Minimal/Nonminimal Codewords in the Second Order Binary Reed-Muller Code: Revisited

Yuri Borissov
Institute of Mathematics and Informatics, Sofia, Bulgaria
Outline of the talk

- Introduction
Outline of the talk

- Introduction
- Background
Outline of the talk

- Introduction
- Background
- Sketch of the proof
Minimal codewords in linear codes have been applied for:

- test sets in "gradient-like" decoding algorithms:
  - Tai-Yang Hwang, "Decoding Linear Block Codes for Minimizing Word Error Rate", IEEE Trans. on Information Theory vol. 25, November 1979, pp. 733-737;
Minimal codewords in linear codes have been applied for:

- test sets in "gradient-like" decoding algorithms:
  - Tai-Yang Hwang, "Decoding Linear Block Codes for Minimizing Word Error Rate", IEEE Trans. on Information Theory vol. 25, November 1979, pp. 733-737;
- to describe minimal access structure in Secret-Sharing Schemes based on these codes:
The problem of describing the set of minimal codewords has been solved:

- completely, for $q$-ary Hamming code and the second order binary Reed-Muller code in [1];
The problem of describing the set of minimal codewords has been solved:

- completely, for $q$-ary Hamming code and the second order binary Reed-Muller code in [1];
- partially, for two-error-correcting binary BCH codes and $r^{th}$ order binary Reed-Muller code, in [5] and [6], respectively;
The problem of describing the set of minimal codewords has been solved:

- completely, for $q$-ary Hamming code and the second order binary Reed-Muller code in [1];
- partially, for two-error-correcting binary BCH codes and $r^{th}$ order binary Reed-Muller code, in [5] and [6], respectively;
- by computer assistance, for some third-order binary Reed-Muller codes in [7] and [13].
Here, we return to the problem for the second order binary Reed-Muller code solved in [1]. A proof of geometric nature (suggested by Juriaan Simonis) was exhibited in:


In this work, it is presented another comprehensive proof based on Dickson’s Theorem.
DEFINITION 0.1. A support of a binary vector $c$ of length $n$, denoted by $\text{supp}(c)$, is defined as the subset of $c$’s nonzero coordinates. A support of a Boolean function is the support of its truth table.

DEFINITION 0.2. A nonzero codeword $c$ of a binary linear code $C$ is called minimal in $C$ if $\text{supp}(c)$ does not cover the support of another nonzero codeword. Otherwise, $c$ is called non-minimal.
Basic properties of minimal codewords

Proposition 0.3. ([1],[4])

1. If \( c \) is minimal codeword in a linear \([n, k]\)-code then its weight satisfies \( wt(c) \leq n - k + 1 \).
2. Any non-minimal codeword \( c \) in a binary linear code can be represented as a sum of two codewords \( c_1 \) and \( c_2 \) having disjoint supports included in \( supp(c) \).
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 < \( 2d_{\text{min}} \) are minimal.
the second-order Reed-Muller code $RM(2, m)$:

- codewords are truth tables (binary vectors of length $2^m$) of Boolean functions of degree $\leq 2$ in $v = v_1, v_2, \ldots, v_m$.
- typical codeword is given by: $S(v) = vQv^T + Lv + \epsilon$, where $Q$ is an upper triangular binary $m \times m$ matrix, $L$ is a binary vector of length $m$, and $\epsilon$ is 0 or 1.
the second-order Reed-Muller code $RM(2, m)$:

- codewords are truth tables (binary vectors of length $2^m$) of Boolean functions of degree $\leq 2$ in $v = v_1, v_2, \ldots, v_m$.
- typical codeword is given by: $S(v) = vQv^T + Lv + \epsilon$, where $Q$ is an upper triangular binary $m \times m$ matrix, $L$ is a binary vector of length $m$, and $\epsilon$ is 0 or 1.

A coset of $RM(1, m)$ in $RM(2, m)$ is characterized by matrix $Q$ or alternatively (as it turns out) by the binary symmetric matrix $B = Q + Q^T$ with zero diagonal. $B$ is called symplectic matrix and the weight-distribution of the coset depends only on the rank of $B$. 
Background: Dickson’s theorem

(1) If $B$ is a symplectic matrix of rank $2h$, then there exists an invertible binary matrix $R$ such that $RBR^T$ has zeros everywhere except on the two diagonals immediately above and below the main diagonal, and there has $1010 \ldots 100 \ldots 0$ with $h$ ones ($0 < h \leq \lfloor m/2 \rfloor$).

(2) Any quadratic function becomes:
$$T(y) = \sum_{i=1}^{h} y_{2i-1}y_{2i} + L_1(y) + \epsilon$$
under the transformation $y = vR^{-1}$ determined by $R$ from Part (1). Moreover $y_1, \ldots, y_{2h}$ are linearly independent.

(3) If $L_1(y)$ is linearly dependent on $y_1, \ldots, y_{2h}$, by an affine transformation $T(y)$ can be written as:
$$\sum_{i=1}^{h} x_{2i-1}x_{2i} + \epsilon_1, \quad \epsilon_1 = 0 \text{ or } 1,$$
where $x_1, \ldots, x_{2h}$ are linearly independent and each $x_i$ is a linear form in $y_1, \ldots, y_{2h}, 1$. 
Background

**Weight-distribution of cosets of** $RM(1, m)$ **in** $RM(2, m)$.

**Theorem 0.4.** *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:*

<table>
<thead>
<tr>
<th>Weight</th>
<th>Number of Vectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^{m-1} - 2^{m-h-1}$</td>
<td>$2^{2h}$</td>
</tr>
<tr>
<td>$2^{m-1}$</td>
<td>$2^{m+1} - 2^{2h+1}$</td>
</tr>
<tr>
<td>$2^{m-1} + 2^{m-h-1}$</td>
<td>$2^{2h}$</td>
</tr>
</tbody>
</table>
Weight-distribution of cosets of $RM(1, m)$ in $RM(2, m)$.

**Theorem 0.6.** If the symplectic matrix determining coset $B$ of $RM(1, m)$ in $RM(2, m)$ has rank $2h$ then the weight distribution of $B$ is as follows:

<table>
<thead>
<tr>
<th>Weight</th>
<th>Number of Vectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^{m-1} - 2^{m-h-1}$</td>
<td>$2^{2h}$</td>
</tr>
<tr>
<td>$2^{m-1}$</td>
<td>$2^{m+1} - 2^{2h+1}$</td>
</tr>
<tr>
<td>$2^{m-1} + 2^{m-h-1}$</td>
<td>$2^{2h}$</td>
</tr>
</tbody>
</table>

**Corollary 0.7.** The number of codewords of weight $2^{m-1}$ in the cosets having rank $2h$ is equal to $A_{2^{m-1}+2^{m-h-1}}(2^{m-2h+1} - 2)$, where $A_w$ denotes the number of codewords of weight $w$. 
Weight-distribution of minimal codewords in $RM(2, m)$.

**Proposition 0.8.** (Ashikhmin & Barg ACCT’94): Let $M_w$ the number of minimal codewords of weight $w$ in $RM(2, m)$. Then:

- $M_w = 0$ for $w = 2^{m-1} + 2^{m-1-h}$, $h = 0, 1, 2$.
- otherwise, $M_w = A_w$, except for the case $w = 2^{m-1}$, where

$$M_w = \sum_{h=2}^{\lfloor m/2 \rfloor} A_{2^{m-1-2^{m-h-1}}}(2^{m-2h+1} - 2)$$
Lemma 0.9. The rank of symplectic matrix corresponding to the sum of two codewords of $RM(2, m)$ is not greater than the sum of the ranks of symplectic matrices associated with these codewords.
Sketch of the proof

Lemma 0.10. The rank of symplectic matrix corresponding to the sum of two codewords of $RM(2, m)$ is not greater than the sum of the ranks of symplectic matrices associated with these codewords.

The smallest two nonzero weights in $RM(2, m)$ are:

$w_1 = 2^{m-2}$ ($h = 1$) and $w_2 = 2^{m-1} - 2^{m-3}$ ($h = 2$).

By Proposition 0.3 Part (2), non-minimal codewords could exist for weights:

$2^{m-1} + 2^{m-h-1} \geq w_1 + w_2$ ($h = 0, 1, 2$) and $2w_1 = 2^{m-1}$.

Accordingly the proof can be split into two parts.
"Non-minimality" of codewords of weights $2^{m-1} + 2^{m-h-1}$:

- $h = 0$, all-one vector 1 of length $2^m$ — non-minimal.
- $h = 1$, affine equivalent to $y_1y_2 + 1$, all non-minimal by Proposition 0.3 Part (1) for $RM(2, 2)$.
- $h = 2$, affine equivalent to $y_1y_2 + y_3y_4 + 1$, all non-minimal by the same reasoning for $RM(2, 4)$. 
Sketch of the proof

"Non-minimality" of codewords of weights $2m-1 + 2m-h-1$:
- $h = 0$, all-one vector $1$ of length $2^m$ – non-minimal.
- $h = 1$, affine equivalent to $y_1y_2 + 1$, all non-minimal by Proposition 0.3 Part (1) for $RM(2, 2)$.
- $h = 2$, affine equivalent to $y_1y_2 + y_3y_4 + 1$, all non-minimal by the same reasoning for $RM(2, 4)$.

"Non-minimality" of codewords of weight $2^{m-1}$. Due to Lemma 0.9, only 3 cases should be considered:
- affine equivalent to $y_1$, all non-minimal since $y_1 = y_1y_2 + y_1(y_2 + 1)$.
- affine equivalent to $y_1y_2 + y_3$, all non-minimal by Proposition 0.3 Part (1) for $RM(2, 3)$.
- affine equivalent to $y_1y_2 + y_3y_4 + y_5$, all minimal!!!
The End

THANK YOU!
References

References
