The Weight Enumerator of GRM codes

Seema Thakran  
Senior Assistant Professor  
Department of applied Sciences,  
The NorthCap University, India  
email: seemathakran@ncuindia.edu

Sonu Kumari  
Research scholar  
The NorthCap University, India  
email: sonu18asd001@ncuindia.edu

Abstract:

The distribution of weight enumerator gives the new idea to contract the information about the code for finding the error probability of a code. In this paper, we have extended the result of the weight enumerator of GRM codes [3]. The weight enumerator of GRM codes for order \((m - 3), m \geq 3, r \geq 0\) has been developed and analyzed.

Keywords:

Reed Muller (RM) codes, Duals of Reed- Muller codes, Generator matrix, Generalized Reed Muller (GRM) codes, Duals of Generalized Reed Muller (DGRM) codes, Weight Enumerator, Punctured vector, MacWilliam Identity.

Introduction:

In Bell System Technical Journal [5], Claude Shannon published a paper titled ‘A Mathematical Theory of Communication’ which gave rise to two fields called “information theory and coding theory”. The basic objective of information theory and coding theory is to make communication efficient and world friendly in this informal environment. For efficiency, channel used for communication should not require much time and effort and to be reliable, the data received by the channel should reach without errors. The fundamental issue is to merge the two preferences like efficiency and reliability as best we can.
The nature of information theory is probabilistic and analytic and it is the study of successfully attaining bounds for transferring the information from one source to another. Whereas, coding theory attempt to meet these bounds that focus on construction by algebraic means. The major concept of Shannon’s paper was to get information about understanding and working on information theory. Prior to Shannon, his colleague Richard Hamming was working on error correcting of early computers and he was successful in some of the first breakthroughs of coding theory.

Coding theory is most commonly used in communication systems, and it has been developed and engineered as one of inevitable release of communication viz. Noise. Noise is always a major part of the communication that will keep on interfering and corrupting data. It can come from a lot of number of sources such as back ground sound of machine or people, radio disturbances, poor typing, lighting, poor hearing etc. Shannon, Hamming, and many of other inventors worked in Bell telephone laboratories for mathematical communication theory which particularly interested in dealing with obstacles inside the message that used to pass through the telephone lines. Also, many more modems transmission and reception capabilities are built into their hardware with embedded error handling capabilities. It is also important to protect communication while keeping all these impurities and to store, secure computer bank data under the intrusion of gamma rays and magnetic interference.

Coding theory is divided into main branches named as source coding and channel coding, these are renamed due to the reason that the former one modified the source to allow more efficient transmission ( i.e smaller size message) while the latter was about those errors that may be introduce in the transmission channel. The basis of this topic is in the work of Nyquist (1924) and Hartely (1928) but, the fundamental work on this topic was done after Second World War when Shannon (1948) considerably as the father of information theory published his paper.

For error correction and detection, numbers of codes are developed and now utilized fundamentally in all applications of quick-witted device such as internet, scanner, T.V, optical device and all telecom equipment. The end result should be a large-scale operation of the computing machine without errors. For this, Hamming (1950) developed codes that could correct and detect a single error during the transmission process. Thereafter in 1954, Reed provided a class of multiple-error correcting codes to direct generalization of Golay (1949) and Hamming.
And most of studies must be limited to the detection and correction of random error in coding theory. Fire (1959) design ‘burst errors’ codes which later become useful for correction of BCH and many burst errors which is already known. In 1960, Abramson created binary codes that could correct all single and double adjacent-errors which later become the cornerstone of an important class in coding theory called ‘burst error correcting codes’ and the occurrence of errors was found more in the pedestal position rather than randomly in practical channels, so this code was used extensively.

In this paper we worked and focused on Generalized Reed Muller (GRM) codes developed from RM codes by Dass and Muttoo by extending/ shortening the RM codes.

RM codes were developed by Muller whereas Reed provided the first effective translation method of these codes. Reed Muller codes are best, oldest and well ancestry of error correcting codes. It forms infinite family of codes, and its important merit is that larger Reed Muller codes can be made from smaller code. The main advantage of Reed Muller code is to encode the message and decode the broadcast received. For this, we use the generator matrices for encoding and decoding using one form of process known as majority logic. In this correction of information transmission, the code has value both on earth and from space.

Reed Muller codes importance can be analyzed by the fact that Mclice and Niederreiter used them for transmitting black and white photographs on Mars by Mariner 9 spacecraft in 1972. Reed Muller code efficient of correcting 7 errors out of 32 bits communicated, including now of 6 data bits and 26 check bits over 16,000 bits per second were import back to earth. Special cases of Reed Muller codes include the Walsh- Hadamard code [14] and Reed- Soloman codes [8], Hadamard codes are related to first order Reed Muller codes.

Reed Muller codes are generalized in so many ways and known as Generalized Reed Muller codes. Generalized Reed Muller codes are studied by V. Tyagi and S. Rani [16], K. G. Paterson and A. E. Jones [9], P. Ding and J. D. Key [11], J. Pujol and J. Rifa [8] and by many other authors. Generalized Reed Muller codes are used in Orthogonal Frequency division Multiplexing (OFDM) [10].

The generalization, we are working and focusing is, known as GRM codes and it is important and useful theoretically as well as practically. In 2012, V. Tyagi and S. Rani [19],
introduced a new construction of GRM codes by combining multiple GRM codes and shown that these codes have same minimum distance and error correcting capabilities as the code having greatest minimum distance in the construction. In [20], the recursive matrix method for GRM and DGRM codes is developed by V. Tyagi and S. Rani.

The weight distribution and list of decoding size of GRM codes for the order \( r = m - 2 \) is given by Dass and Wasan in [3]. In this paper, we have worked on developing the weight enumerator of GRM codes for order \( r = m - 3 \). The weight distribution of an error codes count, for every given parameter, the distribution of weight enumerator of a code is the main characteristic of code and behavior of code from both theoretical as well as practical aspects. The weight distribution of Reed Muller codes in coding theory is open problem form past many years, it has been calculated for only a few families of codes e.g. Hamming codes, 2nd order Reed Muller codes and generalized Reed Muller codes for order \( r = m - 2 \).

The weight distribution of second order q-ary Reed Muller codes has been developed by Sloane and Berlekamp [11]. Further a precise account of weight distribution of second order q-ary Reed Muller codes provided by Shuxing Li [18] with some corrections and also in addition, second order q-ary projective Reed Muller codes and the weight distributions of these codes are homogeneous.

In [6], by taking the advantage of fast Fourier techniques, for a given binary non-linear code a deterministic algorithm is provided to compute distance distribution, its weight, minimum distance and minimum weight. The performance of above algorithm was found to be similar as that of best known algorithm for average case, which is specifically efficient for codes with low information rate. Also in [15], for q-ary simplex code and q-ary first order reed Muller code the extended and generalized weight enumerator has already been studied and for calculation purpose all the codes were used as they corresponds to a projective system containing all the points in a finite projective or affine space. So, weight enumeration has been from the geometric method.

In [12], computed the weight enumerator of affine Reed Muller codes and some projective of order 3 over \( F_q \) which give the answer of enumerative questions about plane cubic curves. Also, it is found that how traces of Hecke operators performing on spaces of cusp forms for \( SL_2(Z) \).
In this paper, we used the most fundamental outcome about weight distribution that are MacWilliams equation, a set of linear relation between the weight distribution of code \((c)\) and dual of code \((c^\perp)\). These equations suggested that the weight distribution of \((c^\perp)\) is uniquely determined by weight distribution of \(c\).

This paper has four Sections. Section 1, contains important definitions used in the paper. In Section 2, theorem on weight enumerator of GRM codes of order \((m-3)\) is stated and proved. In the last Section, conclusion is given.

**Section 1**

**Basic Definitions:**

Reed Muller codes are one of the best understood and well studied families of linear error correcting codes used in the communications. The Reed-Muller codes were first introduced by Muller in 1954. Muller showed that the family of codes he introduced had good distance parameters. These codes are relatively easy to decode by using majority logic systems.

**Definition 1.1**

**Reed Muller codes:**

For any positive integer \(r\) and \(m(r < m)\), there is an RM code of order \(r\) formed by using as a basis of vectors \(v_0, v_1, v_2, \ldots, v_m\) and all vector products of \(v_1, v_2, \ldots, v_m\) taken \(r\) or fewer at a time, where \(v_1, v_2, \ldots, v_m\) are the rows of a matrix that has columns which are binary representation of 0, 1, 2, \ldots, \(2^m - 1\) and the vector \(v_0\) has all its components as 1’s. The minimum distance of RM codes of order \(r\) is \(2^{m-r}\). Also, the generator matrix of Reed Muller codes is denoted by \(G(r,m)\).
Illustration 1.1

\[ RM(1,3) = \begin{bmatrix}
v_0 \\
v_3 \\
v_2 \\
v_1 \\
v_2v_3 \\
v_1v_3 \\
v_1v_2 \\
v_1v_2v_3 \\
1 \\
1 + v_3 \\
1 + v_2 \\
1 + v_1 \\
1 + v_2v_3 \\
1 + v_1v_3 \\
1 + v_1v_2 \\
1 + v_1v_2v_3
\end{bmatrix} \]

\[ RM(1,3) = \begin{bmatrix}
00000000 \\
00001111 \\
00110011 \\
01010101 \\
00111100 \\
01011010 \\
01101001 \\
11111111 \\
11110000 \\
11001100 \\
10101010 \\
11000011 \\
10100101 \\
10011001 \\
10010110
\end{bmatrix} \]
**GRM codes of order** \( r + (r + 1)_{m,s} \)

In 1981, Dass and Muttoo [2] obtained a new class of Generalized Reed-Muller codes known as GRM codes of order \( r + (r + 1)_{m,s} \) by extending/reducing \( r^{th} \) RM codes. The dual of these codes are also studied by Dass and Tyagi [4] and in 1988, it was developed that the order of the dual of GRM(\( r, m, s \)) codes is \( (m - r - 2) + (m - r - 1)_{m,s} \).

**Definition 1.2**

A code of order \( r + (r + 1)_{m,s} \) is constructed by using the basis of the set of vectors \( v_0, v_1, v_2, \ldots, v_m \) and all the vectors taken up to \( r \) along with some \( s \) vectors products \( 1 \leq s \leq \left( \frac{m}{r+1} \right) \) of these vectors taken \( (r+1) \) at a time where \( v_1, v_2, v_3, \ldots, v_m \) are rows of a matrix that has all possible \( m \)-tuples over \( GF(2) \) as columns and \( v_0 \) having one as all components.

Wasan and Games [16] have proved in 1984 that minimum distance of GRM codes of order \( r + (r + 1)_{m,s} \) is \( 2^{m-r-1} \). A code of order \( r + (r + 1)_{m,s} \) is also denoted by \( GRM(r, m, s) \).

If \( GRM(r, m) \) denote by the generator matrix of Reed muller codes of \( r^{th} \) order. Then, the generator matrix of GRM codes \( GRM(r, m, s) \) of order \( r + (r + 1)_{m,s} \) can be written as

\[
G(r,m) \begin{bmatrix} X \\
\end{bmatrix}
\]

where \( X \) is a matrix containing some \( s \) vector product of \( v_1, v_2, \ldots, v_m \) taken \( (r+1) \) vector at a time.

**Illustration 1.2**

Consider the generator matrix of \( GRM(0,3,2) \)

\[
GRM(0,3) = \begin{bmatrix} G(0,3) \\
\end{bmatrix}
\begin{bmatrix} v_1 \\
v_2 \\
\end{bmatrix}
\]
These codes are also studied by B.K. Dass and S.K. Wasan [3], B.K. Dass and V. Tyagi [4], S.K. Muttoo and M.K. Rana [17], and V. Tyagi and S. Rani [19] etc.

Section 2

The weight distribution is a fundamental parameter of Reed Muller codes. Their essential importance as mathematical objects, are mostly used in probability theory to bring in with different ways of decoding. In this paper, we have obtained the weight enumerator of the $GRM(m - 3, m, s)$ using Assmus and Mattson’s result on weight distribution of linear code. This is extension of work done by [3] for order $(m-2)$. The following theorem is on order $(m-2)$.

Theorem 2.1

Statement: The weight enumerator of the $GRM(m - 3, m, s)$ code is

$$H(x) = \frac{1}{2^{n-2}} \left[ 2^t(1+x)^{2^n} + \{A_{2^t,1,2^t+1,s} - 4(2^t - 1)(1-x)^{2^t-1+2^t+1} - (1+x)^{2^t+1+2^t+1} \right]$$

$$\{A_{2^t,1} + 6(2^t - 1)(1+x)^{2^t} (1-x)^{2^t+1} + 2^t(1-x)^{2^n} \}$$

Where $\left\{1 \leq s \leq \binom{m}{r+1} \right\}$, $0 \leq h \leq \left[ \frac{m}{2} \right]$. 
Proof:

In 1978, Assmus and Mattson’s [1] have given result on the weight distribution of a coset of linear code.

Using the result, we are finding the weight enumerator of $GRM(m - 3, m, s)$.

Let $F(x)$, $G(x)$ and $H(x)$ are the polynomials of the weight enumerators of $RM(m - 3, m)$, $RM(m - 3, m)\dagger$ and $GRM(m - 3, m, s)$ respectively.

Since $RM(r, m)\dagger = RM(m - r - 1, m)$, we get $RM(m - 3, m)\dagger = RM(2, m)$

Then, by using Nell and J.A. Sloane [11] result on the weight enumerator for second order Reed Muller codes, we get

$$G(x) = 1 + (A_{2^{m-1}2^{m-1}+1})x^{2^{m-1}2^{m-1}+1} + A_{2^{m-1}}x^{2^{m-1}} + x^{2^n},$$

where the values of $A_{2^{m-1}2^{m-1}+1}$ are weight of 2nd order Reed Muller code where, $A_i$’s be the number of code words of weight $i$ in $RM(2, m)$, then

$$A_i = 0 \text{ unless } i = 2^{m-1} \text{ or } i = 2^{m-1} \pm 2^{m-1-h} \text{ for some } h, 0 \leq h \leq \left\lceil \frac{m}{2} \right\rceil \text{, where } \left\lceil \frac{m}{2} \right\rceil \text{ is the greatest integer function.}$$

Also, we have $A_0 = A_{2^n} = 1$

Therefore, we get the formula for

$$A_{2^{m-1}2^{m-1}+1} = \frac{2^{(h+1)}(2^m - 1)(2^{m-1} - 1)......(2^{m-2h+1} - 1)}{(2^{2h} - 1)(2^{2h-2} - 1)......(2^2 - 1)} \quad \text{for } 0 \leq h \leq \left\lceil \frac{m}{2} \right\rceil$$

Also,

Now, using the result, known as Macwilliam identity [7], we get the weight enumerator of $RM(m - 3, m)$. 

9
Therefore, we get
\[ F(x) = \frac{1}{2^{n+1}} G \left( \frac{1-x}{1+x} \right). \]

So, by using the definition of \( G(x) \), we obtained
\[
F(x) = \frac{1}{2^{n+1}} \left[ (1+x)^{2^n} + \left\{ A_{2^{n-1}2^{n-1}+1} \right\} (1-x)^{2^{n-1}2^{n-1}+1} (1+x)^{2^{n-1}2^{n-1}+1} + A_{2^{n-1}} (1-x)^{2^{n-1}} (1+x)^{2^{n-1}} + (1-x)^{2^n} \right] 
\]
\[ \ldots (1) \]

We have generator matrix of \( \text{GRM} (m-3, m, s) \) as
\[ G = \left[ G(m-3,m) \right] \] where the rows of the matrix \( X \), representing the product of some \( s \) vector of \( v_1, v_2 \ldots v_m \) taken \( (r+1) \) at a time.

Let \( l(X) \) representing the linear combination of the rows of \( X \). The code \( \text{GRM} (m-3, m, s) \) be the disjoint union consist of \( 2^r - 1 \) cosets \( v + \text{RM} (m-3, m) \) and the code \( \text{RM} (m-3, m) \), where \( v \in l(X), v \neq 0 \) in \( l(X) \).

Let, the weight enumerator of a coset \( v + \text{RM} (m-3, m) \) is denoted by \( a(x) \), where \( v \in l(X), v \neq 0 \).

In 1978, Assmus and Mattson [1] developed a result on the weight enumerator of a coset of a linear code. Using the result, we will get
\[ a(x) = \frac{1}{2^{n+1}} \left[ \sum_{i=0}^{2^n} (2b_i - B_i) (1+x)^{2^{n-i}} (1-x)^i \right] \]
\[ \ldots (2) \]

Where, the number of code words of weight \( i \) in \( \text{RM} (m-3, m)^\perp \) is denoted by \( B_i \) and the number of code words in \( \text{RM} (m-3, m)^\perp \) that are also orthogonal to \( v \), is denoted by \( b_i \).

From the expression of \( G(X) \) it follows that
From equation (1) and (3) and (4), we obtained
\[ H(x) = \frac{1}{2^n} \left[ (1+x)^{2^n} + A_{2^n+1} (1-x)^{2^n-1} - A_{2^n+2} (1-x)^{2^n-2} + (1-x)^{2^n} \right] \]

\[ + \left( \frac{2^s-1}{2^{n-k}} \right) (1+x)^{2^n} - 4(1-x)^{2^n-1} (1+x)^{2^n-2} + 6(1-x)^{2^n} (1+x)^{2^n-1} + (1-x)^{2^n} \right] \]

\[ H(x) = \frac{1}{2^n} \left[ 2^s (1+x)^{2^n} + A_{2^n+1} (1-x)^{2^n-1} - 4(2^s-1) (1-x)^{2^n-2} + (1+x)^{2^n} \right] \]

\[ + \left[ A_{2^n+2} + 6(2^s-1) (1-x)^{2^n-1} + 2^s (1-x)^{2^n} \right] \] \hspace{1cm} \ldots(5)

**Illustration 3.1**

Let \( C \) be the code \( GRM (0,3,2) \), generated by the generator matrix

\[
GRM (0,3) = \begin{bmatrix}
11111111 \\
01010101 \\
00110011
\end{bmatrix}
\]

Therefore,

\[
C = GRM (0,3,2) = \begin{bmatrix}
00000000 \\
11111111 \\
01010101 \\
00110011 \\
10101010 \\
11001100 \\
01100110 \\
10011001
\end{bmatrix}
\]

The weight enumerator of code \( C \) is given by

\[ W(x) = 1 + 6x^4 + x^8. \]
Now, from the weight enumerator obtained in the theorem 2.1, we have weight enumerator of the code $GRM (m-3,m,s)$ is given by

$$H(x) = \frac{1}{2^{n-1}} \left[ 2'(1+x)^n + \left\{ A_{2^{m-1}2^{m-1}} - 4(2^r - 1) \right\} (1-x) - 2'(1-x)^2 + \left\{ A_{2^{m-1}} + 6(2^r - 1) \right\} (1-x)^2 \right]$$

Now, putting $m=3, r=0$ and $s=2$ and the values of $A_i's$ which are calculated from the code $RM(2,3)$

As

$A_{2^{m-1}2^{m-1}} = A_3 = A_6 = 28$

$A_{2^{m-1}} = A_4 = 70$

$A_0 = A_8 = 1$

In $H(x)$, we get

$$H(x) = \frac{1}{2^{n-1}} \left[ 2^2(1+x)^8 + \left\{ 28 - 4(2^2 - 1) \right\} (1-x)^2(1+x)^6 + \left\{ 28 - 4(2^2 - 1) \right\} (1-x)^6(1+x)^2 + \right\} (1-x)^4(1+x)^4 + 2^2(1-x)^8$$

After simplifying, we get

$$H(x) = (1 + 6x^4 + x^8) \text{ is same as } W(x).$$

**Illustration 3.2**

Let $C'$ be the code $GRM (0,3,1)$, generated by the generator matrix

$$GRM (0,3) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$
Consequently

\[
C' = \text{GRM (0,3,1)} = \begin{bmatrix}
00000000 \\
11111111 \\
01010101 \\
10101010
\end{bmatrix}
\]

The weight enumerator of code \(C'\) is specified by

\[
W'(x) = 1 + 2x^4 + x^8
\]

Now, the weight enumerator get in theorem 2.1, we have weight enumerator of the code \(\text{GRM (m-3,m,s)}\) is given by \(H(x)\)

Now putting \(m = 3, r = 0, and s = 1\) and the value of \(A_j's\) which are work out from the code \(\text{RM (2,3)}\) as

\[
A_2 = A_6 = 28 \\
A_4 = 70 \\
A_0 = A_8 = 1
\]

In \(H(x)\), we obtained

\[
H(x) = \frac{1}{2^{8-1}} \left[ 2^1(1+x)^8 + \{28-4(2^1-1)\}(1+x)^6(1-x)^2 + \{28-4(2^1-1)\}(1+x)^2(1-x)^6 \right] + \{70+6(2^1-1)\}(1+x)^4(1-x)^4 + 2^1(1-x)^8
\]

After solving, we have

\[H(x) = 1 + 2x^4 + x^8\] is same as \(W'(x)\).

**Section 4**

**Conclusion:**

The work has already been done up to order \((m-2)\) and in this paper, we have extended this work for the weight enumerator of Generalized Reed Muller codes of order \((m-3)\).
References;

[1]. Assmuss and Mattson, (1978), The weight distribution of a coset of a linear code. I.E.E.E. Transactions on Information Theory, Vol.24, No.2, 497-497.

[2]. B.K. Dass and S.K. Muttoo, (1981), A note reed-muller codes, Discrete Applied Mathematics, Vol.2, No.4, 345-348.

[3]. B.K. Dass and S.K. Wasan, (1983), On codes of order $r+(r+1)_{m,s}$, International Journal Electronics’, Vol. 54, No.3, 471-475.

[4]. B.K. Dass and V. Tyagi, (1988), On duals of GRM codes $r+(r+1)_{m,s}$ Bulletin of Calcutta Mathematics Society, Vol.80, 270-277.

[5]. C.E Shannon, (1948), A mathematical theory of communication, Bell System Technical Journals, Vol.27, 379-423.

[6]. E. Bellini and M. Sala, (2018), A deterministic algorithm for the distance and weight distribution of binary non linear codes, International Journal of Information and Coding Theory, 1-8.

[7]. F.J. Macwilliam, (1963), A theorem on the distribution of weight in a systematic code, Bell syst. Technology, Vol.42, 79-94.

[8]. I.S. Reed and G. Solomon, (1960), Polynomial codes over certain finite fields, Journal of the Society for Industrial and Applied Mathematics, Vol.8, 300-304.

[9]. J. Rifa, Pujol and S. I. Faina, (2008), On new quaternary Reed-Muller codes, Int. Conf. Computational Technologies in Electrical and Engineering, Sibiron, IEEE, Vol.8, 16-19.

[10]. K.G. Paterson and A.E. Jones, (2000), Efficient decoding algorithms for generalized Reed Muller codes, IEEE Transaction and Communication, Vol.48, 1272-1285.

[11]. J.A. Sloane and Nell, (1970), Weight enumerator for second order Reed-Muller Codes, I.E.E.E. Transaction on Information Theory, Vol. IT-16, No.6, 745-751.

[12]. N. Kaplan, (2019), Weight enumerators of reed muller codes from cubic curves, Arithmetic Geometry: Computation and Application, 1-19.

[13]. P. Ding and J.D. Key, (2000), Minimum-weight codeword as generators of generalized Reed Muller codes, I.E.E.E. Transaction on Information Theory, Vol.46, 2152-2158.

[14]. R.C. Bose and S.S. Shrikhande, (1959), A note on result in the theory of code Construction, Information and Control, Vol.2, 183-194.
[15]. R.P.M.J. Jurrius, (2012), Weight enumerator of codes from finite space, Design, Codes and Cryptography, 1-10.

[16]. S.K. Wasan and R.A Games, (1984), On a conjecture on reed-muller codes, International Journal of Electronic, Vol.56, No.2, 269-271.

[17]. S.K. Muttoo and M.K. Rana, (2008), A note on dual of GRM codes of order \( r + (r + 1)_{m,n} \), Inverts Journal of Science and Technology, Vol.1, No.5, 172-178.

[18]. S. Li, (2019), On the weight distribution of second order reed muller codes and their relatives, Designs, Codes and Cryptography, 1-14.

[19]. V. Tyagi and S. Rani, (2010), New construction of GRM codes, Asian-European Journal of Mathematics, Vol.5, No.1, 1250012-16.

[20]. V. Tyagi and S. Rani, (2012), Recursive matrix method for GRM and DGRM codes, International Electronic Journal of Pure and Applied Mathematics, Vol.4, No.4, 263-270.