International Electronic Journal of Pure and Applied Mathematics

Volume 4 No. 4 2012, 263-270

RECURSIVE MATRIX METHOD FOR GRM AND DGRM CODES

Vinod Tyagi[1], Seema Rani[2] §

[1]Department of Mathematics
Shyam Lal College (Eve.)
University of Delhi, 110032, INDIA

[2]Department of Mathematics
University of Delhi, 110007, INDIA

Abstract: In this paper,we present a recursive matrix method for constructing Generalised Reed-Muller (GRM) codes and their duals.

AMS Subject Classification: 05E99
Key Words: Reed-Muller (RM) code, generalized Reed-Muller (GRM) code, dual of GRM (DGRM) code, recursive matrix method, generator matrix, punctured vector

1. Introduction

Reed-Muller (RM) codes are one of the best understood and well studied family of binary linear codes. These codes are relatively easy to decode by using majority logic systems. RM codes are now more prevalent as telecommunications have expanded and has developed active use of self-correcting codes. The importance of RM codes can be judged from the facts that way back in 1972, they were used for sending black and white photographs from Mars by Mariner 9 space craft and presently,one of the best public key cryptosystems given by McElice and Niederreiter [13] are based on RM codes. Such important applications of RM codes have encouraged researchers to study their properties in detail.

Received: August 28, 2011

§Correspondence author

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 4 (2012)

Among many important variants of RM codes, there are many generalizations of RM codes, referred to as GRM codes in this paper, some of which are of great practical use whereas others are important from theoretical point of view. Kenneth G. Paterson and Alan E. Jones [6], Peng Ding and Jennifer D.Key[10], Jaume Pujol and Josep Rifa [5] and many other authors have studied generalizations of RM codes that significantly differ from each other. Kenneth G. Paterson and Alan E. Jones have stated in one of their recent work that GRM codes have been used in orthogonal frequency-division multiplexing.

In this paper, we use GRM codes introduced by Dass and Muttoo(1980) to develop a new class of GRM codes by combining two or more such codes.This paper is organized in three sections. In Section 2, we give important definitions that are frequently used in this paper. Section 3, contains the recursive method for GRM and DGRM codes and conclusion is given in Section 4.

2. RM Codes

Definition 2.1. Let $0 \leq r \leq m$, and A be the set consisting of v_0 and all the Boolean products of the elements of $D = \{v_1, v_2, \ldots, v_m\}$ upto degree r.The subspace of $F_{2^{2^m}}$, generated by A is defined as the rth order Reed-Muller code of length 2^m,and is denoted by $RM(r, m)$.

Minimum distance of RM code of order r is 2^{m-r}.

3. GRM Codes of Order $r + (r+1)_{m,s}$

Dass and Muttoo [2] obtained a new class of Generalized Reed-Muller codes, now known as GRM codes of order $r + (r+1)_{m,s}$, by extending/ shortening rth order RM code. Their duals are studied by Dass and Tyagi [3] and it has been proved that the duals are also GRM codes of order $(m-r-2) + (m-r-1)_{m,\binom{m}{m-r-1}-s}$.

Definition 3.1. Let $0 \leq r < m$, and A' be the set consisting of v_0 and all the Boolean products of the elements of $D' = \{v_1, v_2, \ldots, v_m\}$ upto degree r along with some s vector products $\left(1 \leq s < \binom{m}{r+1}\right)$ of these vectors taken $(r+1)$ at a time. The subspace of $F_{2^{2^m}}$, generated by A' defined as the GRM code of order $r + (r+1)_{m,s}$.

Wasan and Games (1982) have shown that the minimum distance of GRM codes of order $r + (r+1)_{m,s}$ is 2^{m-r-1}.

So, if $G(r, m)$ denotes the generator matrix of a $RM(r, m)$ code, then the gen-

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 4 (2012)

erator matrix of a GRM code of order $r+(r+1)_{m,s}$ may be written as $\begin{bmatrix} G(r,m) \\ X \end{bmatrix}$, where X is a matrix containing some s vector products of $v_1, v_2, \ldots, v_m$ taken $(r+1)$ at a time. These codes were also studied by Dass and Wasan [4], Charpin [1] and by Muttoo and Rana [7] and [8].

In [3] Dass and Tyagi has given a conjecture which is as follows:

"A GRM code of order $r+(r+1)_{m,s}, r < m-2$, is capable of correcting all solid bursts of length b, where $b = 1, 3, 5, \ldots, 2^m - 1$.

4. Punctured Vector

Definition 4.1. For a given m, we define the **punctured vector** with respect to vector v_i to be the vector product $v_1v_2v_3 \ldots v_{i-1}v_{i+1} \ldots v_m$ of the $m-1$ vectors. Similarly the punctured vector of v_iv_j is defined to be the vector $v_1v_2 \ldots v_{i-1}v_{i+1\ldots}v_{j-1}v_{j+1} \ldots v_m$ and so on.

5. Recursive Matrix Method for GRM Codes

Let $G_1, G_2, G_3, \ldots, G_{p+q}$ are generator matrices of GRM codes of order $(r+p+q-1)+[(r+p+q-1)+1]_{m,s_1}, (r+p+q-2)+[(r+p+q-2)+1]_{m,s_2}, \ldots,$ $r+(r+1)_{m,s_{p+q}}$, where $1 \le s_i < \begin{pmatrix} m \\ r+p+q-i+1 \end{pmatrix}$, $i = 1(1)p+q$.

Let $G_p^1 = \begin{bmatrix} G_p^0 & G_p^0 \\ O & G_{p+1}^0 \end{bmatrix}$; where $G_p^0 = G_p; p \ge 1$

$$G_p^2 = \begin{bmatrix} G_p^1 & G_p^1 \\ O & G_{p+1}^1 \end{bmatrix}$$

$$G_p^3 = \begin{bmatrix} G_p^2 & G_p^2 \\ O & G_{p+1}^2 \end{bmatrix}$$

$$G_p^4 = \begin{bmatrix} G_p^3 & G_p^3 \\ O & G_{p+1}^3 \end{bmatrix}$$

$$\vdots$$

$$G_p^q = \begin{bmatrix} G_p^{q-1} & G_p^{q-1} \\ O & G_{p+1}^{q-1} \end{bmatrix}; q \ge 1.$$

Now, let us fix $p = 1$,and vary q, we will prove that

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 4 (2012)

$$G_1^q = \begin{bmatrix} G_1^{q-1} & G_1^{q-1} \\ O & G_2^{q-1} \end{bmatrix},$$

generates a GRM code of the same type.

We will prove this by induction on q.

Now, for $q = 1$, result is true by [7].

For $q = 2$, result is true by [11].

For $q = 3$, verified.

Assume that result is true for $q = n$,

i.e. $G_1^n = \begin{bmatrix} G_1^{n-1} & G_1^{n-1} \\ O & G_2^{n-1} \end{bmatrix}$, generates a GRM code of the same type.

We will prove that result holds good for $q = n + 1$.

Now, let us consider

$$G_1^{n+1} = \begin{bmatrix} G_1^n & G_1^n \\ O & G_2^n \end{bmatrix}$$

$$= \begin{bmatrix} G_1^{n-1} & G_1^{n-1} & G_1^{n-1} & G_1^{n-1} \\ O & G_2^{n-1} & O & G_2^{n-1} \\ O & O & G_2^{n-1} & G_2^{n-1} \\ O & O & O & G_3^{n-1} \end{bmatrix}$$

$$= \begin{bmatrix} A & A \\ O & B \end{bmatrix}, \text{ where } A = \begin{bmatrix} G_1^{n-1} & G_1^{n-1} \\ O & G_2^{n-1} \end{bmatrix} \text{ is a GRM code.}$$

$$B = \begin{bmatrix} G_2^{n-1} & G_2^{n-1} \\ O & G_3^{n-1} \end{bmatrix} \text{ is a GRM code.}$$

So, by combining results obtained by Muttoo and Rana [7] and Tyagi and Seema [11], this matrix will generate a GRM code of the same type.

Hence the proof.

Similarly, we can prove that $G_2^q, G_3^q, \ldots, G_p^q$ generates GRM code of the same type.

Discussion

1. For $q = 1$ and $p = 1$, we have $G_1^1 = \begin{bmatrix} G_1^0 & G_1^0 \\ O & G_2^0 \end{bmatrix} = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}$, which is result due to Muttoo and Rana [7].

2. For $q = 2$ and $p = 1$, we get $G_1^2 = \begin{bmatrix} G_1^1 & G_1^1 \\ O & G_2^1 \end{bmatrix}$

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 4 (2012)

$$= \begin{bmatrix} G_1^0 & G_1^0 & G_1^0 & G_1^0 \\ 0 & G_2^0 & 0 & G_2^0 \\ 0 & 0 & G_2^0 & G_2^0 \\ 0 & 0 & 0 & G_3^0 \end{bmatrix}$$

$$= \begin{bmatrix} G_1 & G_1 & G_1 & G_1 \\ 0 & G_2 & 0 & G_2 \\ 0 & 0 & G_2 & G_2 \\ 0 & 0 & 0 & G_3 \end{bmatrix}$$

which is result due to Tyagi and Seema [11].

6. Recursive Matrix Method for DGRM Codes

Let $G_1, G_2, G_3, \ldots, G_{p+q}$ are generator matrices of DGRM codes of orders $r+(r+1)_{m,s_1}, (r+1)+[(r+1)+1]_{m,s_2}, \ldots, (r+p+q-1)+[(r+p+q-1)+1]_{m,s_{p+q}}$, where $1 \leq s_i < \begin{pmatrix} m \\ r+i \end{pmatrix}$, $i = 1(1)p+q$.

Let $G_p^1 = \begin{bmatrix} G_p^0 & G_p^0 \\ O & G_{p+1}^0 \end{bmatrix}$; where $G_p^0 = G_p; p \geq 1$

$$G_p^2 = \begin{bmatrix} G_p^1 & G_p^1 \\ O & G_{p+1}^1 \end{bmatrix}$$

$$G_p^3 = \begin{bmatrix} G_p^2 & G_p^2 \\ O & G_{p+1}^2 \end{bmatrix}$$

$$G_p^4 = \begin{bmatrix} G_p^3 & G_p^3 \\ O & G_{p+1}^3 \end{bmatrix}$$

$$\vdots$$

$$G_p^q = \begin{bmatrix} G_p^{q-1} & G_p^{q-1} \\ O & G_{p+1}^{q-1} \end{bmatrix}; q \geq 1$$

Now, let us fix $p = 1$, and vary q,,we prove that

$$G_1^q = \begin{bmatrix} G_1^{q-1} & G_1^{q-1} \\ O & G_2^{q-1} \end{bmatrix},$$

generates a DGRM code of the same type.
We will prove this by induction on q.
Now, for $q = 1$, result is true by [9].
For $q = 2$, result is true by [12].

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 4 (2012)

For $q = 3$, verified.
Assume that result is true for $q = n$,
i.e. $G_1^n = \begin{bmatrix} G_1^{n-1} & G_1^{n-1} \\ O & G_2^{n-1} \end{bmatrix}$, generates a DGRM code of the same type.
we will prove that result holds good for $q = n + 1$.
Now, consider

$$G_1^{n+1} = \begin{bmatrix} G_1^n & G_1^n \\ O & G_2^n \end{bmatrix}$$

$$= \begin{bmatrix} G_1^{n-1} & G_1^{n-1} & G_1^{n-1} & G_1^{n-1} \\ O & G_2^{n-1} & O & G_2^{n-1} \\ O & O & G_2^{n-1} & G_2^{n-1} \\ O & O & O & G_3^{n-1} \end{bmatrix}$$

$$= \begin{bmatrix} A & A \\ O & B \end{bmatrix}, \text{ where } A = \begin{bmatrix} G_1^{n-1} & G_1^{n-1} \\ O & G_2^{n-1} \end{bmatrix} \text{ is a DGRM code.}$$

$$B = \begin{bmatrix} G_2^{n-1} & G_2^{n-1} \\ O & G_3^{n-1} \end{bmatrix} \text{ is a DGRM code.}$$

So by combining results obtained by Muttoo and Rana [9] and Tyagi, Seema and Navneet [12], this matrix will generate a DGRM code of the same type.

Hence the proof.

Discussion

1. For $q = 1$ and $p = 1$, we have $G_1^1 = \begin{bmatrix} G_1^0 & G_1^0 \\ O & G_2^0 \end{bmatrix} = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}$, which is result due to Muttoo and Rana [9].

2. For $q = 2$ and $p = 1$, we get $G_1^2 = \begin{bmatrix} G_1^1 & G_1^1 \\ O & G_2^1 \end{bmatrix}$

$$= \begin{bmatrix} G_1^0 & G_1^0 & G_1^0 & G_1^0 \\ 0 & G_2^0 & 0 & G_2^0 \\ 0 & 0 & G_2^0 & G_2^0 \\ 0 & 0 & 0 & G_3^0 \end{bmatrix}$$

$$= \begin{bmatrix} G_1 & G_1 & G_1 & G_1 \\ 0 & G_2 & 0 & G_2 \\ 0 & 0 & G_2 & G_2 \\ 0 & 0 & 0 & G_3 \end{bmatrix}$$

which is result due to Tyagi, Seema and Navneet [12].

Similarly, we can prove that $G_2^q, G_3^q \ldots, G_p^q$ generates DGRM code of the same type.

Note. This method is also applicable to DRM(dual of RM code) codes.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 4 (2012)

7. Conclusions

In this paper, by using recursive matrix method we have developed a new class of Generalised Reed Muller codes and their Duals by combining multiple GRM and DGRM codes and observed that GRM codes have the same minimum distance and error correcting capabilities as G_{p+q} and DGRM codes as G_p (both G_{p+q} and G_p have greatest minimum distance among the codes involved in the recursive matrix method).

Acknowledgments

The authors would like to thank Prof. B.K. Dass, Head, Department of Mathematics, University of Delhi, Prof. B.D. Sharma, Department of Mathematics, Jaypee University and Dr. S.K. Muttoo, Department of Computer Science, University of Delhi for their useful suggestions. The authors are also indebted to two anonymous referees for many useful comments.

References

[1] P. Charpin, 1-translated codes of generalised Reed-Muller codes, *Treatment of Signal*, **1**, No. 2 (1984), 121-131.

[2] B.K. Dass and S.K. Muttoo, A note on Reed-Muller codes, *Discrete Applied Mathematics*, **2**, No. 4 (1981), 345-348.

[3] B.K. Dass and Vinod Tyagi, On duals of GRM codes of order $r + (r + 1)_{m,s}$, *Bulletin of Calcutta Mathematical Society*, **80** (1988), 270-277.

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

[5] J. Pujol, J. Rifa and S.I. Faina, On New Quaternary Reed-Muller codes, *International Conference on computational Technologies in Electrical and Electronics Engineering*, Sibircon, IEEE, Region, **8** (2008), 16-19.

[6] K.G. Paterson and A.E. Jones, Efficient Decoding Algorithms for Generalised Reed-Muller Codes, *IEEE Transactions on Communications*, **48**, No. 8 (2000), 1272-1285.

[7] S.K. Muttoo and Manoj Kumar Rana, A note on Generalised RM codes of order $r + (r + 1)_{m,s}$, (*Communicated*) (2008).

[8] S.K. Muttoo and Manoj Kumar Rana, *Reed-Muller codes and their generalisations*, M. Phil dissertation, University of Delhi (unpublished) (1997).

[9] S.K. Muttoo and Manoj Kumar Rana, A Note on Dual of GRM codes of order $r + (r + 1)_{m,s}$, *Invertis Journal of Science and Technology*, **1**, No. 5, 172-178.

[10] P. Ding and J.D. Key, Minimum-weight codewords as generators of generalized Reed-Muller codes, *IEEE Transactions on Information Theory*, **46**, No. 6 (2000).

[11] Vinod Tyagi and Seema Rani, New Construction of GRM Codes (accepted for publication in *Asian European Journal of Mathematics* (2010).

[12] Vinod Tyagi, Navneet Rana and Seema Rani, A Construction of DGRM codes of order $r + (r + 1)_{m,s}$, (*Communicated*) (2010).

[13] V.M. Sidel'nikov, A Public-Key cryptosystems based on Reed-Muller codes, *Discrete Mathematics and Applications*, **4**, No. 3 (1994), 191-207.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 4 (2012)