

# On the Non-Minimal codewords in the binary Reed-Muller Code

Yuri Borissov, Nickolay Manev<sup>1</sup>

Institute of Mathematics and  
Informatics,  
Bulgarian Academy of Sciences,  
8 G.Bonchev, 1113 Sofia, Bulgaria,  
e-mail: yborisov,  
nlmanev@moi.math.bas.bg

Svetla Nikova<sup>2</sup>

Dept. Electr. Eng. ESAT/COSIC,  
Katholieke Universiteit Leuven,  
Kasteelpark Arenberg 10,  
B-3001 Leuven-Heverlee, Belgium,  
e-mail:  
svetla.nikova@esat.kuleuven.ac.be

**Abstract** — We prove that all codewords of weight greater than  $2^m - 2^{m-r+1}$  in the binary Reed-Muller code of order  $r$  are non-minimal.

## I. INTRODUCTION

Let  $C$  be a  $q$ -ary code of length  $n$  and let us denote by  $[n] := \{1, 2, \dots, n\}$  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  $q$ -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 true subset. The support of a minimal codeword is called minimal with respect to  $C$ .

By  $\mathcal{M}(C)$  is denoted the set of minimal vectors of given code  $C$ . The following basic property of  $\mathcal{M}(C)$  is proven in [1]:

**Lemma 2 (Ashikhmin, Barg)** If  $\mathbf{c}$  is minimal codeword in a linear  $[n, k, d]$  code  $C$ , then  $\text{wt}(\mathbf{c}) \leq n - k + 1$ .

Let  $RM(r, m)$  be the binary Reed-Muller code of order  $r$  with the parameters  $[n = 2^m, k = \sum_{i=0}^r \binom{m}{i}, d = 2^{m-r}]$ .

For the boolean function  $f$  let us denote  $\mathcal{T}(f) = \{\bar{x} | f(\bar{x}) = 1\}$ , i.e.  $\mathcal{T}(f)$  is the set of arguments for which the value of  $f$  is 1.

**Lemma 3** Let  $f_1, f_2$  be non-constant boolean functions. Then  $\mathcal{T}(f_1 + f_2) \subset \mathcal{T}(f_1 f_2 + 1)$  and  $\mathcal{T}(f_1 + 1) \subset \mathcal{T}(f_1 f_2 + 1)$ .

In our investigations we use the following theorem by Kasami and Tokura [2].

**Theorem 4 (Kasami, Tokura)** Let  $f(x_1, \dots, x_m)$  be a Boolean function of degree at most  $r$ , where  $r \geq 2$ , such that  $|\mathcal{T}(f)| < 2^{m-r+1}$ . Then  $f$  can be transformed by an invertible affine transformation into either

$$\begin{aligned} (i) \quad f &= x_1 \dots x_{r-2} (x_{r-1} x_r + x_{r+1} x_{r+2} + \dots \\ &\quad + x_{r+2\mu-3} x_{r+2\mu-2}), \quad 2 \leq 2\mu \leq m - r + 2 \\ (ii) \quad f &= x_1 \dots x_{r-\mu} (x_{r-\mu+1} \dots x_r + x_{r+1} \dots x_{r+\mu}), \\ &\quad 3 \leq \mu \leq r, \quad \mu \leq m - r. \end{aligned}$$

<sup>1</sup>The authors were partially supported by Bulgarian NSF Contract I-803

<sup>2</sup>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.

## II. SOME CONNECTIONS BETWEEN NON-MINIMALITY OF THE CODEWORDS AND THEIR WEIGHTS

In this section we estimate the weights of minimal codewords in  $RM(r, m)$ , when  $r \geq \lfloor \frac{m}{2} \rfloor$ , using Lemma 2. Before formulating the first theorem we need to remind the definition of the entropy function  $H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ , where  $0 < x < 1$  and  $H_2(0) = H_2(1) = 0$ .

**Theorem 5** Let  $RM(r, m)$  be binary Reed-Muller code with length  $n$ , dimension  $k$  and  $r \geq \lfloor \frac{m}{2} \rfloor$ , then:

- any codeword of weight greater than  $2^{m-1}$  is non-minimal.
- for all sufficiently large  $m$ , any codeword of weight greater than  $2^{m H_2(\frac{m-1-r}{m})} + 1$  is non-minimal.

Now we will give another more general property of the non-minimal codewords, namely that all codewords of weight greater than  $2^m - 2^{m-r+1}$  are non-minimal in  $RM(r, m)$ . In fact, for  $m \leq 2r + 1$  it is weaker than Theorem 5, but it gives better results than Lemma 2, when  $m$  is sufficiently large with respect to  $r$ .

**Proposition 6** Let  $RM(r, m)$  be the binary Reed-Muller code of order  $r \geq 3$ . Then any codeword  $\mathbf{c}$  of weight

$$\text{wt}(\mathbf{c}) > 2^m - 2^{m-r+1} \quad (1)$$

is non-minimal.

This proposition can be considered as a generalization for any  $r > 1$  of the corresponding Ashikhmin and Barg's result [1] for  $RM(2, m)$ .

It remains an open problem to find the greatest integer  $U = U(r, m)$  such that there exist minimal codewords of weight  $U$  in  $RM(r, m)$ .

Finally, based on the results of [3] we improve the bound (1) for  $RM(3, m)$ .

**Proposition 7** Any codeword of weight either  $2^m - 2^{m-2}$  or  $2^m - 2^{m-2} - 2^{m-6}$  is non-minimal in the binary  $RM(3, m)$  code.

## ACKNOWLEDGMENTS

The authors would like to thank to H. van Tilborg and A. Barg for the helpful discussions and comments.

## REFERENCES

- A. Ashikhmin and A. Barg, "Minimal vectors in linear codes", *IEEE Trans. Inf. Theory*, vol.44, 1998, 5, pp. 2010–2017.
- T. Kasami, N. Tokura, "On the weight structure of Reed-Muller codes", *IEEE Trans. Inf. Theory*, vol.16, 1970, 6, pp. 752–759.
- H. C. A. van Tilborg, "On weights in codes", Dept. of Math., Technological University, Eindhoven, The Netherlands, 1971.