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

Introduction 1

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;
  - A. Barg, "Complexity Issues in Coding Theory", in *Handbook of Coding Theory* (Eds. V. Pless and W. Huffman), Amsterdam, Elsevier Science B.V., 1998.

Introduction 1

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;
  - A. Barg, "Complexity Issues in Coding Theory", in *Handbook of Coding Theory* (Eds. V. Pless and W. Huffman), Amsterdam, Elsevier Science B.V., 1998.
- to describe minimal access structure in Secret-Sharing Schemes based on these codes:
  J. Massey, "Minimal Codewords and Secret Sharing", in Proc. Sixth Joint Swedish-Russian Workshop on Inf. Theory, Molle, Sweden, 1993, pp. 246-249.

Introduction 2

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];

Introduction 2

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;

Introduction 2

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].

Introduction 3

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:
A.Ashikhmin and A. Barg, "Minimal Vectors in Linear Codes", IEEE Trans. on Information Theory vol. 44, September 1998, pp. 2010-2017.
In this work, it is presented another comprehensive proof based on Dickson's Theorem.

Background

DEFINITION 0.1. *A* **support of a binary vector** c *of length* n*, denoted by* $supp(\mathbf{c})$*, is defined as the subset of* $\mathbf{c}$*'s nonzero coordinates. A* **support of a Boolean function** *is the support of its truth table.*

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

Background 2

- **Basic properties of minimal codewords**

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

  - *(1) If* $\mathbf{c}$ *is minimal codeword in a linear* $[n, k]$*-code then its weight satisfies* $wt(\mathbf{c}) \leq n - k + 1$*.*
  - *(2) Any non-minimal codeword* $\mathbf{c}$ *in a binary linear code can be represented as a sum of two codewords* $\mathbf{c}_1$ *and* $\mathbf{c}_2$ *having disjoint supports included in* $supp(\mathbf{c})$*.*
  - *(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* $< 2d_{min}$ *are minimal.*

Background: MacW&Sl, Ch. 15.2

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

Background: MacW&Sl, Ch. 15.2

- the second-order Reed-Muller code $RM(2,m)$:
  - codewords are truth tables (binary vectors of length 2^m) of Boolean functions of degree ≤ 2 in $\mathbf{v} = v_1, v_2, \ldots, v_m$.
  - typical codeword is given by: $S(\mathbf{v}) = \mathbf{v}\mathbf{Q}\mathbf{v}^T + \mathbf{L}\mathbf{v} + \epsilon$, where $\mathbf{Q}$ is an upper triangular binary $m \times m$ matrix, $\mathbf{L}$ is a binary vector of length m, and ϵ is 0 or 1.
- A coset of $RM(1,m)$ in $RM(2,m)$ is characterized by matrix $\mathbf{Q}$ or alternatively (as it turns out) by the binary symmetric matrix $\mathbf{B} = \mathbf{Q} + \mathbf{Q}^T$ with zero diagonal. $\mathbf{B}$ is called symplectic matrix and the weight-distribution of the coset depends only on the rank of $\mathbf{B}$.

Background: Dickson's theorem

- (1) If B is a symplectic matrix of rank $2h$, then there exists an invertible binary matrix $\mathbf{R}$ such that $\mathbf{RBR}^T$ has zeros everywhere except on the two diagonals immediately above and below the main diagonal, and there has $1010\ldots100\ldots0$ with h ones ($0 < h \leq \lfloor m/2 \rfloor$).
- (2) Any quadratic function becomes: $\mathbf{T}(\mathbf{y}) = \sum_{i=1}^{h} y_{2i-1}y_{2i} + \mathbf{L}_1(\mathbf{y}) + \epsilon$ under the transformation $\mathbf{y} = \mathbf{vR}^{-1}$ determined by $\mathbf{R}$ from Part (1). Moreover $y_1, \ldots, y_{2h}$ are linearly independent.
- (3) If $\mathbf{L}_1(\mathbf{y})$ is linearly dependent on $y_1, \ldots, y_{2h}$, by an affine transformation $\mathbf{T}(\mathbf{y})$ can be written as: $\sum_{i=1}^{h} x_{2i-1}x_{2i} + \epsilon_1, \quad \epsilon_1 = 0$ or 1, where $x_1, \ldots, x_{2h}$ are linearly independent and each x_i is a linear form in $y_1, \ldots, y_{2h}, \mathbf{1}$.

Background 5

- **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:*

Weight	Number of Vectors
$2^{m-1} - 2^{m-h-1}$	2^{2h}
2^{m-1}	$2^{m+1} - 2^{2h+1}$
$2^{m-1} + 2^{m-h-1}$	2^{2h}

Background 5

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

  Theorem 0.6. *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:*

Weight	**Number of Vectors**
$2^{m-1} - 2^{m-h-1}$	2^{2h}
2^{m-1}	$2^{m+1} - 2^{2h+1}$
$2^{m-1} + 2^{m-h-1}$	2^{2h}

- **Corollary 0.7.** *The number of codewords of weight 2^{m-1} in the cosets having rank $2h$ is equal to $A_{2^{m-1} \pm 2^{m-h-1}}(2^{m-2h+1} - 2)$, 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* $M_w = \sum_{h=2}^{\lfloor m/2 \rfloor} A_{2^{m-1}-2^{m-h-1}}(2^{m-2h+1} - 2)$

Sketch of the proof 1

- **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 1

- **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.

Sketch of the proof 2

- "Non-minimality" of codewords of weights $2^{m-1} + 2^{m-h-1}$:
  - $h = 0$, all-one vector $\mathbf{1}$ of length 2^m – non-minimal.
  - $h = 1$, affine equivalent to $y_1 y_2 + 1$, all non-minimal by Proposition 0.3 Part (1) for *RM*$(2, 2)$.
  - $h = 2$, affine equivalent to $y_1 y_2 + y_3 y_4 + 1$, all non-minimal by the same reasoning for *RM*$(2, 4)$.

Sketch of the proof 2

- "Non-minimality" of codewords of weights $2^{m-1} + 2^{m-h-1}$:
  - $h = 0$, all-one vector $\mathbf{1}$ 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

[1] A.Ashikhmin and A. Barg, "Combinatorial Aspects of Secret Sharing with Codes", in *Proc. Int. Workshop on Algebraic and Combinatorial Coding Theory*, (Novgorod, Russia, September, 1994), pp. 8-11.

[2] A.Ashikhmin and A. Barg, "Minimal Vectors in Linear Codes", IEEE Trans. on Information Theory vol. 44, September 1998, pp. 2010-2017.

[3] A. Barg, "Complexity Issues in Coding Theory", in *Handbook of Coding Theory* (Eds. V. Pless and W. Huffman), Amsterdam, Elsevier Science B.V., 1998.

References 2

[4] Y. Borissov and N.Manev, "On the minimal words of the primitive BCH codes", in *Proc. Int. Workshop Algebraic and Combinatorial Coding Theory (ACCT-5)* (Sozopol, Bulgaria, June 1996), pp. 59-65.
[5] Yu. Borissov and N. L. Manev, "Minimal Codewords of the Primitive BCH Codes", Problemy Peredachi Informatsii, Vol. 34, Number 3, July-September, 1998, pp. 37-46, in Russian.
[6] Y. Borissov, N. Manev, and S. Nikova, "On the Non-minimal Codewords in Binary Reed-Muller Codes", Discrete Appl. Math., **128** (2003), pp. 65-74.
[7] Y. Borissov and N. Manev, "Minimal Codewords in Linear Codes", Serdica Math. J. **30** (2004), pp. 303-324.

References 3

[8] Tai-Yang Hwang, "Decoding Linear Block Codes for Minimizing Word Error Rate", IEEE Trans. on Information Theory vol. 25, November 1979, pp. 733-737.
[9] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company 1977.
[10] J. Massey, "Minimal Codewords and Secret Sharing", in *Proc. Sixth Joint Swedish-Russian Workshop on Inf. Theory*, Molle, Sweden, 1993, pp. 246-249.
[11] D.R.Stinson, "An Explication of Secret Sharing Schemes", Des. Codes Cryptography, vol. 2, 1992, pp. 357-390.

References 4

[12] P.O. Vontobel, R. Smarandache, N. Kiyavash, J. Teutsch, and D. Vukobratovic, "On the Minimal Pseudo-Codewords of Codes From Finite Geometries", *ISIT 2005, Proc. International Symposium on Information Theory*, 4-9 Sept. 2005, pp. 980 - 984.

[13] K. Yasunaga, T. Fujiwara, and T. Kasami, "Local Weight Distribution of the (256, 93) Third-Order Binary Reed-Muller Code," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E90-A, no. 3, pp. 698 - 701, March 2007.