On the Non-Minimal Codewords in Binary Reed-Muller Codes

Yuri Borissov, Nickolai 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

First, we compute the number of non-minimal codewords of weight $2d_{\min}$ in the binary Reed-Muller code $RM(r,m)$. Second, we prove that all codewords of weight greater than $2^m - 2^{m-r+1}$ in binary $RM(r,m)$, are non-minimal.

Key words:
binary Reed-Muller code, non-minimal codewords, Boolean functions

1 Introduction

In this paper we deal with binary Reed-Muller codes. These codes are usually defined in terms of Boolean functions, namely

Definition 1 ([5]) *For any m and r, $0 \le r \le m$, the binary r^{th} order Reed-Muller code $RM(r,m)$ is defined to be the set of all binary vectors $\mathbf{f}$ of length $n = 2^m$ associated with Boolean polynomials $f(x_1, x_2, \ldots, x_m)$ of degree at most r.*

Email addresses: yborisov@moi.math.bas.bg, nlmanev@moi.math.bas.bg (Yuri Borissov, Nickolai 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.

$RM(r,m)$ has block length $n = 2^m$, dimension $k = 1 + \binom{m}{1} + \cdots + \binom{m}{r}$, and minimum distance $d = 2^{m-r}$.

For more details we refer to [5, Ch. 13]. Here we only recall that the codewords of minimum weight in $RM(r,m)$ are precisely the incidence vectors of the $(m-r)$-dimensional affine subspaces (called also $(m-r)$-flats) of the affine geometry $AG(m,2)$ and they span $RM(r,m)$. This fact allows a geometric look at Reed–Muller codes and many of their properties are better stated in the language of finite geometries. In this paper we will use both geometric and Boolean function approaches.

Let us denote by $[n] := \{1, 2, \ldots, n\}$ the set of code coordinates. A *support* of a vector $\mathbf{c}$ is defined as $supp(\mathbf{c}) = \{i \in [n] : c_i \neq 0\}$. If $supp(\mathbf{c}') \subset supp(\mathbf{c})$ (respectively, $\subseteq$), we also write $\mathbf{c}' \prec \mathbf{c}$ (respectively, $\preceq$).

Definition 2 *Let C be a $q-$ary linear code. A nonzero codeword $\mathbf{c} \in C$ is called* ***minimal*** *if its support does not contain the support of any other nonzero codeword as proper subset. The support of a minimal codeword is called* ***minimal with respect to*** *C.*

The sets of minimal codewords in linear codes were considered in connection with constructing a decoding algorithm (see [4]). For the Euclidean space, this connection was also addressed in [1]. Later the sets of minimal codewords in 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 for the $q-$ary Hamming code and for the second order binary Reed-Muller code $RM(2,m)$.

Lemma 3 ([2]) *Let C be a binary $[n,k,d]$ linear code.*

(i) *Every support of size $\leq 2d-1$ is minimal with respect to C.*

(ii) *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 $\mathbf{c} = \mathbf{c}_1 + \mathbf{c}_2$.*

(iii) *If $\mathbf{c}$ is minimal codeword in C, then $wt(\mathbf{c}) \leq n-k+1$*

As follows from Lemma 3 (i) every codeword in a binary linear code of weight d up to $2d-1$ is minimal. The question that arises is: Whether minimal (non-minimal) codewords of weight $2d$ exist and if they exist how many they are?

For binary Reed-Muller codes the problems of finding the number of the minimal and non-minimal codewords of weight $2d_{\min}$ are equivalent, because the total number of the codewords of weight $2d_{\min}$ is well known (Kasami et al. [8]).

The paper is organized as follows: in the next section we find the number of the non-minimal codewords of weight $2d_{\min} = 2^{m-r+1}$ in an arbitrary binary Reed-Muller code $RM(r,m)$. This result generalizes the result of Ashikhmin and Barg for second order Reed–Muller code [2]. In the last section we first estimate the weights of minimal codewords in $RM(r,m)$, when $r \geq \lfloor \frac{m}{2} \rfloor$, using Lemma 3 (iii). Then we prove that all codewords of weight greater than $2^m - 2^{m-r+1}$ of the considered codes are non-minimal. This is again a generalization of the result in [2] for $RM(2,m)$. Note also that the bound $2^m - 2^{m-r+1}$ is better than the one given by Lemma 3 (iii), when m is sufficiently large with respect to r.

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

According to Lemma 3 (ii) any non-minimal codeword of weight $2d_{\min}$ in a binary linear code is a sum of two codewords of minimum weight having non-intersecting supports. But some non-minimal codewords could have more than one representation as a sum of two codewords of minimum weight. Theorem 5 gives the number of such non-minimal codewords of weight $2d_{\min}$. To prove it we will follow the geometric approach of Juriaan Simonis, which is applied in the proof of Theorem 2.9 in [2]. We will also use the following notation (for $q = 2$).

Definition 4 ([3]) *The quantity known as* ***q-ary gaussian coefficient*** *is defined by:*

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

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

Theorem 5 *The number of non-minimal codewords in* $RM(r,m)$ *of weight* $2d_{\min}$*, which have more than one representation as a sum of two codewords of weight* $d_{\min}$ *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. Let us consider a codeword $\mathbf{c}$ of weight $2d_{\min}$, which has more than one representation as a sum of two codewords of weight d_{min}. In geometric terms it means that there exist two pairs of $(m-r)$-dimensional affine subspaces π_1, π_2 and τ_1, τ_2 of $AG(m,2)$, such that the set M corresponding to $\mathbf{c}$ coincides with $M \equiv \pi_1 \cup \pi_2 \equiv \tau_1 \cup \tau_2$. Since the intersection of two affine

subspaces is again an affine subspace, any of the intersections $\rho_{ij} = \pi_i \cap \tau_j$, $i = 1, 2$, $j = 1, 2$ is an affine subspace of dimension $m - r - 1$. Thus, they are translations of $(m - r - 1)$-dimensional vector subspaces. Let $\rho_{11} = \bar{t} + \xi$, where ξ is a $(m - r - 1)$-dimensional vector subspace and $\bar{t}$ is the translation vector. Then $\pi_1 - \bar{t}$ and $\tau_1 - \bar{t}$ are vector subspaces of dimension $m - r$. Hence, $\rho_{12} - \bar{t} = \bar{a} + \xi$ and $\rho_{21} - \bar{t} = \bar{b} + \xi$. Therefore the set M is a union of four translations of the $(m - r - 1)$-dimensional vector subspace ξ (see Figure 1) and

$$\rho_{12} = \bar{a} + \rho_{11}, \quad \rho_{21} = \bar{b} + \rho_{11}, \quad \rho_{22} = \bar{c} + \rho_{21}, \quad \rho_{22} = \bar{d} + \rho_{12},$$

for some vectors $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{d}$, where $\bar{d} \in (\bar{b} + \bar{c} - \bar{a}) + \xi$.

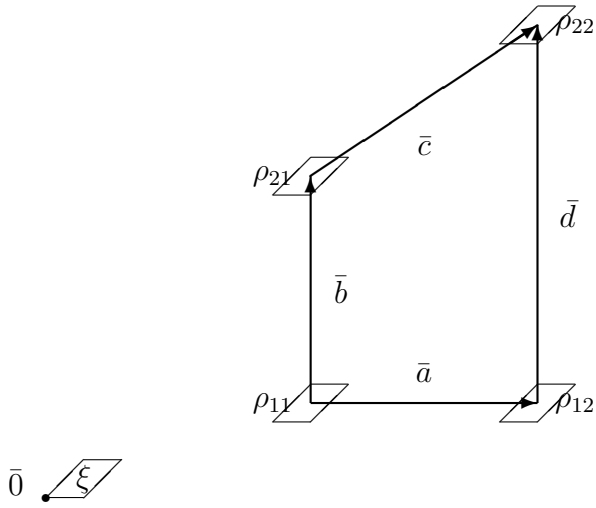

Fig. 1. The vector space ξ and its four translations in some fixed order which constitute the set M

There are two possible cases:
a) If $\bar{c} \in \bar{a} + \xi$ (thus $\bar{d} \in \bar{b} + \xi$), then $M = \bar{t} + \{\xi \cup (\bar{a} + \xi) \cup (\bar{b} + \xi) \cup (\bar{a} + \bar{b} + \xi)\}$ is an affine subspace of dimension $m - r + 1$. (M has dimension $(m - r - 1 + 2)$, since vectors $\bar{a}$, $\bar{b}$, $\bar{c}$ and $\bar{d}$ can be chosen from a 2-dimensional vector subspace having trivial intersection with ξ, and ξ itself has dimension $(m - r - 1)$.) Obviously the converse is true as well. Namely, if M is an affine subspace of dimension $m - r + 1$, then vectors $\bar{a}$, $\bar{b}$, $\bar{c}$ and $\bar{d}$ are from a 2-dimensional vector subspace. Therefore, in this case, the non-minimal codewords of weight $2d_{\min}$ are the affine subspaces in $AG(m, 2)$ of dimension $m - r + 1$. By [3, Th. 13.7.5] their number $A_{r,m}$ is equal to

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

Each codeword is represented as a sum of two codewords of minimum weight in as many ways as half the number of the affine $(m-r)$-dimensional subspaces that it contains, i.e. in

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

different ways.

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

Let $B_{r,m}$ be the number of the non-minimal codewords of weight $2d_{\min}$ described in case **b)**, i.e. which have exactly 3 representations as a sum of two codewords of minimum weight. It can be calculated as follows: the four $(m-r-1)$-flats $\rho_{ij}, i, j = 1, 2$, are translations of $(m-r-1)$-dimensional vector space ξ. Thus, they can be chosen in $\binom{2^{r+1}}{4}$ different ways, since the number of the different translations of a fixed vector space of dimension $m-r-1$ is 2^{r+1}. But we have to exclude the flats that are already counted in case **a)**, i.e. the number of 2-flats in an $r+1$-dimensional vector space. Therefore, the number of the considered in case **b)** translations of a given ξ is:

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

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 case **b)**. Namely, we have

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

□

Theorem 6 *The number of non-minimal codewords in $RM(r, m)$ of weight*

$2d_{\min}$, which have only one representation as a sum of two codewords of minimum weight $d_{\min}$ is given by

$$C_{r,m} = P_{r,m} - S_{r,m},$$

where $S_{r,m}$ is the number of the representations of the codewords considered in Theorem 5 as a sum of two codewords of weight $d_{\min}$ and

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

is the number of the pairs of non-intersecting $(m-r)$-dimensional affine subspaces.

PROOF. According to Theorem 5 $A_{r,m}$ non-minimal codewords of weight $2d_{\min}$ in $RM(r,m)$ have $2^{m-r+1}-1$ representations each as a sum of two codewords of weight d_{min} and $B_{r,m}$ non-minimal codewords have only 3 such representations. Therefore, $S_{r,m} = (2^{m-r+1}-1)A_{r,m} + 3B_{r,m}$. This number can also be rewritten as follows:

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

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

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

Obviously if $m \le 2m-2r-k-1$, i.e. if $k < m-2r$, expression (2) vanishes. 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 $a = \max\{0, m-2r\}$):

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

Let $E_{r,m}$ be the number of those $(m-r)$-flats which do not have common point with π. It is equal to the difference between the number of all $(m-r)$-dimensional affine subspaces in $AG(m,2)$ and 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

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

□

Combining Theorem 5 and Theorem 6 we get

Theorem 7 *The number of the non-minimal codewords of weight $2d_{min} = 2^{m-r+1}$ in $RM(r,m)$ is*

$$N_{r,m} = A_{r,m} + B_{r,m} + C_{r,m}.$$

Example 8 *Let us consider the Reed-Muller code $RM(3,5)$. It has block length 32, minimum weight $d_{\min} = 4$ and it is in fact the extended binary Hamming code. For these parameters we have $A_{3,5} = 620$, $B_{3,5} = 52080$, $C_{3,5} = 277760$. Therefore $N_{3,5} = 330460$, i.e. the number of non-minimal codewords in $RM(3,5)$ of weight 8 is 330460.*

Setting $r = 2$ in Theorem 7 we get

$$N_{2,m} = 2^{m+1} - 2 + (4/3)(2^m - 1)(2^{m-1} - 1)(2^{m-1} - 2),$$

which is the result of Ashikhmin and Barg for the second order Reed-Muller code [2].

Proposition 9 *Let $RM(r,m)$ be a binary Reed-Muller code of order $r > 1$.*

If $\mathbf{c}$ *is non-minimal codeword of weight* $2d_{\min}$ *and* $\mathbf{1}$ *is the all-one vector of length* 2^m *then* $\mathbf{c}+\mathbf{1}$ *is a non-minimal codeword as well.*

PROOF. By Lemma 3 (ii) codeword $\mathbf{c}$ can be presented as a sum of two codewords $\mathbf{c}_1$ and $\mathbf{c}_2$ each of minimum weight $d_{\min}$. As codewords of minimum weght $\mathbf{c}_1$ 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 a 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 is an $(m-2)$-dimensional affine subspace.
2. ρ_1 is an identical with ρ_2.
3. ρ_1 and ρ_2 is an complements to 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 $supp(\mathbf{c}_1)$ or $supp(\mathbf{c}_2)$. $\square$

3 Some links between non-minimality of the codewords and their weights

Theorem 10 *Let* $RM(r,m)$ *be a binary Reed-Muller code of length* $n=2^m$*, dimension* k *and* $r \geq \lfloor \frac{m}{2} \rfloor$*, then:*
a) any codeword of weight greater then 2^{m-1} *is non-minimal.*
b) for $m \to \infty$ *any codeword of weight greater than* $2^{mH_2(\frac{m-1-r}{m})}+1$ *is non-minimal.*

PROOF. a) Since $\sum_{i=0}^{m}\binom{m}{i}=2^m$, we have $k=\sum_{i=0}^{\lfloor \frac{m}{2} \rfloor}\binom{m}{i}+\sum_{i=\lfloor \frac{m}{2} \rfloor+1}^{r}\binom{m}{i} \geq 2^{m-1}$. Hence, $n-k+1 \leq 2^m-2^{m-1}+1=2^{m-1}+1$. Therefore, we may apply Lemma 3 (iii), to deduce that any codeword of weight $> 2^{m-1}$ is non-minimal. (Note that $wt(\mathbf{c})$ is always even except in the trivial case $r=m$.)

b) We may write $k=\sum_{i=0}^{r}\binom{m}{i}=2^m-\sum_{i=0}^{r'}\binom{m}{i}$, where $r'=m-r-1$. Thus, $n-k=2^m-\left[2^m-\sum_{i=0}^{r'}\binom{m}{i}\right]=\sum_{i=0}^{r'}\binom{m}{i}$. Since $\mu=\frac{r'}{m}<\frac{1}{2}$, the inequality (10.20) in [5, Ch.10] gives

$$\sum_{i=0}^{r'}\binom{m}{i} \leq 2^{mH_2(\frac{r'}{m})},$$

where $H_2(x)=-x\log_2 x-(1-x)\log_2(1-x)$, $0 \leq x \leq 1$ is the entropy. Then $n-k+1 \leq 2^{mH_2(\frac{m-1-r}{m})}+1$ and, according to Lemma 3 (iii), any codeword of weight greater than the right-hand side is non-minimal. $\square$

Theorem 13 presents a more general property of the non-minimal codewords in Reed-Muller codes. It can be considered as a generalization of the Ashikhimin and Barg's result [2] for codewords of weight greater than 2^{m-1} in $RM(2,m)$. To prove it we need some properties of Boolean functions.

Let f be a Boolean function and let us denote $T(f) = \{\bar{x} | f(\bar{x}) = 1\}$, i.e. $T(f)$ is the set of arguments for which the value of f is 1. The following Lemma is straightforward.

Lemma 11 *Let f_1, f_2 be Boolean functions such that $T(f_1) \cup T(f_2) \subset F_2^m$. Then $T(f_1 + f_2) \subset T(f_1 f_2 + 1)$.*

Also, we will use the following result due to Kasami and Tokura.

Theorem 12 ([7]) *Let $f(x_1, \ldots, x_m)$ be a Boolean function of degree at most r, where $r \geq 2$, such that $|T(f)| < 2^{m-r+1}$. Then f can be transformed by an affine transformation into either*

$$(i)\ f = x_1 \ldots x_{r-2}(x_{r-1}x_r + x_{r+1}x_{r+2} + \cdots + x_{r+2\mu-3}x_{r+2\mu-2}), \quad 2 \leq 2\mu \leq m - r + 2$$

$$(ii)\ f = x_1 \ldots x_{r-\mu}(x_{r-\mu+1} \ldots x_r + x_{r+1} \ldots x_{r+\mu}), \quad 3 \leq \mu \leq r,\ \mu \leq m - r$$

Theorem 13 *Let $RM(r,m)$ be the binary Reed-Muller code of order $r \geq 3$. Then any codeword $\mathbf{c}$ of weight $wt(\mathbf{c}) > 2^m - 2^{m-r+1}$ is non-minimal.*

PROOF. Let $\mathbf{c} \in RM(r,m)$ be a codeword of weight $wt(\mathbf{c}) > 2^m - 2^{m-r+1}$. Then $\mathbf{c} + \mathbf{1}$ is a codeword of weight $wt(\mathbf{c} + \mathbf{1}) < 2^{m-r+1}$. Let f be the Boolean polynomial of degree r corresponding to $\mathbf{c}$. According to Theorem 12 f can be transformed by an affine transformation into one of the following Boolean functions:

$$(i)\ f = x_1 \ldots x_{r-2}(x_{r-1}x_r + x_{r+1}x_{r+2} + \cdots + x_{r+2\mu-3}x_{r+2\mu-2}) + 1, \quad 2 \leq 2\mu \leq m - r + 2$$

$$(ii)\ f = x_1 \ldots x_{r-\mu}(x_{r-\mu+1} \ldots x_r + x_{r+1} \ldots x_{r+\mu}) + 1, \quad 3 \leq \mu \leq r,\ \mu \leq m - r$$

Let us consider case (i). Setting $f_1 = x_1 \ldots x_{r-2}$ and $f_2 = x_{r-1}x_r + x_{r+1}x_{r+2} + \cdots + x_{r+2\mu-3}x_{r+2\mu-2}$ we have $f = f_1 f_2 + 1$. For at least one point ($\bar{x} = \mathbf{0}$) we have $f_1(\bar{x}) = f_2(\bar{x}) = 0$. Thus $T(f_1) \cup T(f_2) \subset F_2^m$. Analogously, in case (ii) when $r > \mu$, we set $f_1 = x_1 \ldots x_{r-\mu}$ and $f_2 = x_{r-\mu+1} \ldots x_r + x_{r+1} \ldots x_{r+\mu}$. Then $f = f_1 f_2 + 1$ and the condition of Lemma 11 is again satisfied. In both cases $\tilde{f} = f_1 + f_2$ is a Boolean polynomial of degree $\leq r$. Applying Lemma 11 we can conclude that the polynomial $\tilde{f}$ has $T(\tilde{f}) \subset T(f)$, i.e. its corresponding codeword $\tilde{\mathbf{c}}$ is in $RM(r,m)$ and $supp(\tilde{\mathbf{c}}) \subset supp(\mathbf{c})$. Therefore,

$\mathbf{c}$ is non-minimal.
Now let $r = \mu$ in case (ii). Then $f = x_1x_2\dots x_r + x_{r+1}x_{r+2}\dots x_{2r} + 1$ and $2r \leq m$. When $m = 2r$ the non-minimality of $\mathbf{c}$ in $RM(r, 2r)$ follows from Theorem 10 a) since $wt(\mathbf{c}) > 2^{2r} - 2^{r+1} > 2^{2r-1}$. For $m > 2r$ codeword $\mathbf{c}$ is a concatenation of 2^{m-2r} copies of a codeword $\mathbf{c_1} \in RM(r, 2r)$. From the previous case ($m = 2r$) codeword $\mathbf{c_1}$ is non-minimal. Thus, there exists $\mathbf{c_2} \in RM(r, 2r)$, such that $\mathbf{c_2} \prec \mathbf{c_1}$. The concatenation of 2^{m-2r} copies of $\mathbf{c_2}$ will be a codeword of $RM(r, m)$ and the support of $\mathbf{c}$ contains its support. Therefore, $\mathbf{c}$ is non-minimal. $\square$

In fact, Theorem 13 is weaker than Theorem 10 for $m \leq 2r + 1$, but it gives better results than Lemma 3 (iii), when m is sufficiently large with respect to r. For example, if $r = 3,\ m \geq 10$ then $2^m - 2^{m-r+1} < n - k + 1$.

Acknowledgements

The authors would like to thank H. van Tilborg and A. Barg for the helpful discussions and comments. The authors wish to thank the anonymous referees for their careful reading and valuable suggestions which led to a much improved manuscript.

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.

[7] T.Kasami, N.Tokura, *On the weight structure of Reed-Muller codes*, IEEE Trans. Inf. Theory, IT-16, 1970, 6, 752–759.

[8] T.Kasami, N.Tokura, S. Azumi *On the weight enumeration of weights less than 2.5d of Reed-Muller codes*, Inform. and Contr. 30, 1976, 380–395.