Noname manuscript No.
(will be inserted by the editor)

On metric regularity of Reed-Muller codes

Alexey Oblaukhov

Received: date / Accepted: date

Abstract In this work we study metric properties of the well-known family of binary Reed-Muller codes. Let A be an arbitrary subset of the Boolean cube, and $\widehat{A}$ be the metric complement of A — the set of all vectors of the Boolean cube at the maximal possible distance from A. If the metric complement of $\widehat{A}$ coincides with A, then the set A is called a *metrically regular set.* The problem of investigating metrically regular sets appeared when studying *bent functions*, which have important applications in cryptography and coding theory and are also one of the earliest examples of a metrically regular set. In this work we describe metric complements and establish metric regularity of the codes $\mathcal{RM}(0,m)$ and $\mathcal{RM}(k,m)$ for $k \geqslant m-3$. Additionally, metric regularity of the $\mathcal{RM}(1,5)$ code is proved. Combined with previous results by Tokareva N. (2012) concerning duality of affine and bent functions, this proves metric regularity of most Reed-Muller codes with known covering radius. It is conjectured that all Reed-Muller codes are metrically regular.

Keywords metrically regular set · metric complement · covering radius · bent function · Reed-Muller code · deep hole

A. Oblaukhov
Mathematical Center in Akademgorodok,
Sobolev Institute of Mathematics,
Novosibirsk State University,
Laboratory of Cryptography JetBrains Research,
Novosibirsk, Russia
E-mail: oblaukhov@gmail.com

The work was supported by the Russian Foundation for Basic Research (projects no. 18-07-01394, 18-31-00479, 19-31-90093); by the program of basic research of the SB RAS no. I.5.1, project no. 0314-2019-0017; by the Mathematical Center in Akademgorodok, by the Regional Mathematical Center of NSU and by the Laboratory of Cryptography JetBrains Research.

1 Introduction

The problem of investigating and classifying *metrically regular sets* was posed by Tokareva [14, 15] when studying metric properties of *bent functions* [11]. A Boolean function f in even number of variables m is called a *bent function* if it is at the maximal possible distance from the set of affine functions. Thus, the set of bent functions $\mathcal{B}_m$ is the metric complement of the set of affine functions $\mathcal{A}_m$, or, in other words, the metric complement of the Reed-Muller code $\mathcal{RM}(1, m)$. It has been proved by Tokareva [14] that the set of affine functions is, conversely, the metric complement of the set of bent functions. It follows that both of these sets are metrically regular, which establishes metric regularity of the codes $\mathcal{RM}(1, m)$ for even m.

It is straightforward from Neumaier's definition [7] of completely regular codes that they are metrically regular (but the converse is not true). Metric regularity of several classes of *partition set functions* is studied in [13], while the work [4] touches upon metric properties of self-dual bent functions. Metric regularity has been actively investigated by the author: metric complements of linear subspaces of the Boolean cube are studied in the paper [8], while the works [9] and [10] are studying possible sizes of the largest and smallest metrically regular set.

In this work we investigate metric properties of Reed-Muller codes. Among the codes of high order, covering radii of the codes $\mathcal{RM}(k, m)$, for $k \geqslant m - 3$ are known. The covering radius of $\mathcal{RM}(1, m)$ for odd $m > 7$ is unknown, but has been determined for $\mathcal{RM}(1, 5)$ [1] and $\mathcal{RM}(1, 7)$ [6, 3]. In [12], Schatz has found the covering radius of $\mathcal{RM}(2, 6)$, while recently Wang has established the covering radius of $\mathcal{RM}(2, 7)$ [16]. For $m > 9$, the covering radius of $\mathcal{RM}(2, m)$ is still unknown. We prove that the codes $\mathcal{RM}(k, m)$, for $k = 0$ and $k \geqslant m - 3$ and the code $\mathcal{RM}(1, 5)$ are metrically regular and also describe their metric complements.

The paper is structured as follows. After providing necessary definitions and examples, we prove metric regularity of the $\mathcal{RM}(1, 5)$ code. After that we establish metric regularity of Reed-Muller codes of order 0, order $m - 2$ and higher, and then we move onto the codes of order $m - 3$. In order to handle this case, we describe a "syndrome matrices method" of calculating distances from vectors to the punctured $\mathcal{RM}(m-3, m)$ code, based on the "Covering codes" book by Cohen et al [2]. Following the book, we calculate the covering radius of the Reed-Muller code of order $m-3$. Utilizing the method further, we obtain the metric complement of this code. The description of the complement allows us to establish that only the functions from $\mathcal{RM}(m-3, m)$ are contained in the second metric complement, which proves metric regularity of Reed-Muller codes of order $m - 3$. The paper concludes with the overview of the results obtained and a hypothesis regarding metric regularity of all Reed-Muller codes.

2 Definitions and examples

Let $\mathbb{F}_2^n$ be the space of binary vectors of length n with the Hamming metric. The *Hamming distance* $d(\cdot, \cdot)$ between two binary vectors is defined as the number of coordinates in which these vectors differ, while $wt(\cdot)$ denotes the *weight* of a vector, i.e. the number of nonzero values it contains. The plus sign $+$ will denote addition modulo two (componentwise in case of vectors), while the componentwise product of two binary vectors will be denoted as $*$.

Let $X \subseteq \mathbb{F}_2^n$ be an arbitrary set and $y \in \mathbb{F}_2^n$ be an arbitrary vector. The distance from the vector y to the set X is defined as

$$d(y, X) = \min_{x \in X} d(y, x).$$

The *covering radius* of the set X is defined as

$$\rho(X) = \max_{z \in \mathbb{F}_2^n} d(z, X).$$

The set X with $\rho(X) = r$ is also called a *covering code* [2] of radius r.

Consider the set

$$Y = \{y \in \mathbb{F}_2^n | d(y, X) = \rho(X)\}$$

of all vectors at the maximal possible distance from the set X. This set is called the *metric complement* [8] of X and is denoted by $\widehat{X}$. Vectors from the metric complement are sometimes called *deep holes* of a code. If $\widehat{\widehat{X}} = X$ then the set X is said to be *metrically regular* [15].

Note that metrically regular sets always come in pairs, i.e. if A is a metrically regular set, then its metric complement $\widehat{A}$ is also a metrically regular set and both of them have the same covering radius. For some simple examples of metric complements and metrically regular sets, refer to [8–10].

Let $\mathcal{F}^m$ be the set of all Boolean functions in m variables. Reed-Muller code of order k is defined as:

$$\mathcal{RM}(k, m) = \{f \in \mathcal{F}^m : \deg(f) \leqslant k\},$$

where $\deg(\cdot)$ denotes the degree of the *algebraic normal form (ANF)* of the function. These codes may be also represented as sets of *value vectors* of functions. Throughout the paper we will often switch between these two representations. In most cases, m will denote the number of variables, while $n := 2^m$ will denote the dimension of the space of value vectors, which have coordinates numbered from 0 to $2^m - 1$. The i-th coordinate of a value vector is the value of the corresponding function at the binary vector of length m which is a binary representation of the number i. Weights of functions, distances between functions and between a function and a set of functions are defined as distances between their value vectors.

From now on, vectors of length m and square $m \times m$ matrices will be denoted using roman typestyle letters (e.g. x, A), while vectors of length n and vectors derived from them, as well as matrices related to such vectors, will be denoted using bold letters (e.g. $\mathbf{v}, \mathbf{B}$).

Let f and g be two functions in m variables. Denote as $L_{\mathrm{A}}^{\mathrm{b}} : \mathbb{F}_2^m \to \mathbb{F}_2^m$ the affine transformation of the variables with the matrix A and the vector b):

$$(f \circ L_{\mathrm{A}}^{\mathrm{b}})(\mathrm{x}) = f(\mathrm{Ax} + \mathrm{b}).$$

Here $\circ$ denotes the composition of the functions. If the vector b is zero, it will be omitted from the notation. Functions f and g are called *linearly equivalent* if one can be obtained from the other by applying a nonsingular linear transformation to the variables, i.e. $f = g \circ L_{\mathrm{A}}$, where $\det \mathrm{A} \neq 0$.

Extended affine equivalence is more common when classifying boolean functions: functions f and g are called EA-*equivalent* if there exists a nonsingular linear transformation of variables A, a boolean vector b of length m and a function l of degree at most 1 such that $f = g \circ L_{\mathrm{A}}^{\mathrm{b}} + l$.

For our study we will use a variant of these two equivalence relations, which will be referred to as *extended linear equivalence (to the power of k)*. Functions f and g are called EL^k-*equivalent* if there exists a nonsingular binary matrix A and a function c of degree at most k such that

$$f = g \circ L_{\mathrm{A}} + c.$$

It is easy to see that this relation is indeed an equivalence. We will denote this equivalence as $f \overset{k}{\sim} g$.

Reed-Muller code of order k in m variables is usually denoted as $\mathcal{RM}(k, m)$. Since we will refer to these codes regularly, we will instead use $\mathcal{R}_k$ to denote a Reed-Muller code of order k in m variables.

3 Reed-Muller code $\mathcal{RM}(1, 5)$

In the work [1], Berlekamp and Welch presented a partition of all cosets of the $\mathcal{RM}(1, 5)$ code into 48 classes with respect to the EA-equivalence and obtained weight distributions for each class of cosets. Four of these cosets contain only codewords of weight 12 and higher, and those cosets constitute the metric complement of $\mathcal{RM}(1, 5)$. Thus we can present the metric complement of this code as:

$$\widehat{\mathcal{RM}}(1, 5) = \{f : f \overset{\mathrm{EA}}{\sim} g \text{ for some } g \text{ from one of 4 farthest classes}\}$$

Since $\mathcal{RM}(1, 5)$ is linear, it follows [8] that

$$\rho(\widehat{\mathcal{RM}}(1, 5)) = \rho(\mathcal{RM}(1, 5)) = 12$$

and $f \in \widehat{\widehat{\mathcal{RM}}}(1, 5)$ if and only if $f + \widehat{\mathcal{RM}}(1, 5) = \widehat{\mathcal{RM}}(1, 5)$. Thus, in order to establish metric regularity of $\mathcal{RM}(1, 5)$, we must prove that for every $f \notin \mathcal{RM}(1, 5)$ it holds $f + \widehat{\mathcal{RM}}(1, 5) \neq \widehat{\mathcal{RM}}(1, 5)$.

Let $f_c \notin \mathcal{RM}(1, 5)$ be a function from a certain coset equivalence class C. Assume that the function $f_c + g_c$, where $g_c \in \widehat{\mathcal{RM}}(1, 5)$, does not belong to any of the 4 equivalence classes from the complement $\widehat{\mathcal{RM}}(1, 5)$. This implies that $f_c + \widehat{\mathcal{RM}}(1, 5) \neq \widehat{\mathcal{RM}}(1, 5)$ and thus f_c is not in the second metric complement.

Let now $f \notin \mathcal{RM}(1, 5)$ be an arbitrary function from the class C, and let $(\mathrm{A}, \mathrm{b}, l)$ be the matrix, the vector and the affine function such that

$$f \circ L_{\mathrm{A}}^{\mathrm{b}} + l = f_c.$$

Denote

$$g_f = (g_c + l) \circ L_{\mathrm{A}^{-1}}^{\mathrm{A}^{-1}\mathrm{b}}.$$

Then the function $f + g_f$ is EA-equivalent to $f_c + g_c$ and therefore does not belong to $\widehat{\mathcal{RM}}(1, 5)$. Since $g_f \in \widehat{\mathcal{RM}}(1, 5)$, this implies that $f \notin \widehat{\widehat{\mathcal{RM}}}(1, 5)$.

Thus, if we prove that $f+g \notin \widehat{\mathcal{RM}}(1,5)$ for some $f \in C$ and some $g \in \widehat{\mathcal{RM}}(1,5)$, we will prove that no function from the equivalence class C is in the second metric complement.

The list of all representatives of equivalence classes of $\mathcal{RM}(1,5)$ and the proof that none of the classes, except for $\mathcal{RM}(1,5)$ itself, belong to the second metric complement can be found in the Appendix I of the paper under the

Theorem 1 *The code $\mathcal{RM}(1,5)$ is metrically regular.*

4 Reed-Muller codes of orders 0, m, $m-1$ and $m-2$

Reed-Muller codes of orders 0, m and $m-1$ coincide with the repetition code, the whole space and the even weight code respectively. It is trivial that all of them are metrically regular.

The Reed-Muller code of order $m-2$ has covering radius 2 [2]. By definition, it consists of all Boolean functions of degree at most $m-2$. Since all functions of degree m have odd weight, and all functions of smaller degree have even weight, functions of degree m are at distance 1 from $\mathcal{R}_{m-2}$, while functions of degree $m-1$ are at distance 2 and therefore

$$\widehat{\mathcal{R}}_{m-2} = \mathcal{R}_{m-1} \setminus \mathcal{R}_{m-2}.$$

Since $\mathcal{R}_{m-2}$ is linear, $\rho(\widehat{\mathcal{R}}_{m-2}) = \rho(\mathcal{R}_{m-2}) = 2$ and thus functions of degree m are at distance 1 from $\widehat{\mathcal{R}}_{m-2}$. It follows that $\widehat{\widehat{\mathcal{R}}}_{m-2} = \mathcal{R}_{m-2}$ and $\mathcal{R}_{m-2}$ is metrically regular.

5 Reed-Muller codes of order $m-3$: Syndrome method

McLoughlin [5] has proved that

$$\rho(\mathcal{R}_{m-3}) = \begin{cases} m+1, & \text{if } m \text{ is odd,} \\ m+2, & \text{if } m \text{ is even.} \end{cases}$$

We are going to reestablish this result following the "Covering codes" book by Cohen et al, since our new results that follow rely on methods and terminology described in the book. In particular, we will describe the method of obtaining the covering radius of $\mathcal{R}_{m-3}$ using syndrome matrices as it is presented in the book, with few minor adjustments. After that we will proceed to study the metric complement of $\mathcal{R}_{m-3}$. Results in Chapters 5 and 6, as well as general result concerning the covering radius of $\mathcal{R}_{m-3}$, belong to Cohen et al [2], while all subsequent results concerning metric complements and metric regularity of the codes have been obtained by the author.

Let us first consider the covering radius of the punctured Reed-Muller code $\mathcal{R}^{\circ}_{m-3}$, i.e., the code without the 0-th coordinate (which corresponds to the value of the function at zero). Let us denote the parity check matrix of this code as $\mathbf{H}$. The matrix $\mathbf{H}$ coincides with the parity check matrix of the non-punctured code

$\mathcal{R}_{m-3}$, but with the first all-one row and the first column removed. Since $\mathcal{R}_{m-3}$ is dual to the code $\mathcal{R}_2$, the rows of $\mathbf{H}$ are punctured value vectors of the functions

$$x_1, \ldots, x_m, x_1x_2, x_1x_3, \ldots, x_{m-1}x_m.$$

The syndrome $\mathbf{s}$ of an arbitrary vector $\mathbf{v} \in \mathbb{F}_2^{n-1}$ is the product $\mathbf{Hv^T}$. Let us present the syndrome $\mathbf{s}$ as an $m \times m$ symmetric matrix $\mathbf{S}$, where element $s_{i,j}$ of the matrix is equal to the component of the syndrome corresponding to the row x_ix_j of the parity check matrix $\mathbf{H}$. Diagonal element $s_{i,i}$ of this matrix corresponds to the row x_i of the matrix $\mathbf{H}$. Thus we have built a one-to-one correspondence between cosets of $\mathcal{R}_{m-3}^{\circ}$ and syndrome matrices $\mathbf{S}$, i.e., all symmetric binary matrices.

Let $\mathbf{e_1^{\circ}}, \ldots \mathbf{e_m^{\circ}} \in \mathbb{F}_2^{n-1}$ be the punctured value vectors of the functions $x_1, \ldots, x_m$. Notice that the row of $\mathbf{H}$ corresponding to the function x_ix_j is the componentwise product $\mathbf{e_i^{\circ}} * \mathbf{e_j^{\circ}}$.

Consider an $m \times (n-1)$ matrix $\mathbf{B_v}$ which has $\mathbf{e_i^{\circ}} * \mathbf{v}$ as its i-th row. Then the symmetric matrix $\mathbf{S_v} = \mathbf{B_v B_v^T}$ corresponds to the syndrome $\mathbf{Hv^T}$ of the vector $\mathbf{v}$. It is easy to see that if $f_\mathbf{v}$ is a function with the punctured value vector $\mathbf{v}$, then the set of nonzero columns of $\mathbf{B_v}$ is precisely the support of $f_\mathbf{v}$ (bar, possibly, the zero vector). The number of nonzero columns in $\mathbf{B_v}$ is equal to the weight of the vector $\mathbf{v}$.

Given an arbitrary vector $\mathbf{v} \in \mathbb{F}_2^{n-1}$, its distance $d(\mathbf{v}, \mathcal{R}_{m-3}^{\circ})$ from the code is equal to the weight of the coset leader:

$$d(\mathbf{v}, \mathcal{R}_{m-3}^{\circ}) = \min_{\mathbf{u}:\mathbf{Hu^T}=\mathbf{Hv^T}} wt(\mathbf{u}).$$

Using the established correspondences between syndromes and symmetric matrices, we can rewrite this as

$$d(\mathbf{v}, \mathcal{R}_{m-3}^{\circ}) = \min_{\mathbf{u}:\mathbf{B_u B_u^T}=\mathbf{S_v}} Col(\mathbf{B_u}),$$

where $Col(\mathbf{B_u})$ is the number of nonzero columns in the matrix $\mathbf{B_u}$. Let us denote this minimum as $t(\mathbf{S}) := \min_{\mathbf{u}:\mathbf{B_u B_u^T}=\mathbf{S}} Col(\mathbf{B_u})$. Then

$$d(\mathbf{v}, \mathcal{R}_{m-3}^{\circ}) = t(\mathbf{S_v}),$$

and, since the correspondence between all syndromes and all symmetric matrices is one-to-one, we have

$$\rho(\mathcal{R}_{m-3}^{\circ}) = \max_{\mathbf{v}} d(\mathbf{v}, \mathcal{R}_{m-3}^{\circ}) = \max_{\mathbf{S}} t(\mathbf{S}).$$

Moreover, a vector $\mathbf{v}$ is in the metric complement $\widehat{\mathcal{R}}_{m-3}^{\circ}$ if and only if $t(\mathbf{S_v}) = \rho(\mathcal{R}_{m-3}^{\circ})$.

We will call any matrix $\mathbf{B}$ such that $\mathbf{BB^T} = \mathbf{S}$ a *factor* of $\mathbf{S}$. We can thus describe the value $t(\mathbf{S})$ as *the minimum number of nonzero columns in a factor over all factors of* $\mathbf{S}$ *of the form* $\mathbf{B_u}$*, where* $\mathbf{u} \in \mathbb{F}_2^{n-1}$. We will call any factor achieving this minimum a *minimal factor.*

Let us now expand the definition of the value $t(\mathbf{S})$.

Lemma 1 *Let* $\mathbf{S}$ *be a symmetric matrix, and let* $\mathbf{B}$ *be its factor (i.e.* $\mathbf{BB^T} = \mathbf{S}$*). The following operations do not change the property of* $\mathbf{B}$ *being a factor of* $\mathbf{S}$*:*

1. *deleting a zero column;*
2. *deleting two equal columns;*
3. *swapping any two columns;*
4. *adding an arbitrary vector b to each column from some subset of columns of* $\mathbf{B}$ *of even size, given that all columns of this subset sum to zero.*

Proof. Routine, left to the reader. □

Since subsets of nonzero columns of matrices $\{\mathbf{B_u}|\mathbf{u} \in \mathbb{F}_2^{n-1}\}$ are exactly all possible subsets of nonzero columns of length m, and using Lemma 1, we can remove all zero columns from allowed factors and ignore the possibility of duplicate columns and thus reformulate the definition of the value $t(\mathbf{S})$ in the following manner, allowing arbitrary size matrices:

$t(\mathbf{S})$ *is the minimum number of columns in a factor over all factors of* $\mathbf{S}$*. Any factor achieving this minimum is called a minimal factor of* $\mathbf{S}$*.*

Moreover, any factor $\mathbf{B}$ of $\mathbf{S}$ corresponds to exactly one factor of the initial form $\mathbf{B_u}$ — the factor with the set of nonzero columns coinciding with the set of nonzero columns of $\mathbf{B}$. Therefore, presenting a minimal factor for a symmetric matrix $\mathbf{S}$ allows us to obtain a coset leader $\mathbf{u}$ for the coset which this symmetric matrix represents.

6 Reed-Muller codes of order $m-3$: Covering radius

In order to determine the covering radius of $\mathcal{R}^{\circ}_{m-3}$, let us now investigate the maximum value of $t(\mathbf{S})$. Obviously,

$$t(\mathbf{S}) \geqslant \min_{\mathbf{B}:\mathbf{BB^T}=\mathbf{S}} \operatorname{rank}(\mathbf{B}) \geqslant \operatorname{rank}(\mathbf{S})$$

for any matrix $\mathbf{S}$, and therefore

$$\max_{\mathbf{S}} t(\mathbf{S}) \geqslant m.$$

Notice that, if $\mathbf{S} = \mathbf{BB^T}$, then the vector consisting of all diagonal entries of the matrix $\mathbf{S}$ is the sum of all columns of $\mathbf{B}$. Assume that the matrix $\mathbf{S}$ is nonsingular and has an all-zero diagonal. Then all columns of any of its factor $\mathbf{B}$ sum to zero and thus all nonzero columns form a linearly dependent set of vectors. Since $\operatorname{rank}(\mathbf{B}) \geqslant \operatorname{rank}(\mathbf{S}) = m$, this leads to $t(\mathbf{S}) \geqslant m+1$. Note that a matrix $\mathbf{S}$ with such properties exists if and only if m is even (see e.g. [2] p. 249).

Combining these bounds, we obtain

$$\max_{\mathbf{S}} t(\mathbf{S}) \geqslant m + 1 - \pi(m),$$

where $\pi(m)$ is the parity function, equal to 1 for odd m and to 0 for even m.

We will now prove that this bound is tight. The following lemma will help us to characterize minimal factors:

Lemma 2 *Let* $\mathbf{S}$ *be a symmetric matrix, and let* $\mathbf{B}$ *be its minimal factor. Then all proper subsets of columns of* $\mathbf{B}$ *are linearly independent.*

Proof. See Appendix II. □

Assume that for some symmetric matrix $\mathbf{S}$ it holds $t(\mathbf{S}) \geqslant m+2$. This means that any minimal factor $\mathbf{B}$ of $\mathbf{S}$ has at least $m+2$ columns and therefore contains a linearly dependent proper subset of columns, which contradicts Lemma 2. Therefore, $t(\mathbf{S}) \leqslant m+1$ for any matrix $\mathbf{S}$.

7 Reed-Muller codes of order $m-3$: Case m is even

7.1 Covering radius and metric complement of the punctured code

Let the number of variables m be even. Combining the upper and the lower bound obtained in the previous chapter, we get:

$$\rho(\mathcal{R}^{\circ}_{m-3}) = \max_{\mathbf{S}} t(\mathbf{S}) = m+1$$

and a vector $\mathbf{v}$ is in the metric complement of $\mathcal{R}^{\circ}_{m-3}$ if and only if $t(\mathbf{S}_{\mathbf{v}}) = m+1$. The following lemma will help us to characterize the metric complement of $\mathcal{R}^{\circ}_{m-3}$:

Lemma 3 *Let $\mathbf{S}$ be a symmetric $m \times m$ matrix, where m is even. Then $t(\mathbf{S}) = m+1$ if and only if $\mathbf{S} = \mathbf{B}\mathbf{B}^{\mathbf{T}}$ for some $m \times (m+1)$ matrix $\mathbf{B}$ of rank m such that all its columns sum to zero.*

Proof. See Appendix II. □

Clearly, this lemma describes all minimal factors of all matrices $\mathbf{S}$ satisfying $t(\mathbf{S}) = m+1$. Let

$$\begin{aligned}\mathrm{U} = \{\mathbf{u} : \mathbf{B}_{\mathbf{u}} \text{ has } m+1 \text{ nonzero columns, } m \text{ of which are}\\ \text{linearly independent and all of them sum to zero}\}.\end{aligned}$$

It is easy to see that the set of matrices $\{\mathbf{B}_{\mathbf{u}} | \mathbf{u} \in \mathrm{U}\}$ (up to columns permutations and zero columns removal) includes exactly all minimal factors described in the Lemma 3. Thus, if $t(\mathbf{S}) = m+1$ for some matrix $\mathbf{S}$, then there exists a vector $\mathbf{u} \in \mathrm{U}$ such that $\mathbf{S} = \mathbf{B}_{\mathbf{u}}\mathbf{B}_{\mathbf{u}}^{\mathbf{T}}$. Conversely, for any $\mathbf{u} \in \mathrm{U}$ it holds $t(\mathbf{B}_{\mathbf{u}}\mathbf{B}_{\mathbf{u}}^{\mathbf{T}}) = m+1$. Therefore, vectors from the set U cover all cosets contained in the metric complement $\widehat{\mathcal{R}}^{\circ}_{m-3}$:

$$\widehat{\mathcal{R}}^{\circ}_{m-3} = \bigcup_{\mathbf{u} \in \mathrm{U}} \left(\mathbf{u} + \mathcal{R}^{\circ}_{m-3}\right).$$

7.2 Covering radius and metric complement of the non-punctured code

We have obtained the covering radius and described the metric complement of the punctured code. Let us return to the regular, non-punctured Reed-Muller code $\mathcal{R}_{m-3}$. Since it is obtained from the punctured code by adding a parity check bit at 0-th coordinate, the following result will be of use:

Lemma 4 *Let C be a code with the covering radius r and the metric complement $\widehat{C}$. Let C_π be the code obtained from C by adding a parity check bit. Then $\rho(C_\pi) = r+1$ and $\widehat{C}_\pi$ is obtained from $\widehat{C}$ by*

1. *adding a parity check bit to all vectors in case if r is odd or*
2. *adding a reverse parity check bit to all vectors in case if r is even.*

Proof. See Appendix III. □

Using this lemma we can conclude that the covering radius of the non-punctured Reed-Muller code $\mathcal{R}_{m-3}$ is equal to $m+2$ and its metric complement can be described as follows:

$$\widehat{\mathcal{R}}_{m-3} = \bigcup_{\mathbf{u}\in \mathrm{U}} \left((\pi(\mathbf{u}), \mathbf{u}) + \mathcal{R}_{m-3}\right).$$

Recall that, if $f_{\mathbf{v}}$ is the function with the value vector $\mathbf{v}$ (non-punctured), then the set of nonzero columns of the matrix $\mathbf{B}_{\mathbf{v}^\circ}$ coincides with the support of the function $f_{\mathbf{v}}$, bar, possibly, the zero vector. Considering also that all vectors in U have odd weight and added parity check bit corresponds to the value of the function at the all-zero vector, we can rewrite the metric complement of $\mathcal{R}_{m-3}$ in terms of functions instead of their value vectors:

$$\widehat{\mathcal{R}}_{m-3} = \bigcup_{f\in F} \left(f + \mathcal{R}_{m-3}\right),$$

where

$$F = \{f_{(\pi(\mathbf{u}),\mathbf{u})} : \mathbf{u} \in U\} = \{f : \mathrm{supp}(f) = \{0, \mathrm{x}_1, \mathrm{x}_2 \ldots, \mathrm{x}_m, \mathrm{x}_1 + \ldots + \mathrm{x}_m\},$$
$$\{\mathrm{x}_1, \ldots, \mathrm{x}_m\} \text{ are linearly independent}\}.$$

It is easy to see that all functions in F form an equivalence class with respect to linear equivalence. Let us pick any function f^* from this class. We can now say that a function g is in $\widehat{\mathcal{R}}_{m-3}$ if and only if $g = f^* \circ L_{\mathrm{A}} + h$ for some nonsingular matrix A and some function h of degree at most $m-3$.

Recall that functions f and g are EL^k*-equivalent* if there exists a nonsingular binary matrix A and a function h of degree at most k such that $g = f \circ L_{\mathrm{A}} + h$. Therefore, $g \in \widehat{\mathcal{R}}_{m-3}$ if and only if $g \overset{m-3}{\sim} f^*$, where f^* is an arbitrarily chosen representative of the class F. In fact, since all functions in the metric complement are equivalent, we can pick any function from $\widehat{\mathcal{R}}_{m-3}$ as our reference for equivalence (and we will actively change this reference whenever convenient). We will call EL^{m-3}–equivalence just "equivalence" for brevity from now on.

Let us give an explicit (algebraic normal form) description of a certain function from F. Denote as f^* the function with the support $\{0, \mathrm{e}_1, \mathrm{e}_2, \ldots, \mathrm{e}_m, 1\}$, where e_i is the vector with 1 only in the i-th coordinate. Clearly, $f^* \in F$ and it is easy to construct the algebraic normal form of this function: it is the sum of all monomials containing even number of variables, excluding the monomial with all variables included:

$$f^*(\mathrm{x}) = 1 + \sum_{k=1}^{\frac{m}{2}-1} \sum_{1\leqslant i_1<\ldots<i_{2k}\leqslant m} x_{i_1}x_{i_2}\ldots x_{i_{2k}}.$$

This function is equivalent to the sum of all monomials containing $m-2$ variables, so let us use this last function as f^* moving forward. Let $\overline{x_i}$ denote the product of all m variables except x_i, and let $\overline{x_i x_j}$ denote the product of all m variables except x_i and x_j. Using these conventions, we can write this new representative function as follows:

$$f^*(\mathrm{x}) = \sum_{1 \leqslant i < j \leqslant m} \overline{x_i x_j}.$$

7.3 Metric regularity

We have established that

$$\widehat{\mathcal{R}}_{m-3} = \{g : g \overset{m-3}{\sim} f^*\},$$

where f^* is some function from the class F (or from $\widehat{\mathcal{R}}_{m-3}$), and have presented a representative.

Since the code $\mathcal{R}_{m-3}$ is linear, it follows [8] that $\rho(\widehat{\mathcal{R}}_{m-3}) = \rho(\mathcal{R}_{m-3}) = m+2$ and a function f is in $\widehat{\widehat{\mathcal{R}}}_{m-3}$ if and only if $f + \widehat{\mathcal{R}}_{m-3} = \widehat{\mathcal{R}}_{m-3}$. With this in mind, let us prove the metric regularity of $\mathcal{R}_{m-3}$ by proving that no functions other that those contained in $\mathcal{R}_{m-3}$ preserve the metric complement under addition.

Case 1. Let $f \notin \mathcal{R}_{m-3}$ be a function of degree greater than $m-2$. Since EL^{m-3}-equivalence preserves degree of functions with degree higher than $m-3$, any $g \in \widehat{\mathcal{R}}_{m-3}$ has degree $m-2$, while $f+g$ has higher degree and therefore cannot be equivalent to any of the functions from $\widehat{\mathcal{R}}_{m-3}$. Thus, functions of degree greater than $m-2$ do not preserve any function from the metric complement and therefore cannot be in $\widehat{\widehat{\mathcal{R}}}_{m-3}$.

Case 2. Let $f \notin \mathcal{R}_{m-3}$ be a function of degree $m-2$. Let us write it as follows:

$$f(\mathrm{x}) = \sum_{(i,j) \in I} \overline{x_i x_j} + h(\mathrm{x}),$$

where $\deg(h) < m-2$. Denote as $\tilde{f}$ the quadratic function defined by:

$$\tilde{f}(\mathrm{x}) = \sum_{(i,j) \in I} x_i x_j.$$

We will call $\tilde{f}$ the *quadratic dual* of f.

The following result would be of use when handling this case:

Lemma 5 *Let f and g be two function of degree $m-2$. Then $f \overset{m-3}{\sim} g$ if and only if their quadratic duals are* EL^1*-equivalent (*EA*-equivalent).*

Proof. See Appendix III. □

It is known that any quadratic boolean function is EA-equivalent to the function of the form $x_1x_2 + x_3x_4 + \ldots + x_{2k-1}x_{2k}$ for some $k \leqslant \frac{m}{2}$, and any two functions of this form with different number of variables are not EA-equivalent one to the other. Using this result and Lemma 5 we can say that the function f is equivalent to the function p_k for some k $(0 < k \leqslant \frac{m}{2})$, where

$$p_k(\mathrm{x}) = \overline{x_1x_2} + \overline{x_3x_4} + \ldots + \overline{x_{2k-1}x_{2k}} = \sum_{i=1}^{k} \overline{x_{2i-1}x_{2i}}.$$

Let A be the matrix and h be the function of degree at most $m-3$ such that $f \circ L_{\mathrm{A}} + h = p_k$.

Trivially, f^* is equivalent to $p_{\frac{m}{2}}$. Then $f \circ L_{\mathrm{A}} + h + p_{\frac{m}{2}}$ is equivalent to $p_{\frac{m}{2}-k}$, which is (by Lemma 5) not equivalent to $p_{\frac{m}{2}}$ and therefore not equivalent to f^*.

Thus, for an arbitrarily chosen function f of degree $m-2$ we have found a function $g = (h + p_{\frac{m}{2}}) \circ L_{\mathrm{A}^{-1}}$ from the metric complement $\widehat{\mathcal{R}}_{m-3}$ such that $f+g$ is not equivalent to f^*. This means that $f \notin \widehat{\widehat{\mathcal{R}}}_{m-3}$.

Since all functions which are not in $\mathcal{R}_{m-3}$ have degree $m-2$ or higher, we have proven that none of them are in the second metric complement, and therefore $\mathcal{R}_{m-3}$ is metrically regular.

8 Reed-Muller codes of order $m-3$: Case m is odd

8.1 Covering radius and metric complement of the punctured code

Let the number of variables m be odd. Many arguments for this case are similar or identical to the ones for the previous case. The following lemma will be of use:

Lemma 6 *Let* $\mathbf{S}$ *be a symmetric* $m \times m$ *matrix, where* m *is odd. Then* $t(\mathbf{S}) \leqslant m$, *and the equality is achieved if and only if* $\mathbf{S} = \mathbf{B}\mathbf{B}^{\mathbf{T}}$ *for some* $m \times m$ *matrix* $\mathbf{B}$ *which is either nonsingular, or has rank* $m-1$ *and all columns summing to zero.*

Proof. See Appendix II. □

From Lemma 6 we can conclude that, in the case of odd m,

$$\rho(\mathcal{R}^{\circ}_{m-3}) = \max_{\mathbf{S}} t(\mathbf{S}) = m,$$

and a vector $\mathbf{v}$ is in the metric complement of $\mathcal{R}^{\circ}_{m-3}$ if and only if $t(\mathbf{S}_{\mathbf{v}}) = m$.

Lemma 6 also describes all minimal factors of all matrices $\mathbf{S}$ satisfying $t(\mathbf{S}) = m$. Let

$$\mathrm{U}_1 = \{\mathbf{u} : \mathbf{B}_{\mathbf{u}} \text{ has } m \text{ nonzero columns which are linearly independent}\}$$

and

$$\mathrm{U}_2 = \{\mathbf{u} : \mathbf{B}_{\mathbf{u}} \text{ has } m \text{ nonzero columns, } m-1 \text{ of which are}$$
$$\text{linearly independent and the sum of all columns is equal to zero}\}.$$

It is easy to see that the set of matrices $\{\mathbf{B}_{\mathbf{u}} | \mathbf{u} \in \mathrm{U}_1 \cup \mathrm{U}_2\}$ (up to columns permutations and zero columns removal) includes exactly all minimal factors described in the Lemma 6. Thus, if $t(\mathbf{S}) = m$ for some matrix $\mathbf{S}$, then there exists a vector $\mathbf{u} \in \mathrm{U}$ such that $\mathbf{S} = \mathbf{B}_{\mathbf{u}}\mathbf{B}_{\mathbf{u}}^{\mathbf{T}}$. Conversely, for any $\mathbf{u} \in \mathrm{U}$ it holds $t(\mathbf{B}_{\mathbf{u}}\mathbf{B}_{\mathbf{u}}^{\mathbf{T}}) = m$. Therefore, vectors from the set U cover all cosets contained in the metric complement $\widehat{\mathcal{R}}^{\circ}_{m-3}$:

$$\widehat{\mathcal{R}}^{\circ}_{m-3} = \bigcup_{\mathbf{u} \in \mathrm{U}_1 \cup \mathrm{U}_2} \mathbf{u} + \mathcal{R}^{\circ}_{m-3}.$$

8.2 Covering radius and metric complement of the non-punctured code

We have obtained the covering radius and described the metric complement of the punctured code. Let us return to the regular, non-punctured Reed-Muller code $\mathcal{R}_{m-3}$. Since it is obtained from punctured code by adding a parity check bit, using Lemma 4 we can conclude that the covering radius of $\mathcal{R}_{m-3}$ is equal to $m+1$, and its metric complement is

$$\widehat{\mathcal{R}}_{m-3} = \bigcup_{\mathbf{u}\in \mathrm{U}_1\cup \mathrm{U}_2} (\pi(\mathbf{u}), \mathbf{u}) + \mathcal{R}_{m-3}.$$

Recall once again that, if $f_{\mathbf{v}}$ is the function with a value vector $\mathbf{v}$ (non-punctured), then the set of nonzero columns of $\mathbf{B}_{\mathbf{v}^\circ}$ coincides with the support of the function $f_{\mathbf{v}}$, bar, possibly, the zero vector. Considering also that all vectors in $\mathrm{U}_1 \cup \mathrm{U}_2$ have odd weight and added parity check bit corresponds to the value of the function at the all-zero vector, we can rewrite the metric complement of $\mathcal{R}_{m-3}$ in terms of functions instead of their value vectors:

$$\widehat{\mathcal{R}}_{m-3} = \bigcup_{f\in F_1\cup F_2} f + \mathcal{R}_{m-3},$$

where

$$\begin{aligned} F_1 &= \{f_{(\pi(\mathbf{u}),\mathbf{u})} : \mathbf{u} \in \mathrm{U}_1\} = \\ &= \{f : \mathrm{supp}(f) = \{0, \mathrm{x}_1, \mathrm{x}_2 \dots, \mathrm{x}_m\}, \{\mathrm{x}_1, \dots, \mathrm{x}_m\} \text{ are linearly independent}\},\end{aligned}$$

and

$$\begin{aligned} F_2 &= \{f_{(\pi(\mathbf{u}),\mathbf{u})} : \mathbf{u} \in \mathrm{U}_2\} = \\ &= \{f : \mathrm{supp}(f) = \{0, \mathrm{x}_1, \mathrm{x}_2 \dots, \mathrm{x}_{m-1}, \mathrm{x}_1 + \dots + \mathrm{x}_{m-1}\}, \\ &\qquad \{\mathrm{x}_1, \dots, \mathrm{x}_{m-1}\} \text{ are linearly independent}\}.\end{aligned}$$

It is easy to see that all functions in F_1 form an equivalence class with respect to linear equivalence, so do functions in F_2. Let us pick any two functions f_1^*, f_2^* from these two classes, one from each class. We can now say that a function g is in $\widehat{\mathcal{R}}_{m-3}$ if and only if $g = f_1^* \circ L_{\mathrm{A}} + h$ or $g = f_2^* \circ L_{\mathrm{A}} + h$ for some nonsingular matrix A and some function h of degree not greater than $m-3$.

Therefore, $g \in \widehat{\mathcal{R}}_{m-3}$ if and only if $g \overset{m-3}{\sim} f_1^*$ or $g \overset{m-3}{\sim} f_2^*$, where f_1^* is an arbitrarily chosen representative of the class F_1 and f_2^* is an arbitrarily chosen representative of the class F_2. In fact, we can pick any function from EL^{m-3}–equivalence class of F_1 and from EL^{m-3}–equivalence class of F_2 respectively as our references of equivalence f_1^* and f_2^*.

Let us give an explicit (algebraic normal form) description of a certain function from F_1. Denote as f_1^* the function with the support $\{0, \mathrm{e}_1, \mathrm{e}_2, \dots, \mathrm{e}_{m-1}, 1\}$. After a bit of calculation one can explicitly describe its ANF:

$$f_1^*(\mathrm{x}) = \overline{x_m} + (1 + x_m)\left(1 + \sum_{k=1}^{\frac{m-3}{2}} \sum_{1\leqslant i_1<\ldots<i_{2k}\leqslant m-1} x_{i_1}x_{i_2}\dots x_{i_{2k}}\right).$$

This function has degree $m-1$ and, omitting terms of degree less than $m-2$, is trivially EL^{m-3}–equivalent to the following function which we will use as f_1^* from now on:

$$f_1^* = \overline{x_m} + x_m f^\star,$$

where $f^\star$, defined by

$$f^\star(x_1, x_2, \ldots, x_{m-1}) = \left(\sum_{1 \leqslant i < j \leqslant m-1} \overline{x_i x_j} \right)$$

is a function of the first $m-1$ variables. Moving on we will denote the $(m-1)$-tuple of the first $m-1$ variables as $\bar{\mathrm{x}}$. We will also denote affine transforms of the first $m-1$ variables as $\bar{L}_{\mathrm{A}}^{\mathrm{b}}$ (with matrix and vector of corresponding sizes).

Let us now give an explicit description of a certain function from F_2. Denote as f_2^* the function with the support $\{0, \mathrm{e}_1, \mathrm{e}_2, \ldots, \mathrm{e}_{m-1}, \sum_{i=1}^{m-1} \mathrm{e}_i\}$. After a bit of calculation one can explicitly describe its ANF:

$$f_2^*(\mathrm{x}) = (1 + x_m) \left(1 + \sum_{k=1}^{\frac{m-3}{2}} \sum_{1 \leqslant i_1 < \ldots < i_{2k} \leqslant m-1} x_{i_1} x_{i_2} \ldots x_{i_{2k}} \right).$$

This function has degree $m-1$ and is trivially EL^{m-3} equivalent to the function $x_m f^\star$, which we will use as f_2^* from now on.

Note that $f_1^* = \overline{x_m} + f_2^*$.

Let us build some alternative representatives of the equivalence classes of F_1 and F_2. The following lemma will be helpful:

Lemma 7 *Let $f = \overline{x_m} + h$, where $\deg(h) \leqslant m-2$. Let A be a nonsingular $m \times m$ matrix. Then $f \circ L_{\mathrm{A}} = \overline{x_m} + h_1$ for some h_1 of degree at most $m-2$ if and only if matrix A has the following form:*

$$\mathrm{A} = \begin{pmatrix} \bar{\mathrm{A}} & 0^{m-1} \\ \mathrm{w} & 1 \end{pmatrix},$$

where 0^{m-1} is an all-zero column of length $m-1$, $\bar{\mathrm{A}}$ is an arbitrary nonsingular $(m-1) \times (m-1)$ matrix and w is an arbitrary row of length $m-1$.

Proof. See Appendix III. □

This lemma shows us that all linear transformations of the described form, and only such transformations among all linear, transform functions of the form $\overline{x_m} + h$ with $\deg(h) < m-1$ into functions of the same form, preserving $\overline{x_m}$ as the only monomial of degree $m-1$.

Let g be an arbitrary function of degree $m-1$ with the highest-degree component of the form $\overline{x_m}$:

$$g = \overline{x_m} + x_m g_1 + g_2,$$

where g_1, g_2 do not depend on x_m and $\deg(g_1) < m-2$, $\deg(g_2) < m-1$. Let us look at the action of a transformation described in the Lemma 7 onto such function

g. Assume that A is a matrix satisfying conditions of Lemma 7. Discarding terms of degree less than $m-2$, we have:

$$g \circ L_{\mathrm{A}} = \overline{x_m} + x_m(g_1 \circ \bar{L}_{\bar{\mathrm{A}}}) + g_3,$$

where g_3 is some function of degree at most $m-2$ which doesn't depend on the variable x_m.

Let us now build alternative representatives for the metric complement of $\mathcal{R}_{m-3}$. Since $\bar{\mathrm{A}}$ can be an arbitrary nonsingular matrix, choosing $\bar{\mathrm{A}}$ so that $f^\star \circ \bar{L}_{\bar{\mathrm{A}}} = p_{\frac{m-1}{2}}$ (Lemma 5) and filling w with zeroes, we can obtain a matrix A such that

$$f^*_{1\mathrm{A}} := f^*_1 \circ L_{\mathrm{A}} = \overline{x_m} + x_m(f^\star \circ \bar{L}_{\bar{\mathrm{A}}}) + h_1 = \overline{x_m} + x_m p_{\frac{m-1}{2}} + h_1.$$

Here $p_{\frac{m-1}{2}}, h_1$ do not depend on x_m and h_1 has degree at most $m-2$. Additionally,

$$f^*_{2\mathrm{A}} := f^*_2 \circ L_{\mathrm{A}} = x_m(f^\star \circ \bar{L}_{\bar{\mathrm{A}}}) = x_m p_{\frac{m-1}{2}}.$$

We will use these equivalent functions $f^*_{1\mathrm{A}}$ and $f^*_{2\mathrm{A}}$ as class representatives in some cases.

8.3 **Metric regularity**

We have established that

$$\widehat{\mathcal{R}}_{m-3} = \{g : g \overset{m-3}{\sim} f^*_1\} \cup \{g : g \overset{m-3}{\sim} f^*_2\},$$

where f^*_1 is a representative of an EL^{m-3}–equivalence class of F_1 and f^*_2 is a representative of an EL^{m-3}–equivalence class of F_2, and have presented some variants of these representatives.

Since the code $\mathcal{R}_{m-3}$ is linear, it follows [8] that $\rho(\widehat{\mathcal{R}}_{m-3}) = \rho(\mathcal{R}_{m-3}) = m+2$ and function f is in $\widehat{\widehat{\mathcal{R}}}_{m-3}$ if and only if $f + \widehat{\mathcal{R}}_{m-3} = \widehat{\mathcal{R}}_{m-3}$. With this in mind, let us prove the metric regularity of $\mathcal{R}_{m-3}$ by proving that no functions other that those contained in $\mathcal{R}_{m-3}$ preserve the metric complement under addition.

Case 1. Let $f \notin \mathcal{R}_{m-3}$ be a function of degree greater than $m-1$. Since EL^{m-3}–equivalence preserves degree of functions with degree higher than $m-3$, any $g \in \widehat{\mathcal{R}}_{m-3}$ has degree $m-2$ or $m-1$, while $f+g$ has higher degree and therefore cannot be equivalent to any of the functions from $\widehat{\mathcal{R}}_{m-3}$. Thus, functions of degree greater than $m-1$ cannot be in $\widehat{\widehat{\mathcal{R}}}_{m-3}$.

Case 2. Let $f \notin \mathcal{R}_{m-3}$ be a function of degree $m-1$. Any function of degree $m-1$ is trivially EL^{m-3}–equivalent to some function with $\overline{x_m}$ as the only monomial of degree $(m-1)$, so

$$f \circ L_{\mathrm{B}} + h = \overline{x_m} + x_m f_1 + f_2, \tag{1}$$

for some nonsingular B and function h of degree at most $m-3$. Here f_1, f_2 do not depend on x_m, f_1 is either zero or has degree $m-3$, while f_2 is either zero or has degree $m-2$.

Case 2.1. If f_1 in (1) is nonzero, then, using Lemma 7 and Lemma 5, we can pick such a matrix B and function h of degree at most $m-3$ that

$$f \circ L_{\mathrm{B}} + h = \overline{x_m} + x_m p_k + f_3$$

for some $k > 0$ and some f_3 of degree at most $m-2$ (p_k, f_3 do not depend on x_m). If we now sum f and $(f^*_{2\mathrm{A}} + h) \circ L_{\mathrm{B}^{-1}} \in \widehat{\mathcal{R}}_{m-3}$, we obtain a function $f^\dagger$, which is equivalent to:

$$f^\dagger \overset{m-3}{\sim} f^*_{2\mathrm{A}} + f \circ L_{\mathrm{B}} + h = \overline{x_m} + x_m(p_k + p_{\frac{m-1}{2}}) + f_3 \overset{m-3}{\sim} \overline{x_m} + x_m p_{\frac{m-1}{2}-k} + f_4,$$

where f_4 is some function of degree at most $m-2$, not depending on x_m, and the last equivalence is just variable renaming.

Let us denote the function on the right of (1) as $f^{\sim}$. It has degree $m-1$ and therefore cannot be equivalent to f^*_2. It cannot be equivalent to $f^*_{1\mathrm{A}}$ either, because, by Lemma 7, any linear transformation of variables with matrix D preserving $\overline{x_m}$, will act onto it in the following manner:

$$f^{\sim} \circ L_{\mathrm{D}} = \overline{x_m} + x_m(p_{\frac{m-1}{2}-k} \circ \bar{L}_{\bar{\mathrm{D}}}) + f_5,$$

where f_5 is some function of degree at most $m-2$ in the first $m-1$ variables. It is clear that no matrix $\bar{\mathrm{D}}$ can match the $(m-2)$-degree parts of $f^{\sim}$ and $f^*_{1\mathrm{A}}$ containing variable x_m, since $p_{\frac{m-1}{2}-k}$ is not equivalent to $p_{\frac{m-1}{2}}$. Thus, $f^\dagger = f + (f^*_{2\mathrm{A}} + h) \circ L_{\mathrm{B}^{-1}}$ is not in $\widehat{\mathcal{R}}_{m-3}$, and therefore, if f_1 is nonzero, f is not in $\widehat{\widehat{\mathcal{R}}}_{m-3}$.

Case 2.2. If f_1 in (1) is equal to zero, we have a couple more cases to study.

Assume that both f_1 and f_2 are zero and thus

$$f \circ L_{\mathrm{B}} + h = \overline{x_m}.$$

Using transformation $x_1 \to x_1 + x_m$ (and removing terms of degree less than $m-2$), the function $f^*_1 = \overline{x_m} + x_m f^\star$ transforms into $\overline{x_m} + \overline{x_1} + x_m f^\star$.

If we now add f and $(\overline{x_m} + \overline{x_1} + x_m f^\star + h) \circ L_{\mathrm{B}^{-1}} \in \widehat{\mathcal{R}}_{m-3}$ we will obtain a function $f^\dagger$, which is equivalent to:

$$f^\dagger \overset{m-3}{\sim} \overline{x_m} + \overline{x_1} + x_m f^\star + f \circ L_{\mathrm{B}} + h = \overline{x_1} + x_m f^\star.$$

If we swap the variables x_1 and x_m in the right-hand side by another linear transformation and regroup terms, we will obtain the following function:

$$\overline{x_m} + \sum_{2 \leqslant i < j \leqslant m-1} \overline{x_i x_j} + \sum_{i=2}^{m-1} \overline{x_i x_m},$$

which is in turn equivalent to

$$\overline{x_m} + x_m p_{\frac{m-3}{2}} + h^\dagger$$

for some $h^\dagger$ of degree at most $m-2$ in the first $m-1$ variables. By Lemma 7 and Lemma 5, this function cannot be equivalent to $f^*_{1\mathrm{A}}$ and it is not equivalent to f^*_2 by degree comparison. Thus, $f^\dagger = f + (\overline{x_m} + \overline{x_1} + x_m f^\star + h) \circ L^{-1}_{1m}$ is not in $\widehat{\mathcal{R}}_{m-3}$, and therefore f is not in $\widehat{\widehat{\mathcal{R}}}_{m-3}$.

Case 2.3. Assume that f_1 is zero and f_2 is nonzero in (1). Then

$$f \circ L_{\mathrm{B}} + h = \overline{x_m} + f_2.$$

Since f_2 doesn't contain the variable x_m, all terms of f_2 are of the form $\overline{x_i x_m}$ for some i. Without loss of generality (swapping variables among first $m-1$ if needed) we can assume that f_2 contains $\overline{x_{m-1}x_m}$. Renaming variables in $f^*_{2\mathrm{A}}$, we can transform it into:

$$\overline{x_2x_3} + \overline{x_4x_5} + \ldots + \overline{x_{m-1}x_m}.$$

If we now add f and the above function, which belongs to $\widehat{\mathcal{R}}_{m-3}$ we will obtain a function $f^\dagger$, which is equivalent to:

$$f^\dagger \overset{m-3}{\sim} \sum_{k=1}^{\frac{m-1}{2}} \overline{x_{2k}x_{2k+1}} + f \circ L_{\mathrm{B}} + h = \overline{x_m} + \sum_{k=1}^{\frac{m-3}{2}} \overline{x_{2k}x_{2k+1}} + \sum_{i \in I} \overline{x_i x_m}$$

which is equivalent to

$$\overline{x_m} + x_m p_{\frac{m-3}{2}} + h^\dagger$$

for some $h^\dagger$ of degree at most $m-2$ in the first $m-1$ variables. By Lemma 7 and Lemma 5, this function cannot be equivalent to $f^*_{1\mathrm{A}}$ and it is not equivalent to f^*_2 by degree comparison. Thus, $f^\dagger = f + \left(\sum_{k=1}^{\frac{m-1}{2}} \overline{x_{2k}x_{2k+1}} + h \right) \circ L_{\mathrm{B}^{-1}}$ is not in $\widehat{\mathcal{R}}_{m-3}$, and therefore f is not in $\widehat{\widehat{\mathcal{R}}}_{m-3}$.

Case 3. If $f \notin \mathcal{R}_{m-3}$ is a function of degree $m-2$, then, by arguments similar to the case of even m, f is equivalent to p_k (in m variables) for some $k > 0$ using some nonsingular linear transform L and some addition h of degree at most $m-3$. Then

$$f \circ L + h + f^*_{2\mathrm{A}} \overset{m-3}{\sim} p_{\frac{m-1}{2}-k},$$

and therefore $g = h \circ L^{-1} + f^*_{2\mathrm{A}} \circ L^{-1}$ is the function from the metric complement such that $f + g$ is inequivalent to both $f^*_{2\mathrm{A}}$ (because $\frac{m-1}{2} \neq \frac{m-1}{2} - k$) and f^*_1 (by degree comparison).

Since all functions which are not in $\mathcal{R}_{m-3}$ have degree $m-2$ or higher, we have proven that none of them are in the double metric complement, and therefore $\mathcal{R}_{m-3}$ is metrically regular.

9 Conclusion

In this paper we have established metric regularity of the $\mathcal{RM}(1,5)$ code and of the codes $\mathcal{RM}(k,m)$ for $k \geqslant m-3$. Factoring in the result by Tokareva [14], which proves metric regularity of $\mathcal{RM}(1,m)$ for even m, we have covered all infinite families of Reed-Muller codes with known covering radius. The only other Reed-Muller codes with known covering radius, metric regularity of which has not been yet established, are $\mathcal{RM}(1,7)$, $\mathcal{RM}(2,6)$ and $\mathcal{RM}(2,7)$. Given these results, we formulate the following

Conjecture. *All Reed-Muller codes $\mathcal{RM}(k,m)$ are metrically regular.*

References

1. Berlekamp E., Welch L.: Weight distributions of the cosets of the $(32, 6)$ Reed-Muller code. IEEE Transactions on Information Theory. **18**(1), 203–207 (1972).

2. Cohen, G., Honkala, I., Litsyn, S., Lobstein, A.: Covering codes. Elsevier. **54**, (1997).

3. Hou X. D.: Covering Radius of the Reed-Muller code $R(1, 7)$ – A Simpler Proof. Journal of Combinatorial Theory, Series A. **74**(2), 337–341 (1996).

4. Kutsenko, A.: Metrical properties of self-dual bent functions. Designs, Codes and Cryptography (2019). doi:10.1007/s10623-019-00678-x

5. McLoughlin A. M.: The Covering Radius of the $(m - 3)$-rd Order Reed Muller Codes and a Lower Bound on the $(m - 4)$-th Order Reed Muller Codes. SIAM Journal on Applied Mathematics. **37**(2), 419–422 (1979).

6. Mykkeltveit J.: The covering radius of the $(128, 8)$ Reed-Muller code is 56. IEEE Transactions on Information Theory. **26**(3), 359–362 (1980).

7. Neumaier A.: Completely regular codes. Discrete mathematics. **106**, 353–360 (1992).

8. Oblaukhov A. K.: Metric complements to subspaces in the Boolean cube. Journal of Applied and Industrial Mathematics. **10**(3), 397–403 (2016).

9. Oblaukhov A. K.: Maximal metrically regular sets. Siberian Electronic Mathematical Reports. **15**, 1842–1849 (2018).

10. Oblaukhov A.: A lower bound on the size of the largest metrically regular subset of the Boolean cube. Cryptography and Communications. **11**(4), 777–791 (2019).

11. Rothaus O. S.: On “bent” functions. Journal of Combinatorial Theory, Series A. **20**(3), 300–305 (1976).

12. Schatz J.: The second order Reed-Muller code of length 64 has covering radius 18. IEEE Transactions on Information Theory. **27**(4), 529–530 (1981).

13. Stanica P., Sasao T., Butler J. T.: Distance duality on some classes of Boolean functions. Journal of Combinatorial Mathematics and Combinatorial Computing. 2018.

14. Tokareva N.: Duality between bent functions and affine functions. Discrete Mathematics. **312**(3), 666–670 (2012).

15. Tokareva N.: Bent functions: results and applications to cryptography. Academic Press, (2015).

16. Wang Q.: The covering radius of the Reed–Muller code $RM(2, 7)$ is 40. Discrete Mathematics. **342**(12), Article 111625 (2019).

No	Representative f	Added $g \in \widehat{\mathcal{RM}}(1,5)$	$C(g)$	Sum $h = f + g$	$C(h)$
0	0	—	—	—	—
1	2345	123+14+25	22	2345+123+14+25	12
2	2345+14	123+14+25	22	2345+123+25 ∼ 2345+123+34	8
3	2345+24	2345+123+24+35	14	123+35 ∼ 123+14	21
4	2345+24+35	2345+123+24+35	14	123	19
5	2345+14+25	123+14+25	22	2345+123	6
6	2345+123	123+14+25	22	2345+14+25	5
7	2345+123+12	12+34	28	2345+123+34	8
8	2345+123+34	12+34	28	2345+123+12	7
9	2345+123+14	14+25	28	2345+123+25 ∼ 2345+123+34	8
10	2345+123+45	12+45	28	2345+123+12	7
11	2345+123+12+34	12+34	28	2345+123	6
12	2345+123+14+25	123+14+25	22	2345	1
13	2345+123+12+45	12+45	28	2345+123	6
14*	2345+123+24+35	2345+123+24+35	14	0	0
15	2345+123+145	123+14+25	22	2345+145+14+25 ∼ 2345+123+12+34	11
16	2345+123+145+45	123+145+45+24+35	26	2345+24+35	4
17	2345+123+145+24+45	2345+123+24+35	14	145+35+45 ∼ 123+14	21
18	2345+123+145+24+35	2345+123+24+35	14	145 ∼ 123	19
19	123	2345+123+24+35	14	2345+24+35	4
20	123+45	2345+123+24+35	14	2345+24+35+45 ∼ 2345+24+35	4
21	123+14	123+14+25	22	25 ∼ 12	27
22*	123+14+25	123+14+25	22	0	0
23	123+145	123+14+25	22	145+14+25 ∼ 145+25 ∼ 123+14	21
24	123+145+23	23+45	28	123+145+45 ∼ 123+145+23	24
25	123+145+24	123+15+24	22	145+15 ∼ 123	19
26*	123+145+45+24+35	123+145+45+24+35	26	0	0
27	12	12+34	28	34 ∼ 12	27
28*	12+34	12+34	28	0	0

Table 1 Table of even weight cosets of $\mathcal{RM}(1,5)$ [1]. Classes marked with an asterisk are those which constitute $\widehat{\mathcal{RM}}(1,5)$. $C(\cdot)$ denotes the No of the class the function belongs to.

Appendix I: Metric regularity of $\mathcal{RM}(1,5)$

Theorem 1 *The code $\mathcal{RM}(1,5)$ is metrically regular.*

Proof. It is known [1] that the cosets of the $\mathcal{RM}(1,5)$ code can be partitioned into 48 classes with respect to the EA-equivalence. Four of these coset classes contain coset leaders with the largest attainable weight 12 (classes 14, 22, 26 and 28 in the Table 1), which proves

$$\rho(\mathcal{RM}(1,5)) = 12.$$

Since $\rho(\widehat{\mathcal{RM}}(1,5)) = \rho(\mathcal{RM}(1,5)) = 12$, the second metric complement of $\mathcal{RM}(1,5)$ can consist only of the cosets with codewords of even weight. There are 29 classes of such cosets, including the $\mathcal{RM}(1,5)$ code itself; they are listed in the Table 1. Classes marked with an asterisk are those which constitute $\widehat{\mathcal{RM}}(1,5)$. These classes were obtained in the work [1] by Berlekamp and Welch. In this work some of the class representatives were modified from their original variants using simple variable swaps. Functions in the table are presented in an abbreviated notation: the number $i_1 i_2 \dots i_k$ stands for the monomial $x_{i_1} x_{i_2} \dots x_{i_k}$. For example, the representative function for the class 14 is $x_2x_3x_4x_5 + x_1x_2x_3 + x_2x_4 + x_3x_5$.

As has been shown in the Section 3, in order to prove that no codeword from a certain coset class C belongs to the second metric complement $\widehat{\widehat{\mathcal{RM}}}(1,5)$, we must prove that $f + g \notin \widehat{\mathcal{RM}}(1,5)$ for some $f \in C$ and some $g \in \widehat{\mathcal{RM}}(1,5)$. The proof can be found in the Table 1: for a representative f from each even weight coset class we find a function $g \in \widehat{\mathcal{RM}}(1,5)$ such that $f + g$ is equivalent to the representative of some class which is not in $\widehat{\mathcal{RM}}(1,5)$. Thus, the second metric complement $\widehat{\widehat{\mathcal{RM}}}(1,5)$ contains only the code $\mathcal{RM}(1,5)$ itself, proving that $\mathcal{RM}(1,5)$ is metrically regular.

Almost all equivalences presented in the fifth column of the table are variable swaps or additions of the form $x_i \to x_i + 1$, $x_i \to x_i + x_j$ or (for the class 20) $x_i \to x_i + x_j + x_k$.

□

Appendix II: Minimal syndrome matrices

Let us remember Lemma 1, since it is extensively used when proving subsequent lemmas.

Lemma 1 *Let* $\mathbf{S}$ *be a symmetric matrix, and let* $\mathbf{B}$ *be its factor (i.e.* $\mathbf{B}\mathbf{B}^{\mathbf{T}} = \mathbf{S}$*). The following operations do not change the property of* $\mathbf{B}$ *being a factor of* $\mathbf{S}$*:*

1. *deleting a zero column;*
2. *deleting two equal columns;*
3. *swapping any two columns;*
4. *adding an arbitrary vector b to each column from some subset of columns of* $\mathbf{B}$ *of even size, given that all columns of this subset sum to zero.*

Lemma 2 *Let* $\mathbf{S}$ *be a symmetric matrix, and let* $\mathbf{B}$ *be its minimal factor. Then all proper subsets of columns of* $\mathbf{B}$ *are linearly independent.*

Proof. Assume that $\mathbf{B}$ has a proper linearly dependent subset of columns which sum to zero. If this subset has odd number of columns, we make it even by adding a zero vector to it (and to the matrix $\mathbf{B}$).

Let us denote the matrix comprised of the vectors from this subset as $\bar{\mathbf{B}}$. Then, swapping columns if required, the matrix $\mathbf{B}$ can be represented as $\mathbf{B} = (\bar{\mathbf{B}}, \mathbf{D})$, where $\bar{\mathbf{B}}$ has even number of columns summing to zero, while $\mathbf{D}$ is a nonempty matrix, consisting of all remaining columns.

Let $\mathbf{b^1}$ and $\mathbf{d^1}$ be the first (nonzero) columns of $\bar{\mathbf{B}}$ and $\mathbf{D}$ respectively. Let us add the column $\mathbf{b^1} + \mathbf{d^1}$ to all columns of $\bar{\mathbf{B}}$ — we can do that by Lemma 1, without changing the property of $\mathbf{B}$ being a factor of $\mathbf{S}$. Now the first (nonzero) columns of $\bar{\mathbf{B}}$ and $\mathbf{D}$ are equal, and we can delete them by Lemma 1.

Thus, we have added not more that one zero column to the factor $\mathbf{B}$ and then removed two columns from it. This decreases the number of columns in $\mathbf{B}$, which contradicts with its minimality. □

Lemma 3 *Let* $\mathbf{S}$ *be a symmetric $m \times m$ matrix, where m is even. Then* $t(\mathbf{S}) = m + 1$ *if and only if* $\mathbf{S} = \mathbf{B}\mathbf{B}^{\mathbf{T}}$ *for some $m \times (m+1)$ matrix* $\mathbf{B}$ *of rank m such that all its columns sum to zero.*

Proof. $\Longrightarrow$

Assume that $t(\mathbf{S}) = m + 1$, and $\mathbf{B}$ is a minimal factor of $\mathbf{S}$.

If some m-subset of columns of $\mathbf{B}$ is not linearly independent, then, by Lemma 2, $\mathbf{B}$ cannot be a minimal factor of $\mathbf{S}$. Thus, each m-subset of columns of $\mathbf{B}$ is linearly independent and $\mathbf{B}$ has rank m.

Since $\mathbf{B}$ has $m+1$ columns of length m, some subset of them must sum to zero. If all columns of $\mathbf{B}$ do not sum to zero, then it must be a proper subset, which contradicts with the minimality of $\mathbf{B}$ by Lemma 2. Therefore all columns of $\mathbf{B}$ sum to zero.

$\Longleftarrow$

Assume that $\mathbf{S} = \mathbf{B}\mathbf{B}^{\mathbf{T}}$, where $\mathbf{B}$ is a $m \times (m+1)$ matrix of rank m with of all its columns summing to $\mathbf{0}$. It is easy to see that each m-subset of columns of such $\mathbf{B}$ is, in fact, linearly independent. Let us prove that $\mathbf{B}$ is a minimal factor of $\mathbf{S}$.

Assume that $t(\mathbf{S}) = k \leqslant m$ and $\mathbf{D}$ is an arbitrary minimal factor of $\mathbf{S}$ with k columns. Since the sum of all columns of a factor is the vector consisting of the diagonal elements of $\mathbf{S}$, sum of all columns of $\mathbf{D}$ is also equal to zero. This implies that $\mathrm{rank}(\mathbf{D}) < m$, and therefore $\mathrm{rank}(\mathbf{S}) < m$, since $\mathbf{S} = \mathbf{D}\mathbf{D}^{\mathbf{T}}$.

This means that there exists a subset of rows in $\mathbf{S}$ summing to $\mathbf{0}$; we denote these rows as $\mathbf{S}_{\mathbf{i_1}}, \mathbf{S}_{\mathbf{i_2}}, \ldots, \mathbf{S}_{\mathbf{i_p}}$. Since $\mathbf{S}_{\mathbf{i}} = \mathbf{B}_{\mathbf{i}}\mathbf{B}^{\mathbf{T}}$, this implies

$$(\mathbf{B}_{\mathbf{i_1}} + \ldots + \mathbf{B}_{\mathbf{i_p}})\mathbf{B}^{\mathbf{T}} = \mathbf{0}.$$

Denote $\mathbf{b} = \mathbf{B}_{\mathbf{i_1}} + \ldots + \mathbf{B}_{\mathbf{i_p}}$. From the above it follows that the sum of certain columns of $\mathbf{B}$ (in particular, the columns corresponding to 1's in the vector $\mathbf{b}$) is equal to zero.

If the vector $\mathbf{b}$ is zero, then rows of $\mathbf{B}$ are not linearly independent and $\mathrm{rank}(\mathbf{B}) < m$, contradiction.

If it is nonzero and not an all-ones vector, then we obtain a proper subset of columns of $\mathbf{B}$ which sum to 0, contradiction.

If $\mathbf{b}$ is an all-ones vector, then, since m is even, the length of the vector $\mathbf{b}$ is odd and therefore $\mathbf{b}\mathbf{b}^{\mathbf{T}} = 1$, which contradicts with $(\mathbf{B_1} + \ldots + \mathbf{B_k})\mathbf{B}^{\mathbf{T}} = \mathbf{0}$.

Thus, $t(\mathbf{S}) = m+1$ and $\mathbf{B}$ is a minimal factor of $\mathbf{S}$.

□

Proposition 1 *Let* $\mathbf{S}$ *be a symmetric matrix. Then* $t(\mathbf{S}) = m+1$ *if and only if* $\mathrm{rank}(\mathbf{S}) = m$ *and* $\mathbf{S}$ *has an all-zero diagonal.*

Proof. $\Longrightarrow$

Let $\mathbf{S}$ be a symmetric matrix with $t(\mathbf{S}) = m+1$, and let $\mathbf{B}$ be any of its minimal factors. Assume that $\mathrm{rank}(\mathbf{S}) < m$. Then there exists a subset of rows in $\mathbf{S}$ summing to $\mathbf{0}$; we denote these rows as $\mathbf{S}_{\mathbf{i_1}}, \mathbf{S}_{\mathbf{i_2}}, \ldots, \mathbf{S}_{\mathbf{i_p}}$. Since $\mathbf{S}_{\mathbf{i}} = \mathbf{B}_{\mathbf{i}}\mathbf{B}^{\mathbf{T}}$, this implies

$$(\mathbf{B}_{\mathbf{i_1}} + \ldots + \mathbf{B}_{\mathbf{i_p}})\mathbf{B}^{\mathbf{T}} = \mathbf{0}.$$

Denote $\mathbf{b} = \mathbf{B}_{\mathbf{i_1}} + \ldots + \mathbf{B}_{\mathbf{i_p}}$. From the above it follows that the sum of certain columns of $\mathbf{B}$ (in particular, the columns corresponding to ones in the vector $\mathbf{b}$) is equal to zero.

If the vector $\mathbf{b}$ is zero, then $\mathrm{rank}(\mathbf{B}) < m$ and it must have a linearly dependent proper subset of columns, hence $\mathbf{B}$ is not minimal by Lemma 2.

If it is nonzero and not an all-ones vector, then we obtain a proper subset of columns of $\mathbf{B}$ which sum to 0, hence $\mathbf{B}$ is not minimal by Lemma 2.

If $\mathbf{b}$ is an all-ones vector, then all columns of $\mathbf{B}$ sum to zero.

If m is even, then the number of columns in $\mathbf{B}$ is odd and therefore $\mathbf{b}\mathbf{b}^{\mathbf{T}} = 1$, which contradicts with $(\mathbf{B_1} + \ldots + \mathbf{B_k})\mathbf{B}^{\mathbf{T}} = \mathbf{0}$.

If m is odd, then the number of columns in $\mathbf{B}$ is even and all rows have even number of ones, so by Lemma 1, we can add any column of $\mathbf{B}$ to all its columns and then delete a zero column from the result, keeping it a factor of $\mathbf{S}$, which contradicts the minimality of $\mathbf{B}$.

Thus, $\mathrm{rank}(\mathbf{S}) = m$.

Assume that $\mathbf{S}$ has a non-zero diagonal. Since the vector consisting of diagonal elements of $\mathbf{S}$ is the sum of all columns of $\mathbf{B}$, all columns of $\mathbf{B}$ sum to a non-zero vector, which means that $\mathbf{B}$ must have a proper subset of columns summing to $\mathbf{0}$, thus contradicting the minimality of $\mathbf{B}$.

$\Longleftarrow$

Clearly, $t(\mathbf{S}) \geqslant \mathrm{rank}(\mathbf{S}) = m$. Let $\mathbf{B}$ be a minimal factor of $\mathbf{S}$. Trivially, the rank of $\mathbf{B}$ is also equal to m. Since the diagonal of $\mathbf{S}$ is all-zero, all columns of $\mathbf{B}$ sum to zero, hence it cannot have only m columns while having rank m, and must have at least $m + 1$. □

Lemma 6 *Let $\mathbf{S}$ be a symmetric $m \times m$ matrix, where m is odd. Then $t(\mathbf{S}) \leqslant m$, and the equality is achieved if and only if $\mathbf{S} = \mathbf{B}\mathbf{B}^{\mathbf{T}}$ for some $m \times m$ matrix $\mathbf{B}$ which is either nonsingular, or has rank $m - 1$ and all columns summing to zero.*

Proof. As mentioned in the Section 6, $t(\mathbf{S})$ is at most $m + 1$ for any $\mathbf{S}$. Assume that $t(\mathbf{S}) = m + 1$. By Proposition 1, this can only happen if $\mathrm{rank}(\mathbf{S}) = m$ and $\mathbf{S}$ has all-zero diagonal, which is impossible in the case of odd m (see e.g. [2] p. 249). Thus $t(\mathbf{S}) \leqslant m$.

$\Longrightarrow$

Assume that $t(\mathbf{S}) = m$ and let $\mathbf{B}$ be a minimal factor of $\mathbf{S}$ with m columns. If the rank of $\mathbf{B}$ is smaller than $m - 1$, then $\mathbf{B}$ has a proper subset of columns summing to zero, contradicting minimality of $\mathbf{B}$, so the rank of a factor must be at least $m - 1$. If the rank is m, the proof is finished.

Assume that $\mathrm{rank}(\mathbf{B}) = m - 1$. Then some subset of columns of $\mathbf{B}$ must sum to zero. Since $\mathbf{B}$ is minimal, it cannot be a proper subset by Lemma 2, therefore all columns of $\mathbf{B}$ must sum to zero.

$\Longleftarrow$

Clearly, $t(\mathbf{S}) \geqslant \mathrm{rank}(\mathbf{S})$, so if $\mathbf{S} = \mathbf{B}\mathbf{B}^{\mathbf{T}}$ for some nonsingular $m \times m$ matrix $\mathbf{B}$, then the proof is finished.

Let $\mathbf{S} = \mathbf{B}\mathbf{B}^{\mathbf{T}}$ for some $\mathbf{B}$ of rank $m - 1$ with all columns summing to zero.

Assume that $t(\mathbf{S}) = k \leqslant m-1$ and let $\mathbf{D}$ be some minimal factor of $\mathbf{S}$. Note that the sum of all columns of any factor is the vector composed of diagonal elements of $\mathbf{S}$, so the sum of all columns of $\mathbf{D}$ is also zero.

Assume that $k = m - 1$. Then $\mathbf{D}$ has even number of columns, and each row has even number of ones, so we can add an arbitrary vector to all columns of $\mathbf{D}$ while keeping it a factor of $\mathbf{S}$ using Lemma 1. Let us add the first column of $\mathbf{D}$ to all columns of $\mathbf{D}$. Now the first column of $\mathbf{D}$ is zero and we can remove it by Lemma 1. We have now obtained a factor of $\mathbf{S}$ with fewer columns than in $\mathbf{D}$, which contradicts with the minimality of $\mathbf{D}$.

Therefore, k must be at most $m-2$. As mentioned before, the sum of all columns of $\mathbf{D}$ is zero, which means that $\mathbf{D}$ is not a full-rank matrix. Hence $\mathrm{rank}(\mathbf{D})$ is at most $m - 3$, which means that $\mathrm{rank}(\mathbf{S})$ is at most $m - 3$ as well.

Since $\mathbf{S} = \mathbf{B}\mathbf{B}^\mathbf{T}$, by Sylvester's inequality we obtain $\operatorname{rank}(\mathbf{S}) \geqslant \operatorname{rank}(\mathbf{B}) + \operatorname{rank}(\mathbf{B}^\mathbf{T}) - m = m - 2$. But we have just proved that $\operatorname{rank}(\mathbf{S}) \leqslant m - 3$, contradiction. Thus $t(\mathbf{S})$ must be greater than $m - 1$ and is equal to m.

□

Appendix III: Other results

Lemma 4 *Let C be a code with the covering radius r and the metric complement $\widehat{C}$. Let C_π be the code obtained from C by adding a parity check bit. Then $\rho(C_\pi) = r + 1$ and $\widehat{C}_\pi$ is obtained from $\widehat{C}$ by*

1. *adding a parity check bit to all vectors in case if r is odd or*
2. *adding a reverse parity check bit to all vectors in case if r is even.*

Proof. Assume that r is even. Denote

$$C_0 = \{c \in C : wt(c) \text{ is even}\},\ C_1 = \{c \in C : wt(c) \text{ is odd}\},$$

$$\widehat{C}_0 = \{c \in \widehat{C} : wt(c) \text{ is even}\},\ \widehat{C}_1 = \{c \in \widehat{C} : wt(c) \text{ is odd}\}.$$

Due to r being even, vectors from $\widehat{C}_0$ are at distance r from C_0 and at a larger distance from C_1. Similarly, vectors from $\widehat{C}_1$ are at distance r from C_1 and at a larger distance from C_0. Denote

$$C_{\pi,0} = \{(0, c) : c \in C_0\},\ C_{\pi,1} = \{(1, c) : c \in C_1\}.$$

Clearly, $C_\pi = C_{\pi,0} \cup C_{\pi,1}$.

Let $v = (1, c)$, where $c \in \widehat{C}_1$. It is easy to see that $d(v, C_{\pi,1}) = d(c, C_1) = r$. Let $v = (0, c)$, where $c \in \widehat{C}_1$. It follows that $d(v, C_{\pi,1}) = d(c, C_1) + 1 = r + 1$ and $d(v, C_{\pi,0}) = d(c, C_0) \geqslant r + 1$.

Let $v = (0, c)$, where $c \in \widehat{C}_0$. It follows that $d(v, C_{\pi,0}) = d(c, C_0) = r$. Let $v = (1, c)$, where $c \in \widehat{C}_0$. It follows that $d(v, C_{\pi,0}) = d(c, C_0) + 1 = r + 1$ and $d(v, C_{\pi,1}) = d(c, C_1) \geqslant r + 1$.

Let $v = (\epsilon, c)$, where $c \notin \widehat{C}$ and $\epsilon \in \{0, 1\}$. It follows that $d(v, C_\pi) \leqslant d(c, C) + 1 \leqslant r$.

We have examined all possibilities for the vector v and the claim of the Lemma follows from these examinations.

The case of odd r is similar. □

Lemma 5 *Let f and g be two function of degree $m-2$. Then $f \overset{m-3}{\sim} g$ if and only if their quadratic duals are EL^1-equivalent (EA-equivalent).*

Proof. Since EL^{m-3}-equivalence allows us to add functions of degree up to $m-3$, we will assume that both f and g contain only monomials of degree $m - 2$. In what follows we will discard monomials of degree less than $m - 2$ when talking about EL^{m-3}-equivalence, and we will discard monomials of degree less than 2 when talking about EL^1-equivalence.

Let $f(\mathrm{x}) = \sum\limits_{(i,j)\in I} \overline{x_i x_j}$ be the ANF of f. Let us perform the following simple nonsingular linear transformation of variables L_{ij}:

$$L_{ij} : \begin{cases} x_i \to x_i + x_j, & \\ x_k \to x_k & \forall k \neq i. \end{cases}$$

Let us inspect how the function f changes under this transformations (disregarding monomials of degree less than $m-2$):

$$L_{ij} : \begin{cases} \overline{x_i x_k} \to \overline{x_i x_k} & \forall k \neq i, \\ \overline{x_j x_k} \to \overline{x_j x_k} + \overline{x_i x_k} & \forall k \neq i,j, \\ \overline{x_k x_l} \to \overline{x_k x_l} & \forall k,l \neq i,j. \end{cases}$$

Denote the function obtained after this transformation as f_1. Then it is easy to see that the dual $\tilde{f_1}$ is obtained from the dual $\tilde{f}$ (disregarding monomials of degree less than 2 since we consider EL^1-equivalence) by the following linear transformation:

$$\begin{cases} x_j \to x_j + x_i, & \\ x_k \to x_k & \forall k \neq j. \end{cases}$$

which is simply the transposed transformation L_{ji}.

Assume now that g is obtained from f using linear transformation L. Then L can be decomposed into a sequence of simple transformations:

$$L = L_{i_1 j_1} \circ L_{i_2 j_2} \circ \ldots \circ L_{i_s j_s}.$$

From the above we can see that the dual $\tilde{g}$ is obtained from $\tilde{f}$ using the following transformation $\tilde{L}$:

$$\tilde{L} = L_{j_1 i_1} \circ L_{j_2 i_2} \circ \ldots \circ L_{j_s i_s}$$

which is a sequence of transposed simple transformations.

Thus, if $f \overset{m-3}{\sim} g$, then $\tilde{f} \overset{1}{\sim} \tilde{g}$. The reverse can be proven using similar arguments.

□

Lemma 7 *Let $f = \overline{x_m} + h$, where* $\deg(h) \leqslant m-2$. *Let* A *be a nonsingular $m \times m$ matrix. Then $f \circ L_{\mathrm{A}} = \overline{x_m} + h_1$ for some h_1 of degree at most $m-2$ if and only if matrix* A *has the following form:*

$$\mathrm{A} = \begin{pmatrix} \bar{\mathrm{A}} & 0^{m-1} \\ \mathrm{w} & 1 \end{pmatrix},$$

where 0^{m-1} is an all-zero column of length $m-1$, $\bar{\mathrm{A}}$ is an arbitrary nonsingular $(m-1)\times(m-1)$ matrix and w *is an arbitrary row of length $m-1$.*

Proof. $\Longleftarrow$

Trivially, such transformation of the first $m-1$ variables keeps $\overline{x_m}$ in f the only monomial of degree $(m-1)$, and linear transformation cannot increase the degree of h.

$\Longrightarrow$

Assume that $f \circ L_{\mathrm{A}}$ is of the form $\overline{x_m} + h_1$ for some h_1 of degree at most $m-2$, as described in the lemma. This means that the change of variables keeps the monomial $\overline{x_m}$ intact and does not produce any other monomials of degree $m-1$. Clearly, the action of this change on the function h is irrelevant, so let us look at the action on $\overline{x_m}$. It is easy to see that the coefficient of the monomial $\overline{x_i}$ in the resulting function, obtained after applying transformation A to the variables, is precisely the value of a $(m-1) \times (m-1)$ minor, obtained from the matrix A by removing m-th row and i-th column. So we need matrix A to have all such minors be equal to zero, except for the last one, obtained by removing the last column.

Let us denote as $\bar{\mathrm{A}}^1, \bar{\mathrm{A}}^2, \ldots, \bar{\mathrm{A}}^m$ the columns of the matrix A with the last coordinate removed. Denote as $\bar{\mathrm{A}}$ the $(m-1) \times (m-1)$ matrix composed of the first $m-1$ of these columns. Then the condition on the minors can be reformulated as follows: sets of vectors $\{\bar{\mathrm{A}}^1, \ldots, \bar{\mathrm{A}}^{i-1}, \bar{\mathrm{A}}^{i+1}, \ldots, \bar{\mathrm{A}}^m\}$ are linearly dependent for all $i \neq m$, while $\bar{\mathrm{A}}$ is nonsingular. This implies that the following set of equations holds:

$$\begin{cases} \bar{\mathrm{A}}^m + \sum\limits_{j \leqslant m-1} b_{1,j} \bar{\mathrm{A}}^j = 0 \\ \bar{\mathrm{A}}^m + \sum\limits_{j \leqslant m-1} b_{2,j} \bar{\mathrm{A}}^j = 0 \\ \ldots \\ \bar{\mathrm{A}}^m + \sum\limits_{j \leqslant m-1} b_{m-1,j} \bar{\mathrm{A}}^j = 0 \end{cases}$$

where $\mathrm{B} = (b_{i,j})$ is some $(m-1) \times (m-1)$ matrix with $b_{i,i} = 0$ for all i. If we denote rows of the matrix B as B_i, then we can rewrite this in the following manner:

$$\begin{cases} \bar{\mathrm{A}} \cdot \mathrm{B}_1^T = \bar{\mathrm{A}}^m \\ \bar{\mathrm{A}} \cdot \mathrm{B}_2^T = \bar{\mathrm{A}}^m \\ \ldots \\ \bar{\mathrm{A}} \cdot \mathrm{B}_{m-1}^T = \bar{\mathrm{A}}^m \end{cases}$$

Since $\bar{\mathrm{A}}$ is nonsingular, the solution to each equation (which is a system of equations on $b_{i,j}$'s for i-th row) is unique and hence $\mathrm{B}_1 = \mathrm{B}_2 = \ldots = \mathrm{B}_{m-1}$. Since $b_{i,i} = 0$, the matrix B is a zero matrix, which leads to $\bar{\mathrm{A}}^m = 0$. This implies that the last column of A can have 1 only in the last coordinate, and because A is nonsingular, this must be the case. Thus, A is of the form stated in the lemma. □