Discrete Applied Mathematics 6 (1983) 213–214
North-Holland

NOTE

COMMENTS ON "A NOTE ON REED–MULLER CODES"

Manohar Lal KAUSHIK
Department of Mathematics, Shivaji College, New Delhi, India

Received 8 September 1981
Revised 21 December 1981

In the above-mentioned note, Dass and Muttoo [1] claimed, without giving a proof, that a code of order $r+(r+1)_{m,s}$ is self-dual if and only if

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

for non-negative integers r, m and s such that $r<m$ and $1\le s<\binom{m}{r+1}$, where a code or order $r+(r+1)_{m,s}$ is defined as follows:

Let v_0 be an all-one 2^m-tuple, and the 2^m-tuples v_i, $1\le i\le m$, be the rows in the $m\times 2^m$ matrix, the jth column of which is the m-tuple binary representation of $(j-1)$. Then the generator matrix of a code of order $r+(r+1)_{m,s}$ has rows which are $v_0, v_1, \ldots, v_m$ and all (vector) products of these, taking r or less at a time, together with s of those vectors, each of which is a product of $(r+1)$ distinct vectors from $\{v_i : 1\le i\le m\}$.

This result is incorrect and should be changed to:

Theorem. *There exists a self-dual code of order* $r+(r+1)_{m,s}$ *if and only if* $s=2^{m-1}-\sum_{i=0}^{r}\binom{m}{i}$.

Remark. The conditions

(i) $s=2^{m-1}-\sum_{i=0}^{r}\binom{m}{i}$ (implied by the dimension of a self-dual code), and

(ii) $1\le s<\binom{m}{r+1}$ (in the definition of a $r+(r+1)_{m,s}$ code)

are equivalent to

(iii) m is even and $\frac{1}{2}m=r+1$, and

(iv) $s=\frac{1}{2}\binom{m}{m/2}$.

We next give two examples. The first shows that code of order $r+(r+1)_{m,s}$ may not be self-dual even though r, m and s satisfy conditions (iii) and (iv).

Example. For $m \geq 4$, consider two vectors $u = v_1 \cdot v_2 \cdots v_{r+1}$ and $v = v_m \cdot v_{m-1} \cdots v_{m-r}$, where '$\cdot$' denotes the vector product of two vectors. As $s \geq 2$, there exists a code C of order $r+(r+1)_{m,s}$ to which u and v belong. From $m-r=r+2$, it follows that

$$\{1, 2, \ldots, r+1\} \cup \{m, m-1, \ldots, m-r\} = \{1, 2, \ldots, r, r+1, \ldots, m\}.$$

Hence

$$u \cdot v = 000 \cdots 01,$$

implying that u and v are not mutually orthogonal. Thus, there exists a code C of order $r+(r+1)_{m,s}$ that satisfies conditions (iii) and (iv) and is not self-dual. In particular, there exists at least one code of order $2+(3)_{6,10}$ that is not self-dual.

Finally, we give an example of a self-dual code of order $r+(r+1)_{m,s}$ when r, m and s satisfy conditions (iii) and (iv).

Example. For given natural numbers m, r and s, where m is even,

$$r = \tfrac{1}{2}m - 1 \quad \text{and} \quad s = \frac{1}{2}\binom{m}{\frac{1}{2}m} = \binom{m-1}{\frac{1}{2}m},$$

the set P of all those vectors that are products of $r+1$ $(=\frac{1}{2}m)$ distinct vectors from $\{v_i : 1 \leq i \leq m-1\}$, has s distinct members. For u and v belonging to P, v_m is not involved in the (vector) product $u \cdot v$. Further, for vectors x and y, each being product of r or less distinct vectors from $\{v_i : 1 \leq i \leq m\}$, the number of v_i's involved in $u \cdot x$ and $x \cdot y$ does not exceed

$$(r+1)+r = m-1.$$

But, whenever the number of v_i's involved in the product vector of two vectors does not exceed $m-1$, then the weight of the product vector is even, which implies orthogonality of the two vectors. Hence, u, v, x and y are mutually orthogonal. Thus a code C, the rows of a generator matrix of which are $v_0, v_1, \ldots, v_m$, together with their products taken r or less at a time and vectors belonging to P, is a self-dual code of order $r+(r+1)_{m,s}$.

Reference

[1] B.K. Dass and S.K. Muttoo, A note on Reed-Muller codes, Discrete Appl. Math. 2 (1980) 345-348.