Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 47-52*

On McEliece's result about divisibility of the weights in the binary Reed-Muller codes[1]

Yuri L. Borissov youri@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
8 G. Bonchev str., 1113, Sofia, BULGARIA

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. First, we give an alternative proof of the famous McEliece's result about divisibility of the weights of the binary Reed-Muller codes fully relying on knowledge for Boolean functions. Second, we prove that any binary Reed-Muller code $RM(r,m)$ contains codeword such that the highest power of 2 dividing its weight is exactly $2^{[(m-1)/r]}$.

1 Introduction

For basic definitions and facts we refer to [1]. Reed-Muller (or RM) codes are one of the oldest and best understood families of codes. However, there are relatively few general results concerning their weight structure. For instance, the problem of finding the weight-distribution of RM codes of arbitrary possible lengths is solved completely only for the first and second-order codes (and their duals, of course) [2], and for arbitrary order it is determined only for weights less than 2.5 of the minimum distance [3, 4]. Therefore, the general result of R.J.McEliece about divisibility of the weights in the binary RM codes can be considered as a deep and very useful theorem (see, e.g. [5, 6] and [7]).

Apart from the original proof of that theorem based on some facts about binary cyclic codes (see, [1][p. 447] and [8, 9], respectively), J.H. van Lint has exhibited an proof which is based on a specific theorem (again due to R.J.McEliece) stated in terms of zeros of polynomials on many variables over $\mathbf{GF}(2)$ (see, [10][p. 123-125]). In this note, we present another comprehensive proof given in terms of Boolean functions and their weights.

The rest of that note is organized as follows. In the next section, we recall needed knowledge about Boolean functions and the binary RM codes. Then we exhibit our results and their proofs. Finally, some facts about works concerning the topic of divisible codes are present and conclusions are drawn.

[1]This research is partially supported by the Bulgarian NSF grant I01/0003.

2 Preliminaries

We will give shortly some facts about the binary RM codes (see for details, e.g. [1][Ch. 13]). Let $\mathbf{V}_m$ be $m-$dimensional binary vector space. A Boolean function f on m variables $x_1, x_2, \ldots, x_m$ is a mapping from $\mathbf{V}_m$ into $\mathbb{F}_2 = \mathbf{GF}(2)$. Let $\mathcal{F}_m$ be the set of all Boolean functions on m variables. $\mathcal{F}_m$ constitutes a 2^m-dimensional binary vector space. Special kind of Boolean functions which form basis of $\mathcal{F}_m$ are the so-called monomials, i.e. all products (including the "empty" product, 1): $x_{i_1} x_{i_2} \ldots x_{i_\nu}$, where $1 \leq i_1 < i_2 < \ldots < i_\nu \leq m$. So, any $f \in \mathcal{F}_m$ can be uniquely expressed as a linear combination (polynomial) of some monomials, sometimes called Algebraic Normal Form (ANF) of f. Degree of monomial is defined to be the number of its (essential) variables. The greatest degree of a monomial in the ANF of function f is called algebraic degree of f (denoted by $deg(f)$). A truth table of the Boolean function $f \in \mathcal{F}_m$ is the binary vector $\mathbf{f}$ of length 2^m whose coordinates are the values of f arranged according to the ordinary lexicographic order supplied in $\mathbf{V}_m$. The weight of truth table $\mathbf{f}$ (namely the number of its nonzero positions), is called as well weight of f and denoted by $wt(f)$.

Herein, we present without proofs three simple properties of Boolean functions needed in further:

- $\mathcal{P}1$: 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 $g \in \mathcal{F}_m$ is equal to $2^{m-deg(g)}$.

The subset of $\mathcal{F}_m$ consisting of the Boolean functions having degree at most r (or equivalently their truth tables) form a linear subspace of dimension $k = \sum_{i=0}^{r} \binom{m}{i}$, called binary Reed-Muller code $RM(r, m)$ of order r and length 2^m. Further on, we consider only non-trivial case $r > 0$. Recall as well that punctured RM code $RM(r, m)^*$ is equivalent to a cyclic code (see, e.g. [1][p. 383]) which we point out in connection with the original proof mentioned in the Introduction.

The following theorem (subject of this note) is due to McEliece :

Theorem 1. *([9] or [1][p. 447]) The weight of every codeword in $RM(r, m)$ is divisible by $2^{[(m-1)/r]}$.*

3 Proofs

First, we prove the following

Proposition 1. *Let $g_1, g_2, \ldots, g_n$ be n arbitrary Boolean functions from $\mathcal{F}_m$. Then it holds*

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

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

Proof. The proof is by induction on n.

For $n = 2$, it is well-known that:

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

Assume the statement is true for $n = k$. For $n = k + 1$, we have the following chain of equations first making use of (2) and then by inductive hypothesis (simultaneously on $\sum_{i=1}^{k} g_i$ and $\sum_{i=1}^{k} g_i g_{k+1}$), regrouping the summands :

$$wt(\sum_{i=1}^{k+1} g_i) = wt(\sum_{i=1}^{k} g_i + g_{k+1}) = wt(\sum_{i=1}^{k} g_i) + wt(g_{k+1}) - 2wt(\sum_{i=1}^{k} g_i g_{k+1}) =$$

$$\sum_{i=1}^{k+1} wt(g_i) - 2 \sum_{1 \le i,j \le k+1} wt(g_i g_j) + 4 \sum_{1 \le i,j,l \le k+1} wt(g_i g_j g_l) - \ldots +$$

$$+(-2)^k wt(g_1 g_2 \ldots g_{k+1}).$$

(Note that above we have applied also the property $\mathcal{P}1$.)
Thus, (1) is true for $n = k + 1$ and the proof is completed. □

Remark 1. *This proposition is in some sense analogous to the inclusion-exclusion principle from elementary combinatorics and may have individual significance.*

A powerful technique known as combinatorial (or weight) polarization, which is related to the above proposition, was developed in [11] and [12] for the goals of studying the divisibility of group-algebra codes.

Lemma 1. *Let $f \in RM(r,m)$ and $\alpha = [(m-1)/r]$. Then (up to sign) the terms in equation (1) for the $ANF(f)$ involving the products of monomials which consist of $l \leq \alpha$ multipliers, are powers of 2 greater or equal to $2^{m-(r-1)l-1}$.*

Proof. By the common form of terms in equation (1) and properties $\mathcal{P}3$ and $\mathcal{P}2$, taking into account that maximum degree of such product is achieved when all multipliers have disjoint sets of variables of cardinality r (hence, the corresponding power of 2 can always be lower bounded by 2^{m-rl} if the number of multipliers l is at most α). □

Remark 2. *The degree $m-(r-1)l-1$ decreases with l (strictly if $r > 1$). Also, the signs of terms have no significance in studying the divisibility properties of weights through equation (1) and are ignored further on.*

Now, we shall prove the McEliece's theorem on the base of Proposition 1.

Proof. Put $\alpha = [(m-1)/r]$, and let $f \neq 0$ be a Boolean function corresponding to some codeword from $RM(r,m)$. For the proof it is sufficient to show that all of the terms with $l \leq \alpha$ in equation (1) applied for the $ANF(f)$ are greater or equal to 2^α. For that, by Lemma 1 and the subsequent remark, the lowest degree $m-(r-1)\alpha-1$ must be at least α, or equivalently $(m-1)/r \geq \alpha$. But this follows by the definition of α and the proof is completed. □

Making use of Proposition 1, we can also prove the following:

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

Proof. If $r = 1$, the weight-distribution of the first-order RM codes implies that statement is true for all codewords $\neq \mathbf{0}, \mathbf{1}$.

So, further on we assume $r > 1$ and let again $\alpha = [(m-1)/r]$. If $\alpha = 0$, i.e. $m = r$, the monomial $x_1 x_2 \ldots x_m$ has weight 1. Now, let $\alpha > 0$ and $\beta = m - \alpha r$. It is easily seen that $1 \leq \beta \leq r$, and the proof can be split into the following two cases:

- $\beta = 1$. In this case, we construct a Boolean function $f_1 = g_1 + \ldots g_\alpha$ such that each g_i is a monomial of degree r and the sets of essential variables for any pair $(g_i, g_j), 1 \leq i < j \leq \alpha$ are disjoint. (The construction of f_1 is always possible since $m > \alpha r$.) Then applying equation (1) in regard to f_1, it can be easily seen that last term ($l = \alpha$) is exactly $2^{\alpha-1} * 2^\beta = 2^\alpha$ while the preceding ones are powers $> 2^\alpha$ by Lemma 1 and Remark 2.

- $\beta > 1$. In this case, we consider the Boolean function $f_2 = f_1 + g_{\alpha+1}$, where f_1 is described as in the previous case but $g_{\alpha+1}$ is the monomial which contains the remaining $m - \alpha r = \beta \leq r$ variables. Again, the last term ($l = \alpha + 1$) in equation (1) applied for f_2 will be exactly $2^\alpha * 2^0 = 2^\alpha$ while the preceding ones are greater powers of 2 since that of minimum magnitude (corresponding to $g_1 g_2 \ldots g_\alpha$) equals to $2^{\alpha-1} * 2^\beta = 2^{\alpha+\beta-1}$, and the proof follows. □

Example 1. *Let $r = 2$. If $m = 2$ then $\alpha = 0$ and $wt(x_1x_2) = 1$; if $m = 3$ take $f_1 = x_1x_2$; if $m = 4$, $f_2 = x_1x_2 + x_3x_4$. In the last two cases $\alpha = 1$, and it can be easily checked that $wt(f_1) = 2$ while $wt(f_2) = 6$.*

4 Some works on divisible codes

An thorough survey on divisible codes is given in [13]. In this survey, McEliece's theorem is cited in connection with an theorem of Ax about divisibility of the generalized RM codes [14] and its generalizations. Works on divisible codes have been done by the bulgarian coding theory group members, e.g. [15] and [16]. The first one concerns divisibility of a binary Griesmer code whilst the second proves more general theorem for Griesmer codes over prime fields using polynomial methods (see, as well [17]). Another contribution of this topic is [18]. Finally, it is worth noting the existence of link between the McEliece's result and properties of some classes of cryptographic Boolean functions [19].

5 Conclusion

In this note, based on general formula for the weight of sum of arbitrary Boolean functions, we have presented an alternative proof of McEliece's theorem about divisibility of the binary RM codes. We also have shown the bound determined by that theorem is tight.

Acknowledgments. The author would like to thank Gary McGuire for helpful comments and paying attention to the article [11].

References

[1] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes,* North-Holand Publishing Company, Amsterdam-New York-Oxford, 1977.

[2] N. J. A. Sloane, E. R. Berlekamp, Weight enumerator for second-order Reed-Muller codes, *IEEE Trans. Info. Theory,* **16**, 745–751, 1970.

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

[4] T. Kasami, N. Tokura, S. Azumi, On the weight enumeration of weights less than $2.5d$ of Reed-Muller codes, *INFORMATION AND CONTROL,* **30**, 380–395, 1976.

[5] Y. L. Borissov, On the Cusick-Cheon conjecture about balanced Boolean functions in the cosets of the binary Reed-Muller codes, *IEEE Trans. Info. Theory*, **55**, 16-18, 2009.

[6] T. W. Cusick, Y. Cheon, Counting balanced Boolean functions in n variables with bounded degree, *Experimental Mathematics,* **16:1**, 101–105, 2007.

[7] H. C. A. van Tilborg, Weights in the third-order Reed-Muller codes, *JPL Technical Report 32-1526,* vol. **IV**, 86–92, 1971.

[8] R. J. McEliece, On periodic sequences from $GF(q)$, *J. Combin. Theory Ser. A,* **10**, 80–91, 1971.

[9] R. J. McEliece, Weight congruences for p-ary cyclic codes, *Discrete Math.,* **3**, 177–192, 1972.

[10] J. H. van Lint, *Coding theory,* Springer Lecture Notes in Mathematics, No. **201**, Springer-Verlag, Berlin-Heidelberg-New York, 1973.

[11] H. N. Ward, Combinatorial polarization, *Discrete Math.,* **26**, 185–197, 1979.

[12] H. N. Ward, Weight polarization and divisibility, *Discrete Math.,* **83**, 315–326, 1990.

[13] H. N. Ward, Divisible codes - a survey, *Serdica Math. J.,* **27**, 263–278, 2001.

[14] J. Ax, Zeroes of polynomials over finite fields, *Amer. J. Math.,* **86**, 255–261, 1964.

[15] S. M. Dodunekov, N. L. Manev, Minimum possible block length of a linear binary code for some distances, *Problems Inform. Transmission,* **20**, 8–14, 1984.

[16] I. N. Landjev, The geometric approach to linear codes, *In: Finite geometries, Proc. of the Fourth Isle of Thorns Conference*, (eds A. Blokhuis et al.), Kluwer, 247–257, 2001.

[17] H. N. Ward, Divisibility of codes meeting the Griesmer bound, *J. Combin. Theory Ser. A,* **83**, 79–93, 1998.

[18] S. Ball, R. Hill, I. Landjev, H. Ward, On $(q^2+q+2, q+2)$-arcs in the projective plane $PG(2,q)$, *Des. Codes Cryptogr.*, **24**, 205–224, 2001.

[19] P. Sarkar, S. Maitra, Nonlinearity bounds and constructions of resilient Boolean functions, *CRYPTO 2000*, 515–532, 2000.