Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 29-34*

Minimal/nonminimal codewords in the second order binary Reed-Muller codes: revisited

Yuri Borissov youri@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
8 G. Bonchev str., 1113 Sofia, BULGARIA

Abstract. The result on the weight distribution of minimal codewords in the second order binary Reed-Muller code $RM(2,m)$, was announced for the first time by Ashikhmin and Barg at ACCT'94. They gave only a sketch of the proof and later on a short and nice complete proof of geometric nature was exhibited in their paper: A. Ashikhmin and A. Barg, "Minimal Vectors in Linear Codes", IEEE Trans. on Information Theory, vol. 44, September 1998, pp. 2010-2017. The paper presents a different comprehensive proof of this result based on Dickson's Theorem.

1 Introduction

For the first time the sets of minimal codewords in linear codes were considered in connection with a decoding algorithm [8]. A more detailed description of the role of minimal codewords in the so-called "gradient-like" decoding algorithms can be found in [2] and [3, Ch 7]. Recently, the interest in minimal codewords with respect to decoding algorithms was resumed by [12]. Additional interest to them was sparked by the work of J. Massey [10], where it was shown that minimal codewords describe so-called minimal access structure in secret-sharing schemes based on linear codes (see e.g. [11] for definitions).

It seems to be quite difficult to describe the set of minimal codewords for an arbitrary linear code even in the binary case. The problem has been completely solved only for q-ary Hamming codes and for the second order binary Reed-Muller codes [1]. An attempt to characterize minimal codewords for two-error-correcting binary BCH codes ended with only a partial result [4],[5]. Another partial result was established in [6] for the number of non-minimal codewords of weight $2d_{min}$ in the r^{th} order binary Reed-Muller code $RM(r,m)$. The weight distributions of minimal codewords in some third-order binary Reed-Muller codes are determined by computer assistance in [7] and [13].

In this note, we return to the problem of describing the set of minimal/non-minimal codewords in the second order binary Reed-Muller code. A short and nice proof for this case suggested by Juriaan Simonis was exhibited in [2]. That proof is of geometric nature while here we present another comprehensive proof founded on Dickson's Theorem.

2 Background

We assume the reader is familiar with basic definitions, notations and facts about linear codes [9]. We shall need the following definitions.

Definition 2.1 *A support of an n-vector $\mathbf{c}$ over the finite field $\mathbf{F}_q$ is defined as the subset of its nonzero coordinates. A support of a Boolean function is the support of its truth table.*

Definition 2.2 *A nonzero codeword $\mathbf{c}$ of a binary linear code $\mathbf{C}$ is called minimal in $\mathbf{C}$ if its support does not cover the support of another nonzero codeword. Otherwise, $\mathbf{c}$ is called non-minimal.*

Proposition 2.3 *([1], [4])*

1) If $\mathbf{c}$ is minimal codeword in a linear $[n, k]$-code then its weight satisfies $wt(\mathbf{c}) \leq n - k + 1$.

2) Any non-minimal codeword $\mathbf{c}$ in a binary linear code can be represented as a sum of two codewords $\mathbf{c}_1$ and $\mathbf{c}_2$ having disjoint supports contained in the support of $\mathbf{c}$.

3) The automorphisms of a linear code preserve the property of the codewords to be minimal or not.

4) All codewords of a binary linear code with weight $< 2d_{min}$ are minimal.

For basic definitions and facts about second order binary Reed-Muller code (including Dickson's Theorem) we refer to [9, Ch. 15.2].

Let A_w be the number of codewords of weight w in $RM(2, m)$. Then $A_w = 0$ unless $w = 2^{m-1}$ or $w = 2^{m-1} \pm 2^{m-h-1}$ for some h, $0 \leq h \leq \lfloor m/2 \rfloor$.

Here, we shall remind also the theorem for weight distributions of the cosets of $RM(1, m)$ in $RM(2, m)$.

Theorem 2.4 *If the symplectic matrix determining coset $\mathcal{B}$ of $RM(1, m)$ in $RM(2, m)$ has rank $2h$ then the weight distribution of $\mathcal{B}$ is as follows:*

Weight	**Number of Vectors**
$2^{m-1} - 2^{m-h-1}$	2^{2h}
2^{m-1}	$2^{m+1} - 2^{2h+1}$
$2^{m-1} + 2^{m-h-1}$	2^{2h}

From Theorem 2.4 it follows immediately the corollary.

Corollary 2.5 *The number of codewords of weight 2^{m-1} in the cosets having rank $2h$ is equal to $A_{2^{m-1}-2^{m-h-1}}(2^{m-2h+1} - 2)$.*

3 The proof

We shall make use of the following lemma.

Lemma 3.1 *The rank of symplectic matrix corresponding to the sum of two codewords in $RM(2,m)$ is less than or equal to the sum of the ranks of symplectic matrices associated with these codewords.*

Proof. Let $\mathbf{c_1}$ and $\mathbf{c_2}$ be two arbitrary codewords of $RM(2,m)$. According to [9, Ch. 15.2] the corresponding Boolean functions associated with them are of the form: $S_1(\mathbf{v}) = \mathbf{v}\mathbf{Q_1}\mathbf{v}^T + \mathbf{L_1}\mathbf{v} + \epsilon_1$ and $S_2(\mathbf{v}) = \mathbf{v}\mathbf{Q_2}\mathbf{v}^T + \mathbf{L_2}\mathbf{v} + \epsilon_2$, where $\mathbf{Q_1}$, $\mathbf{Q_2}$ are upper triangular binary matrices, $\mathbf{L_1}$, $\mathbf{L_2}$ are binary m-vectors, ϵ_1, ϵ_2 are binary constants, and $\mathbf{v} = (v_1, \ldots, v_m)$ is the vector of variables. Their corresponding symplectic matrices are:

$$\mathbf{B_1} = \mathbf{Q_1} + \mathbf{Q_1}^T \text{ and } \mathbf{B_2} = \mathbf{Q_2} + \mathbf{Q_2}^T$$

Therefore the symplectic matrix corresponding to the sum:

$$S_1(\mathbf{v}) + S_2(\mathbf{v}) = \mathbf{v}(\mathbf{Q_1} + \mathbf{Q_2})\mathbf{v}^T + (\mathbf{L_1} + \mathbf{L_2})\mathbf{v} + (\epsilon_1 + \epsilon_2)$$

is:

$$\mathbf{B} = (\mathbf{Q_1} + \mathbf{Q_2}) + (\mathbf{Q_1} + \mathbf{Q_2})^T = \mathbf{B_1} + \mathbf{B_2}$$

Taking into account, the well-known inequality for the rank of sum of two matrices, we complete the proof. □

Now, let us recall the result stated by Ashikhmin and Barg in [1].

Proposition 3.2 *Let $\mathbf{C} = RM(2,m)$ be the second order binary Reed-Muller code, and A_w, M_w be the number of its codewords and its minimal codewords of weight w, respectively. Then for $w = 2^{m-1} + 2^{m-1-h}, h = 0,1,2$ and $w = 0$ there are no minimal codewords ($M_w = 0$). Otherwise, $M_w = A_w$, except for the case $w = 2^{m-1}$, where*

$$M_w = \sum_{h=2}^{\lfloor m/2 \rfloor} A_{2^{m-1}-2^{m-h-1}} (2^{m-2h+1} - 2) \tag{1}$$

Herein, we present a proof of this proposition different from exhibited in [2].

Proof. The smallest two weights in $\mathbf{C}$ are $w_1 = 2^{m-2}$ and $w_2 = 2^{m-1} - 2^{m-3}$ (corresponding to $h = 1, 2$). By Proposition 2.3 Part 2), the smallest weights of $\mathbf{C}$ where non-minimal codewords could exist are $2w_1 = 2^{m-1}$ and $w_1 + w_2 = 2^{m-1} + 2^{m-3}$. Now, we shall show that all codewords of weight $w \geq 2^{m-1} + 2^{m-h-1}$, whenever $h = 0, 1$ or 2, are non-minimal in $\mathbf{C}$. Let $\mathbf{c}$ be such a codeword. There are three cases to be considered accordingly to the values of h.

- (1) $wt(\mathbf{c}) = 2^m$ $(h = 0)$. The only codeword of this kind is the all-one vector $\mathbf{1}$ which is obviously non-minimal.
- (2) $wt(\mathbf{c}) = 2^{m-1} + 2^{m-2}$ $(h = 1)$. The corresponding symplectic matrix has rank 2. By Dickson's Theorem [9, Ch. 15.2] it follows the existence of an affine transformation by which the Boolean function associated with the codeword $\mathbf{c}$, is reduced to the form $y_1y_2 + 1$. So, the considered codeword is affinely equivalent to concatenation of identical codewords from $RM(2,2)$ having weight 3. Hence, its property to be minimal or not, is the same as the latter one's property because of Proposition 2.3 Part 3). But the non-minimality of the codewords in $RM(2,2)$ of weight > 1 (like of that considered here) is obvious.
- (3) $wt(\mathbf{c}) = 2^{m-1} + 2^{m-3}$ $(h = 2)$. The corresponding symplectic matrix has rank equal to 4 and the Boolean function associated with such a codeword is affinely equivalent to $y_1y_2 + y_3y_4 + 1$. Similarly to the case (2), the non-minimality follows by that of the corresponding codeword in $RM(2,4)$ but this time according to Proposition 2.3 Part 1), since the weight of the latter equals 10 which is $> 16 - dim(RM(2,4)) + 1 = 6$.

So, it remains to consider the codewords of weight 2^{m-1}. Since the minimum weight of $\mathbf{C}$ is 2^{m-2} by Proposition 2.3 Part 2), we conclude that any non-minimal codeword $\mathbf{c}$ of weight 2^{m-1} must be sum of two codewords of weight 2^{m-2}, say $\mathbf{c}_1$ and $\mathbf{c}_2$. Since the symplectic matrices corresponding to $\mathbf{c}_i$, $i = 1, 2$ have rank 2, by Lemma 3.1 it follows the symplectic matrix $\mathbf{B}$ corresponding to $\mathbf{c}$ has rank ≤ 4 (i.e. the possible rank of $\mathbf{B}$ is $2h$ for some $h = 0, 1$ or 2).
Hence, there are again three cases to be considered:

- (1) $h = 0$. According to Dickson's Theorem the corresponding Boolean function is affinely equivalent to $f(\mathbf{y}) = y_1$. The non-minimality of such an "affine" codeword (i.e. $\in RM(1,m)$) follows by the fact that Boolean functions y_1y_2 and $y_1(y_2+1)$ have disjoint supports and their sum is equal to f. By Corollary 2.5 the number of these codewords is $A_0(2^{m+1} - 2)$.
- (2) $h = 1$. The corresponding Boolean function is affinely equivalent to $f(\mathbf{y}) = y_1y_2 + y_3$ and the non-minimality of $\mathbf{c}$ follows by Proposition

2.3 Part 1), since the weight of the corresponding codeword in $RM(2,3)$ equals 4 which is $> 8 - dim(RM(2,3)) + 1 = 2$. For instance, f can be represented as a sum of Boolean functions $y_2y_3 + y_3$ and $y_1y_2 + y_2y_3$ having disjoint supports which are subsets of the support of f. Note that by Corollary 2.5 the number of codewords of this kind is $A_{2^{m-2}}(2^{m-1}-2)$.

- (3) $h = 2$. The Boolean function corresponding to $\mathbf{c}$ is affinely equivalent to $f(\mathbf{y}) = y_1y_2+y_3y_4+y_5$. Let Boolean functions corresponding to $\mathbf{c}_1$ and $\mathbf{c}_2$ be f_1 and f_2, respectively. Let us also consider $\mathbf{c}$ as a concatenation of two codewords $\mathbf{c}', \mathbf{c}''$ of $RM(2, m-1)$ over the hyperplanes $y_5 = 0$ and $y_5 = 1$. The subfunction $f(\mathbf{y}|y_5 = 0)$ is equal to $y_1y_2 + y_3y_4$ and thus $wt(\mathbf{c}') = 2^{m-2} - 2^{m-4} < 2^{m-2} = 2 * 2^{m-3} = 2 * dim(RM(2, m-1))$. Hence, $\mathbf{c}'$ is minimal in $RM(2, m-1)$ and therefore wlog we can assume that $f_1(\mathbf{y}|y_5 = 0) \equiv 0$. So, $f_1(\mathbf{y})$ is of the form $y_5L(\mathbf{y})$, where L depends essentially only on y_1, y_2, y_3 and y_4 and its algebraic degree is strictly less than 2. Then, clearly: $f(\mathbf{y}|y_5 = 1) = f_1(\mathbf{y}|y_5 = 1) + f_2(\mathbf{y}|y_5 = 1) = L(\mathbf{y}) + f_2(\mathbf{y}|y_5 = 1)$. Since $f_1(\mathbf{y}|y_5 = 1) \equiv L(\mathbf{y})$ and $wt(\mathbf{c}_1) = 2^{m-2}$, it follows that L is an affine function of weight 2^{m-2}. Furthermore, obviously $wt(\mathbf{c}'') = 2^{m-2} + 2^{m-4}$ and thus the weight of $f_2(\mathbf{y}|y_5 = 1) = 2^{m-4}$. But this is impossible weight for quadratic function in $m-1$ variables. Therefore $\mathbf{c}$ must not be non-minimal codeword i.e. all codewords of this kind are minimal.

Finally, by the above deductions and Corollary 2.5, for the number of minimal codewords of weight 2^{m-1} in $RM(2,m)$, we obtain:

$$\begin{aligned} M_{2^{m-1}} &= A_{2^{m-1}} - \sum_{h=0}^{1} A_{2^{m-1}-2^{m-h-1}}(2^{m-2h+1} - 2) \\ &= \sum_{h=2}^{\lfloor m/2 \rfloor} A_{2^{m-1}-2^{m-1-h}}(2^{m-2h+1} - 2), \end{aligned}$$

which completes the proof. □

References

[1] A. Ashikhmin, A. Barg, Combinatorial aspects of secret sharing with codes, *Proc. Intern. Workshop ACCT*, Novgorod, Russia, September, 1994, 8-11.

[2] A. Ashikhmin, A. Barg, Minimal vectors in linear codes, *IEEE Trans. Inform. Theory* 44, 1998, 2010-2017.

[3] A. Barg, Complexity Issues in Coding Theory, in *Handbook of Coding Theory* (Eds. V. Pless and W. Huffman), Amsterdam, Elsevier Science B.V., 1998.

[4] Y. Borissov, N. L. Manev, On the minimal words of the primitive BCH codes, *Proc. Intern. Workshop ACCT*, Sozopol, Bulgaria, 1996, 59-65.

[5] Yu. Borissov, N. L. Manev, Minimal codewords of the primitive BCH codes, *Probl. Pered. Inform.* 34, 3, 1998, 37-46 (in Russian).

[6] Y. Borissov, N. Manev, S. Nikova, On the non-minimal codewords in binary Reed-Muller codes, *Discr. Appl. Math.* 128, 2003, 65-74.

[7] Y. Borissov, N. Manev, Minimal codewords in linear codes, *Serdica Math. J.* 30, 2004, 303-324.

[8] Tai-Yang Hwang, Decoding linear block codes for minimizing word error rate, *IEEE Trans. Inform. Theory* 25, 1979, 733-737.

[9] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company 1977.

[10] J. Massey, Minimal codewords and secret sharing, *Proc. Sixth Joint Swedish-Russian Workshop Inform. Theory*, Mölle, Sweden, 1993, 246-249.

[11] D. R. Stinson, An explication of secret sharing schemes, *Des. Codes Crypt.* 2, 1992, 357-390.

[12] P. O. Vontobel, R. Smarandache, N. Kiyavash, J. Teutsch, D. Vukobratovic, On the minimal pseudo-codewords of codes from finite geometries, *ISIT 2005, Proc. Intern. Symp. Inform. Theory*, 2005, 980 - 984.

[13] K. Yasunaga, T. Fujiwara, T. Kasami, Local weight distribution of the (256, 93) third-order binary Reed-Muller code, *IEICE Trans. Fundam. Electr., Commun. Computer Sci.* E90-A, 2007, 698-701.