A lower bound on the optimum distance profiles of the second order Reed-Muller codes

Yanling Chen and A. J. Han Vinck, *Fellow, IEEE*

Abstract

In this paper, we give a lower bound for the optimum distance profiles of the second order Reed-Muller code in the dictionary order and in the inverse dictionary order. In particular, we investigate the second order Reed-Muller codes of length ≤ 256. We show that the bound is tight, in both orders for the codes of length ≤ 128.

Index Terms

Reed-Muller code, optimum distance profile, MacWilliams' identities, Boolean function, symplectic matrix.

I. Introduction

IN WCDMA systems, the transport format combination indicator (TFCI) is used to provide crucial information about the data being transmitted in the current frame. An irrecoverable error in TFCI will cause the whole frame to be improperly recognized. Thus the data of the whole frame can not be received correctly. To tackle this problem, a good error correcting code is necessary and significant. In particular, the system requires the code to be adaptive to variable TFCI information bits (which ranges from 1 to 10 in 3GPP). This can be done by including or excluding some basis codewords of a fixed error correcting code (based on a sub-code of the second order Reed-Muller code in 3GPP defined communication system).

Note that the minimum distance is one of the most important measurements of the code performance. For the scenario as described above, the linear block codes with optimum distance profile (ODP), as defined in [1], are desirable. These codes have the attracting property that by including or excluding the basis codewords one by one, the derived sup-codes or sub-codes keep the minimum distances as large as possible. These codes can be also applied to the channel coding for informed decoders [3] in order to enhance the error correction power. In [1], results are already given for Reed-Solomon codes, Golay codes and the first order Reed-Muller codes. In this paper, we focus on the second order Reed-Muller codes.

The rest of the paper is organized as follows. In Section II, we describe the basic definitions. In Section III, we present our main result on the optimum distance profile of the second order Reed-Muller codes (An additional result is given in Appendix D). Finally, we conclude in Section IV.

II. Preliminary

Let C be an $[n, k, d]$ binary linear code of length n, dimension k and minimum distance d. We say that C is *minimum distance optimal* if it achieves the largest minimum distance for given length and dimension. A *sub-code chain* is a sequence of linear sub-codes $C = C_0 \supset C_1 \supset \cdots \supset C_{k-1}$, where $\dim[C_i] = k - i$ for $0 \leq i \leq k-1$. Their minimum distances $d[C_0], d[C_1], \cdots, d[C_{k-1}]$ build up a *distance profile* of the linear code C. Clearly, $d[C_0] \leq d[C_1] \leq \cdots \leq d[C_{k-1}]$. Correspondingly a generator matrix (not unique) such that its first $k-i$ rows form a generator matrix of C_i for $0 \leq i \leq k-1$, is called a *generator matrix with respect to the distance profile*.

We say a sequence $[a_0, a_1, \cdots, a_{k-1}]$ is an upper bound on $[b_0, b_1, \cdots, b_{k-1}]$, in the dictionary order if there is an integer t such that $a_i = b_i$ for $0 \leq i < t$, and $a_t > b_t$; in the inverse dictionary order if there is an integer t such that $a_i = b_i$ for $t+1 \leq i < k$, and $a_t > b_t$.

A distance profile of the linear code C is called the *optimum distance profile in the dictionary order* (ODP$[C]^{dic}$) if it is an upper bound on any other distance profile of C in the dictionary order. A similar argument gives the definition of the *optimum distance profile in the inverse dictionary order* (ODP$[C]^{inv}$). In this paper, we use ODP$[C]$ to denote the optimum minimum distance profile in both orders. The sub-code chains or generator matrices with respect to ODP$[C]$ are of our interest.

Let ODP$[C](i)$ be the i-th element of the ODP$[C]$ and ODP$[C](I)$ be a vector which contains i-th element of the ODP$[C]$ for $i \in I$. These conventions also apply to ODP$[C]^{dic}$ and ODP$[C]^{inv}$. It is clear that ODP$[C](0) = d_{min}$ and OPD$[C]^{inv}(k-1) = d_{max}$, where d_{min} is the minimum distance of C and d_{max} is the maximum weight of the codewords in C. In particular, OPD$[C]^{inv}(k-1) = n$, if C is a *self-complementary* linear code, i.e., C contains the all-one codeword.

Let G be the generator matrix of C, and let $\mathbf{c}$ be a codeword of weight $wt(\mathbf{c})$. The code generated by the restriction of G to the columns in which $\mathbf{c}$ has zero coordinates is called *residual code* of C with respect to $\mathbf{c}$ and is denoted by $\mathrm{Res}(C, \mathbf{c})$.

Lemma 2.1: (see Lemma 1 in [6].) Let C be an $[n, k, d]$ code and $\mathbf{c} \in C$, $wt(\mathbf{c}) = w$ and $w < 2d$. Then $\mathrm{Res}(C, \mathbf{c})$ has parameters $[n - w, k - 1, d^0]$, where $d^0 \geq d - \lfloor w/2 \rfloor$. ($\lfloor a \rfloor$ denotes the integer part of the real number a.)

By Lemma 2.1 and Construction Y1 in [4], p.592, we have

Corollary 2.2: Let C be an $[n, k, d]$ code whose dual code has minimum distance $d^\perp$. Then there exist an $[n - d, n - k - d + 1, \geq d^\perp]$ code. Its dual code has parameters $[n - d, k - 1, d^0]$, where $d^0 \geq \lfloor d/2 \rfloor$.

Lemma 2.3: (see Lemma 4 in [6].) If all weights in a binary linear code C are divisible by $2p$, then all weights in its residual codes are divisible by p.

If all codewords of a linear code C have even weight, then C is called an *even* code. In particular, if the weight of every codeword of C is divisible by 4, then C is called a *doubly even* code. As a direct consequence of Lemma 2.3, we have

Corollary 2.4: If a binary linear code C is a doubly-even code, then its residual codes are even codes.

Lemma 2.5: If a binary linear code C is a self-complementary even code, then its dual code $C^\perp$ is also a self-complementary even code.

Proof: Since C is an even code, then $C^\perp$ contains the all-one codeword and it is self-complementary. In addition, since C is self-complementary, then $C^\perp$ has codewords only of even weight and thus $C^\perp$ is also an even code. ■

Lemma 2.6: (The MacWilliams' identities, p.129 in [4].) Let C be an $[n, k]$ code. A_w and B_w denote the number of codewords of weight w in the code C and in its dual code $C^\perp$ respectively. Then

$$\sum_{i=0}^{n} A_i P_w(n, i) = 2^k B_w, \quad \text{for} \quad 0 \leq w \leq n,$$

where $P_w(n, i) = \sum_{j=0}^{w} (-1)^j \binom{i}{j} \binom{n-i}{w-j}$ is a Krawtchouk polynomial.

III. Reed-Muller code

It is known that the first order binary Reed-Muller code $\mathcal{R}(1, m)$ is a linear $[2^m, 1+m, 2^{m-1}]$ code. It has weight enumerator $1 + 2(2^m - 1)t^{2^{m-1}} + t^{2^m}$. From its weight distribution and also as shown in [1],

$$\text{ODP}[\mathcal{R}(1, m)] = [2^{m-1}, 2^{m-1}, \cdots, 2^{m-1}, 2^m].$$

Note that $\mathcal{R}(1, m)$ has many interesting properties. It is optimal in the sense that it reaches the Plotkin bound (refer to Theorem 8 of Ch. 2 in [4]). Besides, it is a sub-code of the second order Reed-Muller code $\mathcal{R}(2, m)$. Especially, as shown in Lemma 3.1, it is unique for given parameters $[2^m, 1 + m, 2^{m-1}]$.

Lemma 3.1: (Uniqueness of the first order Reed-Muller code) Any linear code with parameters $[2^m, 1+m, 2^{m-1}]$ is equivalent to the first order Reed-Muller code. They have a unique weight distribution $1 + 2(2^m - 1)t^{2^{m-1}} + t^{2^m}$.

Proof: The proof follows directly from Theorem 2.3 in [9]. ■

As defined in [4], $\mathcal{R}(2, m)$ is the set of all vectors f, where $f(v_1, \cdots, v_m)$ is a Boolean function which is a polynomial of degree at most 2. It is a linear $[2^m, 1 + m + \binom{m}{2}, 2^{m-2}]$ code. For its weight distribution, one can refer to Theorem 8 of Ch. 15 in [4]. As a simplified version, we have the following lemma.

Lemma 3.2: $\mathcal{R}(2, m)$ has weights only of form 2^{m-1} or $2^{m-1} \pm 2^{m-1-h}$ for $0 \leq h \leq [m/2]$.

A. ODP$[\mathcal{R}(2,m)]$ for $m = 2, 3, 4, 5$

Theorem 3.3: For $m = 2, 3, 4, 5$, the optimum distance profiles of $\mathcal{R}(2, m)$ are given as follows.

$$\begin{aligned}
\text{ODP}[\mathcal{R}(2,2)] &= [1,2,2,4],\\
\text{ODP}[\mathcal{R}(2,3)] &= [2,2,2,4,4,4,8],\\
\text{ODP}[\mathcal{R}(2,4)] &= [4,4,4,4,6,6,8,8,8,8,16],\\
\text{ODP}[\mathcal{R}(2,5)] &= [8,8,8,8,8,12,12,12,12,12,16,16,16,16,16,32].
\end{aligned}$$

Proof: For $m = 2, 3$, according to their weight enumerators and the upper bounds of the minimum distance given in [2] for every dimension k, it is easy to verify the validity of the above optimum distance profiles. In addition, the generator matrices with respect to the optimum distance profile can be build up by basis vectors $[\mathbf{1}, \mathbf{v_1}, \mathbf{v_2}, \mathbf{v_1 v_2}]^{\mathrm{T}}$ for $\mathcal{R}(2,2)$ and basis vectors $[\mathbf{1}, \mathbf{v_1}, \mathbf{v_2}, \mathbf{v_3}, \mathbf{v_1 v_2}, \mathbf{v_1 v_3}, \mathbf{v_2 v_3}]^{\mathrm{T}}$ for $\mathcal{R}(2,3)$ (refer to p. 373 of Ch. 13 in [4]).

When $m = 4$, $\mathcal{R}(2,4)$ is a linear [16,11,4] code. From [2], we have the upper bound d_+ of the minimum distance as shown in Table I, for every dimension k also for every step $i = 11 - k$. Due to Lemma 3.2, the weight set of $\mathcal{R}(2,4)$ is $\{0, 4, 6, 8, 10, 12, 16\}$.

TABLE I
ODP$[\mathcal{R}(2,4)]$

i	0	1	2	3	4	5	6	7	8	9	10
k	11	10	9	8	7	6	5	4	3	2	1
d_+	4	4	4	5	6	6	8	8	8	10	16
ODP$[\mathcal{R}(2,4)]$	**4**	4	4	4	**6**	6	**8**	8	8	8	**16**

We first consider the optimum distance profile in the dictionary order.

- For $0 \le i \le 3$, clearly ODP$[\mathcal{R}(2,4)]^{dic}(i) = 4$, since $\mathcal{R}(2,4)$ does not have any codeword of weight 5.
- For $4 \le i \le 5$, ODP$[\mathcal{R}(2,4)]^{dic}(i) = 6$ is due to the existence of the linear [16, 7, 6] code, which is a sub-code of $\mathcal{R}(2,4)$. The basis vectors $[\mathbf{1}, \mathbf{v_1}, \mathbf{v_2}, \mathbf{v_3}, \mathbf{v_4}, \mathbf{v_1 v_2} + \mathbf{v_3 v_4}, \mathbf{v_1 v_2} + \mathbf{v_2 v_4} + \mathbf{v_1 v_3}]^{\mathrm{T}}$ build up a generator matrix of this code.
- By Lemma 3.1, the linear code $[16, 5, 8]$ is unique. It is $\mathcal{R}(1,4)$ and is a sub-code of the linear [16,7,6] code. Therefore, ODP$[\mathcal{R}(2,4)]^{dic}(\{6,7,8,9,10\}) =$ ODP$[\mathcal{R}(1,4)]^{dic}$.

Now we proceed to the optimum distance profile in the inverse dictionary order.

- Clearly ODP$[\mathcal{R}(2,4)]^{inv}(10) = 16$ and ODP$[\mathcal{R}(2,4)]^{inv}(9) = 8$.
- For $0 \le i \le 8$, we have ODP$[\mathcal{R}(2,4)]^{inv}(i) =$ ODP$[\mathcal{R}(2,4)]^{dic}(i)$, due to the facts that the linear [16, 7, 6] is a super-code of $\mathcal{R}(1,4)$; they both contain the all-one codeword and achieve the largest possible minimum distance.

When $m = 5$, $\mathcal{R}(2,5)$ is a linear [32,16,8] code. Its weight set is $\{0, 8, 12, 16, 20, 24, 32\}$ due to Lemma 3.2. From [2], we have the upper bound d_+ of the minimum distance as shown in Table II, for every dimension k also for every step $i = 16 - k$. The optimum distance profiles in both orders follow from the weight possibilities of the

TABLE II
ODP$[\mathcal{R}(2,5)]$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
k	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
d_+	8	8	9	10	10	12	12	12	13	14	16	16	16	18	21	32
ODP$[\mathcal{R}(2,5)]$	**8**	8	8	8	8	**12**	12	12	12	12	**16**	16	16	16	16	**32**

codewords (thus the possible minimum distances), the uniqueness of the [32,6,16] code (i.e., $\mathcal{R}(1,5)$) by Lemma 3.1, and the existence of a [32,11,12] code (refer to [5]) as a sub-code of $\mathcal{R}(2,5)$ and a sup-code of $\mathcal{R}(1,5)$. ■

Remark:

- Note that there is a linear [16,2,10] code, which is a sub-code of the [16,7,6] code mentioned above. It can be generated by basis vectors $[\mathbf{1} + \mathbf{v_1 v_2} + \mathbf{v_3 v_4}, \mathbf{1} + \mathbf{v_1 v_2} + \mathbf{v_2 v_4} + \mathbf{v_1 v_3} + \mathbf{v_1} + \mathbf{v_2}]^{\mathrm{T}}$. However, it is not a sub-code of $\mathcal{R}(1,4)$. As a consequence, this $[16, 2, 10]$ code does not belong to the sub-code chain corresponding

to the ODP$[\mathcal{R}(2,4)]^{dic}$. In fact, the sub-codes of C in the sub-code chain with respect to ODP$[C]$ are often not the optimal sub-codes of C.

- Currently, a [32,10,12] sub-code of $\mathcal{R}(2,5)$ is used in the TFCI coding in WCDMA systems. An easy improvement can be done by extending it to a [32,11,12] sub-code of $\mathcal{R}(2,5)$. From the perspective of their distance profile, the performance is bettered in the sense that, the new scheme is adaptive to more possibilities of the information bits without weakening the error-correcting capabilities.

B. General results on ODP$[\mathcal{R}(2,m)]$

For a given $[n,k,d]$ binary code, the number of its sub-code chains is $\prod_{t=2}^{k}(2^t-1) > 2^{k(k-1)/2}$. When m is small, one can resort to a brute-force search to find ODP$[\mathcal{R}(2,m)]$ easily. However, as m increases, the running time of the brute-force search increases exponentially, e.g.: when $m=6$, there are more than 2^{231} possible sub-code chains. It will take too long to produce a valid result. In addition, it is still an open problem to find the optimal sub-codes of a linear code. Therefore, a good bound with constructive sub-code chain is desirable. In this subsection, we give a general lower bound on ODP$[\mathcal{R}(2,m)]$. The corresponding sub-code chain follows from the constructive proofs of Theorem 3.5 and Theorem 3.6.

Theorem 3.4: For the ODP$[\mathcal{R}(2,m)]$, a lower bound ODP$[\mathcal{R}(2,m)]_{low}$ is given as follows:

If $m=2t+1$ is odd,

$$\text{ODP}[\mathcal{R}(2,m)]_{low}(i) = \begin{cases} 2^{m-1}-2^{m-h-1} & \text{for } (h-1)m \le i < hm \ \&\ 1 \le h \le t, \\ 2^{m-1} & \text{for } tm \le i < (t+1)m, \\ 2^m & \text{for } i = (t+1)m; \end{cases}$$

If $m=2t+2$ is even,

$$\text{ODP}[\mathcal{R}(2,m)]_{low}(i) \begin{cases} 2^{m-1}-2^{m-h-1} & \text{for } (h-1)m \le i < hm \ \&\ 1 \le h \le t, \\ 2^{m-1}-2^{m/2-1} & \text{for } tm \le i < tm+m/2, \\ 2^{m-1} & \text{for } i \ge tm+m/2 \ \&\ i < tm+3m/2, \\ 2^m & \text{for } i = tm+3m/2. \end{cases}$$

The generator matrices with respect to ODP$[\mathcal{R}(2,m)]_{low}$ can be

$$m=2t+1 \qquad\qquad m=2t+2$$

$$\begin{pmatrix} \theta_0^* & 1 \\ \theta_1^* & 0 \\ x\theta_1^* & 0 \\ \vdots & \vdots \\ x^{m-1}\theta_1^* & 0 \\ \theta_{l_t}^* & 0 \\ \vdots & \vdots \\ x^{m-1}\theta_{l_t}^* & 0 \\ \theta_{l_{t-1}}^* & 0 \\ \vdots & \vdots \\ x^{m-1}\theta_{l_{t-1}}^* & 0 \\ \theta_{l_{t-2}}^* & 0 \\ \vdots & \vdots \\ x^{m-1}\theta_{l_1}^* & 0 \end{pmatrix}, \qquad \begin{pmatrix} \theta_0^* & 1 \\ \theta_1^* & 0 \\ x\theta_1^* & 0 \\ \vdots & \vdots \\ x^{m-1}\theta_1^* & 0 \\ \theta_{l_{t+1}}^* & 0 \\ \vdots & \vdots \\ x^{m/2-1}\theta_{l_{t+1}}^* & 0 \\ \theta_{l_t}^* & 0 \\ \vdots & \vdots \\ x^{m-1}\theta_{l_t}^* & 0 \\ \theta_{l_{t-1}}^* & 0 \\ \vdots & \vdots \\ x^{m-1}\theta_{l_1}^* & 0 \end{pmatrix},$$

where $\theta_{l_j}^*$ is the primitive idempotent for $l_j = 1+2^j$, $1 \le j \le \lfloor m/2 \rfloor$. For the definition of the primitive idempotent, one can refer to Ch. 8 in [4].

It is easy to verify that the above bound gives the optimum distance profiles of $\mathcal{R}(2,m)$ for $m \le 5$. For $m=6,7,8$, we will evaluate its performance in the next subsection. The proof of the above theorem follows directly from the following theorems and lemmata.

Theorem 3.5: (See Corollary 17 in Ch. 15 in [4].) Let $m = 2t+1$ be odd, and let h be any number in the range $1 \le h \le t$. Then there exists a

$$[2^m, m(t-h+2)+1, 2^{m-1} - 2^{m-h-1}]$$

sub-code $\mathcal{R}^h_{2t+1}$ of $\mathcal{R}(2,m)$. It is obtained by extending the cyclic sub-code of $\mathcal{R}(2,m)^*$ having idempotent

$$\theta_0 + \theta_1^* + \sum_{j=h}^{t} \theta_{l_j}^*, \quad l_j = 1 + 2^j.$$

The code has codewords of weights 2^{m-1} and $2^{m-1} \pm 2^{m-h'-1}$ for all h' in the range $h \le h' \le t$.

Theorem 3.6: Let $m = 2t+2$ be even, and let h be any number in the range $1 \le h \le t+1$. Then there exists a

$$[2^m, m(t-h+2)+m/2+1, 2^{m-1} - 2^{m-h-1}]$$

sub-code $\mathcal{R}^h_{2t+2}$ of $\mathcal{R}(2,m)$. It is obtained by extending the cyclic sub-code of $\mathcal{R}(2,m)^*$ having idempotent

$$\theta_0 + \theta_1^* + \sum_{j=h}^{t+1} \theta_{l_j}^*, \quad l_j = 1 + 2^j.$$

The code has codewords of weights 2^{m-1} and $2^{m-1} \pm 2^{m-h'-1}$ for all h' in the range $h \le h' \le t+1$.

Proof: Please refer to Appendix A for the proof. ■

Corollary 3.7:

$$\mathcal{R}^t_{2t+1} \subset \mathcal{R}^{t-1}_{2t+1} \subset \cdots \subset \mathcal{R}^1_{2t+1};$$
$$\mathcal{R}^{t+1}_{2t+2} \subset \mathcal{R}^t_{2t+2} \subset \cdots \subset \mathcal{R}^1_{2t+2}.$$

Proof: Please refer to Appendix B for the proof. ■

Theorem 3.8: (See Proposition 14 in [5].) For odd m, the linear $[2^m, 2m+1, 2^{m-1} - 2^{(m-1)/2}]$ code C with $\mathcal{R}(1,m) \subset C \subset \mathcal{R}(2,m)$, whose weight set is $\{0, 2^{m-1} - 2^{(m-1)/2}, 2^{m-1}, 2^{m-1} + 2^{(m-1)/2}, 2^m\}$, is optimal in the sense that no codes exist with the same length and weight set, but with dimension $> 2m+1$.

As a parallel result of Theorem 3.8 for odd m, we have

Theorem 3.9: For even m, if the linear $[2^m, 1+3m/2, 2^{m-1} - 2^{m/2-1}]$ code is self-complementary, then it is minimum distance optimal.

Proof: Let C be a self-complementary linear $[2^m, 1+3m/2, 2^{m-1} - 2^{m/2-1}]$ code. Suppose that the minimum distance d for given length $n = 2^m$ and dimension $k = 1 + 3m/2$ can be larger. That is,

$$d = 2^{m-1} - 2^{m/2-1} + \delta,$$

where δ is a positive integer and $0 < \delta < 2^{m/2-1}$. Due to the Grey-Rankin bound (refer to (46) of Ch. 17 in [4]), we have

$$\begin{aligned} |C| &\le \frac{8d(n-d)}{n-(n-2d)^2} \\ &= \frac{8(2^{m-1} - 2^{m/2-1} + \delta)(2^{m-1} + 2^{m/2-1} - \delta)}{2^m - (2^{m/2} - 2\delta)^2} \\ &= 2 + \frac{2^{m-1}(2^m - 1)}{\delta(2^{m/2} - \delta)} \\ &\overset{(a)}{\le} 2^{3m/2-1} + 2^{m-1} + 2, \end{aligned}$$

where (a) follows from the fact that $\delta(2^{m/2} - \delta) \ge 2^{m/2} - 1$. However, as a contrary, we have $|C| = 2^{1+3m/2} > 2^{3m/2-1} + 2^{m-1} + 2$ for even $m > 0$. Thus we conclude the proof. ■

From Theorem 3.8 and Theorem 3.9, we have the following corollary.

Corollary 3.10:

$$\text{ODP}[\mathcal{R}(2,m)]^{inv}(I) = \text{ODP}[\mathcal{R}(2,m)]_{low}(I),$$

where

$$I = \begin{cases} \{i : \frac{m(m-5)}{2} \le i \le \frac{m(m+1)}{2}\}, & \text{for } m \text{ odd}, \\ \{i : \frac{m(m-2)}{2} \le i \le \frac{m(m+1)}{2}\}, & \text{for } m \text{ even}. \end{cases}$$

TABLE III
A LOWER BOUND OF ODP$[\mathcal{R}(2,6)]$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
k	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
d_-	18	18	19	20	22	22	24	24	24	24	25	26	28	28	28	32	32	32	33	36	42	64
ODP$_{low}$	**16**	16	16	16	16	16	**24**	24	24	24	24	24	**28**	28	28	**32**	32	32	32	32	32	**64**
d_+	20	21	22	22	22	24	24	24	25	26	26	27	28	28	28	32	32	32	33	36	42	64

C. ODP$[\mathcal{R}(2,m)]$ for $m = 6, 7, 8$

For $m = 6, 7, 8$, by Theorem 3.4 and the bounds of the minimum distance given in [2] for given code length n and dimension k, we have Table III, IV and V. For given n, k, d_- is the largest minimum distance of which a linear code has been discovered so far, and d_+ is the upper bound of the minimum distance. In particular, we have the following theorem.

Theorem 3.11:

$$\text{ODP}[\mathcal{R}(2,6)] = \text{ODP}[\mathcal{R}(2,6)]_{low};$$
$$\text{ODP}[\mathcal{R}(2,7)] = \text{ODP}[\mathcal{R}(2,7)]_{low}.$$

Proof: When $m = 6$, $\mathcal{R}(2,6)$ is a [64,22,16] linear code. Due to Lemma 3.2, its weight set is {0, 16, 24, 28, 32, 36, 40, 48, 64}. We can easily verify the validity of most ODP$[\mathcal{R}(2,6)](i)$, where $0 \le i \le 21$, directly from Table III, according to the weight possibilities of the codewords (thus the possible minimum distances). In fact, we only need to prove that ODP$[\mathcal{R}(2,6)](5) = 16$ but not 24.

First we consider the ODP in the inverse dictionary order and show that ODP$[\mathcal{R}(2,6)]^{inv}(5) = 16$. We suppose that there is a [64,17,24] linear code, which is a sup-code of $\mathcal{R}(1,6)$ and a sub-code of $\mathcal{R}(2,6)$. Due to Lemma 3.12, its dual code has minimum distance 8. Furthermore, by Lemma 2.1, there exists a $[40, 16, d^0]$ residue code of the [64,17,24] linear code, where $d^0 \ge 12$ and this residue code is still self-complementary. According to the upper bound of the minimum distance given for a linear code of length 40 and dimension 16 by [2], we have $d^0 \le 12$. Thus $d^0 = 12$. Note that the [64,17,24] code is doubly even. By Corollary 2.4, the residue code [40,16,12] is an even code. Thus, this [40,16,12] code is a self-complementary even code. By Corollary 2.2, it has a dual code with parameters $[40, 24, \ge 8]$. However, such a [40,16,12] code does not actually exist by Lemma 3.13.

Now let us consider the ODP in the dictionary order and show that ODP$[\mathcal{R}(2,6)]^{dic}(5) = 16$. To do that, we need to prove that there is no [64,17,24] linear code, which is a sub-code of $\mathcal{R}(2,6)$. In fact, the arguments for ODP$[\mathcal{R}(2,6)]^{inv}(5) = 16$ have shown that there is no [64,17,24] sub-code of $\mathcal{R}(2,6)$, which is self-complementary. Here we only need to consider the nonexistence of the [64,17,24] sub-code of $\mathcal{R}(2,6)$, which is not self-complementary, i.e., whose weight set is $\{0, 24, 28, 32, 36, 40, 48\}$. Due to Lemma 3.14, such codes do not exist either.

When $m = 7$, $\mathcal{R}(2,7)$ is a [128,29,32] linear code. Due to Lemma 3.2, it has weight set {0, 32, 48, 56, 64, 72, 80, 96, 128}. We can easily verify the validity of most ODP$[\mathcal{R}(2,7)](i)$, where $0 \le i \le 28$, directly from Table IV, according to the weight possibilities of the codewords (thus the possible minimum distances). In fact, we only need to prove that ODP$[\mathcal{R}(2,7)](6) = 32$ and ODP$[\mathcal{R}(2,7)](13) = 48$.

First we consider the ODP in the inverse dictionary order. We need to show that ODP$[\mathcal{R}(2,7)]^{inv}(6) = 32$ and ODP$[\mathcal{R}(2,7)]^{inv}(13) = 48$. Note that the former statement follows from Lemma 3.18, which shows that there does not exist a self-complementary [128,23,48] code, which is a sub-code of $\mathcal{R}(2,7)$; and the latter statement follows from Theorem 3.8, which shows that there does not exist a [128,16,56] code, which is a sup-code of $\mathcal{R}(1,7)$ and a sub-code of $\mathcal{R}(2,7)$.

Now let us consider the ODP in the dictionary order. In order to show that ODP$[\mathcal{R}(2,7)]^{dic}(6) = 32$ and ODP$[\mathcal{R}(2,7)]^{dic}(13) = 48$, we need to prove that there is no [128,23,48] and [128, 16, 56] linear codes, which are sub-codes (not necessarily self-complementary) of $\mathcal{R}(2,6)$. Note that the nonexistence of the [128,23,48] sub-codes follows from Lemma 3.18 and Lemma 3.19; and the nonexistence of the [128, 16, 56] sub-codes follows from Theorem 3.8 and Lemma 3.15. ■

Lemma 3.12: If there exists a binary self-complementary [64,17,24] code which is a sub-code of $\mathcal{R}(2,6)$, then its weight enumerator is $1 + 10416t^{24} + 23808t^{28} + 62622t^{32} + 23808t^{36} + 10416t^{40} + t^{64}$ and its dual code has minimum distance 8.

TABLE IV
A LOWER BOUND OF ODP$[\mathcal{R}(2,7)]$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
k	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9
d_-	44	44	44	44	44	44	44	48	48	48	48	48	49	52	56	56	56	56	57	60	60
ODP$_{low}$	**32**	32	32	32	32	32	32	**48**	48	48	48	48	48	48	**56**	56	56	56	56	56	56
d_+	48	48	48	49	50	50	50	52	52	53	54	54	55	56	56	57	58	58	60	60	61

i	21	22	23	24	25	26	27	28
k	8	7	6	5	4	3	2	1
d_-	64	64	64	64	68	72	85	128
ODP$_{low}$	**64**	64	64	64	64	64	64	**128**
d_+	64	64	64	64	68	72	85	128

Proof: Suppose that there exists a linear [64,17,24] self-complementary code, which is a sub-code of $\mathcal{R}(2,6)$. Then due to Lemma 3.2, its weight set is $\{0, 24, 28, 32, 36, 40, 64\}$. Let $\{A_i, 0 \le i \le 64\}$ be its weight distribution and $\{B_i, 0 \le i \le 64\}$ be the weight distribution of its dual code. Applying the MacWilliams identities, we have the following linear equations.

$$\begin{aligned}
&2^{17}B_0 = 2 + 2A_{24} + 2A_{28} + A_{32};\\
&2^{12}B_2 = 126 + 6A_{24} - A_{32};\\
&2^{13}B_4 = 79422 - 98A_{24} - 42A_{28} + 31A_{32};\\
&2^{12}B_6 = 4685898 - 286A_{24} + 336A_{28} - 155A_{32};\\
&2^{17}B_8 = 88523306 + 181488A_{24} - 91152A_{28} + 35960A_{32}.
\end{aligned}$$

Note that $B_0 = 1$ and $B_2 = 0$. Eliminating A_{24}, A_{28} and A_{32} from the first four linear equations, we have $20B_4 + B_6 = 0$. Thus $B_4 = B_6 = 0$. Easy calculations give $A_{24} = A_{40} = 10416$, $A_{28} = A_{36} = 23808$, $A_{32} = 62622$ and $B_8 = 82584$. ■

Lemma 3.13: There does not exist a binary [40,16,12] self-complementary even code whose dual code has minimum distance at least 8.

Proof: Assume that there is a binary [40,16,12] self-complementary even code C whose dual code $C^\perp$ has minimum distance at least 8. Due to Lemma 2.5, $C^\perp$ is also a self-complementary even code. Let $\{A_i, 0 \le i \le 40\}$ be the weight distribution of C and $\{B_i, 0 \le i \le 40\}$ be the weight distribution of $C^\perp$. Applying the MacWilliams identities for C and $C^\perp$ respectively, we have the following two matrix equations.

$$2^{16}\begin{pmatrix}1\\0\\0\\0\\B_8\end{pmatrix} = P\begin{pmatrix}1\\A_{12}\\A_{14}\\A_{16}\\A_{18}\\A_{20}\end{pmatrix} \quad \text{and} \quad 2^{24}\begin{pmatrix}1\\0\\0\\0\\0\\A_{12}\end{pmatrix} = Q\begin{pmatrix}1\\B_8\\B_{10}\\B_{12}\\B_{14}\\B_{16}\\B_{18}\\B_{20}\end{pmatrix},$$

where

$$P = \begin{pmatrix}
2 & 2 & 2 & 2 & 2 & 1\\
390 & 54 & 26 & 6 & -6 & -5\\
91390 & 446 & -338 & -258 & 46 & 95\\
1919190 & -3066 & -182 & 854 & 42 & -285\\
153809370 & 21978 & 19162 & -11814 & -3366 & 4845
\end{pmatrix},$$

and

$$Q = \begin{pmatrix} 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 \\ 390 & 134 & 90 & 54 & 26 & 6 & -6 & -5 \\ 91390 & 8446 & 2990 & 446 & -338 & -258 & 46 & 95 \\ 1919190 & 28630 & -630 & -3066 & -182 & 854 & 42 & -285 \\ 153809370 & -118310 & -132390 & 21978 & 19162 & -11814 & -3366 & 4845 \\ 105957566 & -91202 & 15938 & 5038 & -4862 & 1342 & 1122 & -969 \\ 1396713370 & 199578 & 66410 & -49958 & 18538 & -614 & -7446 & -4845. \end{pmatrix}.$$

Solving above equations, we have

$$\begin{pmatrix} A_{12} \\ A_{14} \\ A_{16} \\ A_{18} \\ A_{20} \end{pmatrix} = \begin{pmatrix} 0 \\ 10160 \\ -18265 \\ 63440 \\ -45136 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} B_8 \\ B_{10} \\ B_{12} \\ B_{14} \\ B_{16} \\ B_{18} \\ B_{20} \end{pmatrix} = \begin{pmatrix} 2015 \\ 35880 \\ 110500 \\ 908680 \\ 1472640 \\ 4165200 \\ 3387384 \end{pmatrix}.$$

We note that $A_{16} = -18265$ and $A_{20} = -45136$. This contradicts the fact that they are non-negatives. Thus we complete the proof. ■

Lemma 3.14: There does not exist a binary [64,17,24] code with weight set $\{0, 24, 28, 32, 36, 40, 48\}$.

Proof: Suppose that there exists a linear [64,17,24] code, whose weight set is $\{0, 24, 28, 32, 36, 40, 48\}$. Let $\{A_i, 0 \leq i \leq 48\}$ be its weight distribution and $\{B_i, 0 \leq i \leq 64\}$ be the weight distribution of its dual code. Applying the MacWilliams identities, we have the following matrix equation.

$$2^{17} \begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \\ B_6 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 64 & 16 & 8 & 0 & -8 & -16 & -32 \\ 2016 & 96 & 0 & -32 & 0 & 96 & 480 \\ 41664 & 176 & -168 & 0 & 168 & -176 & -4448 \\ 635376 & -784 & -336 & 496 & -336 & -784 & 28144 \\ 7624512 & -4656 & 1512 & 0 & -1512 & 4656 & -125856 \\ 74974368 & -4576 & 5376 & -4960 & 5376 & -4576 & 389792 \end{pmatrix} \begin{pmatrix} A_0 \\ A_{24} \\ A_{28} \\ A_{32} \\ A_{36} \\ A_{40} \\ A_{48} \end{pmatrix}.$$

Easy calculation gives

$$\begin{pmatrix} 4/3 & 2/3 & 197/1008 & 5/63 & 5/252 & 1/189 & 1/1008 \\ 10192 & 2828 & 8999/12 & 433/3 & 71/3 & 10/9 & -5/12 \\ 24832 & 1952 & -6596/7 & -2512/7 & -656/7 & -48/7 & 12/7 \\ 60732 & 1890 & 5471/16 & 225 & 543/4 & 15 & -45/16 \\ 76544/3 & -14048/3 & -7580/9 & 304/9 & -752/9 & -400/27 & 20/9 \\ 9744 & -1932 & 2737/4 & -38 & 17 & 6 & -3/4 \\ 56 & -56 & 197/24 & -20/3 & 5/6 & -4/9 & 1/24 \end{pmatrix} \begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \\ B_6 \end{pmatrix} = \begin{pmatrix} A_0 \\ A_{24} \\ A_{28} \\ A_{32} \\ A_{36} \\ A_{40} \\ A_{48} \end{pmatrix}.$$

From the first row of the above matrix equation, we have

$$4B_0/3 + 2B_1/3 + 197B_2/1008 + 5B_3/63 + 5B_4/252 + B_5/189 + B_6/1008 = A_0,$$

which is impossible due to the fact that $A_0 = B_0 = 1$ and $B_i, 1 \leq i \leq 6$ are non-negatives. This concludes our proof. ■

Using similar method as given in the proof of Lemma 3.14, we have the following lemmata.

Lemma 3.15: There does not exist a [128,16,56] code with weight set $\{0, 56, 64, 72, 80, 96\}$.

Lemma 3.16: There does not exist a [127,23,48] code with weight set $\{0, 48, 56, 64, 72, 80, 96\}$.

Lemma 3.17: There does not exist a [126,22,48] code with weight set $\{0, 48, 56, 64, 72, 80, 96\}$.

Lemma 3.18: There does not exist a self-complementary [128,23,48] code, which is a sub-code of $\mathcal{R}(2, 7)$.

TABLE V
A LOWER BOUND OF ODP$[\mathcal{R}(2,8)]$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
k	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22
d_-	92	92	92	92	96	96	96	96	96	96	96	98	100	100	104	104
ODP$_{low}$	**64**	64	64	64	64	64	64	64	**96**	96	96	96	96	96	96	96
d_+	107	108	108	108	108	108	109	110	111	112	112	113	114	114	115	116

i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
k	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
d_-	112	112	112	112	112	113	114	114	120	120	120	123	128	128	128	128	131	136	146	170	256
ODP$_{low}$	**112**	112	112	112	112	112	112	112	**120**	120	120	120	**128**	128	128	128	128	128	128	128	**256**
d_+	116	117	118	118	120	120	120	121	122	123	124	124	128	128	128	128	131	136	146	170	256

Lemma 3.19: There does not exist a linear [128,23,48] code with weight set $\{0, 48, 56, 64, 72, 80, 96\}$.

Proof: Suppose that there exists a linear [128,23,48] code with weight set $W = \{0, 48, 56, 64, 72, 80, 96\}$. The j-th element of W is denoted to be $W(j)$, where $1 \leq j \leq 7$. Let $\{A_i, 0 \leq i \leq 96\}$ be its weight distribution and $\{B_i, 0 \leq i \leq 128\}$ be the weight distribution of its dual code. First we will show that $B_1 = B_2 = 0$. Suppose that $B_1 \neq 0$. Then one can construct a linear [127,23,48] code with weight set W, which is contrary to Lemma 3.16. Thus we prove that $B_1 = 0$. Further we assume that $B_2 \neq 0$. Then one can construct a linear [126,22,48] code with weight set W, which is impossible due to Lemma 3.17. So we have also $B_2 = 0$.

Now applying the MacWilliams identities, we have the following matrix equation.

$$2^{23} \begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \\ B_6 \\ B_7 \end{pmatrix} = P \begin{pmatrix} A_0 \\ A_{48} \\ A_{56} \\ A_{64} \\ A_{72} \\ A_{80} \\ A_{96} \end{pmatrix},$$

where P is a matrix, whose element in i-th row, j-th column is the value of Krawtchouk polynomial $P_i(128, W(j))$, where $1 \leq i \leq 8$ and $1 \leq j \leq 7$. Due to the fact that $B_0 = 1$ and $B_1 = B_2 = 0$, easy calculations give

$$\begin{pmatrix} B_6 \\ B_7 \end{pmatrix} = \begin{pmatrix} -1680 \\ 9216 \end{pmatrix} + \begin{pmatrix} 32/3 & -20 & -32/3 \\ -1391/3 & 0 & 197/3 \end{pmatrix} \begin{pmatrix} B_3 \\ B_4 \\ B_5 \end{pmatrix}.$$

Thus $7B_6 + B_7 = -2544 - 3949/3B_3 - 140B_4 - 9B_5$, which is impossible due to the fact that $B_i, 3 \leq i \leq 7$ are non-negatives. This concludes our proof. ■

Remarks:

- For $m = 6, 7$, we show that our lower bound is still tight. Comparing the proofs for ODP$[\mathcal{R}(2,m)]^{inv}$ and ODP$[\mathcal{R}(2,m)]^{dic}$, we see that for ODP$[\mathcal{R}(2,m)]^{inv}$, the sub-codes we need to consider are self-complementary and have a symmetric weight distribution. But for ODP$[\mathcal{R}(2,m)]^{dic}$, the sub-codes we need to consider are not necessary self-complementary, which increases the difficulty of the nonexistence proof.
- So far, we have shown that the lower bound given in Theorem 3.4 is tight for $m \leq 7$. In particular, it is easy to verify that most codes in the sub-code chain with respect to the ODP$[\mathcal{R}(2,m)], m \leq 7$ are optimal sub-codes of $\mathcal{R}(2,m)$. When $m = 8$, our lower bound on ODP behaves still quite well especially for $i \geq 8$. As can be seen in Table V, the sub-codes constructed due to Theorem 3.6 achieve the minimum distances very close (limited by its weight possibilities) or equal to d_-. Here d_- is the largest minimum distance, of which a linear code (not necessarily a sub-code of $\mathcal{R}(2,m)$) with the same length and dimension has been discovered up to now.

IV. Conclusion

So far the optimum distance profiles have been investigated for the generalized Reed-Solomon code, the Golay code, the first order Reed-Muller code in [1] and the second order Reed-Muller code in this paper. The desirable property opens a new research field in coding theory from a more practical perspective. Our results serve plenty of alternatives for the applications requiring high error-correcting capability for variable information bits, such as TFCI coding and coding for informed decoders. This research involves the following problems: (a) the weight distribution of a linear code (b) (minimum distance) optimal sub-code or sup-code of a linear code (c) the uniqueness of the weight distribution of certain linear codes (d) nonexistence of certain linear codes (e) the lower and upper bounds on the minimum distance (f) efficient brute-force search algorithm, etc. Many of them are still open problems.

In this paper, we give a lower bound of the optimum distance profiles of the second order Reed-Muller codes. We show that our bound is tight, in both orders for the code of length ≤ 128. In order to support our result, we review the first order and the second order Reed-Muller codes. In particular, for the second order Reed-Muller code $\mathcal{R}(2,m)$, we give a linear sub-code family for even m, which is an extension of Corollary 17 of Ch. 15 in [4]. In Appendix D, we compare our linear sub-code family to the nonlinear sub-code family given in [4], especially the linear sub-code $\mathcal{R}_m^{m/2}$ to the Kerdock code $\mathcal{K}(m)$. As a byproduct, we obtain an additive commutative group of $m \times m$ symplectic matrices. This matrix group has an all-zero matrix as its identity element and other elements are symplectic matrices of full rank. In this group, the inverse of each element is itself. In particular, except the identity element, the symplectic matrices of full rank, preserve full rank under matrix addition. Such a matrix group preserving full rank under matrix addition is new to our knowledge.

Reed-Muller code $\mathcal{R}(r,m), 0 \leq r \leq m$ is one of the important linear codes. The first order Reed-Muller code $\mathcal{R}(1,m)$ is the dual of the extended Hamming code. When $r = m-2$, it is the extended Hamming code. Besides, the Reed-Muller code $\mathcal{R}(r,m)$ is a sub-code of the extended BCH code of designed distance $2^{m-r}-1$. Therefore, research on the optimum distance profile of the Reed-Muller code will also shed lights on the research problem for the Hamming codes and BCH codes. Besides, Reed-Muller code enjoys a nested structure: each Reed-Muller code is a sub-code of the Reed-Muller code of a higher order. Therefore, the minimum distances of the Reed-Muller codes from order m to order 0 and their sub-codes build up a lower bound of the optimum distance profile of the whole space. The generator matrix of $\mathcal{R}(m,m)$ with respect to this lower bound has the property that for $0 \leq r \leq m$, its first $\sum_{i=0}^{r} \binom{m}{i}$ basis rows form a generator matrix of $\mathcal{R}(r,m)$. Note that those codes generated by the first k basis rows, where $\sum_{i=0}^{r} \binom{m}{i} < k < \sum_{i=0}^{r+1} \binom{m}{i}$, are sup-codes of $\mathcal{R}(r,m)$ and sub-codes of $\mathcal{R}(r+1,m)$. They have minimum distances equal to or larger than 2^{m-r-1} and in this lower bound we take value 2^{m-r-1}. Therefore, this lower bound is a nondecreasing sequence of length 2^m, with $\binom{m}{r}$ elements of value 2^r, for each $0 \leq r \leq m$. For instance, the lower bound is $[1,2,2,2,4,4,4,8]$ for $\mathcal{R}(3,3)$ and $[1,2,2,2,2,4,4,4,4,4,4,8,8,8,8,16]$ for $\mathcal{R}(4,4)$.

The last but not least. It deserves mentioning that the concept of the partial distances of a matrix defined in [10], can be considered as a distance profile of the linear code generated by the matrix. Furthermore, the authors of [10] have shown that the partial distances of a matrix completely characterize the rate of the polarization of the corresponding Polar code. Thus known results on the distance profile of the linear codes can be applied to construct Polar codes with good polarizing exponents. In particular, if we construct Polar codes by the generator matrices of the nested structured $\mathcal{R}(m,m)$, then we can use the lower bound on the distance profile of $\mathcal{R}(m,m)$ derived in the last paragraph to calculate their exponents according to Theorem 14 in [10]. Interestingly, this lower bound leads to an exponent $1/2$, which is valid for all $\mathcal{R}(m,m)$. This implies that the Polar codes constructed by $\mathcal{R}(m,m)$ of nested structure achieve exponents always $\geq 1/2$. Note that one can improve the lower bound by applying our results on $\mathcal{R}(2,m)$ and thus even better the exponent. For instance, one can easily improve the lower bound on the distance profile of $\mathcal{R}(4,4)$ to $[1,2,2,2,2,4,4,4,4,6,6,8,8,8,8,16]$ according to Table I, and thus achieves the exponent 0.51828. In [10], this exponent 0.51828 is shown to be the best possible exponent for all Polar codes constructed by 16×16 matrices based on an exhaustive search. So far, we can say that the nested structured Reed-Muller code $\mathcal{R}(m,m)$ is not a bad candidate for a Polar code with a good exponent, especially as m is small.

APPENDIX A

The second order binary Reed-Muller code $\mathcal{R}(2,m)$ is the set of all vectors f, where $f(v_1,\cdots,v_m)$ is a Boolean function of degree ≤ 2. A typical codeword of $\mathcal{R}(2,m)$ is given by the Boolean function

$$\begin{aligned} S(v) &= \sum_{1\leq i\leq j\leq m} q_{ij}v_iv_j + \sum_{1\leq i\leq m} u_iv_i + \epsilon \\ &= vQv^T + Lv^T + \epsilon, \end{aligned}$$

where $v=(v_1,\cdots,v_m)$, $Q=(q_{ij})$ is an upper triangular binary matrix, $L=(u_1,\cdots,u_m)$ is a binary vector and ϵ is 0 or 1. Note that for fixed Q, $S(v)$ runs through a coset of $\mathcal{R}(1,m)$ in $\mathcal{R}(2,m)$. This coset is characterized by Q, or alternatively by the matrix $B=Q+Q^T$. B is a binary symmetric matrix with zero diagonal, which is called *symplectic matrix*. The *symplectic form* associated with B, as defined by equation (4) of Ch. 15 in [4], is

$$\begin{aligned} \mathcal{B}(u,v) &= u(Q+Q^{\mathrm{T}})v^{\mathrm{T}} \\ &= S(u+v)+S(u)+S(v)+\epsilon. \end{aligned}$$

By Theorem 5 at Ch. 15 in [4], the weight distribution of the coset associated with $\mathcal{B}$ depends only on the rank of the matrix B.

The proof of Theorem 3.6 is similar to the proof of Theorem 3.5, but with more delicate treatment of the cyclotomic sets. Recall that a *cyclotomic coset* containing s is defined to be

$$\mathrm{C}_s=\{s,2s,2^2s,2^3s,\cdots,2^{m_s-1}s\},$$

where m_s is the smallest positive integer such that $2^{m_s}\cdot s\equiv s(\mathrm{mod}\ 2^m-1)$. Let

$$T_{m_s}(\gamma)=\gamma+\gamma^2+\gamma^{2^2}+\cdots+\gamma^{2^{m_s-1}}.$$

If $\gamma\in GF(2^{m_s})$, then it is called the *trace* of γ from $GF(2^{m_s})$ to $GF(2)$. Recall that a *primitive idempotent* θ_s is defined by the property

$$\theta_s(\alpha^j)=\begin{cases} 1 & \text{if } j\in \mathrm{C}_s, \\ 0 & \text{otherwise.}\end{cases}$$

The punctured second order Reed-Muller code $\mathcal{R}(2,m)^*$ is generated by idempotent

$$\theta_0+\theta_1^*+\sum_{i=1}^{[\frac{m}{2}]}\theta_{l_i}^*, \quad l_j=1+2^j.$$

Similar to the proof of Theorem 3.5 given in [4], we first consider the punctured second order Reed-Muller code $\mathcal{R}(2,m)^*$. For a general codeword of $\mathcal{R}(2,m)^*$, we analyze its Mattson-Solomon polynomial and corresponding symplectic form. By setting the parameters of the general codeword differently, we obtain a family of sub-codes of $\mathcal{R}(2,m)^*$ of a nested structure. At the end, we derive a sub-code family of $\mathcal{R}(2,m)$ for even m by extending the sub-code family of $\mathcal{R}(2,m)^*$. The detailed proof of Theorem 3.6 is given as follows.

Proof: Let $m=2t+2$. A general codeword of $\mathcal{R}(2,m)^*$ is

$$b\theta_0+a_0x^{i_0}\theta_1^*+\sum_{j=1}^{t+1}a_jx^{i_j}\theta_{l_j}^*, \quad l_j=1+2^j,$$

where $b,a_0,a_j\in GF(2)$, $0\leq i_k\leq 2^m-2$ for $0\leq k\leq t$ and $0\leq i_{t+1}\leq 2^{m/2}-2$. Consider the case $b=0$. Its Mattson-Solomon polynomial is

$$\sum_{s\in \mathrm{C}_1}(\gamma_0 z)^s+\sum_{j=1}^{t+1}\sum_{s\in \mathrm{C}_{l_j}}(\gamma_j z)^s,$$

where $\gamma_0, \gamma_j \in GF(2^m)$. Due to Theorem 1.2 in [8], the corresponding Boolean function is

$$\begin{aligned} S(\xi) &= \sum_{j=0}^{t+1} T_{|\mathrm{C}_{l_j}|}(\gamma_j \xi)^{l_j} \quad \text{for all } \xi \in GF(2^m)^*, \\ &\overset{(a)}{=} \sum_{j=0}^{t} T_m(\gamma_j \xi)^{1+2^j} + T_{m/2}(\gamma_{t+1}\xi)^{1+2^{t+1}}. \end{aligned}$$

Here (a) is due to Lemma C.2. The corresponding symplectic form is

$$\begin{aligned} \mathcal{B}(\xi,\eta) &= S(\xi+\eta) + S(\xi) + S(\eta) \\ &\overset{(b)}{=} \sum_{j=1}^{t} T_m(\gamma_j^{1+2^j}(\xi\eta^{2^j} + \xi^{2^j}\eta)) + T_{m/2}(\gamma_{t+1}^{1+2^{t+1}}(\xi\eta^{2^{t+1}} + \xi^{2^{t+1}}\eta)) \\ &\overset{(c)}{=} T_m\{\sum_{j=1}^{t}(\gamma_j^{1+2^j}\xi\eta^{2^j} + \gamma_j^{1+2^{2t+2-j}}\xi\eta^{2^{2t+2-j}}) + \gamma_{t+1}^{1+2^{t+1}}\xi\eta^{2^{t+1}}\} \\ &= T_m(\xi L_B(\eta)), \end{aligned}$$

where $\xi, \eta \in GF(2^m)^*$ and

$$L_B(\eta) = \sum_{j=1}^{t} \gamma_j[(\gamma_j\eta)^{2^j} + (\gamma_j\eta)^{2^{2t+2-j}}] + \gamma_{t+1}(\gamma_{t+1}\eta)^{2^{t+1}}.$$

Note that (b) is from the fact that $T_m(\alpha+\beta) = T_m(\alpha) + T_m(\beta)$ and

$$(\xi+\eta)^{1+2^j} = (\xi+\eta)(\xi^{2^j} + \eta^{2^j}) = \xi^{1+2^j} + \xi\eta^{2^j} + \xi^{2^j}\eta + \eta^{1+2^j};$$

(c) is due to the fact that

$$\begin{aligned} T_m(\gamma_j^{1+2^j}\xi^{2^j}\eta) &= T_m(\gamma_j^{1+2^{2t+2-j}}\xi\eta^{2^{2t+2-j}}), \\ T_m(\gamma_{t+1}^{1+2^{t+1}}\xi\eta^{2^{t+1}}) &= T_{m/2}(\gamma_{t+1}^{1+2^{t+1}}(\xi\eta^{2^{t+1}} + \xi^{2^{t+1}}\eta)). \end{aligned}$$

Let $1 \le d \le t+1$ and $\gamma_1 = \gamma_2 = \cdots = \gamma_{d-1} = 0$. Then

$$\begin{aligned} L_B(\eta) &= \sum_{j=1}^{t} \gamma_j[(\gamma_j\eta)^{2^j} + (\gamma_j\eta)^{2^{2t+2-j}}] + \gamma_{t+1}(\gamma_{t+1}\eta)^{2^{t+1}} \\ &= \gamma_d(\gamma_d\eta)^{2^d} + \gamma_{d+1}(\gamma_{d+1}\eta)^{2^{d+1}} + \cdots + \gamma_t(\gamma_t\eta)^{2^t} + \gamma_{t+1}(\gamma_{t+1}\eta)^{2^{t+1}} \\ &\quad + \gamma_t(\gamma_t\eta)^{2^{t+2}} + \cdots + \gamma_{d+1}(\gamma_{d+1}\eta)^{2^{2t+1-d}} + \gamma_d(\gamma_d\eta)^{2^{2t+2-d}} \\ &= L'_B(\eta)^{2^d}, \end{aligned}$$

where degree $L'_B(\eta) \le 2^{2t+2-2d}$. Thus the dimension of the space of η for which $L_B(\eta) = 0$ is at most $2t+2-2d$. So rank $B \ge 2t+2-(2t+2-2d) = 2d$ (refer to equation (20) of Ch. 15 in [4]). In particular, when $d = t+1$, rank $B = 2t+2$ and the symplectic matrix B is corresponding to a quadratic bent function.

Note that by setting $\gamma_i = 0$ we are removing the idempotent $\theta^*_{l_i}$ from the code. Setting the first $d-1$ γ_i's equal to 0, we derive a sub-code $\mathcal{R}^{d'}_{2t+2}$, which has a corresponding symplectic form of rank $\ge 2d$. Clearly the code $\mathcal{R}^{d'}_{2t+2}$ has idempotent

$$\theta^*_1 + \sum_{j=d}^{t+1} \theta^*_{l_j}, \quad l_j = 1 + 2^j.$$

According to Lemma C.2, the code has dimension $\sum_{j=d}^{t+1}|\mathrm{C}_{l_j}| = (t+2-d)m + m/2$. Due to Theorem 5 of Ch. 15 in [4], the code has codewords of weights 2^{m-1} and $2^{m-1} \pm 2^{m-h-1}$ for all h in the range $d \le h \le t+1$. Adding the all-one codeword into $\mathcal{R}^{d'}_{2t+2}$, we get a sub-code $\mathcal{R}^{d^*}_{2t+2}$ of $\mathcal{R}(2,m)^*$ having idempotent

$$\theta_0 + \theta_1^* + \sum_{j=d}^{t+1} \theta^*_{l_j}, \quad l_j = 1 + 2^j,$$

of dimension $(t+2-d)m + m/2 + 1$ and minimum distance $2^{m-1} - 2^{m-d-1} - 1$. Adding a parity check bit, we get the extended code $\mathcal{R}^d_{2t+2}$. ■

APPENDIX B

Proof of Corollary 3.7:

Proof: Recall from the proof of Theorem 3.6 that $\mathcal{R}^d_{2t+2}$, $1 \le d \le t+1$, is constructed by extending the sub-code of $\mathcal{R}(2,m)^*$, $\mathcal{R}^{d^*}_{2t+2}$, which has idempotent

$$\theta_0 + \theta_1^* + \sum_{j=d}^{t+1} \theta^*_{l_j}, \quad l_j = 1 + 2^j.$$

The corollary follows directly from the fact that

$$\mathcal{R}^{t+1^*}_{2t+2} \subset \mathcal{R}^{t^*}_{2t+2} \subset \cdots \subset \mathcal{R}^{1^*}_{2t+2}.$$

Clearly the sub-codes in the sub-code family for even m satisfy the nested structure. By a similar proof, the sub-codes in the sub-code family for odd m given by Theorem 3.5 have the same property. ■

APPENDIX C

Lemma C.1:

$$\gcd(2^m - 1, 2^i + 1) = \begin{cases} 1 & \text{if } \gcd(m, 2i) = \gcd(m, i), \\ 2^{\gcd(m,i)} + 1 & \text{if } \gcd(m, 2i) = 2\gcd(m, i). \end{cases}$$

Proof:

$$\begin{aligned} \gcd(2^m - 1, 2^i + 1) &\overset{(a)}{=} \gcd(2^m - 1, 2^i + 1, 2^{m-i} - 2^i) \\ &\overset{(b)}{=} \gcd(2^m - 1, 2^i + 1, 2^{2i} - 1) \\ &\overset{(c)}{=} \gcd(2^{\gcd(m,2i)} - 1, 2^i + 1), \end{aligned}$$

where (a) is from the fact that $2^m - 1 = (2^{m-i} - 1)(2^i + 1) - (2^{m-i} - 2^i)$; (b) is from the fact that $2^m - 1 = 2^i(2^{m-i} - 2^i) + (2^{2i} - 1)$; (c) is from the fact that $\gcd(2^x - 1, 2^y - 1) = 2^{\gcd(x,y)} - 1$.

If $\gcd(m, 2i) = \gcd(m, i)$, we have

$$\begin{aligned} \gcd(2^m - 1, 2^i + 1) &= \gcd(2^{\gcd(m,2i)} - 1, 2^i + 1) \\ &= \gcd(2^{\gcd(m,i)} - 1, 2^i + 1) \\ &\overset{(d)}{\le} \gcd(2^i - 1, 2^i + 1) \\ &\overset{(e)}{=} 1, \end{aligned}$$

where (d) is from the fact that $2^{\gcd(m,i)} - 1 \mid 2^i - 1$; (e) is from the fact that $\gcd(2^i - 1, 2^i + 1) = 1$. Clearly we have in this case $\gcd(2^m - 1, 2^i + 1) = 1$.

If $\gcd(m,2i) = 2\gcd(m,i)$, we have

$$\begin{aligned}\gcd(2^m-1, 2^i+1) &= \gcd(2^{\gcd(m,2i)}-1, 2^i+1)\\ &= \gcd(2^{2\gcd(m,i)}-1, 2^i+1)\\ &\overset{(f)}{=} \gcd(2^{\gcd(m,i)}-1, 2^i+1)\cdot\gcd(2^{\gcd(m,i)}+1, 2^i+1)\\ &= \gcd(2^{\gcd(m,i)}+1, 2^i+1),\\ &\overset{(g)}{=} 2^{\gcd(m,i)}+1,\end{aligned}$$

where (f) is from the fact that $2^{2\gcd(m,i)}-1 = (2^{\gcd(m,i)}-1)(2^{\gcd(m,i)}+1)$ and $\gcd(2^{\gcd(m,i)}-1, 2^{\gcd(m,i)}+1) = 1$. (g) is from the fact that $2^{\gcd(m,i)}+1 \mid 2^i+1$, since $\frac{i}{\gcd(m,i)}$ is odd due to $\gcd(m,2i) = 2\gcd(m,i)$. ■

Lemma C.2: If $m = 2t+1$ is odd, then for $l_i = 1+2^i$, the cyclotomic coset C_{l_i} has size

$$|\mathrm{C}_{l_i}| = m, \quad 1 \le i \le t.$$

If $m = 2t+2$ is even, then for $l_i = 1+2^i$, the cyclotomic coset C_{l_i} has size

$$|\mathrm{C}_{l_i}| = \begin{cases} m & 1 \le i \le t,\\ m/2 & i = t+1.\end{cases}$$

Proof: If $m = 2t+1$ is odd, for $1 \le i \le t$, l_i and 2^m-1 are relatively prime according to Lemma C.1. In this case, it is clear that $|\mathrm{C}_{l_i}| = m$.

If $m = 2t+2$ is even, for $1 \le i \le t$, C_{l_i} consists of

$$\{1+2^i, 2+2^{i+1}, 2^2+2^{i+2}, \cdots, 2^t+2^{i+t}, 2^t+2^{i+t}, 2^{t+1}+2^{i+t+1}\cdots\}.$$

It is easy to see that $|\mathrm{C}_{l_i}| \ge t+2 = m/2+1$. Note that $|\mathrm{C}_{l_i}|$ must be either m or a divisor of m. Therefore, $|\mathrm{C}_{l_i}| = m$ for $1 \le i \le t$. Consider the case $i = t+1$. $\mathrm{C}_{l_{t+1}}$ consists of

$$\{1+2^{t+1}, 2+2^{t+2}, 2^2+2^{t+3}, \cdots, 2^t+2^{2t+1}\}.$$

It is easy to count that $|\mathrm{C}_{l_{t+1}}| = t+1 = m/2$. ■

APPENDIX D

As given in Theorem 3.5, there is a linear sub-code family of $\mathcal{R}(2,m)$ for odd m. Note that the sub-code $\mathcal{R}^t_{2t+1}$ is optimal in the sense that no codes exist with the same length and weight set, but with larger dimension, as shown in Theorem 3.8. Correspondingly for even m, a nonlinear sub-code family (the generalized Kerdock code $\mathcal{DG}(m,d)$) is introduced in Theorem 19. of Ch. 15 in [4]. In particular, when $d = m/2$, $\mathcal{DG}(m,d)$ is one of the best-known nonlinear codes: the Kerdock code $\mathcal{K}(m)$. As shown in [4], these nonlinear sub-codes turn out to have good parameters. However, a linear sub-code family for even m is still of our interest due to the advantages of linear codes in the straightforward decoding and practical implementations. As given in Theorem 3.6, we reconsider the case for even m and build up a linear sub-code family.

For even m, we compare the linear code $\mathcal{R}^{m/2}_m$ to the Kerdock code $\mathcal{K}(m)$. We consider $\mathcal{R}^{m/2}_m$ as $\mathcal{R}(1,m)$ together with $2^{m/2}-1$ cosets of $\mathcal{R}(1,m)$, and $\mathcal{K}(m)$ as $\mathcal{R}(1,m)$ together with $2^{m-1}-1$ cosets of $\mathcal{R}(1,m)$. Note that every coset is corresponding to a quadratic bent function and therefore associated to a symplectic matrix of full rank. It is well known that the cosets of $\mathcal{K}(m)$ are corresponding to the maximal set of symplectic forms with the property that the rank of the sum of any two in the set is still full rank. Clearly $\mathcal{K}(m)$ has much more codewords. However, $\mathcal{R}^{m/2}_m$ enjoys a linear structure. One can correspondingly obtain a set of $2^{m/2}-1$ symplectic matrices of full rank, denoted as $\mathcal{G}^*$, with the property that the rank of the sum of any two, any three and so on in the set is still full rank. Introducing a matrix with all zero elements into $\mathcal{G}^*$, we get a set $\mathcal{G}$. Due to the linearity of $\mathcal{R}^{m/2}_m$, $\mathcal{G}$ is an additive commutative group with the all-zero matrix as its identity element. This matrix group is new to our knowledge in the manner that except its identity element, the symplectic matrices of full rank, preserve full rank under matrix addition.

Theorem D.1: For any even number m, there exists a group $\mathcal{G}$ of $m \times m$ symplectic matrices with respect to the addition operation. There are $2^{m/2}$ symplectic matrices in $\mathcal{G}$. In particular, all the matrices except the matrix with all zero elements have full rank m.

ACKNOWLEDGMENT

The authors would like to thank Prof. Tor Helleseth for pointing out the reference paper by Prof. Henk van Tilborg regarding the uniqueness proof of the first order Reed-Muller code.

REFERENCES

[1] A. J. Han Vinck and Yuan Luo, "Optimum Distance Profiles of Linear Block Codes," *Proc. ISIT 08*, Toronto, Canada, July 2008.
[2] M. Grassl, "Linear Block Codes," *http://www. codetables.de*.
[3] Marten van Dijk, Stan Baggen and Ludo Tolhuizen, "Coding for Informed Decoders," *Proc. ISIT 01*, Washington, DC, June 2001.
[4] F. J. MacWilliams and N. J. A. Sloane, *The theory of Error Correcting codes*, 5th printing, Elsevier Science Publishers, The Netherlands, 1986.
[5] Johannes Maks and Juriaan Simonis, "Optimal Subcodes of Second Order Reed-Muller Codes and Maximal Linear Spaces of Bivectors of Maximal Rank," *Designs, Codes and Cryptography*, vol. 21, pp. 165-180, 2000.
[6] Stefan M. Dodunekov, Silvia B. Encheva and Stoyan N. Kapralow, "On the [28, 7, 12] Binary Self-complementary Codes and Their Residuals," *Designs, Codes and Cryptography*, vol. 4, pp. 57-67, 1994.
[7] Aimo Tietäväinen, "On the Nonexistence of Perfect Codes over Finite Fields," *SIAM J. Appl. Math.*, vol. 24, no. 1, pp. 88-96, Jan. 1973.
[8] Anthony M. Kerdock, F. Jessie MacWilliams and Andrew M. Odlyzko, "A New Theorem about the Mattson-Solomon Polynomial and Some Applications," *IEEE Transactions on Information Theory*, vol. 20, pp. 85-89, Jan. 1974.
[9] H. C. A. van Tilborg, "On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound," *Inform. Contr.*, vol. 44, pp. 16-35, 1980.
[10] Satish Babu Korada, Eren Şaşoğlu and Rödiger Urbanke, "Polar Codes: Characterization of Exponent, Bounds and Constructions," *Proc. ISIT 09*, Seoul, Korea, June 2009.