Discrete Applied Mathematics 2 (1980) 345–348

NOTE

A NOTE ON REED–MULLER CODES*

Bal Kishan DASS

Department of Mathematics, P.G.D.A.V. College, Nehru Nagar, New Delhi-110065, India

Sunil Kumar MUTTOO

Research Scholar, Department of Mathematics, University of Delhi, Delhi-110007, India

Received 2 January 1980
Revised 20 June 1980

In this paper we study linear codes that are obtained by annexing some vectors to the basis vectors of a Reed–Muller code of order r.

Introduction

It is known that Reed–Muller codes [1] of order r are a class of binary group codes. For any m and r $(r<m)$ there is a RM code of order r formed by using a basis of vectors $v_0, v_1, \ldots, v_m$ and all vector products of these vectors taken r or fewer at a time where $v_1, v_2, \ldots, v_m$ are the rows of a matrix that has all possible m-tuples as columns and v_0 having all components as 1. If we consider the null space of a RM code of order r we get the dual of rth order RM code as a RM code of order $m-r-1$.

In this note we study through examples codes formed by using as a basis the vectors $v_0, v_1, \ldots, v_m$ and all vector products of these taken r or fewer at a time along with some vector products of $r+1$ vectors at a time. We shall consider the duals of such codes also.

A code of order $r+(r+1)_{m,s}$

Definition. A code of order $r+(r+1)_{m,s}$ is the one formed by using as a basis the vectors $v_0, v_1, \ldots, v_m$ and all vector products of these vectors taken r or fewer at a time along with some s vector products $(1\leq s<\binom{m}{r+1})$ of $r+1$ vectors.

If $G(r,m)$ denotes the generator matrix for a RM code of order r, then the

* This work was carried out under a research project sponsored by Indian Space Research Organization, Government of India.

generator matrix for a code of order $r+(r+1)_{m,s}$ may be written as

$$G(r+(r+1)_{m,s}, m)=\begin{bmatrix} G(r,m) \\ X \end{bmatrix}$$

where X is a matrix containing s vectors out of the products of $r+1$ vectors at a time.

Example 1. For $m=3$ and $r=2$, a generator matrix for the second order RM code may be written as

$$G(2,3)=\begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_1v_2 \\ v_1v_3 \\ v_2v_3 \end{bmatrix}=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The generator matrices for codes of order $1+(2)_{3,1}$ may be taken as any of the following:

1(a) $$G(1+(2)_{3,1}, 3)=\begin{bmatrix} G(1,3) \\ v_1v_2 \end{bmatrix},$$

1(b) $$G(1+(2)_{3,1}, 3)=\begin{bmatrix} G(1,3) \\ v_1v_3 \end{bmatrix},$$

1(c) $$G(1+(2)_{3,1}, 3)=\begin{bmatrix} G(1,3) \\ v_2v_3 \end{bmatrix}.$$

Also, the generator matrices for the codes of order $1+(2)_{3,2}$ may be any one of the following:

1(d) $$G(1+(2)_{3,2}, 3)=\begin{bmatrix} G(1,3) \\ v_1v_2 \\ v_1v_3 \end{bmatrix},$$

1(e) $$G(1+(2)_{3,2}, 3)=\begin{bmatrix} G(1,3) \\ v_1v_2 \\ v_2v_3 \end{bmatrix},$$

1(f) $$G(1+(2)_{3,2}, 3)=\begin{bmatrix} G(1,3) \\ v_1v_3 \\ v_2v_3 \end{bmatrix}.$$

It can be seen that the minimum weight of the $(8, 5)$ and $(8, 6)$ codes considered in Examples 1(a)–1(c) and 1(d)–1(f) respectively is 2 each which is the same as that of a RM code of order 2. We also see that minimum weight of the $(8, 3)$ codes which are duals of the codes of order $1+(2)_{3,1}$ and that of the $(8, 2)$ codes which are duals of the codes of order $1+(2)_{3,2}$ is 4 each, which is the same as that of dual of a RM code of order one.

Example 2. For $m=4$ and $r=1$, a generator matrix for a code of order $1+(2)_{4,1}$ may be taken as

$$G(1+(2)_{4,1}, 4)=[v_0, v_1, v_2, v_3, v_4, Y]^T$$

where Y is any one of the vectors v_1v_2, v_1v_3, v_1v_4, v_2v_3, v_2v_4, v_3v_4 and v_0, v_1, v_2, v_3, v_4 having the usual meaning. In a similar way we can consider the generator matrices for the codes of order $1+(2)_{4,2}$, $1+(2)_{4,3}$, $1+(2)_{4,4}$ and $1+(2)_{4,5}$.

Again, it is easy to verify that the minimum weight of $(16, 6)$, $(16, 7)$, $(16, 8)$, $(16, 9)$ and $(16, 10)$ codes considered in Example 2 is 4, which is the same as that of a RM code of order 2. If we consider the duals of these codes, we see that the minimum weight of these dual codes is 4, which is equal to the minimum weight of the dual of a RM code of order one. Similar situations can be verified for the codes of order $2+(3)_{4,1}$, $2+(3)_{4,2}$, $2+(3)_{4,3}$ and their duals.

From the discussion of the examples made above, we see that the minimum weight of the code of order $r+(r+1)_{m,s}$ is $2^{m-(r+1)}$ and that of its dual is 2^{r+1}. On the basis of this study, we conjecture the following:

Conjecture. The minimum weight of a code of order $r+(r+1)_{m,s}$ is $2^{m-(r+1)}$ which is the minimum weight of a RM code of order $r+1$; and the dual code has minimum weight 2^{r+1} which is the minimum weight of the dual of a RM code of order r.

We now state a result for a code of order $r+(r+1)_{m,s}$, the proof of which is omitted.

We know that a RM cod of order r is self dual iff $r=\frac{1}{2}(m-1)$.

The following theorem gives an analogue of this result for a code of order $r+(r+1)_{m,s}$.

Theorem. *A code of order $r+(r+1)_{m,s}$ is self dual if and only if*

$$s=2^{m-1}-\sum_{i=0}^{r}\binom{m}{i}.$$

It is hoped that the codes of order $r+(r+1)_{m,s}$ may suit well to systems having storage problems.

Acknowledgements

The authors are thankful to the referee for the critical examination and fruitful comments over the original version of the paper.

Reference

[1] W.W. Peterson and E.J. Weldon, Error Correcting Codes, 2nd ed. (MIT Press, Cambridge, MA, 1972).