On McEliece's Result about Divisibility of the Weights in the Binary Reed-Muller Codes

Yuri Borissov

Department of Mathematical Foundations of Informatics
IMI, BAS, Bulgaria

September 7, 2013

Outline of Topics

- Introduction
- Boolean Algebra Background
- Results and Sketch of Proofs

- the binary Reed-Muller (*RM*) codes
  - one of the oldest families of codes (1950's)
  - easy to decode (majority-logic circuits)

- the binary Reed-Muller (*RM*) codes
  - one of the oldest families of codes (1950's)
  - easy to decode (majority-logic circuits)
- but few general results for the weight structure:
  - weight distribution of *RM* codes known for
    - the 1st and 2nd-order by Sloane & Berlekamp (1970)
    - arbitrary order when $w \leq 2.5 d_{min}$ by Kasami et al. (1976).
  - weight divisibility: McEliece's theorem (1971).

Theorem 1.

(McEliece) All weights in $RM(r, m)$ *are multiples of* $2^{[(m-1)/r]}$.

applied, for instance,

- by H. van Tilborg (1971) for investigating the weight spectrums of $RM(3, 8)$ and $RM(3, 9)$

Theorem 1.

(McEliece) All weights in $RM(r, m)$ *are multiples of* $2^{[(m-1)/r]}$.

applied, for instance,

- by H. van Tilborg (1971) for investigating the weight spectrums of $RM(3, 8)$ and $RM(3, 9)$
- to prove a recent conjecture by Cusick & Cheon on balanced words in $RM(r, m)$, when $r \geq (m-1)/2$.

(at least) two proofs of McEliece's theorem are known:

- the original one, due to McEliece using the fact that *RM* codes are extended cyclic codes and difficult to prove theorem on divisibility of cyclic codes in terms of their nonzeros (**MacWilliams** & **Sloane**, p. 447) (at least) two proofs of McEliece's theorem are known:

- the original one, due to McEliece using the fact that *RM* codes are extended cyclic codes and difficult to prove theorem on divisibility of cyclic codes in terms of their nonzeros (**MacWilliams** & **Sloane**, p. 447)
- due to van Lint (1971), based on specific fact about the zeros of binary polynomials of many variables.

in this work, we:

- present an alternative proof in terms of Boolean functions and their weights in this work, we:

- present an alternative proof in terms of Boolean functions and their weights
- show that bound $2^{[(m-1)/r]}$ is tight for every $r \leq m$ by constructing codewords of relevant weight.

- **Boolean function** f on m variables is a mapping from $\mathbb{F}_2^m$ into $\mathbb{F}_2$, where $\mathbb{F}_2 = \{0, 1\}$

Boolean Algebra Background 1

- **Boolean function** f on m variables is a mapping from $\mathbb{F}_2^m$ into $\mathbb{F}_2$, where $\mathbb{F}_2 = \{0, 1\}$
- any function f is uniquely expressed as a polynomial called **algebraic normal form** of f: $ANF(f)$

- **Boolean function** f on m variables is a mapping from $\mathbb{F}_2^m$ into $\mathbb{F}_2$, where $\mathbb{F}_2 = \{0, 1\}$
- any function f is uniquely expressed as a polynomial called **algebraic normal form** of f: $ANF(f)$
- the greatest degree of monomial present in $ANF(f)$ is called **algebraic degree** of f: $deg(f)$

Boolean Algebra Background 1

- **Boolean function** f on m variables is a mapping from $\mathbb{F}_2^m$ into $\mathbb{F}_2$, where $\mathbb{F}_2 = \{0, 1\}$
- any function f is uniquely expressed as a polynomial called **algebraic normal form** of f: $ANF(f)$
- the greatest degree of monomial present in $ANF(f)$ is called **algebraic degree** of f: $deg(f)$
- the number of nonzero values of the function f is called **weight** of f: $wt(f)$.

Boolean Algebra Background 2

the necessary properties of Boolean functions:

- $\mathcal{P}1$: For arbitrary Boolean function f it holds $f^2 = f$.

the necessary properties of Boolean functions:

- $\mathcal{P}1$: For arbitrary Boolean function f it holds $f^2 = f$.
- $\mathcal{P}2$: Let g be a monomial which is product of $n \geq 2$ monomials $g_1, g_2, \ldots g_n$. Then
$$deg(g) \leq \sum_{i=1}^{n} deg(g_i),$$
and equality holds if and only if the sets of essential variables of any pair (g_i, g_j) are disjoint.

the necessary properties of Boolean functions:

- $\mathcal{P}1$: For arbitrary Boolean function f it holds $f^2 = f$.
- $\mathcal{P}2$: Let g be a monomial which is product of $n \geq 2$ monomials $g_1, g_2, \ldots g_n$. Then
$$deg(g) \leq \sum_{i=1}^{n} deg(g_i),$$
and equality holds if and only if the sets of essential variables of any pair (g_i, g_j) are disjoint.
- $\mathcal{P}3$: The weight of any monomial g on m variables equals to $2^{m-deg(g)}$.

- the subset of all Boolean functions on m variables with degree at most r (the set of their truth tables) is called **binary Reed-Muller code** of order r and length 2^m, denoted by $RM(r, m)$

- the subset of all Boolean functions on m variables with degree at most r (the set of their truth tables) is called **binary Reed-Muller code** of order r and length 2^m, denoted by $RM(r, m)$
- the $RM(r, m)$ code has **dimension** $\sum_{i=0}^{r} \binom{m}{i}$ and **minimum distance** $d_{min} = 2^{m-r}$.

Proposition 2.

Let $g_1, g_2, \ldots, g_n$ be n arbitrary Boolean functions. Then it holds

$$wt(\sum_{i=1}^{n} g_i) = \sum_{i=1}^{n} wt(g_i) - 2\sum_{i,j} wt(g_i g_j) + \ldots \tag{1}$$

$$+(-2)^{l-1} \sum_{i_1, i_2, \ldots, i_l} wt(g_{i_1} g_{i_2} \ldots g_{i_l}) + \ldots + (-2)^{n-1} wt(g_1 g_2 \ldots g_n)$$

Proof: by induction on n using the well-known fact:

$$wt(g_1 + g_2) = wt(g_1) + wt(g_2) - 2wt(g_1 g_2)$$

Remarks

- the above proposition is analogous to the inclusion-exclusion principle from elementary combinatorics
- a powerful technique called combinatorial polarization related to this proposition was developed by H.Ward (1979, 1990) to study the divisibility of group-algebra codes.

Lemma 3.

Let $f \in RM(r, m)$. Then (up to sign) the terms involving the products of l monomials from equation (1) applied for the $ANF(f)$, are powers of 2 not less than $2^{m-(r-1)l-1}$.

- *Proof:* by properties $\mathcal{P}3$ and $\mathcal{P}2$ for the weight of product $g = g_1 \dots g_l$ of l monomials present in the $ANF(f)$, we have:

$$wt(g) = 2^{m-deg(g)} \geq 2^{m-\sum_{i=1}^{l} deg(g_i)} \geq 2^{m-rl}.$$

Lemma 3.

Let $f \in RM(r, m)$. Then (up to sign) the terms involving the products of l monomials from equation (1) applied for the $ANF(f)$, are powers of 2 not less than $2^{m-(r-1)l-1}$.

- *Proof:* by properties $\mathcal{P}3$ and $\mathcal{P}2$ for the weight of product $g = g_1 \dots g_l$ of l monomials present in the $ANF(f)$, we have:

$$wt(g) = 2^{m-deg(g)} \geq 2^{m-\sum_{i=1}^{l} deg(g_i)} \geq 2^{m-rl}.$$

- *Note: the above estimate is nontrivial if $l \leq \alpha$, where*

$$\alpha = [(m-1)/r]$$

Proof of McEliece's theorem

recall that $\alpha = [(m-1)/r]$.

- for the proof is sufficient to show that **all terms** in equation (1) applied for the $ANF(f)$ with $l \leq \alpha$, are **powers of** 2 **not less than** 2^{α}.

Proof of McEliece's theorem

recall that $\alpha = [(m-1)/r]$.

- for the proof is sufficient to show that **all terms** in equation (1) applied for the $ANF(f)$ with $l \leq \alpha$, are **powers of** 2 **not less than** 2^{α}.
- but this follows by the previous lemma and easy to check inequality: $m - (r-1)l - 1 \geq \alpha$ for those l.

Theorem 4.

Any Reed-Muller code $RM(r, m)$ contains codeword such that the highest power of 2 which divides its weight is exactly 2^{α}, where $\alpha = [(m-1)/r]$.

Proof: we may assume $r > 1$.

- if $\alpha = 0$, i.e. $m = r$, $x_1 x_2 \ldots x_m$ has weight 1.
- if $\alpha > 0$ and let $f_1 = g_1 + \ldots g_{\alpha}$:
  - each g_i is a monomial of $deg(g_i) = r$;
  - the sets of variables for any $(g_i, g_j), 1 \leq i, j \leq \alpha$ are disjoint.

  let $\beta = m - \alpha r \geq 1$; the proof is split into two cases:

Theorem 4.

Any Reed-Muller code $RM(r, m)$ contains codeword such that the highest power of 2 which divides its weight is exactly 2^{α}, where $\alpha = [(m-1)/r]$.

Proof: we may assume $r > 1$.

- if $\alpha = 0$, i.e. $m = r$, $x_1 x_2 \ldots x_m$ has weight 1.
- if $\alpha > 0$ and let $f_1 = g_1 + \ldots g_{\alpha}$:
  - each g_i is a monomial of $deg(g_i) = r$;
  - the sets of variables for any $(g_i, g_j), 1 \le i, j \le \alpha$ are disjoint.

  let $\beta = m - \alpha r \ge 1$; the proof is split into two cases:
  - $\beta = 1$, then eq. (1) implies $wt(f_1)$ is suitable;
  - $\beta > 1$, put $f_2 = f_1 + g_{\alpha+1}$, where the last monomial is a product of the remaining $m - \alpha r = \beta \le r$ variables; then then eq. (1) implies $wt(f_2)$ is suitable.

Example 5.

$$r = 3$$

- $\alpha = 0, m = 3, wt(x_1x_2x_3) = 1$
- $\alpha = 1,$
  $m = 4, wt(x_1x_2x_3) = 2;$
  $m = 5, wt(x_1x_2x_3 + x_4x_5) = 10;$
  $m = 6, wt(x_1x_2x_3 + x_4x_5x_6) = 14$
- $\alpha = 2,$
  $m = 7, wt(x_1x_2x_3 + x_4x_5x_6) = 28;$
  $m = 8, wt(x_1x_2x_3 + x_4x_5x_6 + x_7x_8) = 92;$
  $m = 9, wt(x_1x_2x_3 + x_4x_5x_6 + x_7x_8x_9) = 148$
- ...

The End

THANK YOU FOR ATTENTION!