

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

<http://semr.math.nsc.ru>

Том 18, №2, стр. 1358–1366 (2021)

УДК 519.725

DOI 10.33048/semi.2021.18.103

MSC 94B60

MINIMUM WEIGHT BASES FOR QUATERNARY REED –
MULLER CODES

F. I. SOLOV'eva

ABSTRACT. The quaternary Plotkin and BQ-Plotkin constructions giving the families of quaternary Reed – Muller codes were presented in 2009. The Gray map image of the obtained \mathbb{Z}_4 -linear codes have the same parameters and fundamental properties as the codes in the classical binary linear Reed – Muller family. We have found one more general property for the families of quaternary Reed – Muller codes that is common with binary Reed – Muller codes: all these quaternary codes have bases of minimum weight codewords. The bases are constructed by induction.

Keywords: Reed – Muller code, quaternary code, additive code, quaternary Reed – Muller code, minimum weight basis, \mathbb{Z}_4 -linear code.

1. INTRODUCTION

A basis of a linear code is called a *minimum weight basis* if it consists of codewords of minimum nonzero weight. The problem of finding a short representation of group (cyclic) codes is important in coding theory, in graph theory, in cryptography and in testing theory. It concerns to the questions of compact storage of codes, the reconstructions from their minimum distance graphs or designs, for fast isomorphism testing of strongly regular graphs. See the papers [6, 7] and the list of references there for more details. Many good linear or cyclic codes have minimum weight bases such as Hamming, Reed–Solomon, some extended BCH, Griesmer codes, etc., see a short survey in [7].

In [10, 11] some quaternary constructions generalizing the quaternary Plotkin construction given in [12] were presented. Two families of quaternary Reed – Muller

SOLOV'eva, F.I., MINIMUM WEIGHT BASES FOR QUATERNARY REED – MULLER CODES .

© 2021 SOLOV'eva F.I.

The work is supported by RFBR (grant 19-01-00682).

Received December, 12, 2020, published November, 24, 2021.

codes were constructed in [10, 11] and it was proved that under the Gray map the corresponding \mathbb{Z}_4 -linear codes have similar properties (length, dimension, minimum distance, inclusion and duality relationship) as the classical binary linear Reed – Muller codes but these codes are not linear. Moreover the families contain the \mathbb{Z}_4 -linear Hadamard codes and \mathbb{Z}_4 -linear extended 1-perfect codes classified by Krotov in [2, 3]. It was established in [1] that the minimum distance graph of any perfect binary code is connected. The analogous result is true for extended perfect binary code, see [5]. Therefore we have the existence of minimum weight basis for any quaternary perfect code that is included in the class of quaternary Reed – Muller codes. The structures and dimensions of the kernels of the codes in the families were investigated in [9]. Classification of ranks of some of these \mathbb{Z}_4 -linear codes was obtained in [8].

All necessary definitions could be found in [11]. Here we recall some of them. Let \mathbb{Z}_4 be the ring of integers modulo four and \mathbb{Z}_4^N be the set of all quaternary words of length N . The Lee weight of the elements of \mathbb{Z}_4 is $w_L(0) = 0, w_L(1) = w_L(3) = 1$ and $w_L(2) = 2$. The Lee weight $w_L(x)$ of a word in \mathbb{Z}_4^N is the addition of the Lee weights of all its coordinates. The Lee distance $d_L(x, y)$ between two words $x, y \in \mathbb{Z}_4^N$ is defined as $d_L(x, y) = w_L(x - y)$. A nonempty subset \mathcal{C} of \mathbb{Z}_4^N is a quaternary code and a subgroup of \mathbb{Z}_4^N is called a *quaternary linear code*. A quaternary linear code being a subgroup \mathcal{C} of \mathbb{Z}_4^N is isomorphic to an abelian structure of type $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ for some integers γ, δ . Therefore $|\mathcal{C}| = 2^{\gamma+2\delta}$. Such code \mathcal{C} is called a *quaternary linear code of type $(N; \gamma, \delta)$* and its binary image $C = \phi(\mathcal{C})$ under the Gray map is called a *\mathbb{Z}_4 -linear code of type $(N; \gamma, \delta)$* .

In [11] combining two constructions $\lfloor \frac{m+1}{2} \rfloor$ nonequivalent families of quaternary linear Reed – Muller codes for each value of m and any integer r such that $0 \leq r \leq m$ were proposed. For fixed m and r the families were distinguished by their abelian structure.

Recall [4] that the classical binary linear Reed – Muller code $RM(r, m)$ has length $n = 2^m$; the minimum Hamming distance $d = 2^{m-r}$; dimension $k = \sum_{i=0}^r \binom{m}{i}$. For $0 \leq r \leq m$ the code $RM(r, m)$ is the dual code of $RM(m - 1 - r, m)$ and $RM(r - 1, m) \subset RM(r, m)$. The code $RM(m - 2, m)$ is a linear code of parameters $(2^m, 2^m - m - 1, 4)$ which is equivalent to the extended Hamming code of the same length and the code $RM(1, m)$ is equivalent to the linear Hadamard code. The code $RM(m, m)$ consists of the set of all binary vectors of length 2^m and the code $RM(0, m)$ is the repetition code of length 2^m .

The binary Reed – Muller codes have one more fundamental property: they have minimum weight bases, see [4], §13.5. In the paper we investigate such property for the families of quaternary linear Reed – Muller codes from [10, 11]. It is proved that all these quaternary codes not only have bases of minimum weight codewords but the bases could be constructed iteratively. From graph theory point of view it means that the minimum distance graph of any such code is connected, so we generalize the result of the paper [5] given for quaternary codes with parameters of extended perfect binary codes. Applying the Plotkin construction one could obtain iteratively a minimum weight basis for a binary linear Reed – Muller code $RM(r, m)$ (see Corollary 1 below).

2. PLOTKIN AND BQ-PLOTKIN CONSTRUCTIONS

Plotkin construction. Recall the definition of quaternary Plotkin construction [10, 11]. Let \mathcal{A} and \mathcal{B} be any two quaternary linear codes of types $(N; \gamma_{\mathcal{A}}, \delta_{\mathcal{A}})$ and $(N; \gamma_{\mathcal{B}}, \delta_{\mathcal{B}})$ with generator matrices $\mathcal{G}_{\mathcal{A}}$ and $\mathcal{G}_{\mathcal{B}}$. Define a quaternary linear Plotkin code as

$$\mathcal{C} = \{(x|x+y) : x \in \mathcal{A}, y \in \mathcal{B}\}.$$

Its generator matrix is

$$\mathcal{G}_{\mathcal{C}} = \begin{pmatrix} \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} \\ 0 & \mathcal{G}_{\mathcal{B}} \end{pmatrix}$$

and the code \mathcal{C} is of type $(2N; \gamma, \delta)$, where $\gamma = \gamma_{\mathcal{A}} + \gamma_{\mathcal{B}}$ and $\delta = \delta_{\mathcal{A}} + \delta_{\mathcal{B}}$; the binary length is $n = 4N$; the size $2^{\gamma+2\delta}$ and the minimum distance $d = \min\{2d_{\mathcal{A}}, d_{\mathcal{B}}\}$.

Now we apply the Plotkin construction to produce quaternary Reed – Muller codes.

The construction is inductive and for the induction base we take the codes for $m = 1$, so the case of codes of binary length $n = 2$. The quaternary linear Reed – Muller codes $\mathcal{RM}_0(0, 1)$ and $\mathcal{RM}_0(1, 1)$ are the repetition code with only one nonzero vector $\mathbf{2}$ of type $(1; 1, 0)$ and the whole vector space \mathbb{Z}_4^1 , i.e. a quaternary linear code of type $(1; 0, 1)$ respectively. These codes, $\mathcal{RM}_0(0, 1)$ and $\mathcal{RM}_0(1, 1)$, after the Gray map, give binary codes with the same codewords that the corresponding codes $RM(r, 1)$, $r = 0, 1$. The generator matrix of $\mathcal{RM}_0(0, 1)$ is $\begin{pmatrix} 2 \end{pmatrix}$ and the generator matrix of $\mathcal{RM}_0(1, 1)$ is $\begin{pmatrix} 1 \end{pmatrix}$.

Let $\mathcal{RM}_s(r, m-1)$ and $\mathcal{RM}_s(r-1, m-1)$ be any two quaternary linear Reed – Muller codes of types $(N; \gamma_{r, m-1}^s, \delta_{r, m-1}^s)$ and $(N; \gamma_{r-1, m-1}^s, \delta_{r-1, m-1}^s)$ of lengths $N = 2^{m-2}$, sizes 2^{k_r} and $2^{k_{r-1}}$, code distances 2^{m-r-1} and 2^{m-r} respectively, where $k_r = \sum_{i=0}^r \binom{m-1}{i}$ and $k_{r-1} = \sum_{i=0}^{r-1} \binom{m-1}{i}$. In [10, 11] it was established that for any r and $m \geq 2$, $0 < r < m$, the code obtained by using the Plotkin construction

$$(1) \quad \mathcal{RM}_s(r, m) = \{(x|x+y) : x \in \mathcal{RM}_s(r, m-1), y \in \mathcal{RM}_s(r-1, m-1)\},$$

$0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ with the exception m odd and $s = (m-1)/2$ is a quaternary linear code of type $(2N; \gamma_{r, m}^s, \delta_{r, m}^s)$, where $\gamma_{r, m}^s = \gamma_{r, m-1}^s + \gamma_{r-1, m-1}^s$ and $\delta_{r, m}^s = \delta_{r, m-1}^s + \delta_{r-1, m-1}^s$. The length of the code is $2N = 2^{m-1}$, the number of codewords 2^k , where $k = \sum_{i=0}^r \binom{m}{i}$, the code distance 2^{m-r} and it is true that $\mathcal{RM}_s(r-1, m) \subset \mathcal{RM}_s(r, m)$. For $r = 0$, the code $\mathcal{RM}_s(0, m)$ is the repetition code with only one nonzero codeword equaled the all twos vector.

BQ-Plotkin construction. Another construction presented in [10, 11] is the quaternary BQ-Plotkin construction.

Let $\mathcal{G}_{\mathcal{A}}$, $\mathcal{G}_{\mathcal{B}}$ and $\mathcal{G}_{\mathcal{C}}$ be generator matrices of the quaternary linear codes \mathcal{A} , \mathcal{B} and \mathcal{C} , respectively. The code $\mathcal{BQ}(\mathcal{A}, \mathcal{B}, \mathcal{C})$ obtained by the BQ-Plotkin construction is the quaternary linear code generated by the matrix

$$(2) \quad \begin{pmatrix} \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} \\ 0 & \mathcal{G}'_{\mathcal{B}} & 2\mathcal{G}'_{\mathcal{B}} & 3\mathcal{G}'_{\mathcal{B}} \\ 0 & 0 & \hat{\mathcal{G}}_{\mathcal{B}} & \hat{\mathcal{G}}_{\mathcal{B}} \\ 0 & 0 & 0 & \mathcal{G}_{\mathcal{C}} \end{pmatrix}.$$

Here $\mathcal{G}'_{\mathcal{B}}$ is the matrix obtained from $\mathcal{G}_{\mathcal{B}}$ after switching twos by ones in their $\gamma_{\mathcal{B}}$ rows of order two and $\hat{\mathcal{G}}_{\mathcal{B}}$ is the matrix obtained from $\mathcal{G}_{\mathcal{B}}$ after removing their $\gamma_{\mathcal{B}}$ rows of order two. The quaternary linear code $\mathcal{BQ}(\mathcal{A}, \mathcal{B}, \mathcal{C})$ is of type $(4N; \gamma, \delta)$,

where $\gamma = \gamma_{\mathcal{A}} + \gamma_{\mathcal{C}}$ and $\delta = \delta_{\mathcal{A}} + \gamma_{\mathcal{B}} + 2\delta_{\mathcal{B}} + \delta_{\mathcal{C}}$. The binary length of the code is $n = 8N$; the size is $2^{\gamma}4^{\delta}$ and the minimum Lee distance $d = \min\{4d_{\mathcal{A}}, 2d_{\mathcal{B}}, d_{\mathcal{C}}\}$.

Now let us consider the definition of quaternary linear Reed - Muller codes given by the BQ-Plotkin construction. Let $\mathcal{RM}_{s-1}(r, m - 2)$, $\mathcal{RM}_{s-1}(r - 1, m - 2)$ and $\mathcal{RM}_{s-1}(r - 2, m - 2)$, $0 < s \leq \lfloor \frac{m-1}{2} \rfloor$, $m \geq 3$ be any three quaternary linear Reed - Muller codes of types $(N; \gamma_{r,m-2}^{s-1}, \delta_{r,m-2}^{s-1})$, $(N; \gamma_{r-1,m-2}^{s-1}, \delta_{r-1,m-2}^{s-1})$ and $(N; \gamma_{r-2,m-2}^{s-1}, \delta_{r-2,m-2}^{s-1})$ with the generator matrices $\mathcal{G}_{s-1}(r, m - 2)$, $\mathcal{G}'_{s-1}(r - 1, m - 2)$ and $\mathcal{G}_{s-1}(r - 2, m - 2)$ respectively. The codes have length $N = 2^{m-3}$; binary length $n = 2^{m-2}$; number of codewords 2^{k_r} , $2^{k_{r-1}}$ and $2^{k_{r-2}}$; minimum distances 2^{m-r-2} , 2^{m-r-1} and 2^{m-r} respectively. Here $k_r = \sum_{i=0}^r \binom{m-2}{i}$, $k_{r-1} = \sum_{i=0}^{r-1} \binom{m-2}{i}$ and $k_{r-2} = \sum_{i=0}^{r-2} \binom{m-2}{i}$.

Let $\mathcal{G}_s(r, m)$, $0 < r < m - 1$ be the matrix

$$(3) \quad \begin{pmatrix} \mathcal{G}_{s-1}(r, m - 2) & \mathcal{G}_{s-1}(r, m - 2) & \mathcal{G}_{s-1}(r, m - 2) & \mathcal{G}_{s-1}(r, m - 2) \\ 0 & \mathcal{G}'_{s-1}(r - 1, m - 2) & 2\mathcal{G}'_{s-1}(r - 1, m - 2) & 3\mathcal{G}'_{s-1}(r - 1, m - 2) \\ 0 & 0 & \hat{\mathcal{G}}_{s-1}(r - 1, m - 2) & \hat{\mathcal{G}}_{s-1}(r - 1, m - 2) \\ 0 & 0 & 0 & \mathcal{G}_{s-1}(r - 2, m - 2) \end{pmatrix},$$

here the matrices $\mathcal{G}'_{s-1}(r - 1, m - 2)$ and $\hat{\mathcal{G}}_{s-1}(r - 1, m - 2)$ are defined from the matrices $\mathcal{G}_{s-1}(r - 1, m - 2)$ and $\mathcal{G}_{s-1}(r - 1, m - 2)$ analogously as the matrices $\mathcal{G}'_{\mathcal{B}}$ and $\hat{\mathcal{G}}_{\mathcal{B}}$ above in (2). For any r and $m \geq 3$, $0 < r < m - 1$ the code $\mathcal{RM}_s(r, m)$, $0 < s \leq \lfloor \frac{m-1}{2} \rfloor$ is defined by the given above BQ-Plotkin construction

$$(4) \quad \mathcal{RM}_s(r, m) = \mathcal{BQ}(\mathcal{RM}_{s-1}(r, m - 2), \mathcal{RM}_{s-1}(r - 1, m - 2), \mathcal{RM}_{s-1}(r - 2, m - 2))$$

with the generator matrix $\mathcal{G}_s(r, m)$. It is a quaternary linear code of type $(4N; \gamma_{r,m}^s, \delta_{r,m}^s)$, where

$$\gamma_{r,m}^s = \gamma_{r,m-2}^{s-1} + \gamma_{r-2,m-2}^{s-1}, \quad \delta_{r,m}^s = \delta_{r,m-2}^{s-1} + \gamma_{r-1,m-2}^{s-1} + 2\delta_{r-1,m-2}^{s-1} + \delta_{r-2,m-2}^{s-1}.$$

The binary length of the code is $n = 2^m$; the number of codewords 2^k , where $k = \sum_{i=0}^r \binom{m}{i}$; the minimum distance 2^{m-r} and $\mathcal{RM}_s(r - 1, m) \subset \mathcal{RM}_s(r, m)$.

To be coherent with the construction, for $r = -1$, the code $\mathcal{RM}_s(-1, m)$ coincides with the all-zero codeword code, the code $\mathcal{RM}_s(0, m)$ is the repetition code with only one nonzero codeword equaled the all twos quaternary vector. For $r = m - 1$ and $r = m$, the codes $\mathcal{RM}_s(m - 1, m)$ and $\mathcal{RM}_s(m, m)$ are the even weight code and the whole space $\mathbb{Z}_4^{2^{m-1}}$ respectively. The following generator matrices: $(2 \dots 2)$ and $I_{2^{m-1}}$ satisfy the property to have minimum weight rows for the codes $\mathcal{RM}_s(0, m)$ and $\mathcal{RM}_s(m, m)$ respectively, see [11]. The generator matrix $\mathcal{G}_s(m - 1, m)$ is recursively obtained by using the BQ-Plotkin construction

$$\mathcal{BQ}(\mathcal{RM}_{s-1}(m - 2, m - 2), \mathcal{RM}_{s-1}(m - 2, m - 2), \mathcal{RM}_{s-1}(m - 3, m - 2)).$$

To obtain the code $\mathcal{RM}_1(1, 3)$ we have to apply the BQ-Plotkin construction. Then for $m \geq 4$ using the Plotkin construction we can build the two families of the codes $\mathcal{RM}_s(r, 4)$ for $s = 0, 1$, $0 \leq r \leq 4$ from the codes in the families $\mathcal{RM}_s(r, m)$, where $s \in \{0, 1\}$, applying the Plotkin construction for $m = 3$ or the BQ-Plotkin construction for $m = 2$. The code $\mathcal{RM}_0(r, 5)$ only can be obtained applying the Plotkin construction, $\mathcal{RM}_2(r, 5)$ only can be obtained applying the BQ-Plotkin construction, but $\mathcal{RM}_1(r, 5)$ can be obtained using either the Plotkin or the BQ-Plotkin construction.

Note that for the Plotkin construction we have $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ with the exception m odd and $s = (m - 1)/2$ and for the BQ-Plotkin construction it is true $0 < s \leq \lfloor \frac{m-1}{2} \rfloor$. Hence combining the Plotkin and the BQ-Plotkin construction we obtain $\lfloor \frac{m+1}{2} \rfloor$ nonequivalent families of quaternary linear Reed – Muller codes $\mathcal{RM}_s(r, m)$ for each value of $m \geq 2$ and $0 \leq r \leq m$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. The codes are distinguished by their abelian structure. The subindex s from the set $\{0, \dots, \lfloor \frac{m-1}{2} \rfloor\}$ is used to specify the code $\mathcal{RM}_s(r, m)$ for fixed m, r .

3. MINIMUM WEIGHT BASES FOR $\mathcal{RM}_s(r, m)$

Denote by $\mathcal{B}_s(r, m)$ a basis of the code $\mathcal{RM}_s(r, m)$ and by $\mathbf{0}$ the all-zero vector of length 2^{m-1} .

Theorem 1. *Let for any r and $m \geq 2$, $0 \leq r < m$ and for any s , $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ with the exception m odd and $s = (m - 1)/2$ the codes $\mathcal{RM}_s(r, m - 1)$ and $\mathcal{RM}_s(r - 1, m - 1)$ be two quaternary linear Reed – Muller codes having minimum weight bases. Then the quaternary linear code $\mathcal{RM}_s(r, m)$ obtained by the Plotkin construction (1) has a minimum weight basis.*

Proof. Let the sets $\mathcal{B}_s(r, m - 1)$ and $\mathcal{B}_s(r - 1, m - 1)$ (with the exception for s mentioned in the statement of the theorem) be minimum weight bases for quaternary codes $\mathcal{RM}_s(r, m - 1)$ and $\mathcal{RM}_s(r - 1, m - 1)$, $0 \leq s \leq \lfloor \frac{m-2}{2} \rfloor$. By the condition of the theorem the vectors of the bases $\mathcal{B}_s(r, m - 1)$ and $\mathcal{B}_s(r - 1, m - 1)$ are of weights 2^{m-1-r} and 2^{m-r} respectively, where $|\mathcal{B}_s(r, m - 1)| = \sum_{i=0}^r \binom{m-1}{i}$ and $|\mathcal{B}_s(r - 1, m - 1)| = \sum_{i=0}^{r-1} \binom{m-1}{i}$. By the Plotkin construction (1) the subset

$$\mathcal{B} = \{(x|x) | x \in \mathcal{B}_s(r, m - 1)\} \cup \{(\mathbf{0}|y) | y \in \mathcal{B}_s(r - 1, m - 1)\}$$

of the code $\mathcal{RM}_s(r, m)$ is linearly independent in a quaternary sense and

$$(5) \quad |\mathcal{B}| = |\mathcal{B}_s(r, m - 1)| + |\mathcal{B}_s(r - 1, m - 1)| = \sum_{i=0}^r \binom{m}{i} = \dim(\mathcal{RM}_s(r, m)).$$

From $w((x|x)) = 2^{m-r}$, $w((\mathbf{0}|y)) = 2^{m-r}$ and (5) we conclude that the set of codewords \mathcal{B} is a minimum weight basis of the code $\mathcal{RM}_s(r, m)$. \square

Analogously we are able to prove more general result for quaternary Plotkin codes.

Proposition 1. *Let \mathcal{A} and \mathcal{B} be any two quaternary linear codes of types $(N; \gamma_{\mathcal{A}}, \delta_{\mathcal{A}})$ and $(N; \gamma_{\mathcal{B}}, \delta_{\mathcal{B}})$ having minimum weight bases. Then a quaternary linear Plotkin code*

$$\mathcal{C} = \{(x|x + y) : x \in \mathcal{A}, y \in \mathcal{B}\}$$

has minimum weight basis.

Instead of the quaternary codes $\mathcal{RM}_s(r, m - 1)$ and $\mathcal{RM}_s(r - 1, m - 1)$ taking the binary linear Reed – Muller codes $RM(r, m - 1)$ and $RM(r - 1, m - 1)$ respectively by Theorem 1 applying the Plotkin construction to these codes we obtain iteratively a minimum weight basis $\mathcal{B}(r, m)$ for binary linear Reed – Muller code $RM(r, m)$.

Corollary 1. *Let $\mathcal{B}(r, m - 1)$ and $\mathcal{B}(r - 1, m - 1)$ be any minimum weight bases for the binary linear Reed – Muller codes $RM(r, m - 1)$ and $RM(r - 1, m - 1)$ respectively. Then the set $\{(x|x + y) : x \in \mathcal{B}(r, m - 1), y \in \mathcal{B}(r - 1, m - 1)\}$ is the*

minimum weight basis $\mathcal{B}(r, m)$ of the binary linear Reed - Muller code $RM(r, m)$ given by the Plotkin construction

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

Theorem 2. Let for any $m \geq 3$ and $r, 0 \leq r < m - 1$ and any $0 < s \leq \lfloor \frac{m-1}{2} \rfloor$ the codes $\mathcal{RM}_{s-1}(r, m - 2)$, $\mathcal{RM}_{s-1}(r - 1, m - 2)$ and $\mathcal{RM}_{s-1}(r - 2, m - 2)$ be any three quaternary linear Reed - Muller codes having minimum weight bases. Then the quaternary linear code $\mathcal{RM}_s(r, m)$ obtained by the BQ-Plotkin construction (4) has a minimum weight basis.

Proof. Let for any $r \leq m - 2$ the sets $\mathcal{B}_{s-1}(r, m - 2)$, $\mathcal{B}_{s-1}(r - 1, m - 2)$ and $\mathcal{B}_{s-1}(r - 2, m - 2)$ be minimum weight bases for quaternary codes $\mathcal{RM}_{s-1}(r, m - 2)$ and $\mathcal{RM}_{s-1}(r - 1, m - 2)$ and $\mathcal{RM}_{s-1}(r - 2, m - 2)$, $0 < s \leq \lfloor \frac{m-1}{2} \rfloor$ of types $(N; \gamma_{r, m-2}^{s-1}, \delta_{r, m-2}^{s-1})$, $(N; \gamma_{r-1, m-2}^{s-1}, \delta_{r-1, m-2}^{s-1})$ and $(N; \gamma_{r-2, m-2}^{s-1}, \delta_{r-2, m-2}^{s-1})$ respectively. By the condition of the theorem $\mathcal{B}_{s-1}(r, m - 2)$, $\mathcal{B}_{s-1}(r - 1, m - 2)$ and $\mathcal{B}_{s-1}(r - 2, m - 2)$ are bases of minimum weights 2^{m-r-2} , 2^{m-r-1} and 2^{m-r} respectively. Here $|\mathcal{B}_{s-1}(r, m - 2)| = \sum_{i=0}^r \binom{m-2}{i}$, $|\mathcal{B}_{s-1}(r - 1, m - 2)| = \sum_{i=0}^{r-1} \binom{m-2}{i}$ and $|\mathcal{B}_{s-1}(r - 2, m - 2)| = \sum_{i=0}^{r-2} \binom{m-2}{i}$. Providing some equivalent transformations for rows of the generator matrix (3) we construct a minimum weight basis for the code $\mathcal{RM}_s(r, m)$. Let us consider the submatrices

$$(6) \quad G' = \left(\begin{array}{cccc} 0 & \mathcal{G}'_{s-1}(r - 1, m - 2) & 2\mathcal{G}'_{s-1}(r - 1, m - 2) & 3\mathcal{G}'_{s-1}(r - 1, m - 2) \end{array} \right)$$

and

$$(7) \quad G'' = \left(\begin{array}{cccc} 0 & 0 & \hat{\mathcal{G}}_{s-1}(r - 1, m - 2) & \hat{\mathcal{G}}_{s-1}(r - 1, m - 2) \end{array} \right)$$

of the matrix (3). Without loss of generality the rows of G' and G'' could be written in such a way that the rows of G' corresponding to the quaternary part of the submatrix $\mathcal{G}_{s-1}(r - 1, m - 2)$ coincides with $\hat{\mathcal{G}}_{s-1}(r - 1, m - 2)$. So we have

$$(8) \quad G' = \left(\begin{array}{cccc} 0 & \hat{\mathcal{G}}_{s-1}(r - 1, m - 2) & 2\hat{\mathcal{G}}_{s-1}(r - 1, m - 2) & 3\hat{\mathcal{G}}_{s-1}(r - 1, m - 2) \\ 0 & \tilde{\mathcal{G}}_{s-1}(r - 1, m - 2) & 2\tilde{\mathcal{G}}_{s-1}(r - 1, m - 2) & 3\tilde{\mathcal{G}}_{s-1}(r - 1, m - 2) \end{array} \right).$$

By the construction of $\mathcal{RM}_{s-1}(r - 1, m - 2)$ the submatrix $\tilde{\mathcal{G}}_{s-1}(r - 1, m - 2)$ of G' contains $\gamma_{r-1, m-2}^{s-1}$ rows of the matrix $\mathcal{G}_{s-1}(r - 1, m - 2)$ after switching twos by ones in all its binary rows. Adding any i th row, $i \in \{1, 2, \dots, \delta_{r-1, m-2}^{s-1}\}$ of the matrix (7) to the i th row of the matrix (8) over \mathbb{Z}_4 we obtain

$$(9) \quad G = \left(\begin{array}{cccc} 0 & \hat{\mathcal{G}}_{s-1}(r - 1, m - 2) & 3\hat{\mathcal{G}}_{s-1}(r - 1, m - 2) & 0 \\ 0 & \tilde{\mathcal{G}}_{s-1}(r - 1, m - 2) & 2\tilde{\mathcal{G}}_{s-1}(r - 1, m - 2) & 3\tilde{\mathcal{G}}_{s-1}(r - 1, m - 2) \end{array} \right).$$

As the result we have the following generator matrix of the code $\mathcal{RM}_s(r, m)$ that is equivalent to the matrix (3):

$$(10) \quad \left(\begin{array}{cccc} \mathcal{G}_{s-1}(r, m - 2) & \mathcal{G}_{s-1}(r, m - 2) & \mathcal{G}_{s-1}(r, m - 2) & \mathcal{G}_{s-1}(r, m - 2) \\ 0 & \hat{\mathcal{G}}_{s-1}(r - 1, m - 2) & 3\hat{\mathcal{G}}_{s-1}(r - 1, m - 2) & 0 \\ 0 & \tilde{\mathcal{G}}_{s-1}(r - 1, m - 2) & 2\tilde{\mathcal{G}}_{s-1}(r - 1, m - 2) & 3\tilde{\mathcal{G}}_{s-1}(r - 1, m - 2) \\ 0 & 0 & \hat{\mathcal{G}}_{s-1}(r - 1, m - 2) & \hat{\mathcal{G}}_{s-1}(r - 1, m - 2) \\ 0 & 0 & 0 & \mathcal{G}_{s-1}(r - 2, m - 2) \end{array} \right).$$

Let us calculate the Lee weights of the rows of the matrix (10) to show that they are of minimum weight 2^{m-r} .

By the condition of the theorem the Lee weight of any row of the submatrix $\mathcal{G}_{s-1}(r, m-2)$ is 2^{m-r-2} . Therefore the Lee weight of any row of the submatrix

$$(11) \quad (\mathcal{G}_{s-1}(r, m-2) \quad \mathcal{G}_{s-1}(r, m-2) \quad \mathcal{G}_{s-1}(r, m-2) \quad \mathcal{G}_{s-1}(r, m-2))$$

is $4 \cdot 2^{m-r-2} = 2^{m-r}$.

Again by the condition of the theorem the rows of the submatrix

$$(0 \quad \hat{\mathcal{G}}_{s-1}(r-1, m-2) \quad 3\hat{\mathcal{G}}_{s-1}(r-1, m-2) \quad 0)$$

are of the Lee weight $2 \cdot 2^{m-r-1} = 2^{m-r}$.

By the condition of the theorem and by the structure of the matrix $\tilde{\mathcal{G}}_{s-1}(r-1, m-2)$ the Lee weight of any of its $\gamma_{r-1, m-2}^{s-1}$ rows is 2^{m-r-2} . Hence the Lee weight of any row in the matrix

$$(0 \quad \tilde{\mathcal{G}}_{s-1}(r-1, m-2) \quad 2\tilde{\mathcal{G}}_{s-1}(r-1, m-2) \quad 3\tilde{\mathcal{G}}_{s-1}(r-1, m-2))$$

is $2^{m-r-2} + 2 \cdot 2^{m-r-2} + 2^{m-r-2} = 2^{m-r}$. Therefore each row of G has the Lee weight 2^{m-r} .

For the submatrices

$$(0 \quad 0 \quad \hat{\mathcal{G}}_{s-1}(r-1, m-2) \quad \hat{\mathcal{G}}_{s-1}(r-1, m-2))$$

and

$$(0 \quad 0 \quad 0 \quad \mathcal{G}_{s-1}(r-2, m-2))$$

by the condition of the theorem we have the Lee weights of any of their rows $2^{m-r-1} + 2^{m-r-1} = 2^{m-r}$ and 2^{m-r} respectively. Hence all rows of the generator matrix (10) of the code $\mathcal{RM}_s(r, m)$ have minimum weight 2^{m-r} . \square

Again analogously to Theorem 2 one could prove more general result for quaternary BQ-Plotkin codes.

Proposition 2. *Let \mathcal{G}_A , \mathcal{G}_B and \mathcal{G}_C be any three quaternary linear codes of types $(N; \gamma_A, \delta_A)$, $(N; \gamma_B, \delta_B)$ and $(N; \gamma_C, \delta_C)$ having minimum weight bases. Then a quaternary linear BQ-Plotkin code $\mathcal{BQ}(\mathcal{A}, \mathcal{B}, \mathcal{C})$ has minimum weight basis.*

Theorem 3. *For any r and $m \geq 2$, $0 \leq r < m$ and for any s , $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ the quaternary linear code $\mathcal{RM}_s(r, m)$ has a minimum weight basis.*

Proof. The proof will be provided by induction on $m \geq 2$ combining the Plotkin and the BQ-Plotkin quaternary constructions. Recall that any known quaternary linear code $\mathcal{RM}_s(r, m)$, where $m \geq 2$, $0 \leq r < m$ and $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, is obtained either the Plotkin or the BQ-Plotkin construction, see [10, 11]. Note that by the BQ-Plotkin construction (4) the subindices of the obtained Reed – Muller codes could vary from $s = 1$ to $s = \lfloor \frac{m-1}{2} \rfloor$ for the resulting codes and the Plotkin construction is valid for any s , $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ with the exception m odd and $s = (m-1)/2$. Therefore the constructions do not cover each other. Hence we consider for the induction base not only case $m = 2$ but also $m = 3$, where the BQ-Plotkin construction stated to be valid and we have $\mathcal{RM}_0(1, 3) \neq \mathcal{RM}_1(1, 3)$.

For $m = 2$, $s = 0$ it is evident that $\mathcal{B}_0(0, 2) = \{(2, 2)\}$, $\mathcal{B}_0(1, 2) = \{(1, 1), (0, 2)\}$ and $\mathcal{B}_0(2, 2) = \{(1, 0), (0, 1)\}$ are minimum weights bases for $\mathcal{RM}_0(0, 2)$, $\mathcal{RM}_0(1, 2)$ and $\mathcal{RM}_0(2, 2) = \mathbb{Z}_4^2$ respectively.

Let us consider case $m = 3$, $s = 0$. It is easy to see that

$\mathcal{B}_0(0, 3) = \{(2, 2, 2, 2)\}$, $\mathcal{B}_0(2, 3) = \{(0, 1, 0, 1), (1, 0, 1, 0), (0, 0, 1, 1), (0, 0, 0, 2)\}$ and $\mathcal{B}_0(3, 3) = \{(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)\}$ are minimum weight bases for the codes $\mathcal{RM}_0(0, 3)$, $\mathcal{RM}_0(2, 3)$ and $\mathcal{RM}_0(3, 3) = \mathbb{Z}_4^3$ respectively.

The code $\mathcal{RM}_0(1, 3)$ could be constructed from the codes $\mathcal{RM}_0(1, 2)$ and $\mathcal{RM}_0(0, 2)$ by the Plotkin construction (1) and the minimum weight basis is $\mathcal{B}_0(1, 3) = \{(x|x|x|x \in \mathcal{B}_0(1, 2)\} \cup \{(\mathbf{0}|y|y|y \in \mathcal{B}_0(0, 2)\} = \{(1, 1, 1, 1), (0, 2, 0, 2), (0, 0, 2, 2)\}$, here $\mathbf{0} = (0, 0)$.

Let us now consider case $m = 3, s = 1$. It is easy to check that $\mathcal{RM}_1(r, 3) = \mathcal{RM}_0(r, 3)$ for $r \in \{0, 2, 3\}$.

The code $\mathcal{RM}_1(1, 3)$ could be constructed from the codes $\mathcal{RM}_0(1, 1)$ and $\mathcal{RM}_0(0, 1)$ by the BQ-Plotkin construction using the generator matrix (3). The generator matrix of $\mathcal{RM}_1(1, 3)$ is equivalent to the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix}.$$

Then $\mathcal{B}_1(1, 3) = \{(1, 1, 1, 1), (0, 1, 2, 3)\}$ is a minimum weight basis of the code $\mathcal{RM}_1(1, 3)$.

Using this induction base combining the Plotkin and the BQ-Plotkin constructions by Theorems 1 and 2 we construct iteratively a minimum weight basis of the quaternary linear code $\mathcal{RM}_s(r, m)$ for any r and $m \geq 2, 0 \leq r < m$ and for any $s, 0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$. Recall that here we took into account that the condition $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ is obtained from the conditions for the parameter s of both the Plotkin and the BQ-Plotkin constructions. \square

The author is grateful to I. Yu. Mogilnykh for fruitful discussions, which allowed to improve the presentation of the paper.

REFERENCES

[1] S.V. Avgustinovich, *On isometry of close-packed binary codes*. (English. Russian original) Sib. Adv. Math. **5**:3 (1995), 1–4. Zbl 0852.94027

[2] D.S. Krotov, *\mathbb{Z}_4 -linear perfect codes*, Discret. Anal. Isslrd. Oper., Ser. 1, **7**:4 (2000), 78–90. Zbl 1008.94025

[3] D.S. Krotov, *\mathbb{Z}_4 -linear Hadamard and extended perfect codes*, in Augot, Daniel (ed.) et al., *WCC2001 international Workshop on coding and cryptography*, Paris (France), Jan. 8–12, (2001), Elsevier, Electron. Notes Discrete Math., **6**, Amsterdam, 2001. Zbl 0987.94513

[4] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland Publishing Company, Amsterdam etc., 1977. Zbl 0369.94008

[5] I.Yu. Mogilnykh, P.R.J. Östergård, O. Pottonen, F.I. Solov'eva, *Reconstructing extended perfect binary one-error-correcting codes from their minimum distance graphs*, IEEE Trans. Inf. Theory, **55**:6 (2009), 2622–2625. Zbl 1367.94407

[6] I.Yu. Mogilnykh, F.I. Solov'eva, *On explicit minimum weight bases for extended cyclic codes related to Gold functions*, Des. Codes Cryptography, **86**:11 (2018), 2619–2627. Zbl 1397.94120

[7] I.Yu. Mogilnykh, F.I. Solov'eva, *On bases of BCH codes with designed distance 3 and their extensions*, Probl. Inf. Transm., **56**:4 (2020), 309–316. Zbl 07312359

[8] J. Pernas, J. Pujol, M. Villanueva, *Rank for some families of quaternary Reed-Muller codes*, In: Bras-Amorrs M., (ed) et al., *Applied algebra, algebraic algorithms and error-correcting codes*, AAECC 2009, Lecture Notes in Computer Science, **5527**, Springer, Berlin, 2009, 43–52. Zbl 1273.94383

[9] J. Pernas, J. Pujol, M. Villanueva, *Classification of some families of quaternary Reed-Muller codes*, IEEE Trans. Inf. Theory, **57**:9 (2011), 6043–6051. Zbl 1365.94611

[10] J. Pujol, J. Rifà, F.I. Solov'eva, *Quaternary Plotkin constructions and quaternary Reed-Muller codes*, Lecture Notes in Computer Science, **4851**, 2007, 148–157. Zbl 1180.94078

- [11] J. Pujol, J. Rifà, F.I. Solov'eva, *Construction of Z_4 -linear Reed-Muller codes*, IEEE Trans. Inf. Theory, **55**:1 (2009), 99–104. Zbl 1367.94378
- [12] F.I. Solov'eva, *On Z_4 -linear codes with parameters of Reed-Muller codes*, Probl. Inf. Transm., **43**:1 (2007), 26–32. Zbl 1237.94137

FAINA IVANOVNA SOLOV'eva
SOBOLEV INSTITUTE OF MATHEMATICS,
4, ACAD. KOPTYUGA AVE.,
NOVOSIBIRSK, 630090, RUSSIA
Email address: sol@math.nsc.ru