

On the Non-Minimal codewords of weight $2d_{min}$ in the binary Reed-Muller Code

Yuri Borissov, Nickolay Manev ¹

*Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
8 G.Bonchev, 1113 Sofia, Bulgaria*

Svetla Nikova ²

*Dept. Electr. Eng. ESAT/COSIC, Katholieke Universiteit Leuven,
Kardinal Mercierlaan 94, B-3001 Heverlee, Belgium*

Abstract

We compute the number of non-minimal codewords of weight $2d_{min}$ in the binary Reed-Muller code.

Key words:

binary Reed-Muller code, non-minimal codewords

1 Introduction

Let $RM(r, m)$ be the binary Reed-Muller code of order r with the parameters $[n = 2^m, k = \sum_{i=0}^r \binom{m}{i}, d = 2^{m-r}]$. Reed-Muller codes can be defined very simply in terms of Boolean functions. But many properties are best stated in the language of finite geometries. This gives us another way of thinking about the codewords of $RM(r, m)$. It is well known that the codewords of $RM(r, m)$ of minimal weight ($d_{min} = 2^{m-r}$) correspond to $(m - r)$ -dimensional affine subspaces of the affine geometry $AG(m, 2)$ [5].

Email addresses: yborisov@excite.com, nlmanev@moi.math.bas.bg (Yuri Borissov, Nickolay Manev), svetla.nikova@esat.kuleuven.ac.be (Svetla Nikova).

¹ The authors were partially supported by Bulgarian NSF Contract I-803

² The author was partially supported by research fellowship of DWTC, Belgium, NATO research fellowship and Concerted Research Action GOA-MEFISTO-666 of the Flemish Government.

We will use the notation $[n] := \{1, 2, \dots, n\}$ for the set of code coordinates. A *support* of a vector \mathbf{c} is defined as $\text{supp}(\mathbf{c}) = \{i \in [n] : c_i \neq 0\}$. If $\text{supp}(\mathbf{c}') \subset \text{supp}(\mathbf{c})$ (respectively, \subseteq), we also write $\mathbf{c}' \prec \mathbf{c}$ (respectively, \preceq).

Definition 1 *Let C be a linear code over $GF(q)$. A nonzero codeword $\mathbf{c} \in C$ is called minimal if its support does not contain the support of any other nonzero codeword as true subset. The support of a minimal codeword is called minimal with respect to C .*

The sets of minimal codewords of linear codes were considered in connection with constructing a decoding algorithm (Tai-Yang Hwang [4]). For the Euclidean space, this connection was addressed also in [1]. Later the sets of minimal codewords of linear codes were used in a series of papers sparked by [6] to describe minimal access structure in linear secret-sharing schemes. Ashikhmin and Barg [2] have determined the set of minimal codewords (also called projecting set) for the q -ary Hamming code and for the second order Reed-Muller code $RM(2, m)$.

Lemma 2 [2] *Let C be a binary linear code.*

1) *Every support of size $\leq 2d_{\min} - 1$ is minimal.*

2) *If \mathbf{c} is a non-minimal codeword in C there is a pair of nonzero code vectors $\mathbf{c}_1 \prec \mathbf{c}$ and $\mathbf{c}_2 \prec \mathbf{c}$ with disjoint supports, such that $\mathbf{c} = \mathbf{c}_1 + \mathbf{c}_2$.*

As follows from Lemma 2 every codeword in a binary linear code of weight d_{\min} up to $2d_{\min} - 1$ is minimal. The question that arises is: Whether there exist minimal (non-minimal) codewords of weight $2d_{\min}$ and if there exist how many they are?

In this paper we will find the number of the non-minimal codewords of weight $2d_{\min} = 2^{m-r+1}$ in an arbitrary code $RM(r, m)$.

Definition 3 [3] *The quantity known as **q-ary gaussian coefficient** is defined by:*

$$\begin{bmatrix} m \\ i \end{bmatrix} = \prod_{j=0}^{i-1} \frac{q^m - q^j}{q^i - q^j}, \quad \begin{bmatrix} m \\ 0 \end{bmatrix} = 1,$$

for $i = 1, 2, \dots, m$.

2 The number of the non-minimal codewords of weight $2d_{min}$.

By Lemma 2 the non-minimal codewords of weight $2d_{min}$ in a binary linear code are the sum of two codewords of minimal weight and having non-intersecting supports. We should take into account that some of them could have more than one representation as sum of two codewords of minimal weight. In the following Theorem we will exploit the geometric approach of Juriaan Simonis, which is used in the proof of Theorem 2.9 in [2].

Theorem 4 *The number of non-minimal codewords in $RM(r, m)$ of weight $2d$, which have more than one representation as sum of two codewords of weight d is*

$$A_{r,m} + B_{r,m} = 2^{r-1} \begin{bmatrix} m \\ m-r+1 \end{bmatrix} + \frac{2^{r+1}-4}{4} \begin{bmatrix} m \\ m-r-1 \end{bmatrix} \binom{2^{r+1}}{3}$$

PROOF. We will consider codewords of weight $2d$, which have more than one representation as sum of two codewords of weight d . That means that there exist two pairs of $(m-r)$ -dimensional affine subspaces π_1, π_2 and τ_1, τ_2 , such that $\pi_1 \cup \pi_2 \equiv \tau_1 \cup \tau_2$ as sets of points. Let us denote this set with M . Because the intersection of two affine subspaces is again an affine subspace any of the intersections $\pi_i \cap \tau_j, i = 1, 2, j = 1, 2$ is an affine subspace of dimension $m-r-1$. In other words the set M is an union of four translations of the $(m-r-1)$ -dimensional vector subspace ξ (see Figure 1).

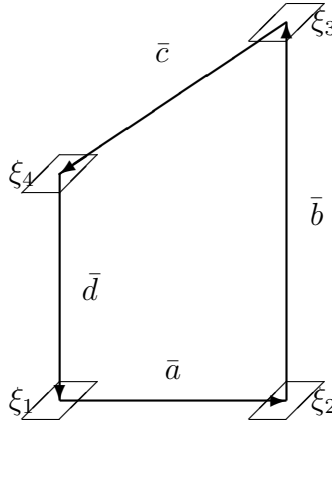


Fig. 1. The vector space ξ and its four translations in some fixed order, which constitute the set M

The vectors \bar{a} , \bar{b} , \bar{c} and \bar{d} are determined within the space ξ . There are two possible cases:

a) If \bar{c} can be chosen equal to \bar{a} , then M is an affine subspace of dimension

$m - r + 1$. (M has dimension $(m - r - 1 + 2)$, since the vectors \bar{a} , \bar{b} , \bar{c} and \bar{d} can be chosen from a 2-dimensional subspace having trivial intersection with ξ , and ξ itself has dimension $(m - r - 1)$.)

b) Otherwise (i.e. if the vectors \bar{a} , \bar{b} and \bar{c} are linearly independent) M can be represented as union of two $(m - r)$ -dimensional affine subspaces in exactly 3 ways. Namely, any of this subspaces is obtained as an union of a pair of the subspaces ξ_i , $i = 1, \dots, 4$. If we suppose that there are more than 3 representations, i.e. if we presume that there is one more pair of affine subspaces, which constitutes M , then it is easy to see that any of the two subspaces in the new pair intersects all the 4 subspaces from the Fig.1 in a subspace of dimension less by one. This means that any of the new two subspaces is an union of 4 translations of the $(m - r - 2)$ -dimensional vector subspace and the translation vectors are the same. But now for these new subspaces we will have the same situation like in case **a)** which contradicts the assumptions of case **b)**.

In the case **a)** the non-minimal codewords of weight $2d$ are the affine subspaces in $AG(m, 2)$ of dimension $m - r + 1$. By [3] their number is

$$A_{r,m} = 2^{r-1} \begin{bmatrix} m \\ m - r + 1 \end{bmatrix} \quad (1)$$

and each codeword is represented as sum of two codewords of minimal weight in as many ways as the number of the affine $(m - r)$ -dimensional subspaces that it contains, divided by 2, i.e

$$\begin{bmatrix} m - r + 1 \\ m - r \end{bmatrix} = 2^{m-r+1} - 1.$$

In the case **b)** the non-minimal codewords of weight $2d$, which have exactly 3 representations as sum of two codewords of minimal weight, can be calculated as follows. The four subspaces of dimension $m - r - 1$ in this case are translations of a $(m - r - 1)$ -dimensional vector space. The number of the different translations of a fixed vector space of dimension $m - r - 1$ is 2^{r+1} . From those four spaces we have to exclude the spaces that are already considered in the case **a)**. Therefore their number is :

$$\binom{2^{r+1}}{4} - \frac{1}{4} \binom{2^{r+1}}{3} = \binom{2^{r+1}}{3} \frac{2^{r+1} - 4}{4}.$$

Finally, we have to multiply it by the number of the $(m - r - 1)$ -dimensional vector spaces in order to obtain the number of the non-minimal codewords

considered in the case **b**). Namely,

$$B_{r,m} = \frac{2^{r+1} - 4}{4} \begin{bmatrix} m \\ m - r - 1 \end{bmatrix} \binom{2^{r+1}}{3}.$$

□

Theorem 5 *The number of non-minimal codewords in $RM(r, m)$ of weight $2d$, which have only one representation as sum of two codewords of weight d is $C_{r,m} = P_{r,m} - S_{r,m}$, where $P_{r,m}$ is the number of the pairs of non-intersecting $(m - r)$ -dimensional affine subspaces and $S_{r,m}$ is the number of the representations of the codewords from cases **a**) and **b**) of Theorem 4 as sum of two codewords of weight d .*

PROOF. We consider the codewords of weight $2d$, which have only one representation as sum of two codewords of minimal weight d .

Using Theorem 4 we recall that the number of non-minimal codewords in $RM(r, m)$ of weight $2d$, which have more than one representation as sum of two codewords of weight d is calculated as the sum of two possible cases **a**) and **b**). In case **a**) this number is $A_{r,m}$ and the possible representations of each codeword are $2^{m-r+1} - 1$. In case **b**) this number is $B_{r,m}$ and there are only 3 possible representations. So the number of the representations of the codewords, which have more than one representation as sum of two codewords of weight d is $S_{r,m} = (2^{m-r+1} - 1)A_{r,m} + 3B_{r,m}$.

It can also be written as follows:

$$S_{r,m} = 2^{r-1}(2^{m-r+1} - 1) \begin{bmatrix} m \\ m - r + 1 \end{bmatrix} + \frac{2^{r+1}(2^{r+1} - 1)(2^{r+1} - 2)(2^{r+1} - 4)}{8} \begin{bmatrix} m \\ m - r - 1 \end{bmatrix}$$

In order to find the number $P_{r,m}$ let us fix an $(m - r)$ -dimensional affine subspace π in $AG(m, 2)$ and let τ be a k -dimensional subspace of π , where $0 \leq k < m - r$. Taking into account that the intersection of affine subspaces is again an affine subspace, the number of $(m - r)$ -dimensional subspaces of $AG(m, 2)$, which intersect π exactly in τ is the following:

$$\begin{aligned} & \frac{(2^m - 2^{m-r})(2^m - 2^{m-r+1}) \dots (2^m - 2^{(m-r)+(m-r-1)-k})}{(2^{m-r} - 2^k)(2^{m-r} - 2^{k+1}) \dots (2^{m-r} - 2^{m-r-1})} \\ &= \frac{2^{m-r}}{2^k} \frac{(2^r - 1)}{(2^{m-r-k} - 1)} \cdot \dots \cdot \frac{2^{m-r}}{2^k} \frac{(2^r - 2^{m-r-k-1})}{(2^{m-r-k} - 2^{m-r-k-1})} \end{aligned} \quad (2)$$

$$= 2^{(m-r-k)^2} \begin{bmatrix} r \\ m-r-k \end{bmatrix}$$

Obviously if $m \leq 2m-2r-k-1$, i.e., if $k < m-2r$, the expression (2) becomes 0. Therefore the number of $(m-r)$ -dimensional affine subspaces, which have non-empty intersection with a fixed $(m-r)$ -dimensional affine subspace π is as follows (let $a = \max\{0, m-2r\}$):

$$\begin{aligned} & \sum_{k=a}^{m-r} 2^{m-r-k} \begin{bmatrix} m-r \\ k \end{bmatrix} 2^{(m-r-k)^2} \begin{bmatrix} r \\ m-r-k \end{bmatrix} \\ &= \sum_{k=a}^{m-r} 2^{(m-r-k)(m-r-k+1)} \begin{bmatrix} m-r \\ k \end{bmatrix} \begin{bmatrix} r \\ m-r-k \end{bmatrix}. \end{aligned} \quad (3)$$

The number of those $(m-r)$ -dimensional affine subspaces, which do not have common point with π we can find it from the number of all affine subspaces of this dimension in $AG(m, 2)$, we deduce the number (3) of $(m-r)$ -dimensional affine subspaces, which have non-empty intersection with π , i.e.,

$$E_{r,m} = 2^r \begin{bmatrix} m \\ m-r \end{bmatrix} - \sum_{k=a}^{m-r} 2^{(m-r-k)(m-r-k+1)} \begin{bmatrix} m-r \\ k \end{bmatrix} \begin{bmatrix} r \\ m-r-k \end{bmatrix}.$$

Therefore for $P_{r,m}$ we have

$$\begin{aligned} P_{r,m} &= \frac{2^r \begin{bmatrix} m \\ m-r \end{bmatrix} E_{r,m}}{2} = 2^{r-1} \begin{bmatrix} m \\ m-r \end{bmatrix} \left(2^r \begin{bmatrix} m \\ m-r \end{bmatrix} \right. \\ &\quad \left. - \sum_{k=a}^{m-r} 2^{(m-r-k)(m-r-k+1)} \begin{bmatrix} m-r \\ k \end{bmatrix} \begin{bmatrix} r \\ m-r-k \end{bmatrix} \right) \end{aligned}$$

□

Corollary 6 *The number of the non-minimal codewords of weight $2d = 2^{m-r+1}$ in $RM(r, m)$ is $N_{r,m}^{2d} = A_{r,m} + B_{r,m} + C_{r,m}$.*

Example 7 *Let us consider the Reed-Muller code $RM(3, 5)$. For this parameters we have $A_{3,5} = 620$, $B_{3,5} = 52080$, $C_{3,5} = 277760$, therefore $N_{3,5}^8 =$*

330460, i.e. the number of non-minimal codewords in $RM(3, 5)$ (which is in fact the extended binary Hamming code) of weight 8 is 330460.

In [2] Ashikhmin and Barg prove that the number of the non-minimal codewords in the second order Reed-Muller code is

$$2^{m+1} - 2 + (4/3)(2^m - 1)(2^{m-1} - 1)(2^{m-1} - 2).$$

Corollary 6 generalize this result for any r .

Proposition 8 *Let $RM(r, m)$ be the binary Reed-Muller code of order $r > 1$. If \mathbf{c} is non-minimal codeword of weight $2d$ then $\mathbf{c} + \mathbf{1}$ is non-minimal codeword as well.*

PROOF. By Lemma 2 the codeword \mathbf{c} can be represented as the sum of two codewords \mathbf{c}_1 and \mathbf{c}_2 each of them of minimal weight d . According to [5], \mathbf{c}_1 and \mathbf{c}_2 are the incidence vectors of two $(m - r)$ -dimensional affine subspaces of $AG(m, 2)$. For each of these subspaces let us take the hyperplane $((m - 1)$ -dimensional affine subspace) which contains it. Denote by ρ_1 and ρ_2 the complements of the above mentioned hyperplanes to $AG(m, 2)$.

There are 3 possibilities:

1. The intersection of ρ_1 and ρ_2 to be $(m - 2)$ -dimensional affine subspace.
2. ρ_1 to be identical with ρ_2 .
3. ρ_1 and ρ_2 to be complements of each other to $AG(m, 2)$.

In the first two cases the statement is obvious. In the third case to conclude the proof we note that each of ρ_1 and ρ_2 contains points only from one of $\text{supp}(\mathbf{c}_1)$ or $\text{supp}(\mathbf{c}_2)$.

□

Note that if $wt(\mathbf{c}) = 2d$ then $wt(\mathbf{c} + \mathbf{1}) = 2^m - 2^{(m-r+1)}$. So, for the second order Reed-Muller code for any minimal word \mathbf{c} of weight $2d$, $\mathbf{c} + \mathbf{1}$ is also minimal. But for $RM(r, m)$, $r > 2$, when there exist minimal codewords of weight $2d$, this is an open problem.

References

- [1] E.Agrell, *Voronoi Regions for Binary Linear Codes* IEEE Trans. Inf. Theory, vol.42, 1996, 1, 310–316.
- [2] A.Ashikhmin, A.Barg, *Minimal Vectors in Linear Codes*, IEEE Trans. Inf. Theory, vol.44, 1998, 5, 2010–2017.
- [3] R.Blahut, *Theory and Practice of Error Control Codes*, (Addison-Wesley Publishing Company, 1984).

- [4] Tai-Yang Hwang, *Decoding linear block codes for minimizing word error rate*, IEEE Trans. on Information Theory, IT-25, 1979, 6, 733-737.
- [5] F.J.MacWilliams and N.J.A.Sloane, *The Theory of Error-Correcting Codes*, (North Holland, Amsterdam, 1977).
- [6] J. Massey, *Minimal Codewords and Secret Sharing*, in Proc. Sixth Joint Swedish-Russian Workshop on Inf. Theory, Molle, Sweden, 1993, 246-249.