Advances in Mathematics of Communications
Volume 5, No. 2, 2011, 333–337

doi:10.3934/amc.2011.5.333

ON THE NON-MINIMALITY OF THE LARGEST WEIGHT CODEWORDS IN THE BINARY REED-MULLER CODES

Andreas Klein and Leo Storme

Department of Mathematics, Ghent University
Krijgslaan 281 - S22, 9000 Ghent, Belgium

(Communicated by Axel Kohnert)

Abstract. The study of minimal codewords in linear codes was motivated by Massey who described how minimal codewords of a linear code define access structures for secret sharing schemes. As a consequence of his article, Borissov, Manev, and Nikova initiated the study of minimal codewords in the binary Reed-Muller codes. They counted the number of non-minimal codewords of weight $2d$ in the binary Reed-Muller codes $\mathrm{RM}(r, m)$, and also gave results on the non-minimality of codewords of large weight in the binary Reed-Muller codes $\mathrm{RM}(r, m)$. The results of Borissov, Manev, and Nikova regarding the counting of the number of non-minimal codewords of small weight in $\mathrm{RM}(r, m)$ were improved by Schillewaert, Storme, and Thas who counted the number of non-minimal codewords of weight smaller than $3d$ in $\mathrm{RM}(r, m)$. This article now presents new results on the non-minimality of large weight codewords in $\mathrm{RM}(r, m)$.

1. Introduction

This article discusses the minimality of codewords in the binary Reed-Muller codes $\mathrm{RM}(r, m)$. We first present the two definitions of minimal codewords and of binary Reed-Muller codes.

Definition 1. Let C be a q-ary linear code. A nonzero codeword c of C is called *minimal* if its support does not contain the support of any other nonzero codeword of C as a proper subset.

Definition 2. 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 f of length 2^m associated with the Boolean polynomials $f(x_1, \ldots, x_m)$ of degree at most r.

It is a known property that the minimum weight codewords of $\mathrm{RM}(r, m)$ have weight $d = 2^{m-r}$ and that they are in fact the incidence vectors of the $(m - r)$-dimensional subspaces of the affine geometry $\mathrm{AG}(m, 2)$ [6]. In two articles [3, 4], the codewords of $\mathrm{RM}(r, m)$ of weight smaller than $5d/2 = 2^{m-r+1} + 2^{m-r-1}$ are classified. In particular, the codewords of weight smaller than $2d$ are the incidence vectors of $(m-r)$-dimensional subspaces of $\mathrm{AG}(m, 2)$, particular quadrics of $\mathrm{AG}(m, 2)$ and of symmetric differences of $(m - r)$-dimensional subspaces of $\mathrm{AG}(m, 2)$ [3, 8].

In [7], Massey showed how minimal codewords can be used to define access structures for secret sharing schemes. This motivated Borissov, Manev, and Nikova to calculate the number of non-minimal codewords of weight $2d$ in $\mathrm{RM}(r, m)$ [2].

2000 *Mathematics Subject Classification:* Primary: 94B05; Secondary: 51E20.
Key words and phrases: Reed-Muller codes, minimal codewords.

Since such a non-minimal codeword c must be the sum $c_1 + c_2$ of two codewords of $\mathrm{RM}(r, m)$ of weight d having disjoint supports, this reduced to the geometrical problem of counting the number of disjoint pairs of $(m - r)$-dimensional subspaces of $\mathrm{AG}(m, 2)$. For the exact formula of the number of non-minimal codewords of weight $2d$ in $\mathrm{RM}(r, m)$, we refer to [2].

By [3, 8], every codeword c in $\mathrm{RM}(r, m)$ of weight smaller than $2d$ corresponds to the incidence vector of an $(m - r)$-dimensional subspace of $\mathrm{AG}(m, 2)$, a particular quadric of $\mathrm{AG}(m, 2)$ or to a symmetric difference of two $(m - r)$-dimensional affine subspaces of $\mathrm{AG}(m, 2)$. This enabled Schillewaert, Storme, and Thas to improve the results of Borissov, Manev, and Nikova by counting the number of non-minimal codewords of $\mathrm{RM}(r, m)$ of every weight in $\mathrm{RM}(r, m)$ smaller than $3d$. For the exact formula of the number of non-minimal codewords of a weight smaller than $3d$ in $\mathrm{RM}(r, m)$, we refer to [8].

But [2] also presented results on the non-minimality of large weight codewords of $\mathrm{RM}(r, m)$, which are summarized in Theorem 1. In the next theorem, $\mathbf{1}$ is the all-one vector of length 2^m and $H_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$, $0 < x < 1$, denotes the entropy.

Theorem 1.
1. *If c is a non-minimal codeword in $RM(r, m)$, $r > 1$, of weight $2d$, then $c + \mathbf{1}$ is a non-minimal codeword as well.*
2. *Let $RM(r, m)$ be the binary Reed-Muller code with $r \geq \lfloor \frac{m}{2} \rfloor$, then*
   - *any codeword of weight larger than 2^{m-1} is non-minimal,*
   - *for $m \to \infty$, any codeword of weight larger than $2^{mH_2(\frac{m-r-1}{m})} + 1$ is non-minimal.*
3. *Consider the binary Reed-Muller code $RM(r, m)$ of order $r \geq 3$, then every codeword c of weight larger than $2^m - 2^{m-r+1}$ is non-minimal.*

To conclude this introduction, we briefly state the concept of using minimal codewords in a linear code to define the access structure of a secret sharing scheme, described by Massey in [7].

Let C be a linear $[n, k, d]$-code over $\mathbb{F}_q$, having the parity check matrix H.

- The secret s is chosen as the first digit of a codeword of C.
- The symbols in $k - 1$ other positions, which together with the first position form an information set for C, are selected uniformly at random over $\mathbb{F}_q$.
- The corresponding codeword $c = (c_1, \ldots, c_n)$ of C is determined.
- The other $n - 1$ positions $c_2, \ldots, c_n$ are the shares distributed to the $n - 1$ participants of the secret sharing scheme.

The access to the secret s goes via the parity check matrix H of C. Namely, suppose that the persons having the shares $c_2, \ldots, c_r$ wish to put their shares together to recover the secret s via the parity check matrix H of c. This is only possible if there is a non-zero codeword $d = (d_1, \ldots, d_n)$ in $C^\perp$ having all its non-zero positions in the first r positions, with $d_1 \neq 0$, because then $c \cdot d = c_1 d_1 + \cdots + c_r d_r = 0$, i.e., $s = c_1 = -(c_2 d_2 + \cdots + c_r d_r)/d_1$.

If the codeword $d \in C^\perp$ is non-minimal, then there is a codeword $d' = (d'_1, \ldots, d'_r, 0, \ldots, 0) \in C^\perp$ with $\mathrm{supp}(d') \subset \mathrm{supp}(d)$, such that $c \cdot d' = c_1 d'_1 + \cdots + c_r d'_r = 0$, i.e., $s = c_1 = -(c_2 d'_2 + \cdots + c_r d'_r)/d'_1$. But since $\mathrm{supp}(d') \subset \mathrm{supp}(d)$, this implies that a smaller number of persons have access to the secret s, than originally.

Since every non-zero codeword in $C^\perp$, with first position different from zero, is either minimal, or is non-minimal and then there is an other non-zero minimal codeword in $C^\perp$, with first position different from zero, the access structure of the secret sharing scheme defined above is completely determined by the minimal codewords of $C^{\perp}$ having a non-zero symbol in the first position, thus motivating the study of minimal codewords in linear codes.

For more properties of minimal codewords, we refer to [1].

2. New results

We now present our new results. We extend the ideas of [2, Section 3]. We rely on results of [4], and therefore use the notations of that article. Let P_r denote the set of binary polynomials $f(x_1, \ldots, x_m)$ of degree at most r. For $f \in P_r$, we write that $f \in P_{r,n}$ if there exist n mutually independent linear polynomials $u_1, \ldots, u_n$ such that $u_1 = \cdots = u_n = 0$ implies that $f \equiv 0$. Equivalently, $f \in P_{r,n}$ if f defines a codeword $c \in \mathrm{RM}(r, m)$ whose support is contained in the union of n mutually independent hyperplanes $u_1 = 1, \ldots, u_n = 1$. We will use in this article the terminology that *the corresponding codeword c is covered by n mutually independent hyperplanes.*

We first mention the following result on the second weight of the binary Reed-Muller code $\mathrm{RM}(r, m)$ [3].

Theorem 2. *The second weight of the binary Reed-Muller code RM(r, m) is equal to* $\frac{3d}{2} = 2^{m-r} + 2^{m-r-1}$.

A key lemma in the classification result of the codewords of weight smaller than $\frac{5}{2}d$ in $\mathrm{RM}(r, m)$ is the following observation.

Lemma 1 ([5], Theorem 1, part 1)**.** *If $f \in P_r$, $r \geq 4$, and $|f| < 2^{m-r+1} + 2^{m-r-1}$, then $f \in P_{r,2}$, i.e. the corresponding codeword c can be covered by two non-parallel hyperplanes.*

The main result of this article is the following generalisation of Lemma 1.

Theorem 3. *Let $k \geq 2$. If $f \in P_r$, $r \geq 4$, and $|f| < (3 - 2^{-k+1})d$, then $f \in P_{r,k}$, i.e. the corresponding codeword c can be covered by k linearly independent hyperplanes.*

Proof. We prove the theorem by induction on k. For a fixed k, we prove the theorem by induction on m. The trivial starting point for the inner induction is the case $r = m$, then the Reed-Muller code $\mathrm{RM}(m, m)$ is the complete binary vector space $V(2^m, 2)$ having minimum distance $d = 1$. Then the upper bound $(3 - 2^{-k+1})d < 3$. So $\mathrm{wt}(c) \leq 2$, and then c is trivially covered by two linearly independent hyperplanes and if $m \geq 2$, even trivially by one hyperplane.

The case $k = 2$ is the result of Kasami *et al* (Lemma 1). Now let $k > 2$.

Step 1: f $\in P_{r,k+1}$.

There is a hyperplane h with $|f_h| \leq \frac{1}{2}|f|$. Here, f_h defines the restriction of f to the hyperplane h and this is a codeword in $\mathrm{RM}(r, m-1)$, where $\mathrm{RM}(r, m-1)$ has minimum weight $d/2$. By the induction on m, f_h can be covered by k hyperplanes in h and hence $f \in P_{r,k+1}$.

Step 2: Find a low weight codimension k space.

Since f is covered by at most $k+1$ linearly independent hyperplanes, we can assume after a coordinate transformation that $f = x_1 f_1 + x_2 f_2 + \cdots + x_{k+1} f_{k+1}$.

By $f_{a_1,\dots,a_{k+1}}$, we denote the restriction of f to the codimension $k+1$ subspace $x_1 = a_1, \dots, x_{k+1} = a_{k+1}$. Since each term of f has a factor x_i, $i \le k+1$, the restriction $f_{a_1,\dots,a_{k+1}}$ has at most degree $r-1$. Furthermore $f_{0,\dots,0} \equiv 0$.

Suppose that $f_{a_1,\dots,a_{k+1}} \equiv 0$ for some $(a_1,\dots,a_{k+1}) \ne 0$. Then the codimension k subspace $\Pi = \{x_1 = \cdots = x_{k+1} = 0 \text{ or } x_1 = a_1, \dots, x_{k+1} = a_{k+1}\}$ has weight zero.

On the other hand, suppose that $f_{a_1,\dots,a_{k+1}} \not\equiv 0$ for $(a_1,\dots,a_{k+1}) \ne 0$. So the $2^{k+1}-1$ parallel codimension $k+1$ spaces are non empty. The minimal weight in a codimension $k+1$ space is $\frac{d}{2^k}$ and the next weight is $\frac{3d}{2^{k+1}}$ (Theorem 2).

Not all those parallel codimension $k+1$ spaces can be of weight $\frac{3d}{2^{k+1}}$ since $(2^{k+1}-1)\frac{3d}{2^{k+1}} > (3-2^{-k+1})d$. So there is a parallel codimension $k+1$ space of weight $\frac{d}{2^k}$. Together with the empty space, we have proven the existence of a codimension k space of weight $\frac{d}{2^k}$.

At this point we have found a codimension k subspace Π which is either empty or of weight $\frac{d}{2^k}$.

Step 3: Count the hyperplanes through Π.

The average weight of a hyperplane through Π can be easily computed and at least one hyperplane must be below or equal to the average weight. Thus there is a hyperplane h with

$$|f_h| \le \frac{2^{k-1}-1}{2^k-1}\left(|f| - \frac{d}{2^k}\right) + \frac{d}{2^k} \tag{1}$$

$$< \frac{2^{k-1}-1}{2^k-1}\left((3-2^{-k+1})d - \frac{d}{2^k}\right) + \frac{d}{2^k} = (3-2^{-k+2})\frac{d}{2}. \tag{2}$$

Step 4: Apply the induction hypothesis.

By the induction hypothesis, f_h has only $k-1$ terms, hence $f \in P_{r,k}$. ☐

3. Applications of Theorem 3

As an application of Theorem 3, we generalise Theorem 1, part (3), that states that large weight codewords in $\mathrm{RM}(r,m)$ are non-minimal.

Lemma 2. *Let $c \in RM(r,m)$, $r \ge 4$, be strictly contained in the union of k hyperplanes $H_1,\dots,H_k$, where the complement hyperplanes $\bar{H}_1,\dots,\bar{H}_k$ intersect in at least an $(m-r)$-space, i.e. $\dim(\bar{H}_1 \cap \cdots \cap \bar{H}_k) \ge m-r$.*

Then $c + \mathbf{1}$ is a non-minimal codeword of $RM(r,m)$.

Proof. Since $\dim(\bar{H}_1 \cap \cdots \cap \bar{H}_k) \ge m-r$, the intersection $\bar{H}_1 \cap \cdots \cap \bar{H}_k$ is a codeword of $\mathrm{RM}(r,m)$. The complement of a codeword in $\mathrm{RM}(r,m)$ is also a codeword of $\mathrm{RM}(r,m)$, i.e. $H_1 \cup \cdots \cup H_k \in \mathrm{RM}(r,m)$.

Thus $c + (H_1 \cup \cdots \cup H_k)$ is a non-zero codeword of $\mathrm{RM}(r,m)$. Since $c \subset H_1 \cup \cdots \cup H_k$, we have $c + (H_1 \cup \cdots \cup H_k) \subset H_1 \cup \cdots \cup H_k$ and hence the non-zero codewords $c + (H_1 \cup \cdots \cup H_k)$ and $\bar{H}_1 \cap \cdots \cap \bar{H}_k$ have disjoint supports.

Thus

$$c + \mathbf{1} = (\bar{H}_1 \cap \cdots \cap \bar{H}_k) + (c + (H_1 \cup \cdots \cup H_k))$$

is a non-minimal codeword of $\mathrm{RM}(r,m)$. ☐

We now can formulate the improvement to Theorem 1, part (3).

Corollary 1. *Let c be a codeword of RM(r, m), $r \geq 4$, of weight larger than $2^m - 3 \cdot 2^{m-r} + 2^{m-2r+1}$, then c is non-minimal.*

Proof. The complement $c + \mathbf{1}$ has weight less than $(3 - 2^{-r+1})d < 2^{m-1}$, hence, by Theorem 3, it is strictly contained in the union of r hyperplanes $H_1, \ldots, H_r$. The intersection $\bar{H}_1 \cap \cdots \cap \bar{H}_r$ has at most codimension r. By Lemma 2, c is a non-minimal codeword. □

Acknowledgements

The authors thank the referees very much for their suggestions which improved the first version of this article.

References

[1] A. Ashikhmin and A. Barg, *Minimal vectors in linear codes*, IEEE Trans. Inform. Theory, **44** (1998), 2010–2017.

[2] Y. Borissov, N. L. Manev and S. Nikova, *On the non-minimal codewords in binary Reed-Muller codes*, Discrete Appl. Math., **128** (2003), 65–74.

[3] T. Kasami and N. Tokura, *On the weight structure of Reed-Muller codes*, IEEE Trans. Inform. Theory, **IT-16** (1970), 752–759.

[4] T. Kasami, N. Tokura and S. Azumi, *On the weight enumeration of weight less than* 2.5d *of Reed-Muller codes*, Rept. of Faculty of Eng. Sci., Osaka Univ., Japan, 1974.

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

[6] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.

[7] J. L. Massey, *Minimal codewords and secret sharing*, in "Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory," (1993), 276–279.

[8] J. Schillewaert, L. Storme and J. A. Thas, *Minimal codewords in Reed-Muller codes*, Des. Codes Crypt., **54** (2010), 273–286.

Received May 2010; revised August 2010.

E-mail address: klein@cage.ugent.be
E-mail address: ls@cage.ugent.be