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 the metric regularity of the codes $\mathcal{RM}(0, m)$ and $\mathcal{RM}(k, m)$ for $k \geqslant m - 3$. Additionally, the metric regularity of the codes $\mathcal{RM}(1, 5)$ and $\mathcal{RM}(2, 6)$ is proved. Combined with previous results by Tokareva N. (2012) concerning duality of affine and bent functions, this establishes the 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
Sobolev Institute of Mathematics,
Novosibirsk, Russia
E-mail: oblaukhov@gmail.com

The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

1 Introduction

The problem of investigating and classifying *metrically regular sets* was posed by Tokareva [20,21] when studying metric properties of *bent functions* [16]. 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.

Bent functions have various applications in cryptography, coding theory and combinatorics. In cryptography, bent functions are valued because of their outstanding nonlinearity, which allows one to construct S-boxes for block ciphers which possess high resistance to the linear cryptanalysis [10]. However, many problems related to bent functions remain unsolved; in particular, the gap between the best known lower and upper bound on the number of bent functions is extremely large; currently known constructions of bent functions are rather scarse (see works [2,3,10,21] for surveys of Boolean/bent functions in cryptography). In 2010 [19], Tokareva has proved that, like bent functions are maximally distant from affine functions, affine functions are at the maximal possible distance from bent functions, thus establishing the *metric regularity* of both sets. This discovery arouses interest in studying the property of metric regularity in order to better understand the structure of the set of bent functions.

From the coding theory standpoint, bent functions form the set of points at the maximal possible distance from the Reed-Muller code of the first order in an even number of variables. Therefore, the aforementioned result by Tokareva establishes the metric regularity of the codes $\mathcal{RM}(1,m)$ for even m. Reed-Muller codes are extensively studied for many years, but their metric properties, like the covering radius, are very elusive and are being discovered to this day; just recently, Wang has found the covering radius of the code $\mathcal{RM}(2,7)$ to be equal to 40 [22]. These problems put Reed-Muller codes in our focus of the research of metric regularity.

Let us briefly overview the results obtained in this area. As mentioned before, Tokareva [19] has established the metric regularity of the sets of affine/bent functions. Metric regularity of several classes of *partition set functions* is studied in [18], while the works [6,7] touch upon metric properties of certain subclasses of 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 [13], while the works [14] and [15] are studying possible sizes of the largest and smallest metrically regular sets.

In this work we investigate the metric regularity of Reed-Muller codes. The problem of finding the covering radius for Reed-Muller codes (which is obviously related to the set of the most distant points and the metric regularity of a code) is a long-standing problem in the theory of covering 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 $\mathcal{RM}(1,7)$ [11,5]. In [17], Schatz has found the covering radius of $\mathcal{RM}(2,6)$, while recently Wang has established the covering radius of $\mathcal{RM}(2,7)$ [22]. For $m > 7$, the covering radius of $\mathcal{RM}(2,m)$ is currently unknown. We prove that the codes $\mathcal{RM}(k,m)$, for $k = 0$ and $k \geqslant m-3$ and the codes $\mathcal{RM}(1,5)$, $\mathcal{RM}(2,6)$ are metrically regular and also describe their metric complements in most cases.

The paper is structured as follows. After providing necessary definitions and examples, we prove the metric regularity of the code $\mathcal{RM}(1,5)$. After that we establish the metric regularity of the 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 the method of "syndrome matrices" of calculating distances from vectors to the punctured $\mathcal{RM}(m-3,m)$ code, based on the "Covering codes" book by Cohen et al., [4]. Following the book, we calculate the covering radius of the Reed-Muller code of order $m-3$, and 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 the metric regularity of the Reed-Muller codes of order $m-3$. We then proceed to establish the metric regularity of the code $\mathcal{RM}(2,6)$, based on the results obtained for the codes $\mathcal{RM}(2,5)$ and $\mathcal{RM}(1,5)$, since the former can be constructed from the latter using the $(\mathbf{u},\mathbf{u}+\mathbf{v})$ construction. The paper concludes with an overview of the results obtained and a hypothesis concerning the 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 $+$ denotes addition modulo two (componentwise in case of vectors), while the componentwise product of two binary vectors is denoted by $*$.

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* [4] 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* [13] of X and is denoted by $\widehat{X}$. Vectors from the metric complement are sometimes called the *deep holes* of a code. If $\widehat{\widehat{X}} = X$ then the set X is said to be *metrically regular* [21].

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 [13–15].

The following trivial auxiliary lemma, established in [13], will be used throughout the paper.

Lemma. *Let $C \subseteq \mathbb{F}_2^n$ be a linear code. Then $\rho(\widehat{C}) = \rho(C)$ and a vector $x \in \mathbb{F}_2^n$ is in $\widehat{\widehat{C}}$ if and only if $x + \widehat{C} = \widehat{C}$.*

Let $\mathcal{F}^m$ be the set of all Boolean functions in m variables. The Reed-Muller code of order k in m variables 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 a function. The Reed-Muller code can be also represented as the set of *value vectors* of the corresponding functions. Throughout the paper we will often switch between these two representations, sometimes "on the fly". 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 the 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.

Throughout the paper, 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 by $L_{\mathrm{A}}^{\mathrm{b}} : \mathbb{F}_2^m \to \mathbb{F}_2^m$ the affine transformation of the variables with the matrix A and the vector b:

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

Here $\circ$ denotes the operation of composition of two 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 binary matrix A, a Boolean vector b of length m and a function h of degree at most 1 such that $f = g \circ L_{\mathrm{A}}^{\mathrm{b}} + h$.

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 h of degree at most k such that

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

It is easy to see that this relation is indeed an equivalence relation. If two functions f and g are EL^k-equivalent, we will denote it by $f \overset{k}{\sim} g$. We will also write $f \overset{k}{=} g$ if f and g differ by a function of degree at most k. Note that the last relation is a subrelation of the EL^k-equivalence.

The Reed-Muller code of order k in m variables is usually denoted by $\mathcal{RM}(k, m)$. Since we will refer to these codes regularly, we will use $\mathcal{R}_{k,m}$ instead. The number of variables will often be omitted from the subscript if it is denoted by m.

No	Representative f	Added $g \in \widehat{\mathcal{R}}_{1,5}$	$C(g)$	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 $\sim$ 2345+123+34	8
3	2345+24	2345+123+24+35	14	123+35 $\sim$ 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 $\sim$ 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
14^1	2345+123+24+35	2345+123+24+35	14	0	0
15	2345+123+145	123+14+25	22	2345+145+14+25 $\sim$ 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 $\sim$ 123+14	21
18	2345+123+145+24+35	2345+123+24+35	14	145 $\sim$ 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 $\sim$ 2345+24+35	4
21	123+14	123+14+25	22	25 $\sim$ 12	27
22^2	123+14+25	123+14+25	22	0	0
23	123+145	123+14+25	22	145+14+25 $\sim$ 145+25 $\sim$ 123+14	21
24	123+145+23	23+45	28	123+145+45 $\sim$ 123+145+23	24
25	123+145+24	123+15+24	22	145+15 $\sim$ 123	19
26^3	123+145+45+24+35	123+145+45+24+35	26	0	0
27	12	12+34	28	34 $\sim$ 12	27
28^4	12+34	12+34	28	0	0

Table 1 Table of even weight coset classes of $\mathcal{R}_{1,5}$. Classes marked with a superscript are the classes which constitute $\widehat{\mathcal{R}}_{1,5}$. $C(\cdot)$ denotes the No of the class the function belongs to. Functions in the table are presented in an abbreviated notation: the number $i_1 i_2 \ldots i_k$ stands for the monomial $x_{i_1} x_{i_2} \ldots x_{i_k}$. For example, the representative function for the class 14 is $x_2x_3x_4x_5 + x_1x_2x_3 + x_2x_4 + x_3x_5$.

3 The Reed-Muller code $\mathcal{R}_{1,5}$

Let us first consider a special case — the code $\mathcal{R}_{1,5}$. This is the set of affine functions, but in 5, hence an odd number of variables, so it is not covered by the result of Tokareva concerning bent functions.

In 1972, Berlekamp and Welch presented a partition of all cosets of the code $\mathcal{R}_{1,5}$ into 48 classes with respect to the EA-equivalence and obtained weight distributions for each class of cosets [1]. The largest minimal weight (and therefore the covering radius of the code) among all classes is equal to 12, and is attained on four coset classes (classes 14, 22, 26 and 28 in Table 1). These four classes constitute the metric complement of $\mathcal{R}_{1,5}$. The following theorem holds.

Theorem 1 *The code $\mathcal{R}_{1,5}$ is metrically regular.*

Proof. Since $\mathcal{R}_{1,5}$ is linear, it follows that $\rho(\widehat{\mathcal{R}}_{1,5}) = \rho(\mathcal{R}_{1,5}) = 12$ and $f \in \widehat{\widehat{\mathcal{R}}}_{1,5}$ if and only if $f + \widehat{\mathcal{R}}_{1,5} = \widehat{\mathcal{R}}_{1,5}$. Thus, in order to establish the metric regularity of $\mathcal{R}_{1,5}$, we have to prove that for every $f \notin \mathcal{R}_{1,5}$ it holds $f + \widehat{\mathcal{R}}_{1,5} \neq \widehat{\mathcal{R}}_{1,5}$.

Since the covering radius of the code is even, the second metric complement of $\mathcal{R}_{1,5}$ can consist only of the cosets with codewords of even weight. There are 29 classes of such cosets, including the $\mathcal{R}_{1,5}$ code itself; they are listed in Table 1. Classes marked with a superscript are those which constitute $\widehat{\mathcal{R}}_{1,5}$. The classification is taken from the paper by Berlekamp and Welch [1], but in this table some of the class representatives were modified from their original variants using simple variable swaps (for the original representatives the reader is referred to Table 5 in the appendix of the paper).

Let us show that only the $\mathcal{R}_{1,5}$ code itself is contained in the second metric complement. Let $f_c \notin \mathcal{R}_{1,5}$ be a function from a certain coset equivalence class C, and assume that the function $f_c + g_c$, where $g_c \in \widehat{\mathcal{R}}_{1,5}$, does not belong to any of the 4 equivalence classes from the complement $\widehat{\mathcal{R}}_{1,5}$. This implies that $f_c + \widehat{\mathcal{R}}_{1,5} \neq \widehat{\mathcal{R}}_{1,5}$ and thus f_c is not in the second metric complement.

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

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

Denote

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

Then the function $f + g_f$ is EA-equivalent to $f_c + g_c$ and therefore does not belong to $\widehat{\mathcal{R}}_{1,5}$. Since $(L_{\mathrm{A}}^{\mathrm{b}})^{-1} = L_{\mathrm{A}^{-1}}^{\mathrm{A}^{-1}\mathrm{b}}$, the function g_f belongs to $\widehat{\mathcal{R}}_{1,5}$ and therefore $f + \widehat{\mathcal{R}}_{1,5} \neq \widehat{\mathcal{R}}_{1,5}$, which implies that $f \notin \widehat{\widehat{\mathcal{R}}}_{1,5}$.

Thus, if $f + g \notin \widehat{\mathcal{R}}_{1,5}$ for some $f \in C$ and some $g \in \widehat{\mathcal{R}}_{1,5}$, then the reasonings above imply that no function from the equivalence class C is in the second metric complement.

We prove this for each class C (see Table 1): for a representative f from each even weight coset class we find a function $g \in \widehat{\mathcal{R}}_{1,5}$ such that $f + g$ is equivalent to the representative of some class which is not in $\widehat{\mathcal{R}}_{1,5}$. Thus, the second metric complement $\widehat{\widehat{\mathcal{R}}}_{1,5}$ contains only the code $\mathcal{R}_{1,5}$ itself, proving that $\mathcal{R}_{1,5}$ is metrically regular.

□

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

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

The 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 covering radius of the Reed-Muller code of order $m - 2$ is equal to 2 [4]. By definition, this code consists of all Boolean functions of degree at most $m - 2$. Since functions of degree m have odd weights, while functions of smaller degree have even weights, 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 The Reed-Muller codes of order $m-3$: Syndrome matrices

In 1979, McLoughlin [9] 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 book "Covering codes" by Cohen et al., since our new results that follow rely on the 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 Section 5 and 6, as well as general results concerning the covering radius of $\mathcal{R}_{m-3}$, belong to Cohen et al. [4], while all subsequent results concerning the metric complement and the metric regularity of the code 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 $\mathbf{H}$ denote the parity check matrix of this code. 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 $\mathcal{R}_2$, we can choose the rows of $\mathbf{H}$ to be the punctured value vectors of the functions

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

The *syndrome* $\mathbf{s}$ of an arbitrary vector $\mathbf{v} \in \mathbb{F}_2^{n-1}$ is the product $\mathbf{H}\mathbf{v}^{\mathbf{T}}$. Let us consider the syndrome $\mathbf{s}$ as an $m \times m$ symmetric matrix $\mathbf{S}$, where the 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 $\mathbf{H}$, while the diagonal element $s_{i,i}$ is equal to the component of the syndrome corresponding to the row x_i of the matrix $\mathbf{H}$. This is a one-to-one correspondence between all cosets of $\mathcal{R}^{\circ}_{m-3}$ and all symmetric binary matrices ("syndrome matrices").

Let $\mathbf{e^{\circ}_1}, \dots \mathbf{e^{\circ}_m} \in \mathbb{F}_2^{n-1}$ be the punctured value vectors of the functions $x_1, \dots, x_m$. Notice that the row of $\mathbf{H}$ corresponding to the function x_ix_j is the componentwise product $\mathbf{e^{\circ}_i} * \mathbf{e^{\circ}_j}$.

Consider an $m \times (n-1)$ matrix $\mathbf{B_v}$ which has $\mathbf{e^{\circ}_i} * \mathbf{v}$ as its i-th row. Then the symmetric matrix $\mathbf{S_v} = \mathbf{B_v}\mathbf{B_v^T}$ corresponds to the syndrome $\mathbf{H}\mathbf{v}^{\mathbf{T}}$ of the vector $\mathbf{v}$. It is easy to see that if f is a function with a punctured value vector equal to $\mathbf{v}$, then the set of nonzero columns of $\mathbf{B_v}$ is precisely the support of the function f (bar, possibly, the all-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 from the code is equal to the weight of the coset leader:

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

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

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

where $Col(\mathbf{B_u})$ is the number of nonzero columns in the matrix $\mathbf{B_u}$. Let us denote the minimum on the right by $t(\mathbf{S}) := \min\limits_{\mathbf{u}:\mathbf{B_u}\mathbf{B_u^T}=\mathbf{S}} Col(\mathbf{B_u})$. Then

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

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

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

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

Let us 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. The proof is routine and is left to the reader. □

Since the subsets of nonzero columns of matrices $\{\mathbf{B_u} : \mathbf{u} \in \mathbb{F}_2^{n-1}\}$ are precisely all possible subsets of nonzero columns of length m, Lemma 1 allows us to remove 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 the use of arbitrarily-sized matrices:

The value $t(\mathbf{S})$ *is equal to 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 any 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 The Reed-Muller codes of order $m-3$: Covering radius

In order to determine the covering radius of $\mathcal{R}^{\circ}_{m-3}$ we will now investigate the maximum possible 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

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

This gives us a trivial lower bound. The following proposition provides a simple upper bound:

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 [4], pp. 249–250.

□

Corollary 1 $t(\mathbf{S}) \leqslant m+1$ *for any symmetric* $m \times m$ *matrix* $\mathbf{S}$.

Proof. 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. □

This bound, combined with the previous one, shows us that the largest value of $t(\mathbf{S})$ is either m or $m+1$. The following result describes the matrices with the larger value of $t(\mathbf{S})$.

Lemma 3 *Let* $\mathbf{S}$ *be a symmetric matrix. Then* $t(\mathbf{S}) = m+1$ *if and only if* $\operatorname{rank}(\mathbf{S}) = m$ *and* $\mathbf{S}$ *has an all-zero diagonal.*

Proof. $\Longleftarrow$

Assume that the matrix $\mathbf{S}$ is nonsingular and has an all-zero diagonal, and let $\mathbf{B}$ be any of its factors. Notice that the vector consisting of all diagonal entries of the matrix $\mathbf{S}$ is the sum of all columns of $\mathbf{B}$. Therefore all columns of $\mathbf{B}$ sum to zero, which means that all its nonzero columns form a linearly dependent set of vectors. Since $\operatorname{rank}(\mathbf{B}) \geqslant \operatorname{rank}(\mathbf{S}) = m$, the matrix $\mathbf{B}$ has at least $m+1$ nonzero columns and therefore $t(\mathbf{S}) = m+1$.

$\Longrightarrow$

Assume that $t(\mathbf{S}) = m+1$. Let $\mathbf{B}$ be a minimal factor of $\mathbf{S}$. Note that all proper subsets of columns of $\mathbf{B}$ are linearly independent by Lemma 2, which implies that all columns of $\mathbf{B}$ sum to zero (since $\mathbf{B}$ is an $m \times (m+1)$ matrix). Since the vector consisting of diagonal elements of $\mathbf{S}$ is the sum of all columns of $\mathbf{B}$, $\mathbf{S}$ has an all-zero diagonal.

Assume that $\operatorname{rank}(\mathbf{S}) < m$. Then there exists a subset of rows in $\mathbf{S}$ summing to $\mathbf{0}$; we denote these rows by $\mathbf{S_{i_1}}, \mathbf{S_{i_2}}, \ldots, \mathbf{S_{i_p}}$. Since $\mathbf{S_i} = \mathbf{B_i}\mathbf{B^T}$, this implies

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

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

If the vector $\mathbf{b}$ is zero, then $\operatorname{rank}(\mathbf{B}) < m$ and it must have a linearly dependent proper subset of columns, which contradicts 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, which contradicts Lemma 2.

Assume that $\mathbf{b}$ is an all-ones vector, and so 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 $\mathbf{b}\mathbf{B}^{\mathbf{T}} = \mathbf{0}$.

If m is odd, then the number of columns in $\mathbf{B}$ is even and all rows have an even number of ones. By Lemma 1, we can add any column of $\mathbf{B}$ to all its columns and then remove a zero column from the resulting matrix, keeping it a factor of $\mathbf{S}$. This contradicts the minimality of $\mathbf{B}$.

Thus, $\operatorname{rank}(\mathbf{S})$ is equal to m.

□

Note that a matrix $\mathbf{S}$ with the properties described in the lemma (nonsingular with an all-zero diagonal) exists if and only if m is even (see e.g. [4], p. 249). This means that

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

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

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

7.1 The covering radius and the metric complement of the punctured code

Let the number of variables m be even. From previous sections we know that:

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

Let us describe the metric complement of the code. A vector $\mathbf{v} \in \mathbb{F}_2^{n-1}$ is in the metric complement of $\mathcal{R}^{\circ}_{m-3}$ if and only if $t(\mathbf{S}_{\mathbf{v}}) = m+1$. The following statements will help us to characterize the syndromes of such vectors:

Lemma 4 *Let $\mathbf{S}$ be a symmetric $m \times m$ matrix, m even. Then $t(\mathbf{S}) = m + 1$ if and only if $\mathbf{S}$ has a factor of rank m with $m + 1$ columns which sum to zero.*

Proof. $\Longrightarrow$

Assume that $t(\mathbf{S}) = m + 1$ and let $\mathbf{B}$ be an arbitrary minimal factor of $\mathbf{S}$. By Proposition 1, $\operatorname{rank}(\mathbf{S}) = m$ and $\mathbf{S}$ has an all-zero diagonal. Therefore, $\operatorname{rank}(\mathbf{B}) = m$ and all its columns sum to zero.

$\Longleftarrow$

Let $\mathbf{B}$ be a factor of $\mathbf{S}$ of rank m with $m + 1$ columns which sum to $\mathbf{0}$.

Assume that $t(\mathbf{S}) = k \leqslant m$ and let $\mathbf{D}$ be 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 $\mathbf{S}$, the sum of all columns of $\mathbf{D}$ is also equal to zero. This implies that $\operatorname{rank}(\mathbf{D}) < m$, and therefore $\operatorname{rank}(\mathbf{S}) < m$.

It is easy to see that each proper subset of columns of $\mathbf{B}$ is linearly independent. Notice that the existence of a factor with this property is shown to contradict with the assumption "$\operatorname{rank}(\mathbf{S}) < m$" in the proof of Proposition 1, and in the case when m is even the proof does not rely on the minimality of $\mathbf{B}$.

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

□

Lemma 4 describes all minimal factors of all matrices $\mathbf{S}$ satisfying $t(\mathbf{S}) = m+1$. Let us construct the following set of vectors:

$$\mathrm{U} = \{\mathbf{u} \in \mathbb{F}_2^{n-1} : \mathbf{B_u} \text{ has } m+1 \text{ nonzero columns, } m \text{ of which are} \\ \text{linearly independent and all of them sum to zero}\}.$$

It is easy to see that the set of matrices $\{\mathbf{B_u} : \mathbf{u} \in \mathrm{U}\}$ (up to columns permutations and zero columns removal) includes exactly all minimal factors described in Lemma 4. Therefore, if $t(\mathbf{S}) = m+1$ for some matrix $\mathbf{S}$, then there exists a vector $\mathbf{u} \in \mathrm{U}$ such that $\mathbf{S} = \mathbf{B_u}\mathbf{B_u^T}$. Conversely, for any $\mathbf{u} \in \mathrm{U}$ it holds $t(\mathbf{B_u}\mathbf{B_u^T}) = m+1$. Thus, the vectors from the set U cover all cosets contained in the metric complement of $\mathcal{R}_{m-3}^{\circ}$:

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

7.2 The covering radius and the 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 the 0-th coordinate, the following result will be of use:

Lemma 5 *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 to all codewords of C (in the front). 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 an inversed parity check bit to all vectors in case if r is even.*

Proof. Obviously, $\rho(C_\pi) \leqslant r+1$.

Let us prove (2). Assume that r is even. Denote

$$C_i = \{c \in C : wt(c) \bmod 2 = i\},\ \widehat{C}_i = \{c \in \widehat{C} : wt(c) \bmod 2 = i\},\ i = 0,1.$$

Since r is 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.

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

Let $c \in \widehat{C}_1$. Then $d((1,c), C_\pi) = \min(d(c, C_1), d(c, C_0)+1) = r$, while $d((0,c), C_\pi) = \min(d(c, C_1)+1, d(c, C_0)) > r$.

Let $c \in \widehat{C}_0$. Similarly, $d((1,c), C_\pi) = \min(d(c, C_1), d(c, C_0)+1) > r$, while $d((0,c), C_\pi) = \min(d(c, C_1)+1, d(c, C_0)) = r$.

Therefore, the vectors $\{(1,c) | c \in \widehat{C}_0\} \cup \{(0,c) | c \in \widehat{C}_1\}$ are the only ones at a distance larger than r from C_π, and this distance can be only equal to $r+1$. The claim (2) of the lemma is proved.

The proof of the case (1) is completely similar to the above: we only need to replace the sets C_i ($\widehat{C}_i$) with the sets C_{1-i} ($\widehat{C}_{1-i}$) in certain formulas.

□

Using this lemma we find 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:

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

Let $f_{\mathbf{v}}$ denote the function with the value vector $\mathbf{v} \in \mathbb{F}_2^n$ (non-punctured). Recall that 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. Since all vectors in U have odd weights and added parity check bit corresponds to the value of the function at the all-zero vector, we can describe the metric complement of $\mathcal{R}_{m-3}$ in terms of functions instead of their value vectors as follows:

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

where

$$G = \{f_{(1,\mathbf{u})} : \mathbf{u} \in \mathrm{U}\} = \{g : \mathrm{supp}(g) = \{0, \mathrm{x}_1, \mathrm{x}_2 \ldots, \mathrm{x}_m, \mathrm{x}_1 + \ldots + \mathrm{x}_m\},\\ \{\mathrm{x}_1, \ldots, \mathrm{x}_m\} \text{ are linearly independent}\}.$$

All functions in G form an equivalence class with respect to the linear equivalence. Recall that two functions f and g are called EL^k*-equivalent* if there exists a nonsingular binary matrix A and a function h of degree at most k such that $g = f \circ L_{\mathrm{A}} + h$. It is now easy to see that a function g is in $\widehat{\mathcal{R}}_{m-3}$ if and only if it is EL^{m-3}-equivalent to some function from G. Since all functions in the metric complement are equivalent, we can pick any function from it as the equivalence class representative (and we will change this representative when it is convenient). We will call the 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 G. Denote by g^* the function with the support $\{0, \mathrm{e}_1, \mathrm{e}_2, \ldots, \mathrm{e}_m, 1\}$, where $\mathrm{e}_i \in \mathbb{F}_2^m$ is the vector with 1 only in the i-th coordinate. Clearly, $g^* \in G$ and it is straightforward to construct the algebraic normal form of this function: it is the sum of all monomials containing an even number of variables, excluding the monomial with all variables included:

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

This function is equivalent to the sum of all monomials containing $m-2$ variables, so let us use this last function as g^* moving forward. Let $\overline{x_i}$ denote the product of all m variables except x_i, and let $\overline{x_ix_j}$ 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:

$$g^*(\mathrm{x}) := \sum_{1\leqslant i<j\leqslant m} \overline{x_ix_j}.$$

7.3 **Metric regularity**

We have established that

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

where g' is an arbitrary function from the class G (or from $\widehat{\mathcal{R}}_{m-3}$), and have constructed a certain representative of this equivalence class — g^*.

Since the code $\mathcal{R}_{m-3}$ is linear, $\rho(\widehat{\mathcal{R}}_{m-3}) = \rho(\mathcal{R}_{m-3}) = m+2$ and a function f is in $\widehat{\widehat{\mathcal{R}}}_{m-3}$ if and only if $f + \widehat{\mathcal{R}}_{m-3} = \widehat{\mathcal{R}}_{m-3}$. 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.

Let $f \notin \mathcal{R}_{m-3}$ be an arbitrary function. Since $\widehat{\mathcal{R}}_{m-3}$ is an EL^{m-3}-equivalence class, in order to show that $f + \widehat{\mathcal{R}}_{m-3} \neq \widehat{\mathcal{R}}_{m-3}$ it is enough to show that there exists a function f' such that $f' \overset{m-3}{\sim} f$ and $f' + \widehat{\mathcal{R}}_{m-3} \neq \widehat{\mathcal{R}}_{m-3}$.

Case 1. Let $f \notin \mathcal{R}_{m-3}$ be a function of degree greater than $m-2$. Since EL^{m-3}-equivalence preserves the degree for functions of degree higher than $m-3$, any $g \in \widehat{\mathcal{R}}_{m-3}$ has degree $m-2$ (like g^*), while $f+g$ has a 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 $m-2$. We can uniquely present 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 by $\tilde{f}$ the following quadratic function:

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

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

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

Lemma 6 *Let f and g be two functions 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}:

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

The function f changes under this transformation (disregarding monomials of degree less than $m-2$) in the following manner:

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

Let f_1 denote the function obtained after this transformation. Then it is easy to see that the dual function $\tilde{f}_1$ is obtained from the dual function $\tilde{f}$ (disregarding monomials of degree less than 2 since we consider EL^1-equivalence) by the following linear transformation:

$$L_{ji}:\begin{cases}x_j \leftarrow x_j + x_i,\\ x_k \leftarrow x_k & \forall k \neq j.\end{cases}$$

which is simply the transposed transformation.

Assume now that g is obtained from f using some linear transformation L. Trivially, 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 function $\tilde{g}$ 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 we have established that, if $f \overset{m-3}{\sim} g$, then $\tilde{f} \overset{1}{\sim} \tilde{g}$. The reverse can be shown using similar argumentation.

□

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. From this result and Lemma 6 we can conclude that f is equivalent to the function p_k for some k $(0 < k \leqslant \frac{m}{2})$, where

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

Trivially, g^* is equivalent to $p_{\frac{m}{2}}$. Then $p_k + p_{\frac{m}{2}}$ is equivalent to $p_{\frac{m}{2}-k}$, which is (by Lemma 6) not equivalent to $p_{\frac{m}{2}}$ and therefore not equivalent to g^*. This means that $f + \widehat{\mathcal{R}}_{m-3} \neq \widehat{\mathcal{R}}_{m-3}$ and therefore $f \notin \widehat{\widehat{\mathcal{R}}}_{m-3}$.

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

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

8.1 The covering radius and the 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, however, the proof is a bit more complicated. From Section 6 we have:

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

and a vector $\mathbf{v}$ is in the metric complement of $\mathcal{R}^{\circ}_{m-3}$ if and only if $t(\mathbf{S_v}) = m$. The following lemma will help to characterize the matrices which achieve this maximum:

Lemma 7 *Let $\mathbf{S}$ be a symmetric $m \times m$ matrix, where m is odd. Then $t(\mathbf{S}) = m$ if and only if $\mathbf{S}$ has an $m \times m$ factor which is either nonsingular, or has rank $m-1$ and all columns summing to zero.*

Proof. $\Longrightarrow$

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, which contradicts the minimality of $\mathbf{B}$, so the rank of the factor must be at least $m-1$. If the rank is m, the proof is finished.

Assume that $\operatorname{rank}(\mathbf{B}) = m-1$. 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, $t(\mathbf{S}) \geqslant \operatorname{rank}(\mathbf{S})$, 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 a minimal factor of $\mathbf{S}$. Since the sum of all columns of any factor is the vector composed of the diagonal elements of $\mathbf{S}$, the sum of all columns of $\mathbf{D}$ is also zero.

Assume that $k = m-1$. Then $\mathbf{D}$ has an even number of columns, and each row has an 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 its columns. Now the first column of $\mathbf{D}$ is zero and we can remove it by Lemma 1. We have now obtained a factor of $\mathbf{S}$ which has less columns than $\mathbf{D}$. This contradicts the minimality of $\mathbf{D}$.

Therefore, k can be at most $m-2$. Since all columns of $\mathbf{D}$ sum to zero, it is not a full-rank matrix. Hence $\operatorname{rank}(\mathbf{D})$ is at most $m-3$, which means that $\operatorname{rank}(\mathbf{S})$ 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 established that $\operatorname{rank}(\mathbf{S}) \leqslant m-3$, contradiction.

Thus, $t(\mathbf{S})$ has to be greater than $m-1$ and is equal to m.

□

Lemma 7 describes all minimal factors of all matrices $\mathbf{S}$ satisfying $t(\mathbf{S}) = m$. Let us put

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

and

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

Denote $\mathrm{U} = \mathrm{U}_1 \cup \mathrm{U}_2$. 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 Lemma 7. 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, the vectors from the set U cover all cosets contained in the metric complement of $\mathcal{R}^{\circ}_{m-3}$:

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

8.2 The covering radius and the metric complement of the non-punctured code

Let us return to the regular, non-punctured Reed-Muller code $\mathcal{R}_{m-3}$. As with the case when m is even, since the code is obtained from the punctured one by adding a parity check bit, using Lemma 5 we conclude that the covering radius of $\mathcal{R}_{m-3}$ is equal to $m+1$, and its metric complement is

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

Recall once again that for any $\mathbf{v} \in \mathbb{F}_2^n$, 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. Since 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:

$$\widehat{\mathcal{R}}_{m-3} = \bigcup_{g \in G_1 \cup G_2} g + \mathcal{R}_{m-3},$$

where

$$\begin{aligned}&G_1 = \{f_{(1,\mathbf{u})} : \mathbf{u} \in \mathrm{U}_1\} =\\ &\quad = \{g : \mathrm{supp}(f) = \{0, \mathrm{x}_1, \mathrm{x}_2 \ldots, \mathrm{x}_m\}, \{\mathrm{x}_1, \ldots, \mathrm{x}_m\} \text{ are linearly independent}\},\end{aligned}$$

and

$$\begin{aligned}G_2 = \{f_{(1,\mathbf{u})} &: \mathbf{u} \in \mathrm{U}_2\} =\\ &= \{g : \mathrm{supp}(g) = \{0, \mathrm{x}_1, \mathrm{x}_2 \ldots, \mathrm{x}_{m-1}, \mathrm{x}_1 + \ldots + \mathrm{x}_{m-1}\},\\ &\qquad\qquad \{\mathrm{x}_1, \ldots, \mathrm{x}_{m-1}\} \text{ are linearly independent}\}.\end{aligned}$$

It is easy to see that all functions in G_1 form an equivalence class with respect to the linear equivalence, so do functions in G_2. Let us pick two arbitrary functions $g_1 \in G_1$, $g_2 \in G_2$ from these two classes. Then it follows from the definition of the EL^k-equivalence that a function g is in $\widehat{\mathcal{R}}_{m-3}$ if and only if $g \overset{m-3}{\sim} g_1$ or $g \overset{m-3}{\sim} g_2$. In fact, we can pick any function from the EL^{m-3}-equivalence class of G_1 and from the EL^{m-3}-equivalence class of G_2 respectively as our class representatives.

Let us give an explicit (algebraic normal form) description of a certain function from G_1. Denote by g_1^* the function with the support $\{0, \mathrm{e}_1, \mathrm{e}_2, \ldots, \mathrm{e}_{m-1}, 1\}$. After a bit of calculation one can explicitly describe its ANF:

$$g_1^*(\mathrm{x}) = \overline{x_m} + (1 + x_m)\left(1 + \sum_{k=1}^{\frac{m-3}{2}} \sum_{1 \leqslant i_1 < \ldots < i_{2k} \leqslant m-1} x_{i_1} x_{i_2} \ldots x_{i_{2k}}\right).$$

This function has degree $m-1$ and, omitting all terms of degree less than $m-2$, it is trivially EL^{m-3}-equivalent to the following function which we will denote as g_1^* from now on:

$$g_1^* := \overline{x_m} + x_m g^\star, \tag{1}$$

where $g^\star$, defined by

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

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 transformations of the first $m-1$ variables as $\bar{L}_{\mathrm{A}}^{\mathrm{b}}$ (with the matrix and the vector of corresponding sizes).

Let us now give an explicit description of a certain function from G_2. Denote by g_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:

$$g_2^*(\mathrm{x}) = (1 + x_m)\left(1 + \sum_{k=1}^{\frac{m-3}{2}} \sum_{1 \leqslant i_1 < \ldots < i_{2k} \leqslant m-1} x_{i_1} x_{i_2} \ldots x_{i_{2k}}\right).$$

This function has degree $m-1$ and is trivially EL^{m-3}-equivalent to the function $x_m g^\star$, which we will denote as g_2^* from now on:

$$g_2^* := x_m g^\star. \tag{2}$$

Note that $g_1^* = \overline{x_m} + g_2^*$.

Before we proceed to establish the metric regularity of $\mathcal{R}_{m-3}$, we will build some alternative representatives of the equivalence classes of G_1 and G_2. The following lemma will be helpful:

Lemma 8 *Let f be a function such that $f \overset{m-2}{=} \overline{x_m}$. Let A be a nonsingular $m \times m$ matrix. Then $f \circ L_{\mathrm{A}} \overset{m-2}{=} \overline{x_m}$ if and only if the 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 the all-zero column of length $m-1$, $\bar{\mathrm{A}}$ is a nonsingular $(m-1) \times (m-1)$ matrix and w is a row of length $m-1$.

Proof. $\Longleftarrow$

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

$\Longrightarrow$

Assume that $f \circ L_{\mathrm{A}} \overset{m-2}{=} \overline{x_m}$. 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 of variables on monomials of degree $m-2$ and fewer is irrelevant, so let us inspect 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 L_{A} to the variables, is precisely the value of the $(m-1)\times(m-1)$ minor obtained from the matrix A by removing the m-th row and the i-th column. Therefore, all minors of the matrix A of this form must be equal to zero, except for the last one, obtained by removing the last column.

Let $\bar{\mathrm{A}}^1, \bar{\mathrm{A}}^2, \dots, \bar{\mathrm{A}}^m$ denote the columns of the matrix A with the last coordinate removed. Then the condition on the minors described above can be reformulated as follows: sets of columns $\{\bar{\mathrm{A}}^1, \dots, \bar{\mathrm{A}}^{i-1}, \bar{\mathrm{A}}^{i+1}, \dots, \bar{\mathrm{A}}^m\}$ are linearly dependent for all $i \neq m$, while the set of the first $m-1$ columns is linearly independent. This implies that the following set of equations holds:

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

where $\mathrm{B} = (b_{i,j})$ — the coefficients matrix — is an $(m-1)\times(m-1)$ matrix with $b_{i,i} = 0$ for all i.

If we denote the rows of the matrix B by B_i, and denote by $\bar{\mathrm{A}}$ the $(m-1)\times(m-1)$ matrix composed of the first $m-1$ columns $\bar{\mathrm{A}}^1, \dots, \bar{\mathrm{A}}^{m-1}$, we can rewrite this in the following manner:

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

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 $\mathrm{B}_1 = \mathrm{B}_2 = \dots = \mathrm{B}_{m-1}$. Since $b_{i,i} = 0$, the matrix B is a zero matrix, which means that $\bar{\mathrm{A}}^m = 0$. This implies that the last column of the matrix A can have 1 only in the last coordinate, and since A is nonsingular, this has to be the case. Thus, A is of the form stated in the lemma.

□

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 $\deg(h) \leqslant m-2$ into functions of the same form, preserving $\overline{x_m}$ as the only monomial of degree $m-1$. Let us describe more precisely how such transformations act on monomials of lesser degree:

Corollary 2 *Let f be a function of degree $m-1$ of the following form:*

$$f = \overline{x_m} + x_m f_1 + f_2,$$

where f_1, f_2 do not depend on x_m and $\deg(f_1) \leqslant m-3$, $\deg(f_2) \leqslant m-2$*. Let* A *be a matrix satisfying the conditions of Lemma 8. Then*

$$f \circ L_{\mathrm{A}} \overset{m-3}{=} \overline{x_m} + x_m(f_1 \circ \bar{L}_{\bar{\mathrm{A}}}) + f_3,$$

where f_3 is some function of degree at most $m-2$ which does not depend on the variable x_m.

Proof. Straighforward from the proof of Lemma 8. □

Let us now build alternative representatives for the metric complement of $\mathcal{R}_{m-3}$. Since $\bar{\mathrm{A}}$ in Lemma 8 can be any nonsingular matrix, choosing $\bar{\mathrm{A}}$ so that $g^\star \circ \bar{L}_{\bar{\mathrm{A}}} \overset{m-3}{=} p_{\frac{m-1}{2}}$, (this is possible by Lemma 6) and filling the vector w with zeroes, we obtain a matrix A such that

$$g_1^{**} := g_1^* \circ L_{\mathrm{A}} \overset{m-3}{=} \overline{x_m} + x_m(g^\star \circ \bar{L}_{\bar{\mathrm{A}}}) + h_1 \overset{m-3}{=} \overline{x_m} + x_m p_{\frac{m-1}{2}} + h_1. \tag{3}$$

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

$$g_2^{**} := g_2^* \circ L_{\mathrm{A}} \overset{m-3}{=} x_m(g^\star \circ \bar{L}_{\bar{\mathrm{A}}}) \overset{m-3}{=} x_m p_{\frac{m-1}{2}}. \tag{4}$$

We will use these equivalent functions g_1^{**} and g_2^{**} as class representatives in some cases.

8.3 Metric regularity

We have established that

$$\widehat{\mathcal{R}}_{m-3} = \{g : g \overset{m-3}{\sim} g_1\} \cup \{g : g \overset{m-3}{\sim} g_2\},$$

where g_1 is an arbitrary representative of an EL^{m-3}-equivalence class of G_1 and g_2 is an arbitrary representative of an EL^{m-3}-equivalence class of G_2, and have presented some variants of these representatives — functions g_1^*, g_2^*, g_1^{**} and g_2^{**} (equations (1)-(4)).

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

Let $f \notin \mathcal{R}_{m-3}$ be an arbitrary function. Since $\widehat{\mathcal{R}}_{m-3}$ is a union of two EL^{m-3}-equivalence classes, in order to show that $f + \widehat{\mathcal{R}}_{m-3} \neq \widehat{\mathcal{R}}_{m-3}$ it is enough to show that there exists a function f' such that $f' \overset{m-3}{\sim} f$ and $f' + \widehat{\mathcal{R}}_{m-3} \neq \widehat{\mathcal{R}}_{m-3}$.

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 $m-1$ or $m-2$ (like g_1^* and g_2^* respectively), 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 a function with $\overline{x_m}$ as the only monomial of degree $m-1$, so

$$f \overset{m-3}{\sim} \overline{x_m} + x_m f_1 + f_2, \tag{5}$$

where 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. Assume that f_1 in (5) is nonzero. Then, from Lemma 8 and Lemma 6 it follows that

$$f \overset{m-3}{\sim} \overline{x_m} + x_m p_k + f_3 =: f' \tag{6}$$

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 $g_2^{**} \in \widehat{\mathcal{R}}_{m-3}$, we obtain:

$$g_2^{**} + f' \overset{m-3}{=} \overline{x_m} + x_m(p_k + p_{\frac{m-1}{2}}) + f_3 \overset{m-3}{\sim} \overline{x_m} + x_m p_{\frac{m-1}{2}-k} + f_4,$$

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

Let us denote this last function as g'. It has degree $m-1$ and therefore cannot be equivalent to the functions from G_2. It cannot be equivalent to the functions from G_1 either, because, by Lemma 8, any linear transformation of variables with matrix D which preserves $\overline{x_m}$ will act onto it in the following manner:

$$g' \circ L_{\mathrm{D}} \overset{m-3}{=} \overline{x_m} + x_m(p_{\frac{m-1}{2}-k} \circ \bar{L}_{\bar{\mathrm{D}}}) + f_5,$$

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 monomials of degree $m-2$ containing variable x_m of the function g' and of the function g_1^{**}, since $p_{\frac{m-1}{2}-k}$ is not equivalent to $p_{\frac{m-1}{2}}$. Thus, the function $g' = g_2^{**} + f'$ 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 Assume that both f_1 and f_2 in (5) are zero. Then

$$f \overset{m-3}{\sim} \overline{x_m} =: f'.$$

Using the transformation $L_{1m} : x_1 \leftarrow x_1 + x_m$ (and removing the terms of degree less than $m-2$), the function $g_1^* = \overline{x_m} + x_m g^\star$ transforms into $g_1^* \circ L_{1m} \overset{m-3}{=} \overline{x_m} + \overline{x_1} + x_m g^\star$.

If we now sum f' and $g_1^* \circ L_{1m} \in \widehat{\mathcal{R}}_{m-3}$ we will obtain the function $g' \overset{m-3}{=} \overline{x_1} + x_m g^\star$. If we swap the variables x_1 and x_m by another linear transformation and regroup terms, we see that

$$g' \overset{m-3}{\sim} \overline{x_m} + \sum_{2 \leqslant i < j \leqslant m-1} \overline{x_i x_j} + \sum_{i=2}^{m-1} \overline{x_i x_m} \overset{m-3}{\sim} \overline{x_m} + x_m p_{\frac{m-3}{2}} + h$$

for some h of degree at most $m-2$ in the first $m-1$ variables. By Lemma 8 and Lemma 6, this function cannot be equivalent to g_1^{**} and it is not equivalent to g_2^* by degree comparison. Therefore, g' is not in $\widehat{\mathcal{R}}_{m-3}$, and hence f is not in $\widehat{\widehat{\mathcal{R}}}_{m-3}$.

Case 2.3 Assume that f_1 in (5) is zero and f_2 is nonzero. Then

$$f \stackrel{m-3}{\sim} \overline{x_m} + f_2 =: f'.$$

Since f_2 does not 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 the first $m-1$ if needed) we can assume that f_2 contains $\overline{x_{m-1} x_m}$. Renaming variables, we can transform g_2^{**} into:

$$g_2^{**} \stackrel{m-3}{\sim} \overline{x_2 x_3} + \overline{x_4 x_5} + \ldots + \overline{x_{m-1} x_m}.$$

If we now add f' and the function above, which belongs to $\widehat{\mathcal{R}}_{m-3}$, we obtain the function $g' := \overline{x_m} + \sum_{k=1}^{\frac{m-3}{2}} \overline{x_{2k} x_{2k+1}} + \sum_{i \in I} \overline{x_i x_m}$, which is equivalent to

$$g' \stackrel{m-3}{\sim} \overline{x_m} + x_m p_{\frac{m-3}{2}} + h$$

for some h of degree at most $m-2$ in the first $m-1$ variables. By Lemma 8 and Lemma 6, this function cannot be equivalent to g_1^{**} and it is not equivalent to g_2^* by degree comparison. Therefore, g' is not in $\widehat{\mathcal{R}}_{m-3}$, and thus 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 $k > 0$. Then

$$p_k + g_2^{**} \stackrel{m-3}{\sim} p_{\frac{m-1}{2}-k}.$$

The function on the right is inequivalent to both g_2^{**} (because $\frac{m-1}{2} \neq \frac{m-1}{2} - k$) and g_1^* (by degree comparison), therefore $f \notin \widehat{\widehat{\mathcal{R}}}_{m-3}$.

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 when m is odd.

Factoring in the results from Section 7, we have proved the following

Theorem 2 *$\mathcal{R}_{m-3}$ is metrically regular for any $m \geqslant 3$.*

9 The Reed-Muller code $\mathcal{RM}(2,6)$

Let us consider one other special case. It is known that each Reed-Muller code (for $m > 1$, $r > 0$) can be inductively defined as follows [8]:

$$\mathcal{R}_{r,m} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) : \mathbf{u} \in \mathcal{R}_{r,m-1}, \mathbf{v} \in \mathcal{R}_{r-1,m-1}\}.$$

In particular,

$$\mathcal{R}_{2,6} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) : \mathbf{u} \in \mathcal{R}_{2,5}, \mathbf{v} \in \mathcal{R}_{1,5}\}.$$

Since both $\mathcal{R}_{2,5}$ and $\mathcal{R}_{1,5}$ were shown to be metrically regular, this recursive construction proves useful and allows us to establish the metric regularity of the code $\mathcal{R}_{2,6}$ as well. From now on, vectors in bold will represent value vectors of functions in 5 variables (of length 32), while value vectors of 6-variable functions will be presented as pairs of value vectors of 5-variable functions. Additionaly, in this section we will use the notion of an *automorphism* of a set, which will denote an isometric bijective mapping from the whole space to itself which maps the given set to itself.

First, let us establish one of the basic tools for the following investigations. Recall that $\rho(\mathcal{R}_{2,5}) = 6$ (Section 8), $\rho(\mathcal{R}_{1,5}) = 12$ [1] and $\rho(\mathcal{R}_{2,6}) = 18$ [17].

Lemma 9 *Let* $(\mathbf{y}, \mathbf{w})$ *be in* $\widehat{\mathcal{R}}_{2,6}$*. Then* $\mathbf{y} \in \widehat{\mathcal{R}}_{2,5}$ *and for any* $\mathbf{u} \in \mathcal{R}_{2,5}$ *such that* $d(\mathbf{y}, \mathbf{u}) = 6$ *it holds* $d(\mathbf{w} + \mathbf{u}, \mathcal{R}_{1,5}) = 12$*, i.e.* $(\mathbf{w} + \mathbf{u}) \in \widehat{\mathcal{R}}_{1,5}$*.*

Proof. Assume that $\mathbf{y} \notin \widehat{\mathcal{R}}_{2,5}$, i.e. $d(\mathbf{y}, \mathcal{R}_{2,5}) < 6$. Then there exists a vector $\mathbf{u} \in \mathcal{R}_{2,5}$ such that $d(\mathbf{y}, \mathbf{u}) < 6$. From the inductive construction of $\mathcal{R}_{2,6}$ it follows that the distance between $(\mathbf{y}, \mathbf{w})$ and $\mathcal{R}_{2,6}$ is at most the distance between $\mathbf{y}$ and $\mathbf{u}$ plus the distance between $\mathbf{w}$ and $\mathbf{u} + \mathcal{R}_{1,5}$. The latter is in turn equal to $d(\mathbf{w} + \mathbf{u}, \mathcal{R}_{1,5})$, which is bounded by the covering radius of $\mathcal{R}_{1,5}$. Therefore,

$$d((\mathbf{y}, \mathbf{w}), \mathcal{R}_{2,6}) \leqslant d(\mathbf{y}, \mathbf{u}) + d(\mathbf{w} + \mathbf{u}, \mathcal{R}_{1,5}) < 6 + 12 = 18.$$

This contradicts with $(\mathbf{y}, \mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}$, hence $\mathbf{y}$ is in $\widehat{\mathcal{R}}_{2,5}$.

The second part is now trivial: if $\mathbf{u} \in \mathcal{R}_{2,5}$ is a vector such that $d(\mathbf{y}, \mathbf{u}) = 6$, then the distance $d(\mathbf{w} + \mathbf{u}, \mathcal{R}_{1,5})$ has to achieve the maximum of 12 in order for the vector $(\mathbf{y}, \mathbf{w})$ to be in the metric complement of $\mathcal{R}_{2,6}$. □

Let $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}} + \tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$. We will prove that $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}} + \tilde{\mathbf{v}})$ is in $\mathcal{R}_{2,6}$ in two steps: first we establish that $\tilde{\mathbf{u}}$ is in $\mathcal{R}_{2,5}$, then we prove that $\tilde{\mathbf{v}}$ is in $\mathcal{R}_{1,5}$.

Recall (Section 8) that $\widehat{\mathcal{R}}_{2,5} = \{g : g \overset{2}{\sim} g_1\} \cup \{g : g \overset{2}{\sim} g_2\}$, where g_1 and g_2 are some representatives of two EL^2-equivalence classes. Let us denote

$$\widehat{\mathcal{R}}^1_{2,5} := \{g : g \overset{2}{\sim} g_1\}, \ \widehat{\mathcal{R}}^2_{2,5} := \{g : g \overset{2}{\sim} g_2\}.$$

Then the following lemma is useful for proving the first half.

Lemma 10 *For each* $i = 1, 2$ *one of the following statements holds:*

1. $\forall \mathbf{y} \in \widehat{\mathcal{R}}^i_{2,5}$ $\forall \mathbf{w} \in \mathbb{F}_2^{32}$ *it holds* $(\mathbf{y}, \mathbf{w}) \notin \widehat{\mathcal{R}}_{2,6}$*;*
2. $\forall \mathbf{y} \in \widehat{\mathcal{R}}^i_{2,5}$ $\exists \mathbf{w} \in \mathbb{F}_2^{32}$ *such that* $(\mathbf{y}, \mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}$*;*

Proof. Assume that for some i the second statement does not hold. This means that the negation of it holds:

$$\exists \mathbf{y}^* \in \widehat{\mathcal{R}}^i_{2,5} : \forall \mathbf{w} \in \mathbb{F}_2^{32} \text{ it holds } (\mathbf{y}^*, \mathbf{w}) \notin \widehat{\mathcal{R}}_{2,6}$$

We will now prove that any $\mathbf{y} \in \widehat{\mathcal{R}}^i_{2,5}$ satisfies the claim of this statement and not just the vector $\mathbf{y}^*$. First, note that the statement "$\forall \mathbf{w} \in \mathbb{F}_2^{32}$ it holds $(\mathbf{y}^*, \mathbf{w}) \notin \widehat{\mathcal{R}}_{2,6}$" is equivalent to the following:

$$\forall \mathbf{w} \in \mathbb{F}_2^{32} \ \exists \mathbf{u} \in \mathcal{R}_{2,5} : d(\mathbf{y}^*, \mathbf{u}) + \min_{\mathbf{v} \in \mathcal{R}_{1,5}} d(\mathbf{w} + \mathbf{u}, \mathbf{v}) < 18. \qquad (7)$$

Let $\mathbf{y}$ be an arbitrary vector from $\widehat{\mathcal{R}}^i_{2,5}$. Since all functions in $\widehat{\mathcal{R}}^i_{2,5}$ are EL^2-equivalent, there exists a nonsingular linear transformation of variables L and a function $g \in \mathcal{R}_{2,5}$ such that $f_{\mathbf{y}} = f_{\mathbf{y}^*} \circ L + g$. Let us denote as $\mathbf{g}$ the value vector of g and as $\mathbf{L}$ the linear transformation on $\mathbb{F}_2^{32}$, corresponding to the transformation L on functions. Then $\mathbf{y} = \mathbf{L}\mathbf{y}^* + \mathbf{g}$.

Let us take an arbitrary vector $\mathbf{w} \in \mathbb{F}_2^{32}$ and let us denote $\mathbf{w}_{\mathbf{y}} = \mathbf{L}^{-1}(\mathbf{w} + \mathbf{g})$. Then, by (7), there exists a vector $\mathbf{u} \in \mathcal{R}_{2,5}$ such that

$$d(\mathbf{y}^*, \mathbf{u}) + \min_{\mathbf{v} \in \mathcal{R}_{1,5}} d(\mathbf{w}_{\mathbf{y}} + \mathbf{u}, \mathbf{v}) < 18. \tag{8}$$

Trivially, the transformation $\mathbf{L}$, as well as the addition of the function $\mathbf{g}$ are both automorphisms of $\mathbb{F}_2^{32}$. So let us apply $\mathbf{L}$ to all vectors being compared in (8) and add $\mathbf{g}$ to some of them, without changing the inequality:

$$d(\mathbf{L}\mathbf{y}^* + \mathbf{g}, \mathbf{L}\mathbf{u} + \mathbf{g}) + \min_{\mathbf{v} \in \mathcal{R}_{1,5}} d(\mathbf{L}\mathbf{w}_{\mathbf{y}} + \mathbf{L}\mathbf{u}, \mathbf{L}\mathbf{v}) < 18. \tag{9}$$

Note that the transformation $\mathbf{L}$ is also an automorphism of the codes $\mathcal{R}_{1,5}$ and $\mathcal{R}_{2,5}$. Let us denote $\mathbf{u}_{\mathbf{y}} := \mathbf{L}\mathbf{u} + \mathbf{g}$. Then $\mathbf{u}_{\mathbf{y}} \in \mathcal{R}_{2,5}$ and (9) can be transformed into

$$d(\mathbf{y}, \mathbf{u}_{\mathbf{y}}) + \min_{\mathbf{v} \in \mathcal{R}_{1,5}} d(\mathbf{w} + \mathbf{u}_{\mathbf{y}}, \mathbf{v}) < 18. \tag{10}$$

Thus, for an arbitrary $\mathbf{w} \in \mathbb{F}_2^{32}$ we have found a vector $\mathbf{u}_{\mathbf{y}} \in \mathcal{R}_{2,5}$ such that (10) holds. This means that (7) holds for the vector $\mathbf{y}$ that we have previously selected from $\widehat{\mathcal{R}}_{2,5}^i$. Since our selection was arbitrary, we have proved that the first statement of the lemma holds for the set $\widehat{\mathcal{R}}_{2,5}^i$ in question. □

Proposition 1 *Let* $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}} + \tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$. *Then* $\tilde{\mathbf{u}} \in \mathcal{R}_{2,5}$.

Proof. Let us denote $Y := \{\mathbf{y} \in \mathbb{F}_2^{32} \mid \exists \mathbf{w} \in \mathbb{F}_2^{32}; (\mathbf{y}, \mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}\}$. From Lemma 9 it follows that $Y \subseteq \widehat{\mathcal{R}}_{2,5}$ and is nonempty. From Lemma 10 we can conclude that Y can only coincide with one of the three sets: $\widehat{\mathcal{R}}_{2,5}^1$, $\widehat{\mathcal{R}}_{2,5}^2$ or $\widehat{\mathcal{R}}_{2,5}$.

Let $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}} + \tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$. Then, as we know, $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}} + \tilde{\mathbf{v}}) + \widehat{\mathcal{R}}_{2,6} = \widehat{\mathcal{R}}_{2,6}$. This implies that $\tilde{\mathbf{u}} + Y = Y$. Since $\mathcal{R}_{2,5}$ is proven to be metrically regular, we know that only the vectors from $\mathcal{R}_{2,5}$ preserve its metric complement under addition. Following the proof of the metric regularity of the code $\mathcal{R}_{m-3,m}$ for m odd (Subsection 8.3), it is easy to see that the same can be shown true for the sets $\widehat{\mathcal{R}}_{2,5}^1$ and $\widehat{\mathcal{R}}_{2,5}^2$ if they are considered separately one from another. Therefore, regardless of the contents of Y, only vectors from $\mathcal{R}_{2,5}$ preserve it under addition, and therefore $\tilde{\mathbf{u}} \in \mathcal{R}_{2,5}$. □

Recall from Section 3 that $\widehat{\mathcal{R}}_{1,5}$ is composed of 4 EA-equivalence classes: $\widehat{\mathcal{R}}_{1,5} = \bigcup_{i=1}^4 \widehat{\mathcal{R}}_{1,5}^i$. Similar to Lemma 10, the following statement holds:

Lemma 11 *For each* $i = 1, 2, 3, 4$ *one of the following statements holds:*

1. $\forall \mathbf{w}' \in \widehat{\mathcal{R}}_{1,5}^i \ \forall (\mathbf{y}, \mathbf{w}) \in \widehat{\mathcal{R}}_{2,6} \ \forall \mathbf{u} \in \mathcal{R}_{2,5} \ (d(\mathbf{y}, \mathbf{u}) = 6 \to \mathbf{w} + \mathbf{u} \neq \mathbf{w}')$;
2. $\forall \mathbf{w}' \in \widehat{\mathcal{R}}_{1,5}^i \ \exists (\mathbf{y}, \mathbf{w}) \in \widehat{\mathcal{R}}_{2,6} \ \exists \mathbf{u} \in \mathcal{R}_{2,5} : (d(\mathbf{y}, \mathbf{u}) = 6 \wedge \mathbf{w} + \mathbf{u} = \mathbf{w}')$;

Proof. Assume that for some i the second statement does not hold. Then there exists a vector $\mathbf{w}^* \in \widehat{\mathcal{R}}^i_{1,5}$ such that

$$\forall(\mathbf{y},\mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}\ \forall\mathbf{u} \in \mathcal{R}_{2,5}\ (d(\mathbf{y},\mathbf{u}) = 6 \to \mathbf{w}+\mathbf{u} \neq \mathbf{w}^*) \tag{11}$$

Let us show that this also holds for other vectors from the class. Let $\mathbf{w}'$ be an arbitrary vector from $\widehat{\mathcal{R}}^i_{1,5}$. Since all functions in $\widehat{\mathcal{R}}^i_{1,5}$ are EA-equivalent, there exists a nonsingular affine transformation of variables A and a function $g \in \mathcal{R}_{1,5}$ such that $f_{\mathbf{w}'} = f_{\mathbf{w}^*} \circ A + g$. Let us denote as $\mathbf{g}$ the value vector of g and as $\mathbf{A}$ the linear transformation on $\mathbb{F}_2^{32}$, corresponding to the transformation A on functions. Then $\mathbf{w}' = \mathbf{A}\mathbf{w}^* + \mathbf{g}$.

Let $(\mathbf{y},\mathbf{w})$ be an arbitrary vector from $\widehat{\mathcal{R}}_{2,6}$ and $\mathbf{u}$ be an arbitrary vector from $\mathcal{R}_{2,5}$. Since $\mathbf{A}$ is an automorphism of the codes $\mathcal{R}_{2,5}$ and $\mathcal{R}_{1,5}$, the vector $\mathbf{A^{-1}u}$ is in $\mathcal{R}_{2,5}$ and $(\mathbf{A},\mathbf{A})\cdot\mathcal{R}_{2,6} = \mathcal{R}_{2,6}$. Since the addition of $\mathbf{g}$ is an automorphism of $\mathcal{R}_{2,5}$, $\mathcal{R}_{1,5}$ and $\mathbb{F}_2^{32}$, the vector $(\mathbf{A^{-1}y}, \mathbf{A^{-1}}(\mathbf{w}+\mathbf{g}))$ is in $\widehat{\mathcal{R}}_{2,6}$. Hence, from (11) it follows that:

$$d(\mathbf{A^{-1}y}, \mathbf{A^{-1}u}) = 6 \to \mathbf{A^{-1}}(\mathbf{w}+\mathbf{g}) + \mathbf{A^{-1}u} \neq \mathbf{w}^*. \tag{12}$$

Applying $\mathbf{A}$, (12) shows to be equivalent to the following statement:

$$d(\mathbf{y},\mathbf{u}) = 6 \to \mathbf{w}+\mathbf{u} \neq \mathbf{w}'. \tag{13}$$

Hence, we have shown that for an arbitrary vector $\mathbf{w}'$ from $\widehat{\mathcal{R}}^i_{1,5}$, an arbitrary vector $(\mathbf{y},\mathbf{w})$ from $\widehat{\mathcal{R}}_{2,6}$ and an arbitrary $\mathbf{u}$ from $\mathcal{R}_{2,5}$ the statement (13) holds. This proves that the first statement of the lemma holds for the class $\widehat{\mathcal{R}}^i_{1,5}$.

□

The following result shows that any of the EA-equivalence classes of the metric complement of $\mathcal{R}_{1,5}$ are also rather "unstable" when summed with a non-affine function:

Lemma 12 *For any* $\mathbf{v} \notin \mathcal{R}_{1,5}$ *and any* $i = 1,2,3,4$ *there exists a vector* $\mathbf{w} \in \widehat{\mathcal{R}}^i_{1,5}$ *such that* $\mathbf{v}+\mathbf{w} \notin \widehat{\mathcal{R}}_{1,5}$.

Proof. Like in Section 3, in order to prove the statement it is enough to show that for any $i = 1,2,3,4$ and any EA-equivalence class C of $\mathbb{F}_2^{32}$ of even weight (other than $\mathcal{R}_{1,5}$) there exists a function $f \in C$ and a function $g \in \widehat{\mathcal{R}}^i_{1,5}$ such that $f + g \notin \widehat{\mathcal{R}}_{1,5}$. The proof for this can be found in the appendix in Tables 2-5. □

The last two lemmas allow us to prove the following result.

Theorem 3 *The code* $\mathcal{R}_{2,6}$ *is metrically regular.*

Proof. Since any linear code is a subset of its second metric complement, we only need to prove that $\widehat{\widehat{\mathcal{R}}}_{2,6} \subseteq \mathcal{R}_{2,6}$. Let $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}}+\tilde{\mathbf{v}})$ be a vector from $\widehat{\widehat{\mathcal{R}}}_{2,6}$. We have already proved that $\tilde{\mathbf{u}}$ is in $\mathcal{R}_{2,5}$, therefore the vector $(\mathbf{0},\tilde{\mathbf{v}})$ is also in $\widehat{\widehat{\mathcal{R}}}_{2,6}$. Let us prove that $\tilde{\mathbf{v}}$ is in $\mathcal{R}_{1,5}$.

Assume that $\tilde{\mathbf{v}} \notin \mathcal{R}_{1,5}$. Since (by Lemma 9) for an arbitrary $(\mathbf{y},\mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}$ there exists a vector $\mathbf{u} \in \mathcal{R}_{2,5}$ such that $(\mathbf{w}+\mathbf{u}) \in \widehat{\mathcal{R}}_{1,5}$, for some i the second statement of Lemma 11 must hold.

By Lemma 12, for this i there exists a vector $\mathbf{w}^* \in \widehat{\mathcal{R}}^i_{1,5}$ such that $\tilde{\mathbf{v}} + \mathbf{w}^* \notin \widehat{\mathcal{R}}_{1,5}$.

By the second statement of Lemma 11, for this $\mathbf{w}^*$ there exists a vector $(\mathbf{y}, \mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}$ and a vector $\mathbf{u} \in \mathcal{R}_{2,5}$ such that $(d(\mathbf{y}, \mathbf{u}) = 6 \wedge \mathbf{w} + \mathbf{u} = \mathbf{w}^*)$. Since $(\mathbf{0}, \tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$, $(\mathbf{y}, \mathbf{w} + \tilde{\mathbf{v}})$ is also in $\widehat{\mathcal{R}}_{2,6}$, and since $d(\mathbf{y}, \mathbf{u}) = 6$, by Lemma 9 the vector $\mathbf{w} + \tilde{\mathbf{v}} + \mathbf{u}$ is in $\widehat{\mathcal{R}}_{1,5}$. But $\mathbf{w} + \tilde{\mathbf{v}} + \mathbf{u} = \tilde{\mathbf{v}} + \mathbf{w}^* \notin \widehat{\mathcal{R}}_{1,5}$, contradiction. Therefore, $\tilde{\mathbf{v}} \in \mathcal{R}_{1,5}$ and hence $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}} + \tilde{\mathbf{v}}) \in \mathcal{R}_{2,6}$. □

10 Conclusion

In this paper we have established the metric regularity of the codes $\mathcal{RM}(1,5)$, $\mathcal{RM}(2,6)$ and of the codes $\mathcal{RM}(k,m)$ for $k \geqslant m-3$. Factoring in the result by Tokareva [19], which proves the metric regularity of $\mathcal{RM}(1,m)$ for even m, all infinite families of Reed-Muller codes with known covering radius are covered. Given these results, we formulate the following

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

The only other Reed-Muller codes with known covering radius, metric regularity of which has not been yet established, are $\mathcal{RM}(1,7)$ and $\mathcal{RM}(2,7)$.

The availability of the coset weight distributionfor allowed us to consider the code $\mathcal{RM}(1,5)$, and the fact that the covering radius of $\mathcal{RM}(2,6)$ attains the upper bound given by the $(\mathbf{u}, \mathbf{u}+\mathbf{v})$ construction [17] allowed us to establish its metric regularity even without describing the metric complement. However, the codes $\mathcal{RM}(1,7)$ and $\mathcal{RM}(2,7)$ are much harder to consider because of the lack of similar regularities, the larger number of variables, the larger covering radius and the unconstructive nature of the results which describe their covering radius.

I would like to thank Natalia Tokareva, Alexander Kutsenko and the collective of the Selmer Center of the University in Bergen for the inspiration and helpful remarks during the development of this work.

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. Carlet C., Crama Y., Hammer P. L.: Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monograph "Boolean Models and Methods in Mathematics, Computer Science, and Engineering". Cambridge University Press, 257–397 (2010).
3. Carlet C., Mesnager S. Four decades of research on bent functions. Designs, Codes and Cryptography. **78**(1), 5–50 (2016).
4. Cohen G., Honkala I., Litsyn S., Lobstein A.: Covering codes. Elsevier. **54**, (1997).
5. 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).
6. Kolomeec N.: The graph of minimal distances of bent functions and its properties. Designs, Codes and Cryptography. **85**(3), 395–410 (2017).
7. Kutsenko A.: Metrical properties of self-dual bent functions. Designs, Codes and Cryptography (2019). doi:10.1007/s10623-019-00678-x
8. MacWilliams F. J., Sloane N. J. A.: The theory of error correcting codes. Elsevier. **16**, (1977).
9. 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).

10. Mesnager S.: Bent Functions: Fundamentals and Results. Springer International Publishing, (2016).
11. Mykkeltveit J.: The covering radius of the $(128, 8)$ Reed-Muller code is 56. IEEE Transactions on Information Theory. **26**(3), 359–362 (1980).
12. Neumaier A.: Completely regular codes. Discrete mathematics. **106**, 353–360 (1992).
13. Oblaukhov A. K.: Metric complements to subspaces in the Boolean cube. Journal of Applied and Industrial Mathematics. **10**(3), 397–403 (2016).
14. Oblaukhov A. K.: Maximal metrically regular sets. Siberian Electronic Mathematical Reports. **15**, 1842–1849 (2018).
15. 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).
16. Rothaus O. S.: On "bent" functions. Journal of Combinatorial Theory, Series A. **20**(3), 300–305 (1976).
17. 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).
18. Stanica P., Sasao T., Butler J. T.: Distance duality on some classes of Boolean functions. Journal of Combinatorial Mathematics and Combinatorial Computing. 2018.
19. Tokareva N. N.: The group of automorphisms of the set of bent functions. Discrete Mathematics and Applications. **20**(5–6), 655–664 (2010).
20. Tokareva N.: Duality between bent functions and affine functions. Discrete Mathematics. **312**(3), 666–670 (2012).
21. Tokareva N.: Bent functions: results and applications to cryptography. Academic Press, (2015).
22. Wang Q.: The covering radius of the Reed–Muller code $RM(2, 7)$ is 40. Discrete Mathematics. **342**(12), Article 111625 (2019).

Appendix

Tables 2-5 show that for any EA-equivalence class $\widehat{\mathcal{R}}^i_{1,5}$ of $\widehat{\mathcal{R}}_{1,5}$ and for each EA-equivalence class C of $\mathbb{F}_2^{32}$ there exists a function $f \in C$ and a function $g \in \widehat{\mathcal{R}}^i_{1,5}$ such that $f + g$ does not belong to $\widehat{\mathcal{R}}_{1,5}$. Note that, if this function f is not in $\widehat{\mathcal{R}}_{1,5}$ and $f + g$ belongs to a class C', then we do not have to search for a function with such properties in the class C' since $(f + g) + g = f$ does not belong to $\widehat{\mathcal{R}}_{1,5}$ — this is why some rows in the following tables are skipped.

Notations in Tables 2-5 are the same as in Table 1 (see Section 3). The second column of Table 5 contains "canonical" representatives for each EA-equivalence class, as they were obtained in the paper [1] by Berlekamp and Welch. In other columns and tables, some representatives are changed by either simple variable swaps or more complex transformations. These more complex transformations are marked with an asterisk and explained below for each table, along with other clarifications. Hereafter "$i {\leftarrow} i + j$" stands for "$x_i {\leftarrow} x_i + x_j$", while two-way arrows denote variable swapping; all transformations are applied consecutively.

Table 2: Representatives f for classes 7, 9, 10 and 22 (column 2) are obtained from "canonical" using the following transformations:
(7) 3←3+0; (9) 4←4+3+0; (10) 1←1+0; (22) 4↔5; 1↔3;
Functions g from $\widehat{\mathcal{R}}^1_{1,5}$ (third column) are obtained from "canonical" using transformations:
2345+123+24+35 ∘ (2←2+0) = 2345+345+123+13+24+35;
2345+123+24+35 ∘ (5←5+0) = 2345+234+123+24+35;
2345+123+24+35 ∘ (1←1+0) = 2345+123+24+35+23;

Transformations which produce function in column 5 from h in column 4:
(1) 2←2+0; 4←4+0; 1↔3; (2) 2←2+0; 4←4+0; 1←1+4; 3←3+0; 5←5+2; 1↔3;

2↔4; 3↔5; (3) 1↔3; 4↔5; (5) 3←3+0; 1↔2; (6) 3←3+0; 1↔3; 3↔4; 4↔5;
(7) 5←5+0; 1↔5; 3↔4; (8) 1↔3; 2↔5; (9) 4←4+0; 1←1+2; 1↔4; 2↔5;
(10) 4←4+3; 2←2+5; 1↔4; (11) 1←1+4; (12) 1←1+2; 2↔4; (13) 3←3+0; 4←4+0;
1↔4; 2↔5; 4↔5; (15) 3←3+0; 1↔4; 2↔3; 4↔5; (16) 1←1+0; 3←3+0; 1↔4; 2↔3;
4↔5; (17) 1←1+0; 1↔5; 3↔4; 2↔5; (18) 2↔4; 3↔5; (20) 4←4+3+0; 5←5+2+0;
(23) 2↔4; 3↔5; 5←5+2+0; 1←1+0; 4←4+3+0; (24) 2↔4; 3↔5; 5←5+2+0;
1←1+0; 4←4+3+0; (26) 2↔4; 3↔5;

Table 3: Functions g from $\widehat{\mathcal{R}}^2_{1,5}$ (third column) are obtained from "canonical" using variable swaps. Transformations which produce function in column 5 from h in column 4:
(1) 2↔3; (2) 4←4+2+0; 2↔3; (3) 1←1+0; 2↔3; (4) 3←3+2+0; 1←1+2+3;
(7) 4←4+2+0; 2↔4; 3↔5; (8) 2↔4; (10) 2←2+4+0; 2↔4; 3↔5; (11) 2←2+5+0;
(13) 2←2+5+0; 5←5+3+0; 3↔5; (15) 2↔4; 3↔5; (16) 1←1+0; 2↔4; 3↔5;
(17) 1←1+0; 2↔5; 3↔4; (18) 2↔4; 3↔5; (19) 3←3+0; 1↔5; (21) 1↔5;
(23) 5←5+0; 1↔5; 2↔4; 3↔5; (24) 5←5+0; 3←3+5; 2↔4; 3↔5; (25) 4←4+0; 2↔4;
3↔5; (26) 4←4+0; 2←2+5; 2↔4; 3↔5; (27) 1↔2; 4↔5;

Table 4: Representatives f for classes 4 and 9 (column 2) are obtained from "canonical" using the following transformations: (4) 3←3+0; (9) 1←1+2;
Functions g from $\widehat{\mathcal{R}}^3_{1,5}$ (third column) are obtained from "canonical" using transformations:

123+145+23+24+35 $\circ$ (1←1+2) = 123+145+245+24+35;
123+145+245+24+35 $\circ$ (3←3+0) = 123+145+245+24+35+12;
123+145+245+24+35+12 $\circ$ (4↔5) = 123+145+245+25+34+12;
123+145+245+24+35+12 $\circ$ (2↔4; 3↔5) = 123+145+234+24+35+14;
123+145+23+24+35 $\circ$ (2↔4; 3↔5) = 123+145+45+24+35;

Transformations which produce function in column 5 from h in column 4:
(1) 3←3+0; (2) 3←3+0; (4) 1←1+0; (5) 1←1+2; 1←1+0; (6) 2←2+5+0;
3←3+4+0; 1←1+0; 2↔4; 3↔5; (7) 3←3+4; 1←1+4; 2↔4; 3↔5; (8) 2←2+5+0;
2↔4; 3↔5; (9) 5←5+0; 2←2+5+0; 2↔4; 3↔5; (11) 3←3+2; 2↔4; 3↔5; 2↔3;
(14) 2↔4; 3↔5; (15) 5←5+2+0; 3↔4; (16) 3↔4; (17) 4←4+3+0; (19) 1←1+0;
3←3+4; 2←2+5; 2↔4; 3↔5; (21) 3←3+0; 1↔4; 2↔3; 4↔5; (22) 5←5+0; 2←2+4;
2↔4; 3↔5; (23) 5←5+0; 1↔5; 3↔4; (24) 5←5+0; 5←5+2+0; 1↔5; 3↔4;
(27) 5←5+2; 1←1+0; 3←3+4;

Table 5: Functions g from $\widehat{\mathcal{R}}^4_{1,5}$ (third column) are obtained from "canonical" using variable swaps. Transformations which produce function in column 5 from h in column 4:
(2) 2↔4; (7) 2↔3; (9) 2↔3; 4↔5; (16) 1←1+0; (17) 1←1+0; (19) 3←3+0;
(21) 1↔2; 4↔5; (23) 1←1+0; (24) 1←1+0; (25) 2↔3; 4↔5; (27) 1↔3; 2↔4;

No	Representative f	g from $\widehat{\mathcal{R}}^1_{1,5}(14)$	Sum $h = f+g$	h is equal to	$C(h)$
0	0	—	—	—	—
1	2345	2345+345+123+13+24+35	123+345+13+24+35	123+145+24	25
2	2345+12	2345+345+123+13+24+35	123+345+12+13+24+35	123+145+23	24
3	2345+24	2345+123+24+35	123+35	123+14	21
4	2345+24+35	2345+123+24+35	123	←	19
5	2345+12+35	2345+123+24+35	123+12+24	123+14	21
6	2345+123	2345+234+123+24+35	234+24+35	123+14	21
7	2345+245+123*	2345+123+24+35	245+24+35	123+14	21
8	2345+123+24	2345+123+24+35	35	12	27
9	2345+123+14+13*	2345+345+123+13+24+35	345+14+24+35	123+14	21
10	2345+123+45+23*	2345+123+24+35	23+24+35+45	12	27
11	2345+123+12+35	2345+123+24+35	12+24	12	27
12	2345+123+14+35	2345+123+24+35	14+24	12	27
13	2345+123+13+45	2345+345+123+13+24+35	345+24+35+45	123+14	21
14^1	2345+123+24+35	2345+123+24+35	0	←	0
15	2345+123+145	2345+234+123+24+35	145+234+24+35	123+145+24	25
16	2345+123+145+45	2345+234+123+24+35	145+234+24+35+45	123+145+24	25
17	2345+123+145+24+45	2345+123+24+35	145+45+35	123+14	21
18	2345+123+145+24+35	2345+123+24+35	145	123	19
19	123	—	—	—	—
20	123+45	2345+123+24+35	2345+24+35+45	2345+23+45	4
21	123+14	—	—	—	—
22^2	123+24+35*	2345+123+24+35	2345	←	1
23	123+145	2345+123+24+35+23	2345+145+24+35+23	2345+123+45	10
24	123+145+23	2345+123+24+35	2345+145+24+35+23	2345+123+45	10
25	123+145+24	—	—	—	—
26^3	123+145+23+24+35	2345+123+24+35	2345+145+23	2345+123+45	10
27	12	—	—	—	—
28^4	24+35	2345+123+24+35	2345+123	←	6

Table 2 Proof of Lemma 12 for the class $\widehat{\mathcal{R}}^1_{1,5}$.

No	Representative f	g from $\widehat{\mathcal{R}}^2_{1,5}(22)$	Sum $h = f+g$	h is equal to	$C(h)$
0	0	—	—	—	—
1	2345	123+14+25	2345+123+14+25	2345+123+14+35	12
2	2345+12	123+14+25	2345+123+12+14+25	2345+123+14+35	12
3	2345+23	123+14+25	2345+123+23+14+25	2345+123+14+35	12
4	2345+25+34	123+14+25	2345+123+14+34	2345+123+14	9
5	2345+14+25	123+14+25	2345+123	←	6
6	2345+123	—	—	—	21
7	2345+123+12	123+14+25	2345+12+14+25	2345+12+34	5
8	2345+123+25	123+14+25	2345+14	2345+12	2
9	2345+123+14	—	—	—	21
10	2345+123+45	123+14+25	2345+14+25+45	2345+12+34	5
11	2345+123+12+34	123+15+34	2345+12+15	2345+12	2
12	2345+123+14+35	—	—	—	27
13	2345+123+12+45	123+15+34	2345+12+15+45+34	2345+12+34	5
14^1	2345+123+24+35	123+24+35	2345	←	1
15	2345+123+145	123+14+25	2345+145+14+25	2345+12+34	11
16	2345+123+145+45	123+14+25	2345+145+14+25+45	2345+12+34	11
17	2345+123+145+24+45	123+24+35	2345+145+35+45	2345+123+24	8
18	2345+123+145+24+35	123+24+35	2345+145	2345+123	6
19	123+235	123+14+25	235+14+25	123+45	20
20	123+45	—	—	—	—
21	123+14	123+14+25	25	12	27
22^2	123+14+25	123+14+25	0	←	0
23	123+145	123+14+25	145+14+25	123+14	21
24	123+145+23	123+14+25	145+14+25+23	123+45	20
25	123+145+24	123+15+24	145+15	123	19
26^3	123+145+23+24+35	123+15+24	145+15+23+35	123+45	20
27	14	123+14+25	123+25	123+14	21
28^4	14+25	123+14+25	123	←	19

Table 3 Proof of Lemma 12 for the class $\widehat{\mathcal{R}}^2_{1,5}$.

No	Representative f	g from $\widehat{\mathcal{R}}^3_{1,5}(26)$	Sum $h = f{+}g$	h is equal to	$C(h)$
0	0	—	—	—	—
1	2345	123+145+245+24+35+12	2345+123+145+245+24+35+12	2345+123+145+24+35	18
2	2345+12	123+145+245+24+35	2345+123+145+245+24+35+12	2345+123+145+24+35	18
3	2345+23	123+145+23+24+35	2345+123+145+24+35	←	18
4	2345+245+23+45*	123+145+245+24+35	2345+123+145+23+24+35+45	2345+123+145+24+35	18
5	2345+12+35	123+145+245+24+35+12	2345+123+145+245+24	2345+123+145+24+45	17
6	2345+123	123+145+23+24+35	2345+145+23+24+35	2345+123+45	10
7	2345+123+12	123+145+245+24+35	2345+145+245+24+35+12	2345+123+35+14	12
8	2345+123+24	123+145+23+24+35	2345+145+23+35	2345+123+45	10
9	2345+123+14+23+24*	123+145+234+24+35+14	2345+145+234+23+35	2345+123+12+45	13
10	2345+123+45	—	—	—	—
11	2345+123+12+34	123+145+245+25+34+12	2345+145+245+25	2345+123+24	8
12	2345+123+14+35	—	—	—	—
13	2345+123+12+45	—	—	—	—
14[1]	2345+123+24+35	123+145+23+24+35	2345+145+23	2345+123+45	10
15	2345+123+145	123+145+23+24+35	2345+23+24+35	2345+23+45	4
16	2345+123+145+45	123+145+45+24+35	2345+24+35	2345+23+45	4
17	2345+123+145+24+45	123+145+23+24+35	2345+23+35+45	2345+23+45	4
18	2345+123+145+24+35	—	—	—	—
19	123	123+145+23+24+35	145+23+24+35	123+45	20
20	123+45	—	—	—	—
21	123+14	123+145+234+24+35+14	145+234+24+35	123+145+24	25
22[2]	123+14+25	123+145+23+25+34	145+14+23+34	123+45	20
23	123+145	123+145+245+24+35	245+24+35	123+14	21
24	123+145+23	123+145+245+24+35	245+23+24+35	123+14	21
25	123+145+24	—	—	—	—
26[3]	123+145+23+24+35	123+145+23+24+35	0	←	0
27	35	123+145+45+24+35	123+145+45+24	123+145+23	24
28[4]	24+35	123+145+23+24+35	123+145+23	←	24

Table 4 Proof of Lemma 12 for the class $\widehat{\mathcal{R}}^3_{1,5}$.

No	Representative f	g from $\widehat{\mathcal{R}}^4_{1,5}(28)$	Sum $h = f{+}g$	h is equal to	$C(h)$
0	0	—	—	—	—
1	2345	12+34	2345+12+34	←	5
2	2345+12	12+34	2345+34	2345+23	3
3	2345+23	—	—	—	—
4	2345+23+45	23+45	2345	←	1
5	2345+12+34	—	—	—	—
6	2345+123	12+34	2345+123+12+34	←	11
7	2345+123+12	12+34	2345+123+34	2345+123+24	8
8	2345+123+24	—	—	—	—
9	2345+123+14	14+35	2345+123+35	2345+123+24	8
10	2345+123+45	12+45	2345+123+12	←	7
11	2345+123+12+34	—	—	—	—
12	2345+123+14+35	14+35	2345+123	←	6
13	2345+123+12+45	12+45	2345+123	←	6
14[1]	2345+123+24+35	24+35	2345+123	←	6
15	2345+123+145	24+35	2345+123+145+24+35	←	18
16	2345+123+145+45	23+45	2345+123+145+23	2345+123+145+45	16
17	2345+123+145+24+45	23+45	2345+123+145+24+23	2345+123+145+24+45	17
18	2345+123+145+24+35	—	—	—	—
19	123	12+45	123+12+45	123+45	20
20	123+45	—	—	—	—
21	123+14	14+25	123+25	123+14	21
22[2]	123+14+25	14+25	123	←	19
23	123+145	23+45	123+145+23+45	123+145	23
24	123+145+23	23+45	123+145+45	123+145+23	24
25	123+145+24	24+35	123+145+35	123+145+24	25
26[3]	123+145+23+24+35	24+35	123+145+23	←	24
27	12	12+34	34	12	27
28[4]	12+34	12+34	0	←	0

Table 5 Proof of Lemma 12 for the class $\widehat{\mathcal{R}}^4_{1,5}$.