Metric regularity of Reed-Muller codes *

Alexey Oblaukhov[1,2]

[1]Sobolev Institute of Mathematics, Novosibirsk, Russia
[2]Novosibirsk State University, Novosibirsk, Russia

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 proves the metric regularity of most Reed-Muller codes with known covering radius. It is conjectured that all Reed-Muller codes are metrically regular.

1 Introduction

The problem of investigating and classifying *metrically regular sets* was posed by Tokareva [14, 15] when studying metric properties of *bent functions* [11]. A Boolean function f in even number of variables m is called a *bent function* if it is at the maximal possible distance from the set of affine functions.

Bent functions have various applications in cryptography, coding theory and combinatorics [6, 15]. 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 [6]. 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. In 2012 [14], 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.

Let us briefly overview the results obtained in this area. Metric regularity of several classes of *partition set functions* is studied in [13]. The work [4] examines metric properties of self-dual bent functions. Metric regularity has been actively investigated by the author: metric complements of linear subspaces of the Boolean cube are studied in the paper [8], while the works [9] and [10] are studying possible sizes of the largest and smallest metrically regular set.

In this work we investigate metric properties of Reed-Muller codes. Among the codes of high order, covering radii of the codes $\mathcal{RM}(k,m)$, for $k \geqslant m-3$ are known. The covering radius of $\mathcal{RM}(1,m)$ for odd $m > 7$ is unknown, but has been determined for $\mathcal{RM}(1,5)$ [1] and $\mathcal{RM}(1,7)$ [7, 3]. In [12], Schatz has found the covering radius of $\mathcal{RM}(2,6)$, while recently Wang has

*The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by Russian Foundation for Basic Research (projects no. 18-07-01394, 19-31-90093) and Laboratory of Cryptography JetBrains Research.

established the covering radius of $\mathcal{RM}(2,7)$ [16]. For $m > 7$, the covering radius of $\mathcal{RM}(2,m)$ is still unknown. We prove that the codes $\mathcal{RM}(k,m)$, for $k = 0$ and $k \geqslant m-3$ and the codes $\mathcal{RM}(1,5)$ and $\mathcal{RM}(2,6)$ are metrically regular and also describe their metric complements in most cases.

2 Preliminaries

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).

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

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

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

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

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

Consider the set

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

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

Note that metrically regular sets always come in pairs, i.e. if A is a metrically regular set, then its metric complement $\widehat{A}$ is also a metrically regular set and both of them have the same covering radius. For some simple examples of metric complements and metrically regular sets, refer to [8, 9, 10].

The following trivial auxiliary lemma, established in [8], will be used throughout the paper.

Lemma 2.1 *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 is defined as:

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

where $\deg(\cdot)$ denotes the degree of the *algebraic normal form (ANF)* of the function.

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

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

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

Extended affine equivalence is more common when classifying boolean functions: functions f and g are called EA-*equivalent* if there exists a nonsingular linear transformation of variables A, a boolean vector b of length m and a function 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. We will denote this equivalence by $f \overset{k}{\sim} g$.

The Reed-Muller code of order k in m variables is usually denoted as $\mathcal{RM}(k, m)$. Since we will refer to these codes regularly, we will instead often use $\mathcal{R}_{k,m}$ to denote the Reed-Muller code of order k in m variables. We will sometimes omit the number of variables m if it is clear from the context.

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

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

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

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 must prove that for every $f \notin \mathcal{R}_{1,5}$ it holds $f + \widehat{\mathcal{R}}_{1,5} \neq \widehat{\mathcal{R}}_{1,5}$.

This is done by taking a representative f_c from every class of cosets C (aside from $\mathcal{R}_{1,5}$ itself) and showing that there exists a function $g_c \in \widehat{\mathcal{R}}_{1,5}$ such that $f_c + g_c \notin \widehat{\mathcal{R}}_{1,5}$. Since the metric complement $\widehat{\mathcal{R}}_{1,5}$ consists of EA-equivalence classes, this proves that none of the functions from the class C belong to $\widehat{\mathcal{R}}_{1,5}$. Therefore, the following holds:

Theorem 3.1 *The code $\mathcal{R}_{1,5}$ is metrically regular.*

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

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

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

5 The Reed-Muller code of order $m-3$

5.1 Covering radius

McLoughlin [5] has proved that

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

This result is reestablished by Cohen et al in the book "Covering codes" [2], using a method of syndrome matrices, different from that in [5]. This method allows us not only to obtain covering radius of the Reed-Muller code of order $m-3$, but also to describe the metric complement of this code. As with the covering radius, the cases of even and odd m are distinct.

5.2 Case m is even

In this case, the metric complement can be described as follows:

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

where

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

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

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

where g^* is some function from the class G (or from $\widehat{\mathcal{R}}_{m-3}$, since all functions in metric complement are EL^{m-3}-equivalent).

5.3 Case m is odd

In this case, the metric complement can be described as follows:

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

where

$$G_1 = \{g : \mathrm{supp}(g) = \{0, \mathrm{x}_1, \mathrm{x}_2 \ldots, \mathrm{x}_m\}, \{\mathrm{x}_1, \ldots, \mathrm{x}_m\} \text{ are linearly independent}\},$$

and

$$G_2 = \{g : \mathrm{supp}(f) = \{0, \mathrm{x}_1, \mathrm{x}_2 \ldots, \mathrm{x}_{m-1}, \mathrm{x}_1 + \ldots + \mathrm{x}_{m-1}\}, \\ \{\mathrm{x}_1, \ldots, \mathrm{x}_{m-1}\} \text{ are linearly independent}\}.$$

Same as with the case of even m, all functions in G_1 form an equivalence class with respect to the linear equivalence, so do functions from G_2. If we now choose a representative from each class, g_1^* from G_1 and g_2^* from G_2, we can describe metric complement in the following manner:

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

5.4 Metric regularity

Since the code $\mathcal{R}_{m-3}$ is linear, it follows that $\rho(\widehat{\mathcal{R}}_{m-3}) = \rho(\mathcal{R}_{m-3})$ and a function f is in $\widehat{\widehat{\mathcal{R}}}_{m-3}$ if and only if $f + \widehat{\mathcal{R}}_{m-3} = \widehat{\mathcal{R}}_{m-3}$. Thus, like in the Section 3, we 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, using the representations of metric complements obtained in the previous subsections.

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

Let us consider one other special case. If we change the order of values in the value vectors of functions so that the first half of values corresponds to the values of the function when the last variable is set to 0, and the other half corresponds to the values of the function when the last variable is set to 1, then each Reed-Muller code (for $m > 1$, $r > 0$) can be inductively defined as follows:

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

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 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.

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 $\mathcal{R}_{1,5}$. The following results heavily rely on the fact that $\mathcal{R}_{2,6}$ attains the upper bound on the covering radius provided by the $(\mathbf{u}, \mathbf{u}+\mathbf{v})$ construction, i.e. $\rho(\mathcal{R}_{2,6}) = \rho(\mathcal{R}_{2,5}) + \rho(\mathcal{R}_{1,5})$ [12].

Recall (Section 5) 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

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

The following lemma is useful when proving that $\tilde{\mathbf{u}} \in \mathcal{R}_{2,5}$:

Lemma 6.1 *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* $(\mathbf{y}, \mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}$;

This lemma tells us that for each EL^2-equivalence class of $\widehat{\mathcal{R}}_{2,5}$, either all vectors appear in the metric complement of $\mathcal{R}_{2,6}$ as the first half of the vector, or no vectors do. Since for any $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}}+\tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$ it holds $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}}+\tilde{\mathbf{v}}) + \widehat{\mathcal{R}}_{2,6} = \widehat{\mathcal{R}}_{2,6}$, it is easy to show that $\tilde{\mathbf{u}}$ must keep $\widehat{\mathcal{R}}_{2,5}$, $\widehat{\mathcal{R}}^1_{2,5}$ or $\widehat{\mathcal{R}}^2_{2,5}$ in place under addition. From the proof of the metric regularity of the code $\mathcal{R}_{m-3,m}$ for odd m it is not hard to see that only the vectors from $\mathcal{R}_{2,5}$ do that, and thus the following holds:

Proposition 6.2 *Let $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}}+\tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$. Then $\tilde{\mathbf{u}} \in \mathcal{R}_{2,5}$.*

Recall from Section 3 that $\widehat{\mathcal{R}}_{1,5}$ is composed of 4 EA-equivalence classes: $\widehat{\mathcal{R}}_{1,5} = \bigcup_{i=1}^4 \widehat{\mathcal{R}}^i_{1,5}$. Somewhat similar to Lemma 6.1, the following statement holds:

Lemma 6.3 *For each $i = 1, 2, 3, 4$ one of the following statements holds:*

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

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 6.4 *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 $\mathbf{v} + \mathbf{w} \notin \widehat{\mathcal{R}}_{1,5}$.*

These last two lemmas allow us to show that for any $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}} + \tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$, the vector $\tilde{\mathbf{v}}$ is in $\mathcal{R}_{1,5}$. Combined with Proposition 6.2, this results in the

Theorem 6.5 *Let* $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}} + \tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$. *Then* $(\tilde{\mathbf{u}}, \tilde{\mathbf{u}} + \tilde{\mathbf{v}}) \in \mathcal{R}_{2,6}$.

Since the inverse inclusion holds for any linear code, Theorem 6.5 establishes the metric regularity of the code $\mathcal{R}_{2,6}$.

7 Conclusion

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 [14], which proves the metric regularity of $\mathcal{RM}(1,m)$ for even m, we have covered all infinite families of Reed-Muller codes with known covering radius. The only other Reed-Muller codes with known covering radius, metric regularity of which has not been yet established, are $\mathcal{RM}(1,7)$ and $\mathcal{RM}(2,7)$. Given these results, we formulate the following

Conjecture 1 *All Reed-Muller codes* $\mathcal{RM}(k,m)$ *are metrically regular.*

References

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

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

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

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

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

[6] Mesnager S.: *Bent Functions: Fundamentals and Results.* Springer International Publishing, (2016).

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

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

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

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

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

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

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

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

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

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