SⓔMR

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ
Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru
ISSN 1813-3304

Vol. 20, No. 2, pp. 144–145 (2023) УДК 519.725
https://doi.org/10.33048/semi.2023.20.??? MSC 94B25

SWITCHING METHOD FOR GENERALIZED REED-MULLER CODES

A.M. ROMANOV

Communicated by P.P. Petrov

Abstract: In this paper, we consider some switching transformations of generalized Reed-Muller codes of order $(q-1)m-2$. Using these switching transformations, we prove that for $q \geq 3$, $m \geq 3$, $n = q^m$, and any $t \in \{1, 2, \ldots, m+1\}$, there exist nonlinear 1-quasi-perfect q-ary codes of length n and rank $n - m - 1 + t$. In particular, we prove that for $q \geq 3$, $m \geq 3$, $n = q^m$, there exist nonlinear 1-quasi-perfect q-ary codes of full rank. We also provide a bound on the kernel dimension for some nonlinear 1-quasi-perfect q-ary codes.

Keywords: Galois geometry, generalized Reed–Muller code, quasi-perfect code, nonlinear code, code rank, code kernel, switching.

1 Introduction

Switching is a local transformation of a combinatorial structure that does not change its basic parameters. The transformation is usually carried out using a switching set $\mathcal{S}$, which is replaced by some other set $\mathcal{S}'$. For example:

(1) In the case of error-correcting codes, $\mathcal{S}$ is a subset of the codewords.

(2) In the case of combinatorial designs, $\mathcal{S}$ is a subset of the blocks, and in this case switching is sometimes called trade [1].

Romanov, A.M., Switching method for generalized Reed-Muller codes.

This research was carried out within the State Contract of the Sobolev Institute of Mathematics (FWNF-2022-0017).

Received January, 1, 2023, Published December, 31, 2023.

(3) In the case of strongly regular graphs, $\mathcal{S}$ is a subset of edges together with a subset of non-edges [2, Ch. 7].

Below are some examples of the application of switching transformations in various areas of combinatorics and discrete mathematics.

In 1962, Vasiliev [3] proposed a switching construction of 1-perfect binary codes. He showed that from any 1-perfect binary code $\mathcal{C}$ of length n, using his construction, one can construct $2^{|\mathcal{C}|}$ different 1-perfect binary codes of length $2n+1$. Since $n = 2^m-1$ and $|\mathcal{C}| = 2^{n-m}$, the number of nonequivalent Vasiliev codes grows doubly exponentially. It is known that there are 19 nonequivalent Vasiliev codes (including the Hamming code) of length 15 [4]. The question of the number of nonequivalent Vasiliev codes of length 31 remains open.

Etzion and Vardy [5], based on Vasiliev's ideas, proposed switching transformations of the binary Hamming code and constructively proved the existence of 1-perfect binary codes of full rank. They also showed that no previously known method could construct full-rank 1-perfect binary codes.

Phelps and Villanueva [6], based on the ideas of Etzion and Vardy, proposed a non-constructive version of the switching transformation of Hamming codes defined over an arbitrary finite field $\mathbb{F}_q$. Phelps and Villanueva established that for $m \geq 4$ there exist 1-perfect q-ary codes of length $n = \frac{q^m-1}{q-1}$ and $\operatorname{rank}(\mathcal{C}) = n - m + s$ for any $s \in \{1, \dots, m\}$.

A 2-design (balanced incomplete block design, BIBD) is *quasi-symmetric* with intersection numbers x and y ($x < y$) if any two blocks intersect in either x or y points. The block graph of a quasi-symmetric design, where two blocks are adjacent if they intersect in x points, is strongly regular. There is a close relationship between certain quasi-symmetric designs and codes that meet the Grey-Rankin bound. In [7], Jungnickel and Tonchev used maximal arcs for a switching transformation of quasi-symmetric designs, leading to the construction of new quasi-symmetric designs.

In [8], Crnković and Švob proposed another switching transformation of 2-designs. They showed that this switching transformation can be applied to symmetric designs related to Bush-type Hadamard matrices, and constructed new Bush-type Hadamard matrices of orders 36 and symmetric (100, 45, 20) designs yielding Bush-type Hadamard matrices of order 100.

In [9], Orrick defined several operations that switch substructures of Hadamard matrices, thereby creating new, generally nonequivalent, Hadamard matrices. To illustrate the capabilities of the method, he used them to significantly improve the lower bounds on the number of equivalence classes of Hadamard matrices of orders 32 and 36.

Using switching, Ihringer [10] found 16,565,438 strongly regular graphs with parameters $(81, 30, 9, 12)$, whereas only 15 appear to be described in the literature. The first example of a strongly regular graphs with parameters $(81, 30, 9, 12)$ was constructed by van Lint and Schrijver in [11] as the point graph of a partial geometry.

A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *almost perfect nonlinear* (APN) if the equation

$$f(x+a) + f(x) = b$$

has exactly 0 or 2 solutions for any $b \in \mathbb{F}_{2^n}$ and any nonzero $a \in \mathbb{F}_{2^n}$. APN functions were introduced by Nyberg, who identified them as the mappings with the highest resistance to differential cryptanalysis. Finding new APN functions is an important research topic in cryptography. In [12], Edel and Pott applied the switching construction to known examples of APN functions in low dimensions ($n \leq 9$). In particular, they constructed a new non-quadratic APN function and proved that this new function is not equivalent to power functions and quadratic functions. This is the only known function with such properties.

A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called *planar* if the equation

$$f(x+a) + f(x) = b$$

has exactly 1 solution for any $b \in \mathbb{F}_{p^n}$ and any nonzero $a \in \mathbb{F}_{p^n}$. In [13], Pott and Zhou discuss possible extensions of the switching developed in [12] to the case of planar functions. Pott and Zhou showed that some of the known planar functions can be constructed from each other by switching.

Using switching, Minjia Shi et al. [14] constructed a huge class of MRD codes and showed that the cardinality of this class grows doubly exponentially.

In [14], switching transformations of generalized Reed-Muller codes of order $(q-1)m-2$ are proposed and it is proved that the number of nonequivalent quasi-perfect Reed-Muller-like codes of order $(q-1)m-2$ grows doubly exponentially.

There is a close relationship between 1-perfect codes and Reed-Muller-like codes of order $(q-1)m-2$ (see [16, 17]). There is also a close relationship between extended 1-perfect q-ary codes and Reed-Muller-like codes of order $(q-1)m-2$ (see [18]).

The classification and enumeration of 1-perfect codes over finite fields is a widely open problem in coding theory [19, p. 180].

The generalized Reed-Muller code of order $(q-1)m-2$ is dual to the first-order generalized Reed-Muller code. The study of first-order Reed-Muller codes is of great importance, especially in cryptography.

The question of the rank and dimension of the kernel is natural for nonlinear codes and is related to the classification of codes.

In [20] it is proved that for any $t \in \{1, 2, \ldots, m+1\}$ there exist nonlinear 1-quasi-perfect q-ary codes of length n and rank $n-m-1+t$, where $n = q^m$. Here, $m \geq 5$ for $q = 3$ and 4, $m \geq 4$ for $5 \leq q \leq 19$, and $m \geq 3$ for $q \geq 23$.

In the present paper we consider some switching transformations of generalized Reed-Muller codes of order $(q-1)m-2$. Using these switching transformations we prove that for $q \geq 3$, $m \geq 3$, $n = q^m$, and any $t \in \{1, 2, \ldots, m+1\}$, there exist nonlinear 1-quasi-perfect q-ary codes of length

n and rank $n - m - 1 + t$. We also prove that for $q \geq 3$, $m \geq 3$, $n = q^m$, there exist nonlinear 1-quasi-perfect q-ary codes of full rank.

Furthermore, for $q \geq 3$, $m \geq 3$, $n = q^m$ we prove the existence of nonlinear 1-quasi-perfect q-ary codes of length n with kernel dimension at least $n - [m]_q - q^{m-1}$, where $[m]_q$ is the q-analog of the natural number m. By definition,

$$[m]_q := 1 + q + \cdots + q^{m-1}.$$

2 Preliminaries

In this section we present the definitions and main results that we need in what follows.

Let $\mathbb{F}_q^n$ be a vector space of dimension n over a finite field $\mathbb{F}_q$ of order q, where q is a power of a prime number p. We will consider vectors belonging to $\mathbb{F}_q^n$ as words of length n over the alphabet $\mathbb{F}_q$. For any pair of words $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ in $\mathbb{F}_q^n$, we define the *Hamming distance* $d(\mathbf{x}, \mathbf{y})$. Put

$$d(\mathbf{x}, \mathbf{y}) := |\{i \mid x_i \neq y_i\}|.$$

A *code* $\mathcal{C}$ is just a subset of $\mathbb{F}_q^n$ equipped with the Hamming distance. The words belonging to a code $\mathcal{C}$ will be called *codewords*. A code is said to be linear if it is a *linear* subspace over $\mathbb{F}_q$. Otherwise, a code is said to be *nonlinear*.

The weight of a word $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ is equal to the number of nonzero components in $\mathbf{x}$ and is denoted by $wt(\mathbf{x})$.

A *Hamming sphere* of radius r centered at $\mathbf{x}$ is the set

$$B_r(\mathbf{x}) := \{\mathbf{y} \in \mathbb{F}_q^n \mid d(\mathbf{x}, \mathbf{y}) \leq r\}.$$

The *packing radius* $e(\mathcal{C})$ of a code $\mathcal{C}$ of length n is the maximum number $e \in \{0, 1, \ldots, n\}$ such that

$$B_e(\mathbf{u}) \cap B_e(\mathbf{v}) = \varnothing \quad \text{for all } \mathbf{u}, \mathbf{v} \in \mathcal{C},\ \mathbf{u} \neq \mathbf{v}.$$

The *covering radius* $\rho(\mathcal{C})$ of a code $\mathcal{C}$ of length n is the smallest number $\rho \in \{0, 1, \ldots, n\}$ such that

$$\bigcup_{\mathbf{c} \in \mathcal{C}} B_\rho(\mathbf{c}) = \mathbb{F}_q^n.$$

A code $\mathcal{C}$ is *perfect* if $\rho(\mathcal{C}) = e(\mathcal{C})$, and $\mathcal{C}$ is *quasi-perfect* if $\rho(\mathcal{C}) = e(\mathcal{C}) + 1$. If the packing radius of a perfect (quasi-perfect) code is e, then the code is said to be e-perfect (e-quasi-perfect).

The *minimum distance* of the code $\mathcal{C}$ is

$$d(\mathcal{C}) := \min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\}.$$

We will use the notation $(n, M, d)_q$ for a q-ary code of length n, size M, and minimum distance d. For a linear q-ary code of length n, dimension k and minimum distance d, we will use the notation $[n, k, d]_q$. In the case of binary codes, the index q can be omitted.

The *rank* of a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is the dimension of the subspace spanned by $\mathcal{C}$. We will denote the rank of a code $\mathcal{C}$ by $\operatorname{rank}(\mathcal{C})$. If $\mathcal{C}$ is a linear code of dimension k, then $\operatorname{rank}(\mathcal{C}) = k$. If $\mathcal{C}$ is a nonlinear code of length n and contains q^k codewords, then $k + 1 \le \operatorname{rank}(\mathcal{C}) \le n$. A code $\mathcal{C}$ of length n is called a *full-rank* code if $\operatorname{rank}(\mathcal{C}) = n$.

The *kernel* of a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is the set

$$\ker(\mathcal{C}) := \left\{ \mathbf{x} \in \mathbb{F}_q^n \;\middle|\; \lambda \cdot \mathbf{x} + \mathcal{C} = \mathcal{C} \text{ for any } \lambda \in \mathbb{F}_q \right\}.$$

One can easily see that if the all-zero word belongs to $\mathcal{C}$, then $\ker(\mathcal{C})$ is a linear subcode of $\mathcal{C}$, and $\mathcal{C}$ is the union of cosets of the subspace $\ker(\mathcal{C})$. We will denote the dimension of the kernel of $\mathcal{C}$ by $\dim(\ker(\mathcal{C}))$.

By $AG(m, q)$ we denote the affine space of dimension m over $\mathbb{F}_q$. The vectors of the vector space $\mathbb{F}_q^n$ are points of the affine space $AG(m, q)$. The cosets of k-dimensional linear subspaces of the vector space $\mathbb{F}_q^n$ are k-dimensional affine subspaces of the affine space $AG(m, q)$. Lines are 1-dimensional affine subspaces. For example, the affine plane $AG(2, 3)$ contains 9 points and 12 lines. For more details on finite affine geometry, see, e.g., [21, Ch. 3].

The classical Reed–Muller codes are binary codes [19, Ch. 13]. A generalization of Reed–Muller codes to the q-ary case was proposed by Kasami et al. in [25].

Let $\mathbb{F}_q[X_1, X_2, \dots, X_m]$ be the polynomial algebra in m variables over $\mathbb{F}_q$. For a polynomial $f \in \mathbb{F}_q[X_1, X_2, \dots, X_m]$, we denote its total degree by $\deg(f)$. Let $n = q^m$ and let r be an integer such that $0 \le r \le (q-1)m$. Let the points $P_1, P_2, \dots, P_n$ of the affine space $AG(m, q)$ be ordered in some way. A *generalized Reed–Muller code* of order r over $\mathbb{F}_q$ is the subspace

$$\left\{ (f(P_1), f(P_2), \dots, f(P_n)) \;\middle|\; f \in \mathbb{F}_q[X_1, X_2, \dots, X_m],\ \deg(f) \le r \right\}.$$

The generalized Reed-Muller code $RM_q(r, m)$ of order $r = (q-1)m - 2$ with $q \ge 3$ has parameters $[n = q^m, n - m - 1, 3]_q$ (see [17]). In the binary case, the generalized Reed–Muller code $RM_q(r, m)$ of order $r = (q-1)m-2$ is an extended Hamming code and has parameters $[n = 2^m, n - m - 1, 4]$.

Generalized Reed–Muller codes $RM_q(r, m)$ of order $r = (q-1)m - 2$ are linear 1-quasi-perfect codes [17].

3 Switching of linear codes

In this section, we propose an approach to constructing a switching set for linear codes.

Definition 1. *Let $\mathcal{C}$ be a code with parameters $(n, M, d)_q$. A set $\mathcal{S} \subseteq \mathcal{C}$ is called a* switching set *of $\mathcal{C}$ if there exists a set $\mathcal{S}' \subseteq \mathcal{C}$ different from $\mathcal{S}$ and such that the code $\mathcal{C}' = (\mathcal{C} \setminus \mathcal{S}) \cup \mathcal{S}'$ has parameters that coincide with the parameters of $\mathcal{C}$, that is, $(n, M, d)_q$.*

Let $\mathbf{e}_i$ be a vector of length n, all components of which are equal to zero except for the ith component, which is equal to 1.

Proposition 1. *Let $\mathcal{S} \subseteq \mathcal{C}$, $d(\mathcal{C}) = d$. Suppose that for any codeword $\mathbf{c} \in \mathcal{S}$, all codewords $\mathbf{c}' \in \mathcal{C}$ such that $d(\mathbf{c} + \mathbf{e}_i, \mathbf{c}') = d - 1$ belong to $\mathcal{S}$. Then the set $\mathcal{S}$ is a switching set of $\mathcal{C}$ and $\mathcal{S}' = \mathcal{S} + \mathbf{e}_i$.*

Proof. Let us show that the minimum distance of $\mathcal{C}' = (\mathcal{C} \setminus \mathcal{S}) \cup \mathcal{S}'$ is d. Let $\mathbf{x} \in \mathcal{S}$ and $\mathbf{y} \in \mathcal{C} \setminus \mathcal{S}$. Assume that $d(\mathbf{x} + \mathbf{e}_i, \mathbf{y}) = d - 1$. Then $\mathbf{y} \in \mathcal{S}$. We arrive at a contradiction. Hence, the minimum distance of $\mathcal{C}'$ is d. □

Theorem 1. *Let $i \in \{1, \ldots, n\}$ and $\mathcal{C}$ be a linear code with parameters $[n, k, d]_q$. Let $\mathcal{S}_i$ be a subspace spanned by the set of all codewords of minimum weight that have 1 in the ith coordinate. Then the subspace $\mathcal{S}_i$ is a switching set of $\mathcal{C}$ and $\mathcal{S}'_i = \mathcal{S}_i + \lambda \cdot \mathbf{e}_i$ for any $\lambda \in \mathbb{F}_q \setminus \{0\}$.*

Proof. Let us show that the minimum distance of $\mathcal{C}' = (\mathcal{C} \setminus \mathcal{S}_i) \cup \mathcal{S}'_i$ is d. Let $\mathbf{x} \in \mathcal{S}_i$ and $\mathbf{y} \in \mathcal{C} \setminus \mathcal{S}_i$. Assume that $d(\mathbf{x} + \lambda \cdot \mathbf{e}_i, \mathbf{y}) = d - 1$. Then $d(\lambda \cdot \mathbf{e}_i, \mathbf{y} - \mathbf{x}) = d - 1$. Thus, $(\mathbf{y} - \mathbf{x})$ is a codeword of minimum weight and $(\mathbf{y} - \mathbf{x}) \in \mathcal{S}_i$. Therefore, $\mathbf{y} \in \mathcal{S}_i$. We arrive at a contradiction. Hence, the minimum distance of $\mathcal{C}'$ is d. □

Corollary 1. *Let $\mathbf{x} \in \mathcal{C}$. Then the code*

$$\mathcal{C}' = \mathcal{C} \setminus (\mathcal{S}_i + \mathbf{x}) \cup (\mathcal{S}_i + \mathbf{x} + \lambda \cdot \mathbf{e}_i)$$

has parameters $(n, M = q^k, d)_q$.

4 Switching of generalized Reed-Muller codes

In this section, we describe the switching transformations of the generalized Reed–Muller codes of order $(q-1)m - 2$.

The parity-check matrix H of $RM_q((q-1)m - 2, m)$ is a matrix of size $(m+1) \times q^m$, containing the all-one vector of length $n = q^m$, i.e. a vector all components of which are equal to 1, and containing all transposed vectors from $\mathbb{F}_q^m$ of height m (see [26]). Let

$$H = [\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n],$$

where $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n$ are the columns of H. Let points $P_1, P_2, \ldots, P_n$ of the affine space $AG(m, q)$ correspond to the columns $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n$ of the parity-check matrix H and also correspond to the coordinates $i_1, i_2, \ldots, i_n$ of the vector space $\mathbb{F}_q^n$, and let these correspondences be one-to-one.

The *support* of a nonzero vector $\mathbf{x} = (x_1, \ldots, x_n)$, $x_i \in \mathbb{F}_q$ is the set of indices of its nonzero components: $supp(\mathbf{x}) := \{i \mid x_i \neq 0\}$.

We will call a codeword of weight 3 of the code $RM_q((q-1)m - 2, m)$ a *triple*. Let $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ be a triple, and let $supp(\mathbf{c}) = \{i, j, k\}$. Then

(1) The triple $\mathbf{c}$ lies on a line l if $\{P_i, P_j, P_k\} \subseteq l$;

(2) The corresponding columns $\mathbf{h}_i, \mathbf{h}_j, \mathbf{h}_k$ are linearly dependent, i.e.,

$$c_i\mathbf{h}_i + c_j\mathbf{h}_j + c_k\mathbf{h}_k = \mathbf{0}.$$

Let $i \in \{1, \dots, n\}$. Then by $\mathcal{R}_i$ we denote the subspace spanned by the set of all triples of $RM_q((q-1)m-2, m)$, that have 1 in the ith coordinate. By the definition, the minimum distance of the linear code $\mathcal{R}_i$ is 3.

Proposition 2. *Let $q \geq 3$, $m \geq 1$ and $n = q^m$. Then for any $i \in \{1, 2, \dots, n\}$ the dimension of the linear code $\mathcal{R}_i$ is $n - [m]_q - 1$, where $[m]_q$ is the q-analog of the natural number m.*

Proof. It is known that for $q \geq 3$ every line of the affine space $AG(m, q)$ lies in the code $\mathcal{R}_i$ is $n - [m]_q - 1$ (see [27, 28]). The generalized Reed–Muller code $RM_q((q-1)m-2, m)$ is spanned by codewords of the minimum weight [28, 29]. In the affine space $AG(m, q)$ there are $\frac{n-1}{q-1}$ lines passing through each point, and each line contains q points. For every two distinct points, there exists a unique line passing through them. Thus, for each line, there are $q-2$ linearly independent triples lying on this line. Hence, the number of linearly independent triples spanning $\mathcal{R}_i$ is

$$(q-2)\frac{n-1}{q-1} = n - [m]_q - 1.$$

□

Proposition 2 was first proven in [15], but we provide the proof for the sake of completeness.

Proposition 3. *Let $q \geq 3$, $m \geq 2$, $n = q^m$, $\mathbf{x} \in RM_q((q-1)m-2, m)$. Then for any $i \in \{1, 2, \dots, n\}$ and for any $\lambda \in \mathbb{F}_q \setminus \{0\}$ the set*

$$\mathcal{C}' = \Big(RM_q((q-1)m-2, m) \setminus (\mathcal{R}_i + \mathbf{x})\Big) \cup \Big(\mathcal{R}_i + \mathbf{x} + \lambda \cdot \mathbf{e}_i\Big)$$

is a nonlinear code with parameters $(n, q^{n-m-1}, 3)_q$.

Proof. Clearly, $\mathcal{C}'$ is a nonlinear code. By Corollary 1 the minimum distance of $\mathcal{C}'$ is 3. □

Proposition 4. *Let $q \geq 3$, $m = 2$, $n = q^m$. Then for any $i, j \in \{1, 2, \dots, n\}$, $i \neq j$, we have*

$$dim(\mathcal{R}_i \cap \mathcal{R}_j) \geq q(q-2) - 1.$$

Proof. For $m = 2$ and for any $i, j \in \{1, 2, \dots, n\}$, $i \neq j$, we have the following:

$$\dim(RM_q((q-1)m-2, m)) \geq \dim(\mathcal{R}_i + \mathcal{R}_j),$$

$$\dim(\mathcal{R}_i + \mathcal{R}_j) = \dim(\mathcal{R}_i) + \dim(\mathcal{R}_j) - \dim(\mathcal{R}_i \cap \mathcal{R}_j).$$

The dimension of $RM_q((q-1)m-2, m)$ is known to be $n - m - 1$ (see [22]). By Proposition 2, for $m = 2$ we have

$$\dim(\mathcal{R}_i) = \dim(\mathcal{R}_j) = q(q-1) - 2.$$

Hence, for $m = 2$ and for any $i, j \in \{1, 2, \dots, n\}$, $i \neq j$, we have

$$\dim(\mathcal{R}_i \cap \mathcal{R}_j) \geq q(q-2) - 1.$$

□

Proposition 5. *Let $q \geq 3$, $m \geq 2$, $n = q^m$. Then for any $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, we have*

$$dim(\mathcal{R}_i \cap \mathcal{R}_j) \geq n - [m]_q - q^{m-1}.$$

Proof. Let l_{ij} be a line passing through the points P_i and P_j. For $m = 2$, the line l_{ij} has $q - 2$ linearly independent elements of the basis of the subspace $\mathcal{R}_i \cap \mathcal{R}_j$, and the remaining elements of the basis of $\mathcal{R}_i \cap \mathcal{R}_j$ belong to a plane passing through the line l_{ij}. In the affine space $AG(m, q)$, the number of planes passing through a given line is $\frac{q^{m-1}-1}{q-1}$. By Proposition 4, for $m = 2$ and for any $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, the basis of the subspace $\mathcal{R}_i \cap \mathcal{R}_j$, contains at least $q(q-2) - 1$ linearly independent vectors. Hence, for $m \geq 2$ and for any $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, the basis of $\mathcal{R}_i \cap \mathcal{R}_j$ contains at least

$$\frac{q^{m-1} - 1}{q - 1}\Big(q(q-2) - 1 - (q-2)\Big) + (q-2)$$

elements. Since

$$\frac{q^{m-1} - 1}{q - 1}\Big(q(q-2) - 1 - (q-2)\Big) + (q-2) = n - [m]_q - q^{m-1},$$

for $m \geq 2$ and for any $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, we have

$$\dim(\mathcal{R}_i \cap \mathcal{R}_j) \geq n - [m]_q - q^{m-1}.$$

□

For a given code $RM_q((q-1)m - 2, m)$ and $t = 0, 1, 2$ we define the sets $RM_q^{(t)}((q-1)m - 2, m)$ as

$$RM_q^{(t)}((q-1)m - 2, m) := \big\{\mathbf{x} \in \mathbb{F}_q^n \;\big|\; d\big(\mathbf{x}, RM_q((q-1)m - 2, m)\big) = t\big\}.$$

The sets $RM_q^{(t)}((q-1)m - 2, m)$ are referred to as *subconstituents* of the 1-quasi-perfect code $RM_q((q-1)m - 2, m)$.

Proposition 6. *Let $q \geq 3$, $m \geq 2$. Let $\mathbf{x} \in RM_q^{(2)}((q-1)m - 2, m)$, $wt(\mathbf{x}) = 2$ and $supp(\mathbf{x}) = \{j, k\}$. Let $i \neq j$, $i \neq k$ and let the points P_i, P_j, P_k are collinear. Then there exists a triple $\mathbf{c} \in \mathcal{R}_i$ such that $supp(\mathbf{c}) = \{i, j, k\}$ and $d(\mathbf{c}, \mathbf{x}) = 2$.*

Proof. Consider a codeword

$$\mathbf{x} = (x_1, x_2, \ldots, x_n) \in RM_q^{(2)}((q-1)m - 2, m),$$

where $n = q^m$. Let $wt(\mathbf{x}) = 2$ and $supp(\mathbf{x}) = \{j, k\}$. Then there exist $q - 2$ linearly independent triples lying on the line l, passing through the points P_j and P_k. Let $i \neq j$, $i \neq k$, and let the points P_i, P_j, P_k are collinear. Then the line l contains a triple $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ such that $supp(\mathbf{c}) = \{i, j, k\}$. For some scalar $\mu \in \mathbb{F}_q \setminus \{0\}$, we have either $x_j = \mu \cdot c_j$ or $x_k = \mu \cdot c_k$. Hence, $d(\mathbf{x}, \mu \cdot \mathbf{c}) = 2$. □

By M_i we denote the matrix whose rows correspond to all triples of $RM_q((q-1)m-2,m)$ that have 1 in the ith coordinate, and whose columns correspond to the coordinates of $\mathbb{F}_q^n$. Each row of M_i contains 3 nonzero elements of $\mathbb{F}_q$, and the elements of the ith column of M_i are all equal to 1.

Proposition 7. *Let $q \geq 3$, $m \geq 1$, and $n = q^m$. Any column of M_i other than the ith column contains $q-2$ distinct nonzero elements of $\mathbb{F}_q$ and does not contain -1.*

Proof. Let $j \in \{1, 2, \dots, n\}$ and $j \neq i$. First, we show that any jth column of M_i contains $q-2$ nonzero elements of $\mathbb{F}_q$. Since only one line passes through any two points in $AG(m,q)$, all rows of M_i that have a nonzero element in the jth column are linearly independent. As noted in Proposition 2, all $q-2$ linearly independent triples lying on some line belong to $RM_q((q-1)m-2,m)$. Therefore, any jth column of M_i contains $q-2$ nonzero elements of $\mathbb{F}_q$. Since only one line passes through any two points in $AG(m,q)$, all $q-2$ nonzero elements in any jth column of M_i are different.

Since the parity-check matrix H of $RM_q((q-1)m-2,m)$ contains a row all of whose elements are equal to 1, and each row of M_i contains only 3 nonzero elements, one of which is equal to 1, then any jth column of the matrix M_i does not contain -1. □

Proposition 8. *Let $q \geq 3$, $m \geq 2$. Let $\mathbf{x} \in RM_q^{(2)}((q-1)m-2,m)$, $wt(\mathbf{x}) = 2$ and $supp(\mathbf{x}) = \{j,k\}$. Let $i \neq j$, $i \neq k$ and let the points P_i, P_j, P_k are not collinear. Then for any $\lambda \in \mathbb{F}_q \setminus \{0\}$ there exists a codeword $\mathbf{c} \in \mathcal{R}_i + \lambda \cdot \mathbf{e}_i$ such that $wt(\mathbf{c}) = 4$ and $d(\mathbf{c}, \mathbf{x}) = 2$.*

Proof. By the conditions of Proposition 8, $supp(\mathbf{x})$ belongs to 2 lines passing through the point P_i and passing through the points P_j, P_k. Therefore, by Proposition 7 there exists a codeword $\mathbf{c}' = (c_1', c_2', \dots, c_n') \in \mathcal{R}_i$ such that $wt(\mathbf{c}') = 5$ and $c_i' = -\lambda$, $c_j' = x_j$, $c_k' = x_k$. □

5 Rank and kernel dimension of quasi-perfect Reed-Muller-like codes

In this section we prove the existence of 1-quasi-perfect Reed-Muller-like q-ary codes of various ranks.

Let $t \in \{2, 3, \dots, m+1\}$. We say that the coordinates $i_1, i_2, \dots, i_t$ of the vector space $\mathbb{F}_q^n$ are *independent* if the columns $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_t$ of the parity-check matrix H of $RM_q((q-1)m-2,m)$ that correspond to these coordinates are linearly independent.

Note that any pair of coordinates $i, j \in \{1, 2, \dots, n\}$, $i \neq j$, is independent, since the minimum distance of $RM_q((q-1)m-2,m)$ is 3.

Proposition 9. *Let $q \geq 3$, $m \geq 3$ and $n = q^m$. Let $t \in \{2, 3, \dots, m+1\}$ and $i_1, i_2, \dots, i_t$ be independent coordinates of $\mathbb{F}_q^n$. Then in $RM_q((q-1)m-2,m)$ there exist codewords $\mathbf{x}_{i_1}, \mathbf{x}_{i_2}, \dots, \mathbf{x}_{i_t}$ such that $\mathbf{x}_{i_s} \in RM_q((q-1)m-2,m) \setminus$*

$\mathcal{R}_{i_s}$ for $i_s \in \{i_1, i_2, \dots, i_t\}$ and such that

$$(\mathcal{R}_i + \mathbf{x}_i) \cap (\mathcal{R}_j + \mathbf{x}_j) = \varnothing$$

for any $i, j \in \{i_1, i_2, \dots, i_t\}$, $i \neq j$.

Proof. Since the dimension of $RM_q((q-1)m-2, m)$ is $n-m-1$, and the dimension of $\mathcal{R}_i$ is $n - [m]_q - 1$, then for any $i \in \{1, 2, \dots, n\}$ the subspace $\mathcal{R}_i$ splits $RM_q((q-1)m-2, m)$ into $q^{[m]_q - m}$ cosets. By Proposition 5, for any $i, j \in \{1, 2, \dots, n\}$, $i \neq j$, the dimension of $\mathcal{R}_i \cap \mathcal{R}_j \geq n - [m]_q - q^{m-1}$. Consequently, each element of the partition of $RM_q((q-1)m-2, m)$ into cosets formed by $\mathcal{R}_i$ intersects at most $q^{q^{m-1}-1}$ elements of the partition of $RM_q((q-1)m-2, m)$ into cosets formed by $\mathcal{R}_j$. Since for $m \geq 3$ the relation $q^{m-1} - 1 \ll [m]_q - m$ holds, then for $m \geq 3$ there exist codewords $\mathbf{x}_1, \mathbf{x}_2$ such that $\mathbf{x}_s \in RM_q((q-1)m-2, m) \setminus \mathcal{R}_{i_s}$ for $s \in \{1, 2\}$ and such that

$$(\mathcal{R}_i + \mathbf{x}_1) \cap (\mathcal{R}_j + \mathbf{x}_2) = \varnothing.$$

It is easy to calculate that for $m \geq 3$ we can choose $m+1$ independent coordinates $i_1, i_2, \dots, i_{m+1}$ and $m+1$ codewords $\mathbf{x}_{i_1}, \mathbf{x}_{i_2}, \dots, \mathbf{x}_{i_{m+1}}$ such that $\mathbf{x}_{i_s} \in RM_q((q-1)m-2, m) \setminus \mathcal{R}_{i_s}$ for $i_s \in \{i_1, i_2, \dots, i_t\}$ and such that

$$(\mathcal{R}_i + \mathbf{x}_i) \cap (\mathcal{R}_j + \mathbf{x}_j) = \varnothing$$

for any $i, j \in \{i_1, i_2, \dots, i_t\}$, $i \neq j$. □

Theorem 2. *Let $q \geq 3$, $m \geq 3$ and $n = q^m$. Let $t \in \{1, 2, \dots, m+1\}$ and $i_1, i_2, \dots, i_t$ be independent coordinates of $\mathbb{F}_q^n$. Let the codewords $\mathbf{x}_{i_s} \in RM_q((q-1)m-2, m) \setminus \mathcal{R}_{i_s}$ for $i_s \in \{i_1, i_2, \dots, i_t\}$ be such that*

$$(\mathcal{R}_i + \mathbf{x}_i) \cap (\mathcal{R}_j + \mathbf{x}_j) = \varnothing$$

for any $i, j \in \{i_1, i_2, \dots, i_t\}$, $i \neq j$. Then for any $\lambda_{i_1}, \lambda_{i_2}, \dots, \lambda_{i_t} \in \mathbb{F}_q \setminus \{0\}$ the set

$$\mathcal{C}_t = \Big(RM_q((q-1)m-2, m) \setminus \bigcup_{s=1}^{t} (\mathcal{R}_{i_s} + \mathbf{x}_{i_s})\Big) \cup \Big(\bigcup_{s=1}^{t} (\mathcal{R}_{i_s} + \mathbf{x}_{i_s} + \lambda_{i_s} \cdot \mathbf{e}_{i_s})\Big)$$

is nonlinear 1-quasi-perfect code with parameters $(n, q^{n-m-1}, 3)_q$.

Furthermore,

1. *$rank(\mathcal{C}_t) = n - m - 1 + t$,*
2. *$dim(ker(\mathcal{C}_t)) \geq n - [m]_q - q^{m-1}$ for $t = 2$.*

Proof. Let us show that the code $\mathcal{C}_t$ is a nonlinear 1-quasi-perfect code with parameters $(n, q^{n-m-1}, 3)_q$. It is obvious that the code $\mathcal{C}_t$ is nonlinear. From Proposition 9 and the conditions of the theorem it follows that the number of codewords in $\mathcal{C}_t$ is equal to the number of codewords in $RM_q((q-1)m-2, m)$. Therefore, the number of codewords in $\mathcal{C}_t$ is q^{n-m-1}. From Propositions 3, 9 and the conditions of the theorem it follows that the minimum distance of $\mathcal{C}_t$ is 3.

Let us show that $\rho(\mathcal{C}_t)=2$. Let us assume that $\mathbf{y}\in RM_q^{(2)}((q-1)m-2,m)$. Then there exists a word $\mathbf{c}\in RM_q((q-1)m-2,m)$ such that $d(\mathbf{c},\mathbf{y})=2$. Assume that $\mathbf{c}\in\mathcal{R}_{i_s}+\mathbf{x}_{i_s}$. Since $wt(\mathbf{y}-\mathbf{c})=2$, then let $supp(\mathbf{y}-\mathbf{c})=\{j,k\}$.

Assume that points P_{i_s}, P_j and P_k are collinear. Then:

(1) If $i_s=j$ or $i_s=k$, then it is obvious that there exists a triple $\mathbf{c}'\in\mathcal{R}_{i_s}$ such that $d(\mathbf{y},\mathbf{c}+\mathbf{c}'+\lambda_{i_s}\cdot\mathbf{e}_{i_s})=2$ and $\mathbf{c}+\mathbf{c}'\in\mathcal{R}_{i_s}+\mathbf{x}_{i_s}$.

(2) If $i_s\neq j$ and $i_s\neq k$, then by Proposition 6 there exists a triple $\mathbf{c}'\in\mathcal{R}_{i_s}$ such that $d(\mathbf{y},\mathbf{c}+\mathbf{c}'+\lambda_{i_s}\cdot\mathbf{e}_{i_s})=2$ and $\mathbf{c}+\mathbf{c}'\in\mathcal{R}_{i_s}+\mathbf{x}_{i_s}$.

Assume that points P_{i_s}, P_j and P_k are not collinear. Then, by Proposition 8, there exists a triple $\mathbf{c}'\in\mathcal{R}_{i_s}$ such that $d(\mathbf{y},\mathbf{c}+\mathbf{c}'+\lambda_{i_s}\cdot\mathbf{e}_{i_s})=2$ and $\mathbf{c}+\mathbf{c}'\in\mathcal{R}_{i_s}+\mathbf{x}_{i_s}$.

Now we show that $\operatorname{rank}(\mathcal{C}_t)=n-m-1+t$. It is known that $\operatorname{rank}(\mathcal{C}_1)=n-m$ (see [20]). Assume that $\operatorname{rank}(\mathcal{C}_{t-1})=n-m-1+t-1$. Then

$$\operatorname{rank}\big(\mathcal{C}_{t-1}\setminus(\mathcal{R}_{i_t}+\mathbf{x}_{i_t})\big)=n-m-1+t-1.$$

By the conditions of Theorem 2, coordinates $i_1,i_2,\ldots,i_t$ are independent. Therefore, words from the set $\mathcal{R}_{i_t}+\mathbf{x}_{i_t}+\lambda_{i_t}\cdot\mathbf{e}_{i_t}$ cannot be generated by words from $\mathcal{C}_{t-1}$. Thus, $\operatorname{rank}(\mathcal{C}_t)=n-m-1+t$.

Next we show that for $t=2$ the kernel of the code

$$\mathcal{C}_2=\Big(RM_q((q-1)m-2,m)\setminus\bigcup_{s=1}^{2}(\mathcal{R}_{i_s}+\mathbf{x}_{i_s})\Big)\cup\Big(\bigcup_{s=1}^{2}(\mathcal{R}_{i_s}+\mathbf{x}_{i_s}+\lambda_{i_s}\cdot\mathbf{e}_{i_s})\Big)$$

contains at least $n-[m]_q-q^{m-1}$ linearly independent vectors.

Since by the conditions of Theorem 2 the zero vector belongs to $\mathcal{C}_2$, we have $\ker(\mathcal{C}_2)\subseteq\mathcal{C}_2$. Assume that $\mathbf{y}\in\ker(\mathcal{C}_2)$. Then it is clear that

$$\mathbf{y}\in\Big(RM_q((q-1)m-2,m)\setminus\bigcup_{s=1}^{2}(\mathcal{R}_{i_s}+\mathbf{x}_{i_s})\Big).$$

Hence,

$$(\mathcal{R}_{i_1}+\mathbf{x}_{i_1})+\mathbf{y}\subseteq RM_q((q-1)m-2,m)$$

and

$$(\mathcal{R}_{i_1}+\mathbf{x}_{i_1})+\mathbf{y}+\lambda_{i_1}\cdot\mathbf{e}_{i_1}\subseteq RM_q((q-1)m-2,m)+\lambda_{i_1}\cdot\mathbf{e}_{i_1}.$$

By the assumption, we have $\mathbf{y}\in\ker(\mathcal{C}_2)$. Hence,

$$(\mathcal{R}_{i_1}+\mathbf{x}_{i_1}+\lambda_{i_1}\cdot\mathbf{e}_{i_1})+\mathbf{y}\subseteq\mathcal{C}_2.$$

Since

$$(RM_q((q-1)m-2,m)+\lambda_{i_1}\cdot\mathbf{e}_{i_1})\cap\mathcal{C}_2=\mathcal{R}_{i_1}+\mathbf{x}_{i_1}+\lambda_{i_1}\cdot\mathbf{e}_{i_1},$$

we have

$$(\mathcal{R}_{i_1}+\mathbf{x}_{i_1})+\mathbf{y}+\lambda_{i_1}\cdot\mathbf{e}_{i_1}\subseteq\mathcal{R}_{i_1}+\mathbf{x}_{i_1}+\lambda_{i_1}\cdot\mathbf{e}_{i_1}.$$

Therefore, $\mathbf{y}\in\mathcal{R}_{i_1}$.

On the other hand,

$$(\mathcal{R}_{i_2}+\mathbf{x}_{i_2})+\mathbf{y}\subseteq RM_q((q-1)m-2,m).$$

Thus, $\mathbf{y} \in \mathcal{R}_{i_2}$. By Proposition 5 we have $\mathcal{R}_{i_1} \cap \mathcal{R}_{i_2} \geq n - [m]_q - q^{m-1}$. Therefore, we conclude that

$$\dim(\ker(\mathcal{C}_2)) \geq n - [m]_q - q^{m-1}.$$

□

Corollary 2. *For $q \geq 3$, $m \geq 3$, $n = q^m$ there exist full-rank nonlinear 1-quasi-perfect q-ary codes of length n.*

References

[1] E.J. Billington, *Combinatorial trades: a survey of recent results*, in W.D. Wallis (ed.), *Designs 2002: Further Computational and Constructive Design Theory*, Kluwer, Boston, 2003, 47–67.

[2] Y.J. Ionin, M.S. Shrikhande, *Combinatorics of symmetric designs*, *New Mathematical Monographs*, **5**, Cambridge University Press, Cambridge, 2006.

[3] Yu.L. Vasiliev, *On Nongroup Densely Packed Codes*, Probl. Kibern., **8** (1962), 337—339.

[4] F. Hergert, *The equivalence classes of the Vasil'ev codes of length 15*, in D. Jungnickel, K. Vedder (ed.), *Combinatorial Theory*, Lecture Notes in Math., **969**, Springer-Verlag, Berlin, Heidelberg, 1982, 176–186.

[5] T. Etzion, A. Vardy, *Perfect binary codes: constructions, properties, and enumeration*, IEEE Trans. Inform. Theory, **40**:3 (1994), 754–763.

[6] K.T. Phelps, M. Villanueva, *Ranks of q-ary 1-perfect codes*, Des. Codes Cryptogr., **27**:1-2 (2002), 139–144.

[7] D. Jungnickel, V.D. Tonchev, *Exponential number of quasi-symmetric SDP designs and codes meeting the Grey-Rankin bound*, Des. Codes Cryptogr., **1**:3 (1991), 247–253.

[8] D. Crnković, A. Švob, *Switching for 2-designs*, Des. Codes Cryptogr., **90**:7 (2022), 1585–1593.

[9] W.P. Orrick, *Switching operations for Hadamard matrices*, SIAM J. Discrete Math.,**22** (2008):1, 31–50.

[10] F. Ihringer, *Switching for small strongly regular graphs*, Australas. J. Combin., **84**:1 (2022), 28–48.

[11] J.H. van Lint, A. Schrijver, *Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields*, Combinatorica, **1**:1 (1981), 63–73.

[12] Y. Edel, A. Pott, *A new almost perfect nonlinear function which is not quadratic*, Adv. Math. Commun., **3**:1 (2009), 59–81.

[13] A. Pott, Y. Zhou, *Switching construction of planar functions on finite fields*, in M.A. Hasan, T. Helleseth (eds.), *Arithmetic of Finite Fields*. Lect. Notes Comput. Sci., **6087**, Springer-Verlag, Berlin, Heidelberg, 2010, 135–150.

[14] M. Shi, D.S. Krotov, F. Özbudak, *Constructing MRD codes by switching*, J. Combin. Des., **32**:5 (2024), 219–237.

[15] A.M. Romanov, *On the number of q-ary quasi-perfect codes with covering radius 2*, Des. Codes Cryptogr., **90**:8 (2022), 1713–1719.

[16] A.M. Romanov, *On non-full-rank perfect codes over finite fields*, Des. Codes Cryptogr., **87**:5 (2019), 995–1003.

[17] A.M. Romanov, *Perfect mixed codes from generalized Reed-Muller codes*, Des. Codes Cryptogr., **92**:6 (2024), 1747–1759.

[18] A.M. Romanov, *On the kernels of nonlinear quasi-perfect codes*, Sib. Elektron. Math. Izv., to appear.

[19] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[20] A.M. Romanov, *On nonlinear 1-quasi-perfect codes and their structural properties*, Probl. Inf. Transm. **60**:3 (2024), 141–154.

[21] E.F. Assmus, J.D. Key, *Designs and their codes*, Cambridge University Press, Cambridge, 1992.

[22] A.M. Romanov, *On perfect and Reed–Muller codes over finite fields*, Probl. Inf. Transm. **57**:3 (2021), 199–211.

[23] T. Kasami, S. Lin, W.W. Peterson, *New generalizations of the Reed-Muller codes. Part I: Primitive codes*, IEEE Trans. Inform. Theory, **14**:2 (1968), 189–199.

[24] E.F. Assmus, J.D. Key, *Polynomial codes and finite geometries*, in *Handbook of Coding Theory*, V.S. Pless, W. C. Huffman, R. A. Brualdi, eds., **II**, Elsevier, Amsterdam, 1998, 1269–1344.

[25] T. Kasami, S. Lin, W.W. Peterson, *Polynomial codes*, IEEE Trans. Inform. Theory, **14**:6 (1968), 807–814.

[26] P. Delsarte, J.M. Goethals, F.J. MacWilliams, *On generalized Reed-Muller codes and their relatives*, Inform. Contr., **16**:5 (1970), 403–442.

[27] P. Ding, J.D. Key, *Minimum-weight codewords as generators of generalized Reed-Muller codes*, IEEE Trans. Inform. Theory, **46**:6 (2000), 2152–2158.

Alexander Mikhailovich Romanov
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: rom@math.nsc.ru