ON THE ENUMERATION OF COSTS OF FIRST ORDER REED MILLER 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

ABSTRACT

The aim of this paper is (i) to give a systematic method for enumerating the costs 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 cost leaders of the first order RM code which is simpler than Hobbs' approximation.

1. INTRODUCTION

As pointed out by Berlekamp in a survey of unsolved problems in coding theory, little is known about the enumeration of the costs of even the simplest families of error correcting codes. Sloane2 and Fontaine and Petersen obtained the objective of the cost leaders of some optimal codes of length $2^9$. Wallis7 has considered costs of BCH codes. An approximation to the cost distribution of a code given by Hobbs8, 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

$$q_1 = \frac{1}{2} \sqrt{2N} \log N$$

$$q_2 = \frac{1}{2} (N - \frac{1}{2} \log N),$$

where $\varepsilon$ denotes a number which approaches zero as the block length $N$ approaches infinity.

Recently Berlekamp and Welch5 have shown that the enumeration of costs 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 costs of the length 32 first order RM code.

In Section 2 we give a method (different from that of [5]) for the enumeration of the costs of the shortened first order RM (or binary simplex) code, the expurgated first order RM (or ortho normalal) 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 $SC(Y)$. Costs of the simplex code are then classified by the structure code of their cost leaders. Theorems 1 to 4 give the weight distribution of a code and the number of costs with this weight distribution, in terms of the weight distribution of the structure code of a cost leader. Theorem 5 contains a similar result for the weight distribution of a code of the first order RM code. As an example these theorems are used to enumerate the costs of the (15, 5) simplex code and the (16, 5) first order RM code (Tables 3, 4).

The enumeration of cost leaders permits calculation of the exact probability of error when maximum likelihood decoding is used. Finally, it should be mentioned that Hadamard matrices have recently been suggested for the coding of TV pictures by7,8 and optical spectras9,10. The detailed analysis of at least one of these schemes10 requires knowledge of the weight distribution of the costs of first order Reed Muller codes.

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

Definition of Codes

$C_9$, the shortened first order RM code (or binary simplex code) of length $n = 2^9 - 1$ and dimension $m$, is generated by the rows of the $m \times (2^9 - 1)$ matrix whose columns are the binary representations of the numbers from 1 to $2^9 - 1$. 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 $C_9$ can be taken as the rows of Table 1. Rows 2-4 give the coordinate vectors of the positions of the codewords.

Table 1. Codewords of Simplex Code of Length $7$

| 0 0 0 0 0 0 0 |
| 0 0 0 1 1 1 1 |
| 0 1 0 0 1 1 1 |
| 1 0 1 0 1 0 0 |
| 0 1 1 1 1 0 0 |
| 1 0 0 1 1 0 0 |
| 1 1 0 0 0 0 1 |

$C_9$, the expurgated first order RM code (or orthogonal code) is obtained by augmenting an overall parity check to $C_9$. $C_9$, the first order RM code (or biorthogonal code) has as codewords those of $C_9$, together with their complements.

The Structure Code of a Vector

Let $Y$ be any binary $n$-tuple, with 1's in positions $S_1$, ... , $S_e$ (say), where $e = \text{weight}(Y)$. The set $S = \{S_1, ... , S_e\}$ is a subset of $S$, and the points in $S$ will in general satisfy certain linear equations with binary coefficients, of the form $S_1 + S_2 + S_3 + ... = \alpha$. These equations may be added to one another and themselves form a binary vector, 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, the equations form a linear group code of length $e$, which cannot occur. Therefore $SC(Y)$ is (at least) single-error-correcting.

An equivalent definition of $SC(Y)$ is to puncture the simplex code $C_9$ by deleting all positions of the codes 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 indices in $S$. Every linearly independent constraint on $S$ reduces its rank by 1, so

$$\text{rank}(Y) = \text{dimension of } SC(Y) - e$$

Example. Let $Y = 0110101$, of weight $e = 4$. From Table 1, $Y$ has 1's in positions $S_1 = \{1\}$, $S_2 = \{2\}$, $S_3 = \{3\}$, $S_4 = \{4\}$.
Let $C_1, \ldots, C_n$ be all the non-equivalent codes with weight distribution $[A_i]$ (using equivalence in the usual sense of Peterson p. 42). Let $G$ be the permutation group of $C_i$, i.e., the group of all permutations of the codeword positions that preserve the set of codewords, and let $G_i = [G_i \cdot]$.

**Theorem 1.** The number of cosets in $\mathcal{F}(A_i)$ is
\[
\left\lfloor \frac{2^n - 2}{2^{n-2}} \right\rfloor \sum_{i=1}^{n-1} \frac{1}{d_i}.
\]

**Proof.** Let $\Psi_i = \{Y : SC(Y) = C_i\}$, $i = 1, \ldots, v$. Then the number of vectors in $\Psi_i$ is
\[
N_i = \left\lfloor \frac{2^n - 2}{2^{n-2}} \right\rfloor \sum_{i=1}^{n-1} \frac{1}{d_i}.
\]

From Burnside's theorem (114) p. 150 and the fact that $r$ non-zero independent points can be chosen from an $n$-dimensional binary vector space in $(2^m - 2)(2^m - 2^1) \ldots (2^m - 2^{r-1})$ ways.

Then $\Psi = \Psi_1 \cup \ldots \cup \Psi_v$ contains all vectors $Y$ such that the weight distribution of $SC(Y) = [A_i]$; these are exactly all the coset leaders of codes in $\mathcal{F}(A_i)$. Also
\[
N = \sum_{i=1}^{v} N_i.
\]

By Theorem 1 there are $1 + 2^{n-2} d_{m-2}$ leaders in each coset. Therefore the number of cosets is
\[
\frac{N}{1 + 2^{n-2} d_{m-2}}.
\]

Equations (2-4) together prove the theorem.

**Relation Between Cosets of** $C_a, C_b$ **and** $C_c$ **codes.**

Since the all-1's vector is not in $C_a$ or $C_b$, it can be added to any code with weights $a_1, a_2, \ldots$ to give a code with the complementary weights $n - a_1, n - a_2, \ldots$. Thus the cosets of $C_0$ and $C_0$ occur in complementary pairs (see for example Table III). The cosets of $C_0$ consist of those of $C_0$ (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 $C_0$ are obtained from those of $C_0$ by adding together the weights of the complementary codes (since the codewords of $C_0$ are obtained in that way). Using Theorem 1, we obtain the following result for the weight distribution of a code of $C_0$.

**Theorem 2.** Let $Y$ be a vector of weight $e$ of the first order RM code of length $n = 2^m$. If $Y$ has $1$ in its overall parity check position, let $Y'$ be $Y$ with this $1$ changed to $0$. Under this change $Y'$ contains a codeword $Y$ of weight $e$. Let $r = Y$ and let $[S_i]$ be the weight distribution of the dual code of $[S_i]$. Then the weight distribution of the code containing $Y$ is given by Table II.

**Example.** Cosets of $C_0$ and $C_0$ when $m = 4$.

We begin by finding the cosets of the simplex code of length 15 (see Table III). Using Theorems 1, 3 and 4, the number of cosets in a code of $C_0$ is

\[
\frac{N}{1 + 2^{n-2} d_{m-2}}.
\]
Table II. Weight Distribution of the Cosets of the First Order RM Code
(e is the weight of the coset leader.)

<table>
<thead>
<tr>
<th>Weight</th>
<th>e and N - e</th>
<th>( \frac{1}{2}N - e )</th>
<th>( \frac{1}{2}N + 21, 0 &lt; e &lt; e )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>1</td>
<td>( 2^{N-e} )</td>
<td>( 2^{N-e} )</td>
</tr>
</tbody>
</table>

\( e = N/4 \)  
\( e > N/4 \)  
(\( e = r \cdot N \) in this case)

<table>
<thead>
<tr>
<th>Weight</th>
<th>e and N - e</th>
<th>( \frac{1}{2}N - e + 21, e - N/4 &lt; i &lt; N/4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>1 + ( B_{N/4} + B_{N/4} )</td>
<td>( B_{1} + B_{e=1} )</td>
</tr>
</tbody>
</table>

Table III. Cosets of the Length 15 Simplex Code
The rows of the table give the weight distribution of the cosets.

<table>
<thead>
<tr>
<th>Weights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>105</td>
</tr>
<tr>
<td>420</td>
</tr>
<tr>
<td>35</td>
</tr>
<tr>
<td>420</td>
</tr>
<tr>
<td>28</td>
</tr>
<tr>
<td>28</td>
</tr>
<tr>
<td>420</td>
</tr>
<tr>
<td>35</td>
</tr>
<tr>
<td>560</td>
</tr>
<tr>
<td>840</td>
</tr>
<tr>
<td>448</td>
</tr>
<tr>
<td>28</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

Table IV. Cosets of the Length 16 First Order Reed Muller Code
The rows of the table give the weight distribution of the cosets.

<table>
<thead>
<tr>
<th>Weights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>16</td>
</tr>
<tr>
<td>120</td>
</tr>
<tr>
<td>560</td>
</tr>
<tr>
<td>840</td>
</tr>
<tr>
<td>35</td>
</tr>
<tr>
<td>448</td>
</tr>
<tr>
<td>28</td>
</tr>
<tr>
<td>15</td>
</tr>
</tbody>
</table>

36-4
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 \( q^N \), the number of coset leaders of weight \( h \) in the biorthogonal code of length \( N = 2^n \).

The weights \( \{q^N\} \) are the weights of the correctable errors when optimum decoding is used. If the codewords are represented by \( \pm 1 \)'s, that is, if 0's are changed to +1's and -1's to \( \pm 1 \)'s, an optimum decoding of a received sequence of \( \pm 1 \)'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 \( \pm 1 \)'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 \( q^N \), 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 \( I \) independent identically distributed normal random variables with mean 0 and variance 1. Then the probability density of \( H = \sqrt{N - \text{dot product chosen}} \) 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

\[
Z = \max_{1}^{I} \{X_i\}.
\]

The density of \( Z \) is

\[
\phi_2(x) = 2\sqrt{N} \phi \left( \frac{x}{\sqrt{N}} \right) \left[ \Phi \left( \frac{x}{\sqrt{N}} \right) - 1 \right]^{N-1}
\]

where \( \phi \) and \( \Phi \) are the normal density and distribution functions. Then the number of cosets of weight \( h \) (total number of cosets) \( \beta \left| \{N-h\} \right| < \frac{1}{2} \)

\[
= \frac{2^N}{2^N} \beta \left| \{N-2h-1 \} \right| < Z < N-2h \right| \right) = \frac{2^N}{2^N} \beta \left| \{N-2h \} \right|.
\]

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

\[
q^N = \frac{2^{N-h}}{\sqrt{\pi}} \phi \left( \frac{N-2h}{\sqrt{\pi}} \right) \left[ \Phi \left( \frac{N-2h}{\sqrt{\pi}} \right) - 1 \right]^{N-1}
\]

\[\text{Equation 5}\]

\[\text{Figure 1}\]

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

Solid Line = True Distribution
Broken Line = Hobbs Approximation
Curve = Approximation of Equations 5.

36-5
A similar approximation can be written down for the orthogonal code.

Hobbs’ approximation \( \alpha_n \) for this code is

\[
\alpha_n = \left( \frac{n}{h} \right) \left[ 1 - \left( \frac{n}{h} \right)^{-1} \sum_{r=0}^{h-1} e_{\alpha} \left( \frac{h}{r} \right) \left( \frac{n}{r} \right) \right]^{2n-2}
\]

where \( e_{\alpha} = \frac{1}{2} \) if \( r = \frac{n}{h} \), \( e_{\alpha} = 1 \) if \( r > \frac{n}{h} \).

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) is given in Figure 1.

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

\[
\alpha_1 = \frac{1}{2} N^2 \sqrt{2 \log N} (1+\varepsilon)
\]

at

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

and falling to zero at

\[
2 = \frac{1}{2} (N - a \sqrt{N})
\]

where \( a = \Phi^{-1}(\frac{1}{2}) + \varepsilon \approx 0.665 + \varepsilon \), and where \( \varepsilon \) denotes a quantity which approaches zero as \( N \) approaches infinity. However, the true value of \( 2 \) is known to be \( (153) \frac{1}{2} [N - \sqrt{N}] \).

4. DISCUSSION

Part 2 of this paper has demonstrated a method for enumerating cosets of the shortened first order BCH 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 of a coset code of a coset leader \( Y \) independent of the choice of \( Y \) within a coset? (R. P. |Kushn} \( ^4 \) 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?

ACKNOWLEDGEMENT

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

REFERENCES


