$ if $r = \frac{N}{4}$, $\epsilon_r = 1$ if $r > \frac{N}{4}$.

Asymptotically the two approximations can be shown to be the same. The estimation of the error is an open problem. A comparison of the approximations with the true values in the case $N = 32$ (using the results of Berlekamp and Welch[5]) is given in Figure 1.

Using known bounds on $\Phi(x)$ it can be shown that, from (5), α_h is a unimodal function of h, rising to a maximum of

$$\alpha_{h_1} = N^{-\frac{3}{2}} 2^N \sqrt{2 \log N}\,(1+\varepsilon)$$

at

$$h_1 = \tfrac{1}{2}\{N - (1+\varepsilon)\sqrt{2N \log N}\},$$

and falling to zero at

$$h_2 = \tfrac{1}{2}(N - a\sqrt{N})$$

where $a = \Phi^{-1}\left(\frac{3}{4}\right) + \varepsilon \approx 0.665 + \epsilon$, and where ε denotes a quantity which approaches zero as N approaches infinity. However, the true value of h_2 is known to be ([15]) $\frac{1}{2}(N - \sqrt{N})$.

4. DISCUSSION

Part 2 of this paper has demonstrated a method for enumerating cosets of the shortened first order RM code in terms of the weight distributions of (at least) single error correcting codes associated with the coset leaders. Some questions that remain unanswered are:

(1) Is the structure code of a coset leader Y independent of the choice of Y within a coset? (R. P. Kurshan[16] has recently given a negative answer to this question.)

(2) Characterize the codes that appear as structure codes of coset leaders.

(3) How many non-equivalent codes have a given weight distribution?

ACKNOWLEDGMENT

The authors wish to thank Professor Terrence Fine for his assistance with Section 3.

REFERENCES

1. E. R. Berlekamp, Weight Enumeration Theorems, Proceedings of the Sixth Allerton Conference on Circuits and Systems, University of Illinois, October 2, 1968.

2. D. Slepian, A Class of Binary Signalling Alphabets, Bell System Tech. J., Vol. 35, pp. 203-234, 1956.

3. A. B. Fontaine and W. W. Peterson, Group Code Equivalence and Optimum Codes, IRE Trans. Info. Theory, Vol. IT-5, Special Supplement, pp. 60-70, 1959.

4. C. F. Hobbs, Approximating the Performance of a Binary Group Code, IEEE Trans. Info. Theory, Vol. IT-11, pp. 142-144, 1965.

5. E. R. Berlekamp and L. R. Welch, Weight Distributions of the Cosets of the (32,6) Reed Muller Codes, (to appear).

6. Peter Gottlieb, A Television Scanning Scheme for a Detector-Noise-Limited System, IEEE Trans. Info. Theory, Vol. IT-14, pp. 428-433, 1968.

7. W. K. Pratt, J. Kane, and H. C. Andrews, Hadamard Transform Image Coding, Proc. IEEE, Vol. 57, pp. 58-68, 1969.

8. E. R. Berlekamp, Some Mathematical Properties of a Scheme for Reducing the Bandwidth of Motion Pictures by Hadamard Smearing, Bell Syst. Tech. J., Vol. 49, pp. 696-986, 1970.

9. Neil J. A. Sloane, Terrence Fine, Perry G. Phillips, and Martin Harwit, Codes for Multislit Spectrometry, Applied Optics, Vol. 8, pp. 2103-2106, 1969.

10. Martin Harwit, P. G. Phillips, T. Fine, and N. J. A. Sloane, Doubly Multiplexed Spectrometry, Applied Optics, Vol. 9, pp. 1149-1154, 1970.

11. E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, 1968.

12. Jessie MacWilliams, The Structure and Properties of Binary Cyclic Alphabets, Bell Syst. Tech. J., Vol. 44, pp. 303-332, 1965.

13. W. W. Peterson, Error-Correcting Codes, MIT Press, 1961.

14. N. G. de Bruijn, Pólya's Theory of Counting, in Applied Combinational Mathematics, ed. E. F. Beckenbach, John Wiley, 1964.

15. O. S. Rothaus, private communication, 1966.

16. R. P. Kurshan and N. J. A. Sloane, Coset Analysis of Reed Muller Codes via Translates of Finite Vector Spaces, to appear.

17. J. K. Wolf, Adding Two Information Symbols for Certain Nonbinary BCH Codes and Some Applications, Bell Syst. Tech. J., 48, pp. 2405-2424, 1969.