Weight distributions of a class of codes with parameters of Reed – Muller codes

I.Yu.Mogilnykh and F. I. Solov'eva

Sobolev Institute of Mathematics, Russian Academy of Sciences, Russia
ivmog@math.nsc.ru, sol@math.nsc.ru

Abstract. We generalize the Pulatov construction and obtain a rich class of new codes with parameters of the classical binary Reed – Muller codes. We investigate the weight distribution and a distance-invariance property for the class of the codes. A large class of codes having the same weight distribution and parameters as Reed – Muller codes and nonequivalent to them is constructed.

Keywords: Reed – Muller code, weight distribution, distance-invariant code, generalized Pulatov construction

1 Introduction

The binary linear *Reed – Muller code of order* r, denoted by $RM(r,m)$, $0 \leq r \leq m$, is the set vectors of length $n = 2^m$ for any $m \geq 1$ that correspond to the boolean functions of m variables of degree less or equal to r. The code has size $2^k, k = \sum_{i=0}^{r} \binom{m}{i}$ and *code distance* 2^{m-r}. For any admissible r and m the code $RM(r,m)$ has a basis of codewords having minimum nonzero weight, see [7]. We call such basis *minimum weight basis*. Recall that the code $RM(r+1,m+1)$ could be represented by the well-known Plotkin construction [7]:

$$\{(x+y|x) : x \in RM(r+1,m), y \in RM(r,m)\}. \quad (1)$$

The problem of the description of the weight distribution of classical binary Reed – Muller codes is still open regardless of numerous improvements. The information concerning the weight distribution of the codes could be found in the work of Kasami and Tokura [5]. For recent developments we refer to [1, 6].

Large classes of binary nonlinear codes with the parameters of the classical binary Reed – Muller codes were constructed and investigated by many authors, see [8] and the paper [11] with the list of references there.

In 2009 Jungnickel and Tonchev [9] found polarity designs that have the same parameters as projective geometry designs but are not isomorphic to them. This disproves the well known Hamada's conjecture for designs [3]. The extension of the binary code spanned by the blocks of a polarity design obtained from

$PG(2s, 2)$ is a binary linear code that is majority-logic decodable and has parameters of the Reed – Muller code $RM(s, 2s+1)$ but inequivalent to it, see [10]. In work [4] it is shown that some of these codes even have an exquisite property of having the same weight distribution as that of Reed-Muller codes.

The Reed – Muller codes being completely different from BCH codes sometimes are closely connected with them. The class of binary narrow-sense BCH codes of length $2^m - 1$ with designed distance $2^{m-2} + 1$ do not possess a minimum weight basis since the minimum weight codewords of the code coincides with those of the punctured Reed – Muller code of order 2, see the paper [2]. Analogous statement is not valid for BCH codes with designed distance 7 for small length, see [2].

In the paper we present a generalized Pulatov construction for codes with parameters of the classical binary Reed – Muller codes. For the class of these codes we investigate the important invariants and properties such as weight distributions and distance-invariance. We find conditions when the new code has the same weight distribution as that of $RM(r, m)$ and when the new code is distance-invariant. We demonstrate that distance-invariant codes from the obtained class of codes with the same weight distribution as the classical Reed – Muller code and nonisomorphic to them are rare. In particular we show that there are no such codes among Pulatov's class.

2 Construction

We assume familiarity with basic notions and definitions of coding theory, see also [7]. Throughout the paper d denotes a code distance and $w(x)$ denotes the weight of a vector x. The *weight distribution* of a code C is the array W_C, such that $W_{C,i}$ equals the number of codewords of C of weight i. A binary code C containing the all-zero vector $\mathbf{0}$ is called *distance-invariant* if $W_C = W_{C+x}$ for any $x \in C$. For two vectors y and x we denote $y \preceq x$ if $y_i \leq x_i$ for all $i = 1, \ldots, n$.

Proposition 1. *For any vectors z, y we have $w(y + z|z) \geq w(y)$ with equality if and only if $z \preceq y$.*

Recall the Pulatov switching construction [8] for codes with parameters of binary Reed – Muller codes that is a generalization of the classical Vasil'ev switching construction for perfect codes [13]. It should be noted that a switching approach turned out to be very fruitful for solving many problems for perfect q-ary codes, $q \geq 2$, see [11].

Throughout the paper we have $n = 2^m$. Let e_i be the vector of length n and weight one with 1 in the ith coordinate position. Let $\lambda : RM(r, m) \to \{0, 1\}$ be an arbitrary function. Then the code

$$\{(x + y + e_1\lambda(y)|x + e_1\lambda(y)) : x \in RM(r + 1, m), y \in RM(r, m)\}$$

is the extended Pulatov code, which has the same parameters as the Reed – Muller code $RM(r+1, m+1)$. We see that for the all-zeros function λ the formula represents the code $RM(r + 1, m + 1)$ in the well-known Plotkin approach (1).

We suggest the following generalization of the Pulatov construction. Denote by $\mathcal{L}$ a set of representatives (leaders) of the cosets of $RM(r+1,m)$ in F^n, with one vector in $\mathcal{L}$ taken for each coset exactly. Let $\lambda : RM(r,m) \to \mathcal{L}$ be an arbitrary function. Denote by $RM^{\lambda}(r+1,m+1)$ the following code:

$$\{(x+y+\lambda(y)|x+\lambda(y)) : x \in RM(r+1,m), y \in RM(r,m)\}. \tag{2}$$

For any fixed y of $RM(r,m)$ we also consider the subcode

$$R_y^{\lambda} = \{(x+y+\lambda(y)|x+\lambda(y)) : x \in RM(r+1,m)\}$$

of $RM^{\lambda}(r+1,m+1)$. The latter is the union of the subcodes R_y^{λ}:

$$RM^{\lambda}(r+1,m+1) = \bigcup_{y \in RM(r,m)} R_y^{\lambda}. \tag{3}$$

If λ is the all-zero, we use notation R_y to denote $\{(x+y|x) : x \in RM(r+1,m)\}$ and again we have the following representation of classical Reed-Muller code (1):

$$RM(r+1,m+1) = \bigcup_{y \in RM(r,m)} R_y. \tag{4}$$

For any $y \in RM(r,m)$ the minimum distance of the subcode R_y^{λ} coincides with the minimum distance $d = 2^{m-r}$ of $RM(r,m)$. For distinct $y, y' \in RM(r,m)$ and any x, $x' \in RM(r+1,m)$ we see that by Proposition 1

$$w(x+y+\lambda(y)+x'+y'+\lambda(y')|x+\lambda(y)+x'+\lambda(y')) \geq w(y+y'),$$

which in turn is at least d. We conclude that the minimum distance of $RM^{\lambda}(r+1,m+1)$ is d. Depending on the choice of the function λ the obtained code $RM^{\lambda}(r+1,m+1)$ could be linear or nonlinear. We obtain the following

Theorem 1. *Let $\mathcal{L}$ be the set of the representatives of the cosets of $RM(r+1,m)$ in F^n. For any $\lambda : RM(r,m) \to \mathcal{L}$ the code $RM^{\lambda}(r+1,m+1)$ has the same length, size and the minimum distance as those of $RM(r+1,m+1)$.*

Corollary 1. *For different functions λ and λ' such that $\lambda, \lambda' : RM(r,m) \to \mathcal{L}$ the codes $RM^{\lambda}(r+1,m+1)$ and $RM^{\lambda'}(r+1,m+1)$ are different. In particular, there are*

$$|RM(m-r-2,m)|^{|RM(r,m)|}$$

setwise different codes, obtained by construction (2).

3 Main results

Further we restrict ourselves to the case when the function λ is such that $y \in RM(r,m)$ and $w(\lambda(y)) < d/4$. Throughout this section $d = 2^{m-r}$ is the minimum distance of $RM(r,m)$ and $RM^{\lambda}(r+1,m+1)$.

3.1 Low weight distribution of $RM^{\lambda}(r+1, m+1)$

In this section we are concerned with the weight distribution of the code (3) and we are particularly interested in the number of low weight codewords (less than $3d/2$). The following implies that these codewords cannot arise from the subcodes R_y^{λ} for y of weight greater than d.

Proposition 2. *Let x be a codeword of $RM(r+1, m)$, y be a codeword of $RM(r, m)$ such that $w(y) > d$, where $d = 2^{m-r}$. Then for any vector $u \in F^{2^m}$*

$$w(y + u + x|u + x) \geq w(y) \geq 3d/2.$$

Proof. The inequality $w(y+u+x|u+x) \geq w(y)$ holds by Proposition 1. The distribution of low, i.e. close to minimum, weights in a Reed – Muller code is known, see [5]. In particular, the second to the lowest nonzero weight of $RM(r, m)$ is equal to $3d/2$, so $w(y) \geq 3d/2$ and we are done. ▲

Moreover, taking relatively small weights for functions λ the lemma below implies that the codewords of $RM^{\lambda}(r+1, m+1)$ of minimum weight arise only from $(x + y|x)$ of minimum or zero weight.

Lemma 1. *Let $\lambda : RM(r, m) \to \mathcal{L}$ be any function such that $\lambda(\mathbf{0}) = \mathbf{0}$ and $w(\lambda(y)) < d/4$ for any $y \in RM(r, m)$.*

1. If $y \in RM(r, m)$ is such that $w(y) = d$ and $w(x + y + \lambda(y)|x + \lambda(y)) = d$, for some $x \in RM(r+1, m)$ then $w(x + y|x) = d$.

2. For any $y \in RM(r, m)$ we have $W_{R_y^{\lambda},d} \leq W_{R_y,d}$ and $W_{RM^{\lambda}(r+1,m+1),d} \leq W_{RM(r+1,m+1),d}$.

Proof. 1. Suppose the opposite, i.e. $w(x+y|x) > d$. Then by Kasami and Tokura Theorem [5] the codeword $(x + y|x)$ of $RM(r+1, m+1)$ is of weight at least $3d/2$. We see that $w(x + y + \lambda(y)|x + \lambda(y))$ cannot be d because $w(\lambda(y)) < d/4$, a contradiction.

2. Recall that

$$R_y^{\lambda} = \{(x + y + \lambda(y)|x + \lambda(y)) : x \in RM(r+1, m)\}$$

and

$$R_y = \{(x + y|x) : x \in RM(r+1, m)\}.$$

By (3) the code $RM^{\lambda}(r+1, m+1)$ is $\bigcup_{y \in RM(r,m)} R_y^{\lambda}$, whereas the original Reed-Muller code $RM(r+1, m+1)$ is $\bigcup_{y \in RM(r,m)} R_y$, see (4). For each $y \in RM(r, m)$ we compare the numbers of vectors of weight d in R_y^{λ} and R_y.

If $y = \mathbf{0}$, then because $\lambda(\mathbf{0}) = \mathbf{0}$, we have $R_{\mathbf{0}}^{\lambda} = R_{\mathbf{0}}$ and $W_{R_y^{\lambda},d} = W_{R_y,d}$.

If $w(y) = d$, the first statement of the current lemma implies that there is an injection of vectors of R_y^{λ} having weight d into that of R_y via translation to $(\lambda(y)|\lambda(y))$. So we have that $W_{R_y^{\lambda},d} \leq W_{R_y,d}$.

Any vector of R_y is $(x+y+\lambda(y)|x+\lambda(y))$ for some $x \in RM(r+1,m)$. For $w(y) > d$ taking $u = \lambda(y)$ in Proposition 2 we see that $w(x+y+\lambda(y)|x+\lambda(y)) > 3d/2$ and there are no vectors of R_y^λ with weight d.

▲

Now we consider the case that gives the codes with weight distribution different from that of $RM(r+1,m+1)$.

Lemma 2. *Let $\lambda : RM(r,m) \to \mathcal{L}$ be any function such that $\lambda(\mathbf{0}) = \mathbf{0}$ and $w(\lambda(y)) < d/4$ for any $y \in RM(r,m)$. If there is a codeword y' of $RM(r,m)$ such that $w(y') = d$, $\lambda(y') \not\preceq y'$, then $W_{R^\lambda_{y'},d} = 0$ and $W_{RM^\lambda(r+1,m+1),d} < W_{RM(r+1,m+1),d}$.*

Proof. Suppose the opposite, i.e. the vectors $(x+y'+\lambda(y')|x+\lambda(y'))$ and y' are of weight d. Then by Lemma 1 the vector $(x+y|x)$ is of weight d. This implies that $x \preceq y'$ by Proposition 1. Again, Proposition 1 applied to $(x+y'+\lambda(y')|x+\lambda(y'))$, gives that $x+\lambda(y') \preceq y'$. We have that $x \preceq y'$, $x+\lambda(y') \preceq y'$, $\lambda(y') \not\preceq y'$, a contradiction.

▲

The following proposition describes a "good case" in the sense that weight distributions of $RM^\lambda(r+1,m+1)$ and $RM(r+1,m+1)$ coincide.

Proposition 3. *Let $\lambda : RM(r,m) \to \mathcal{L}$ be any function such that $\lambda(y) \preceq y$ holds for any $y \in RM(r,m)$. Then $W_{RM^\lambda(r+1,m+1)} = W_{RM(r+1,m+1)}$.*

3.2 Distance-invariance in case of two-valued functions

In this section we consider two-valued functions λ taking only relatively small weights.

Lemma 3. *For any r,m such that $0 \le r \le m$, $1 \le m$ and $i \in \{1,\dots,2^m\}$ the code*

$$\{y : y \in RM(r,m), y_i = 0\}$$

has a minimum weight basis.

Proposition 4. *Let i be in $\{1,\dots,2^m\}$ and the function λ be such that $\lambda(y) = y_i e_i$ for any $y \in RM(r,m)$. Then the code $RM^\lambda(r+1,m+1)$ coincides with $RM(r+1,m+1)$ up to a permutation.*

Theorem 2. *For any $r,m, 0 \le r \le m$, $1 \le m$ and any $u \in F^{2^m}$, $w(u) < d/4$, let λ be any function from $RM(r,m)$ to $\{\mathbf{0},u\}$ such that $\lambda(\mathbf{0}) = \mathbf{0}$. Then the code $RM^\lambda(r+1,m+1)$ is distance-invariant and $W_{RM^\lambda(r+1,m+1)} = W_{RM(r+1,m+1)}$ if and only if it is the Reed-Muller code $RM(r+1,m+1)$ up to a permutation.*

Proof. The sufficiency follows from Proposition 4.

Let us prove the necessity. Let i be such that u_i is 1. The code $RM(r,m)$ is the union of $\{y : y \in RM(r,m), y_i = 0\}$ and its coset $\{y : y \in RM(r,m), y_i = 1\}$. We denote these subcodes by $RM_0(r,m)$ and $RM_1(r,m)$ respectively. We now consider the values of λ on $RM_0(r,m)$.

Let $RM^{\lambda}(r+1,m+1)$ be distance-invariant and have the same weight distribution as $RM(r+1,m+1)$. We first show that λ is all-zero on $RM_0(r,m)$. Suppose that opposite. Because $\lambda(\mathbf{0}) = \mathbf{0}$ and λ takes value u on a vector of $RM_0(r,m)$ by Lemma 3 there is a sequence of codewords $y^1, \ldots, y^t$ from the code $RM_0(r,m)$ satisfying $y^1 = \mathbf{0}$, $\lambda(\mathbf{0}) = \mathbf{0}$, $\lambda(y^t) = u$ such that for any $j \in \{1, \ldots, t-1\}$ we have $d(y^j, y^{j+1}) = d$. Therefore, in this sequence there are two vectors of $RM_0(r,m)$, which we denote by $\tilde{y}$ and $\overline{y}$, at distance d such that $\lambda(\tilde{y}) = \mathbf{0}$, $\lambda(\overline{y}) = u$.

Since $\lambda(\tilde{y}) = \mathbf{0}$ the vector $(\tilde{y}|\mathbf{0})$ is a codeword of $RM^{\lambda}(r+1,m+1)$. We show that $W_{RM^{\lambda}(r+1,m+1)+(\tilde{y}|\mathbf{0}),d} < W_{RM(r+1,m+1),d}$.

Consider the function λ' such that for any $y \in RM(r,m)$

$$\lambda'(y) = \lambda(y + \tilde{y}).$$

In view of the function λ' introduced above it is not hard to see that

$$RM^{\lambda}(r+1,m+1) + (\tilde{y}|\mathbf{0}) = RM^{\lambda'}(r+1,m+1).$$

By the choice of $\overline{y}$ and $\tilde{y}$ in $RM_0(r,m)$ at distance d, the vector $\overline{y} + \tilde{y}$ has weight d and belongs to $RM_0(r,m)$. Moreover, by the definition of the function λ', we have that $\lambda'(\overline{y}+\tilde{y}) = \lambda(\overline{y}+\tilde{y}+\tilde{y}) = \lambda(\overline{y}) = u$. Note that the ith position of the vectors in $RM_0(r,m)$ is zero whereas the ith position of the vector u is 1, so $u \not\preceq \overline{y} + \tilde{y}$.

We apply Lemma 2 to the function λ' and $y' = \overline{y} + \tilde{y}$ and we obtain

$$W_{RM^{\lambda'}(r+1,m+1),d} = W_{RM^{\lambda}(r+1,m+1)+(\tilde{y}|\mathbf{0}),d} < W_{RM(r+1,m+1),d}.$$

We conclude that when λ has nonzeros on $RM_0(r,m)$ the code $RM^{\lambda}(r+1,m+1)$ can not be distance invariant and have the weight-distribution as Reed-Muller code simultaneously.

The same argument for the values of λ on the coset $RM_1(r,m)$ of $RM_0(r,m)$ implies that either λ is the all-zero on $RM_1(r,m)$ or λ is constant, which is equal to u. In the latter case the function λ is zero only on the subcode $\{y \in RM(r,m), y_i = 0\}$. If we assume that u is of weight greater than 1, we repeat the proof above for any $i', u_{i'} = 1, i' \neq i$ and obtain that λ has zeros only on $\{y \in RM(r,m), y_{i'} = 0\}$, a contradiction.

We see that if $RM^{\lambda}(r+1,m+1)$ is distance-invariant and has the same weight distribution as $RM(r+1,m+1)$, then λ is the all-zero function or there is $i \in \{1, \ldots, 2^m\}$ such that $\lambda(y) = y_i e_i$ for all $y \in RM(r,m)$. In the first case the code $RM^{\lambda}(r+1,m+1)$ coincides with $RM(r+1,m+1)$ and in the second case by Proposition 4 it is equivalent to $RM(r+1,m+1)$.

▲

Proposition 5. *Let $\lambda : RM(r,m) \to \mathcal{L}$ be a linear function. Then the code $RM^{\lambda}(r+1,m+1)$ is linear.*

A large class of distance-invariant codes can be obtained from linear functions. However, in case of functions taking only two values of relatively small weights, the weight distributions of the obtained codes do not coincide with that of classic Reed – Muller codes or gives such codes up to permutations, see Theorem 2.

Corollary 2. *There are at least*

$$(|RM(r,m)|-1)(-1+\sum_{i=0}^{d/4-1}\tbinom{2^m}{i})-2^m+1$$

pairwise distinct linear codes $RM^{\lambda}(r+1,m+1)$ such that $W_{RM^{\lambda}(r+1,m+1),d} < W_{RM(r+1,m+1),d}$.

Proof. We take any linear function $\lambda : RM(r,m) \to \{\mathbf{0}, u\}$, $w(u) < d/4$ which is not the all-zero function and not $\lambda(y) = y_i e_i$, $i \in \{1,\dots,2^m\}$. The corollary follows from Proposition 5 and Theorem 2. ▲

Conclusion. We suggested a new construction for codes with parameters of Reed – Muller codes. In view of Proposition 3 we see that there are many codes with the same parameters and weight distribution as Reed – Muller codes. The results given in Section 3 demonstrate that it is rather difficult to find distance-invariant codes with the same number of the minimum weight codewords as in any Reed-Muller code.

References

1. E. Abbe, A. Shpilka, M. Ye, Reed-Muller Codes: Theory and Algorithms, IEEE Trans. Inform. Theory 67(6) (2021) 3251–3277.
2. D. Augot, P. Charpin and N. Sendrier, Studying the locator polynomials of minimum weight codewords of BCH codes, IEEE Trans. Inform. Theory, 30(3) (1992) 960–973.
3. N. Hamada, On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its application to error-correcting codes, Hiroshima Math. J., 3 (1973) 153–226.
4. M. Harada, E. Novak, V. Tonchev, The weight distribution of the self-dual [128, 64] polarity design code, Adv. Math. Commun., 10(3) (2016) 643–648.
5. T. Kasami, N. Tokura, On the weight structure of the Reed – Muller codes, IEEE Trans. Inform. Theory, 16 (1970) 752-759.
6. T. Kaufman, S. Lovett, and E. Porat, Weight distribution and list-decoding size of Reed-Muller codes, IEEE Trans. Inform. Theory, 58(5) (2012) 2689–2696.
7. F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland Publishing Company, 1977.

8. A. K. Pulatov, Lower bound on a complexity of the circuit implementation for one class of codes, Diskretn. Analiz, Novosibirsk, 25 (1974) 56–61 (in Russian).
9. D. Jungnickel and V. D. Tonchev, Polarities, quasi-symmetric designs, and Hamada's conjecture, Des. Codes Cryptogr., 51 (2009) 131–140.
10. D. Clark and V. D. Tonchev, A new class of majority-logic decodable codes derived from polarity designs, Adv. Math. Commun., 7 (2013) 175–186.
11. F. I. Solov'eva, On intersection of Reed – Muller like codes, Problems of Inform. Transm., 57(4) (2021) 353–363.
12. F. I. Solov'eva, Switchings and perfect codes, Numbers, Information and Complexity. I. Althofer, N. Gai, G. Dueck, L. Khachatrian, M.Pinsker, A. Sarkozy, I. Wegener and Z. Zhang (eds.), Kluwer Academic Publisher. (2000) 311–324.
13. Yu. L. Vasil'ev, On closely-packed nongroup codes, Probl. Kibern., 8 (1962) 337–339 (in Russian). Translated in: Yu. L. Vasil'yev. Nongroup close-packed codes. In: Algebraic Coding Theory: History and Development. Ed. I. F. BLAKE. Dowden, Hutchinson & Ross., (1973) 351–357 (reprint).