UDC 519.7 DOI 10.17223/20710410/49/3

# ON METRIC COMPLEMENTS AND METRIC REGULARITY IN FINITE METRIC SPACES[1]

A. K. Oblaukhov

*Sobolev Institute of Mathematics, Novosibirsk, Russia,*
*Novosibirsk State University, Novosibirsk, Russia,*
*Laboratory of Cryptography JetBrains Research, Novosibirsk, Russia*

**E-mail:** oblaukhov@gmail.com

This review deals with the metric complements and metric regularity in the Boolean cube and in arbitrary finite metric spaces. Let $A$ be an arbitrary subset of a finite metric space $M$, and $\widehat{A}$ be the *metric complement* of $A$ — the set of all points of $M$ at the maximal possible distance from $A$. If the metric complement of the set $\widehat{A}$ coincides with $A$, then the set $A$ is called a *metrically regular set*. The problem of investigating metrically regular sets was posed by N. Tokareva in 2012 when studying metric properties of *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 paper, main known problems and results concerning the metric regularity are overviewed, such as the problem of finding the largest and the smallest metrically regular sets, both in the general case and in the case of fixed covering radius, and the problem of obtaining metric complements and establishing metric regularity of linear codes. Results concerning metric regularity of partition sets of functions and Reed — Muller codes are presented.

**Keywords:** *metrically regular set, metric complement, covering radius, bent function, deep hole, Reed — Muller code, linear code.*

## 1. Introduction

The problem of investigating and classifying *metrically regular sets* was posed by N. Tokareva [1, 2] when studying metric properties of *bent functions* [3]. A Boolean function in even number of variables 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 [2, 4, 5]. In cryptography, bent functions are valued because of their outstanding nonlinearity, which helps to construct S-boxes for block ciphers with high resistance to linear cryptanalysis, and, as it turned out, good diffusion properties and high resistance to differential cryptanalysis [5]. Bent functions were also used in the construction of the stream cipher Grain, being a part of a nonlinear feedback shift register [2]. 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 $\mathcal{RM}(1, m)$ in even number of variables $m$. Bent functions are used to construct Kerdock codes, which are optimal and have large code distances (see more in [5]). Bent functions also have a number of representations

[1]The work was carried out under the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by RFBR (projects no. 18-07-01394, 19-31-90093) and Laboratory of Cryptography JetBrains Research.

and relations to different combinatorial objects: Hadamard difference sets, block designs, etc. [2, 5].

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 2010 [6], N. 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. Combined with the importance of bent functions in cryptography and coding theory, this arouses the interest in studying the property of metric regularity and in the classification of metrically regular sets.

This paper deals with the metrically regular sets in the Boolean cube and in arbitrary finite metric spaces. Published results concerning the topic, as well as some currently unpublished, are overviewed.

Section 2 provides necessary basic definitions, simple examples of metrically regular sets and some of their trivial properties. Section 3 describes the results of Stănică, Sasao and Butler [7] concerning metric complements and metric regularity of *partition sets of functions*. Section 4 deals with the problem of finding the smallest and the largest metrically regular sets, both in general and in the case of fixed distance between sets [8]. *Strongly metrically regular sets* are introduced in Section 5 as a subclass of metrically regular sets. These allow one to obtain iterative constructions of metrically regular sets and get an estimate on how big the largest metrically regular set with fixed covering radius can be [9]. Section 6 touches upon the problem of describing metric complements and establishing metric regularity of linear codes. General results are presented, and the metric regularity of several families of Reed — Muller codes is established [10, 11].

## 2. Preliminaries

### 2.1. Definitions

Let $M$ be a finite discrete metric space with a metric $d(\cdot,\cdot)$, which admits values from a set $D$. From now on, every space mentioned in the paper will be a finite discrete metric space. Let $X \subseteq M$ be an arbitrary subset of the space (in this paper, whenever the symbol "$\subset$" is used, it will imply a nonempty proper subset) and $y \in M$ be an arbitrary point. The distance $\mathrm{d}(y, X)$ from the point $y$ to the set $X$ is equal to $\min\limits_{x\in X} \mathrm{d}(y, x)$. The *covering radius* of the set $X$ is defined as follows:

$$\rho(X) = \max_{z\in M} \mathrm{d}(z, X).$$

A set $X$ with the covering radius $r$ is also sometimes called a *covering code* [12] of radius $r$.

Consider the following set

$$\{y \in M : \mathrm{d}(y, X) = \rho(X)\}$$

of all vectors at the maximal possible distance from the set $X$. This set is called the *metric complement* [10] of $X$ and is denoted by $\widehat{X}$. If $\widehat{\widehat{X}} = X$, the set $X$ is said to be *metrically regular* [1].

Note that metrically regular sets always come in pairs, i.e. if $A$ is a metrically regular set, its metric complement $\widehat{A}$ is also a metrically regular set. In this paper, a pair consisting of a metrically regular set $A$ and its metric complement $B = \widehat{A}$ will sometimes be referred to as "a pair of metrically regular sets $A$, $B$".

Throughout the paper, we will mostly consider the metric space $\mathbb{F}_2^n$ of binary vectors of length $n$ equipped with the Hamming metric. The *Hamming distance* $\mathrm{d_H}(\cdot,\cdot)$ between

two binary vectors is defined as the number of coordinates in which these vectors differ, while $\mathrm{wt}(\cdot)$ denotes the *Hamming weight* of a vector, i.e., the number of nonzero values it contains. Since $\mathbb{F}_2$ is a field, $\mathbb{F}_2^n$ is also considered as a vector space with the plus sign "+" denoting addition of vectors modulo two. A *Boolean function* in $m$ variables is an arbitrary mapping from $\mathbb{F}_2^m$ to $\mathbb{F}_2$.

### 2.2. Examples and basic results

Let us consider some simple examples of metric complements and metrically regular sets in the space $\mathbb{F}_2^n$.

1) Let $X = \{x\}$ be the set consisting of one binary vector. It has covering radius $n$ and its metric complement is the set $\widehat{X} = \{x + \mathbf{1}\}$, consisting only of the opposite vector (here $\mathbf{1}$ is the all-ones vector). It follows that $\widehat{\widehat{X}} = X$, so $X$ is a metrically regular set.
2) Consider a ball of radius $r$ centered at $x$, i.e., $X = \{y \in \mathbb{F}_2^n : \mathrm{d}(x, y) \leqslant r\}$. Then the vector $x + \mathbf{1}$ will be at the distance $n - r$ from the set $X$, while any other vector will be at a smaller distance. Therefore, the covering radius of $X$ is equal to $n - r$ and its metric complement is the set $\widehat{X} = \{x + \mathbf{1}\}$. Then $\widehat{\widehat{X}} = \{x\}$, which shows us that, unless $r = 0$, the ball of radius $r$ is not a metrically regular set.

For other examples of metric complements and metrically regular sets the reader is referred to [8 – 10].

Let us return to an arbitrary metric space $M$ with a metric admitting values from a set $D$ and present some basic results concerning metric regularity.

An *automorphism* of a set $X \subseteq M$ is an isometric mapping from $M$ into $M$ which maps $X$ into itself. The following result [10] is straightforward from the definition of metric regularity, and is also described in [6, 1] for affine/bent functions.

**Theorem 1** [10]. Let $X \subset M$ be a metrically regular set. Then sets of automorphisms of $X$ and $\widehat{X}$ coincide: $\mathrm{Aut}(X) = \mathrm{Aut}(\widehat{X})$.

As we could see from examples, not every set is metrically regular, which means that we can apply the procedure of taking metric complement more than twice and obtain new sets. It has been proven [10] that this process stabilizes for any set after not more than $|D| - 1$ repetitions.

**Proposition 1** [10]. Let $X$ be an arbitrary subset of $M$. Let us denote $X_0 = X$, $X_{k+1} = \widehat{X}_k$ for $k \geqslant 0$. Then there exists a number $N \leqslant |D| - 1$ such that $X_n$ is a metrically regular set for any $n \geqslant N$.

Using this proposition, we can, for example, split the set $2^M$ of all subsets of $M$ into equivalence classes, and call two sets $X$,$Y \subseteq M$ equivalent if and only if the pair of metrically regular sets $A, A^*$, which we obtain from the set $X$ by repeatedly obtaining metric complement as in Proposition 1, coincides with the pair of metrically regular sets $B, B^*$ which we obtain from the set $Y$. How would the equivalence classes look? The description has not yet been given.

Proposition 1 is also useful when conducting experiments with metrically regular sets using computers.

## 3. Partition sets of functions

In [7], authors introduce the notion of *partition sets of functions* and study their metric complements and metric regularity.

A set $\mathcal{S}$ of Boolean functions in $m$ variables is said to be a *partition set* with respect to a partition $\mathcal{U}$ of the set $\mathbb{F}_2^m$, if the elements in the same block of $\mathcal{U}$ all map to 0 or all map to 1, and all combinations of assignments to the blocks are included in $\mathcal{S}$. Partition set functions include, for example, symmetric functions, rotation symmetric functions, self-anti-dual-functions and linear structure functions.

The following theorem presents the main result of [7], describing the covering radius and the metric complement of a partition set of functions.

**Theorem 2** [7]. Consider a partition set of functions $\mathcal{S}$, and let us denote the covering radius of $\mathcal{S}$ as $\rho_{\mathcal{S}}$. Let $N_{\mathcal{S}}$ be the number of Boolean functions at distance $\rho_{\mathcal{S}}$ from $\mathcal{S}$. Then,

$$\rho_{\mathcal{S}} = \sum_{i=1}^{l} \lfloor k_i/2 \rfloor \quad \text{and} \quad N_{\mathcal{S}} = \prod_{i=1}^{l} \frac{1}{2 - k_i \bmod 2} \left( \binom{k_i}{\lfloor k_i/2 \rfloor} + \binom{k_i}{\lceil k_i/2 \rceil} \right),$$

where $k_i$ is the cardinality of the $i$-th block of the $l$ blocks in partition $\mathcal{U}$.

The proof of the theorem is constructive and gives an explicit description of the metric complement $\widehat{\mathcal{S}}$. From this description, the equality $\widehat{\widehat{\mathcal{S}}} = \mathcal{S}$ is trivially established, showing that all partition sets of functions are metrically regular.

The authors then proceed to investigate special cases of partition sets of functions, namely, *symmetric* and *rotation symmetric* functions. They calculate covering radii for both of these sets, give characterization for the set of maximally asymmetric functions (the metric complement of the set of symmetric functions) and calculate the number of such functions. They also study the weight distribution of maximally asymmetric functions, as well as their algebraic degrees, and provide a classification of all functions with respect to the distance from the set of symmetric functions. For details, the reader is referred to [7].

## 4. Largest and smallest metrically regular sets

Let us return to affine and bent functions. Since the gap between the best known upper and lower bounds on the size of the set of bent functions is so large, it is interesting to investigate possible cardinalities of metrically regular sets, particularly, the extreme cardinalities, in an attempt to improve known bounds. The paper [8] focuses on the problem of finding the largest and the smallest metrically regular sets.

### 4.1. General problem

In the Boolean cube $\mathbb{F}_2^n$ with the Hamming distance, any smallest metrically regular set has cardinality 1, as can be seen from the simplest example $X = \{x\}$, $x \in \mathbb{F}_2^n$. For the largest metrically regular set the solution is not so trivial. The following theorem reduces the general problem to a special case.

**Theorem 3** [8]. Let $A, B \subset \mathbb{F}_2^n$ be a pair of metrically regular sets, i.e., $A = \widehat{B}$, $B = \widehat{A}$. Then there exists a pair of metrically regular sets $A^*$, $B^*$ at distance 1 from each other such that either $A \subseteq A^*$, $B \subseteq B^*$, or both $A$,$B \subseteq A^*$.

The Theorem 3 tells us that for each metrically regular set in the Boolean cube there exists a metrically regular superset with the covering radius of 1. Therefore, the covering radius of the largest metrically regular set in the Boolean cube is equal to 1. Since for any set $A$ with $\rho(A) = 1$ it holds $A \cup \widehat{A} = \mathbb{F}_2^n$, the largest metrically regular set is the metric (and ordinary) complement of the smallest metrically regular set with the covering radius equal to 1.

The problem is reduced further by the following fact.

**Proposition 2** [8]. If $C \subseteq \mathbb{F}_2^n$ is a minimal covering code of radius 1, then $C$ is metrically regular.

It follows from the Proposition 2 that any smallest covering code of radius 1 is also a smallest metrically regular set with the covering radius 1. Combined with Theorem 3, this shows that the problem of finding the largest metrically regular set is equivalent to the problem of finding the smallest covering code of radius 1. This is an open problem of coding theory [12] and is solved mostly for particular cases and small dimensions.

Proposition 2 is conjectured to hold true for larger values of the covering radius, however, this has not been proved yet.

**Conjecture 1** [8]. If $C \subseteq \mathbb{F}_2^n$ is a covering code of radius $r$ of minimal size, then $C$ is metrically regular.

The conjecture was computationally checked [8] for several minimal covering codes with $n = 2r+3, 2r+4$, where $r$ equals 2 or 3. Constructions of these codes can be found in [13, 14].

### 4.2. Fixed distances

As we see from the previous subsection, the general problems of finding the largest and the smallest metrically regular sets are reduced to the cases when the covering radius is trivial (equal to either 1 or $n$). However, the set $\mathcal{B}_m$ of bent functions in $m$ variables has the covering radius $2^{m-1} - 2^{m/2-1}$. In [8], the sizes of the sets at a fixed distance $r$ from each other are considered. Theses sizes are estimated nondirectly, through estimating the size of the union of two metrically regular sets, maximally distant one from another. Let us return to the general finite metric space $M$ with a metric $d(\cdot, \cdot)$ admitting values from a set $D$. Then, the following bound holds.

**Theorem 4** [8]. Let $A$,$B \subseteq M$ be a pair of metrically regular sets at distance $r \in D$ from each other, and let $C_k$ be the size of the largest sphere of radius $k \in D$ in $M$. Then

$$|A| + |B| \geqslant \frac{2|M|}{1 + \sum\limits_{\substack{k \in D \\ k<r}} C_k}.$$

This bound is very similar to the sphere-packing bound on the size of a code, well-known in the coding theory. In the case when the space $M$ is $\mathbb{F}_2^n$ with the Hamming metric, the bound becomes:

**Corollary 1.** Let $A$,$B \subseteq \mathbb{F}_2^n$ be a pair of metrically regular sets at distance $r$ from each other. Then

$$|A| + |B| \geqslant \frac{2^{n+1}}{1 + \sum\limits_{k=0}^{r-1} \binom{n}{k}}.$$

## 5. Strongly metrically regular sets

### 5.1. Preliminaries

Metrically regular sets are defined by their outstanding metric properties, but a lot of them possess even more regularity. In order to investigate largest and smallest metrically regular sets further, the notion of a *strongly metrically regular* set was introduced in [9].

Let $A \subset \mathbb{F}_2^n$ be a set with the covering radius $r$. The set $A$ is called *strongly metrically regular*, if for any vector $x \in \mathbb{F}_2^n$ it holds

$$\mathrm{d}(x, A) + \mathrm{d}(x, \widehat{A}) = r.$$

In other words, any vector of the Boolean cube belongs to some shortest path from the set $A$ to the set $\widehat{A}$. It is clear from the definition that any strongly metrically regular set is metrically regular.

The following pair of metrically regular sets gives us a simple example: $A = \{\mathbf{0}\}, \widehat{A} = \{\mathbf{1}\}$. Any vector $x \in \mathbb{F}_2^n$ with the Hamming weight $k$ is at distance $k$ from the set $A$ and at distance $(n-k)$ from the set $\widehat{A}$, so the sum of both distances is equal to $n$, which is the covering radius of these sets.

But not all metrically regular sets are strongly metrically regular. One of the problems of the International Cryptographic Olympiad NSUCRYPTO 2016 [15] was to find a metrically regular set which is not strongly metrically regular (or prove that such set does not exist), and several contestants managed to find a solution. The smallest known example of such a set is contained in the Boolean cube of dimension 7.

Let $A$ be an arbitrary subset of the Boolean cube $\mathbb{F}_2^n$. The *layer representation* of $\mathbb{F}_2^n$ with respect to the set $A$ is the sequence of layers defined as follows:

$$A_k = \{x \in \mathbb{F}_2^n : \mathrm{d}(x, A) = k\},\ k = 0, 1, \ldots, r,$$

where $r$ is the covering radius of $A$. Using layer representation, strongly metrically regular sets can alternatively be defined as follows:

**Proposition 3** [9]. Set $A$ is strongly metrically regular if and only if for any $k$ from 0 to $r$ it holds $A_k = \widehat{A}_{r-k}$, where $r$ is the covering radius of both sets.

It is easy to see that completely regular codes [16] are strongly metrically regular. The converse is not true: an example of a strongly metrically regular set which is not a completely regular code is the set $A = \{(000), (011), (111)\}$ in $\mathbb{F}_2^3$.

### 5.2. Iterative constructions

In [9], several iterative constructions of strongly metrically regular sets are obtained.

**Theorem 5** [9]. Let $A$ be a strongly metrically regular set with the covering radius $r$. Then $C = A \cup \widehat{A}$ is also a strongly metrically regular set.

Then this theorem is generalized to obtain more iterative constructions of strongly metrically regular sets.

**Theorem 6.** Let $A$ be a strongly metrically regular set with the covering radius $r > 0$ (case $r = 0$ is trivial). Let $i_1, \ldots, i_s$ be a sequence of indices satisfying $0 \leqslant i_1 < i_2 < \ldots < i_{s-1} < i_s \leqslant r$. Then the union $C = \bigcup\limits_{k=1}^{s} A_{i_k}$ is a strongly metrically regular set if and only if there exists a number $\rho > 0$ such that all the following conditions are satisfied:

1) for any $k \in \{1, \ldots, s-1\}$ the distance $(i_{k+1} - i_k)$ is equal to 1, $2\rho$ or $2\rho + 1$;
2) for any $k \in \{2, \ldots, s-1\}$ at least one of the distances $(i_{k+1} - i_k), (i_k - i_{k-1})$ is greater than 1;
3) $i_1$ is either $\rho$ or 0, and if $i_1 = 0$, then $i_2 - i_1 = 2\rho$ or $2\rho + 1$ if $i_2$ exists;
4) $i_s$ is either $r - \rho$ or $r$, and if $i_s = r$, then $i_s - i_{s-1} = 2\rho$ or $2\rho + 1$ if $i_{s-1}$ exists;

The number $\rho$ is the covering radius of $C$.

Theorem 6 allows one to construct many new strongly metrically regular sets with smaller covering radii given a strongly metrically regular set with the covering radius $r$. For example, consider a strongly metrically regular set with the covering radius 20. Then, if we take the union of layers with indices $\{2, 3, 7, 12, 16, 20\}$, it will be a strongly metrically regular set with the covering radius 2 and its metric complement will consist of layers with indices $\{0, 5, 9, 10, 14, 18\}$.

The number of strongly metrically regular sets with the covering radius $r$ which can be constructed using Theorem 6 is also calculated.

**Theorem 7** [9]. Let $A$ be a strongly metrically regular set with the covering radius $r > 0$. Then the number $G_\rho(r)$ of different strongly metrically regular sets with covering radius $\rho$ that can be obtained by applying Theorem 6 to the set $A$ can be calculated using the following recurrent formulas:

$$G_\rho(r) = \begin{cases} G_\rho(r-\rho) + G_\rho(r-\rho-1), & \text{when } r > \rho, \\ 2, & \text{when } r = \rho, \\ 0, & \text{when } 0 \leqslant r < \rho. \end{cases}$$

### 5.3. Special constructions and lower bounds

Utilizing Theorem 6 and other considerations, two families of "large" strongly metrically regular sets $\{Y_n^r\}$, $\{Z_n^r\}$ for $n \geqslant 2r$, $r \geqslant 1$ are constructed in [9]. Here, $Y_n^r, Z_n^r \subseteq \mathbb{F}_2^n$ and $\rho(Y_n^r) = \rho(Z_n^r) = r$. Sets from these families asymptotically cover a large part of the Boolean cube:

$$|Y_n^r| \overset{n\to\infty}{\sim} \frac{2}{2r+1}2^n, \quad |Z_n^r| = 2^{n-2r}\binom{2r}{r} \overset{r\to\infty}{\sim} \frac{1}{\sqrt{\pi r}}2^n.$$

The lower bound on the sizes of sets from the family $\{Y_n^r\}$ is obtained, which results in the following lower bound on the size of the largest metrically regular set for fixed covering radius.

**Theorem 8.** Let $A$ be the largest metrically regular set with the covering radius $r$ in the Boolean cube of dimension $n$ ($n \geqslant 2r$), and let $\rho$ be the remainder of $n+1$ divided by $2r+1$. Then

$$|A| \geqslant \max\left\{2^n\left(\frac{2}{2r+1} - \frac{2}{\sqrt{n-\rho+1}}\right), 2^{n-2r}\binom{2r}{r}\right\}.$$

Construction of the family of strongly metrically regular sets $\{Y_n^r\}$ allows one to obtain metrically regular sets with the covering radius $r$ that cover roughly the fraction $\dfrac{2}{2r+1}$ of the whole Boolean cube when $n$ is big enough, while the family $\{Z_n^r\}$ contains metrically regular sets with the covering radius $r$ that cover roughly the fraction $\dfrac{1}{\sqrt{\pi r}}$ of the Boolean cube for large values of $r$.

## 6. Metric complements and metric regularity of linear codes

### 6.1. General results

The papers [10, 11] touch upon the topic of metric complements of linear codes in the Boolean cube. First, let us formulate some basic results.

**Proposition 4.** Let $L \subseteq \mathbb{F}_2^n$ be a linear code. Then the metric complement of $L$ is the union of cosets of $L$.

This result follows directly from the equality $\mathrm{d_H}(x, y) = \mathrm{wt}(x + y)$ and the linearity of the code. The following bound is also a simple and well-known result.

**Proposition 5.** Let $L \subseteq \mathbb{F}_2^n$ be a linear code of dimension $k$. Then $\rho(L) \leqslant n - k$.

The paper [10] describes sufficient and necessary conditions on an arbitrary linear code $L$ to attain this bound, as well as some sufficient conditions for $\rho(L) = n - k - 1$ or $\rho(L) = n - k - 2$. Both of these results also present explicit form of the metric complement of the linear code in question, and in the case when $\rho(L) = n - k$, the code $L$ is found to be metrically regular.

The following characterization of the second metric complement using the first is also presented in [10, 1].

**Proposition 6.** Let $L \subseteq \mathbb{F}_2^n$ be a linear code. Then $\rho(\widehat{L}) = \rho(L)$ and a vector $x$ is in $\widehat{\widehat{L}}$ if and only if $x + \widehat{L} = \widehat{L}$.

**Corollary 2.** Let $L \subseteq \mathbb{F}_2^n$ be a linear code. Assume that $\widehat{L}$ is an affine subspace, i.e., $\widehat{L} = a + L_1$ for some linear code $L_1$. Then $\widehat{\widehat{L}} = L_1$.

### 6.2. Sets of affine/bent functions

Let us remember that the notion of a metrically regular set and the problem of investigating and classifying metrically regular sets was first posed by N. Tokareva in [1] when studying metric properties of bent functions, particularly, the duality between bent functions and affine functions.

A Boolean function in even number $m$ of variables is called a *bent function*, if it is at the maximal possible distance from the set of affine functions $\mathcal{A}_m$. If we denote the set of bent functions as $\mathcal{B}_m$, then we have, by definition, $\mathcal{B}_m = \widehat{\mathcal{A}}_m$.

Despite the fact that all characterizations of the set of bent functions that are currently known are rather ineffective when it comes to counting and constructing bent-functions, it turned out that these characterizations are enough to establish metric regularity of the set of affine/bent functions.

It follows from Proposition 6 that a linear code is metrically regular if and only if no vectors other that those from the code keep its metric complement stable under addition. This property of linear codes was used in [6, 1] to establish that the set of affine functions is the metric complement of the set of bent functions: N. Tokareva has shown that, for any non-affine function $f$, there exists a bent function $g$ (from the Maiorana — McFarland class of bent functions) such that $f + g$ is not a bent function. Thus, the following holds.

**Theorem 9.** Sets of affine functions $\mathcal{A}_m$ and bent functions $\mathcal{B}_m$ are metrically regular.

A. Kutsenko studied metric properties of two subclasses of bent functions called *self-dual* and *anti-self-dual* bent functions. In [17], he shows that the set of self-dual bent functions is the metric complement of the set of anti-self-dual bent functions and vice versa, thus establishing the metric regularity of both of these sets. Other metric properties of bent functions (e.g. the graph of minimal distances between bent functions) were also studied by N. Kolomeec in [18 – 21].

### 6.3. Reed — Muller codes

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 follows:

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

where $\deg(\cdot)$ denotes the degree of the *algebraic normal form* [2] of the function. These codes may also be represented as sets of *value vectors* of corresponding functions: binary vectors of length $2^m$, containing values which a function assumes on all vectors of $\mathbb{F}_2^m$, listed in some fixed order. Distances between functions can therefore be defined as distances between their value vectors.

The Reed — Muller code of order 1 is, by definition, the set of affine functions, which is, in the case of even number of variables $m$, metrically regular (as is its metric complement — the set of bent functions). Does this hold for other codes from this family? In [11], this metric property for other Reed — Muller codes is being investigated.

In [22], E. Berlekamp and N. Welch presented a partition of all cosets of the $\mathcal{RM}(1,5)$ code into 48 classes with respect to the EA-equivalence (extended affine equivalence), providing a representative for each class. Then they obtained weight distributions for each class of cosets. This weight distribution allows one to explicitly describe the metric complement of the code by selecting classes with the largest minimal weigth. Proposition 6 is then used to establish the metric regularity of $\mathcal{RM}(1,5)$ in [11]. It is shown that, for any equivalence class of cosets (other than the $\mathcal{RM}(1,5)$ itself), adding a function from that class to some function from the metric complement $\widehat{\mathcal{RM}}(1,5)$ yields a function outside of the metric complement, leading to the following

**Theorem 10.** The code $\mathcal{RM}(1,5)$ is metrically regular.

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. Metric regularity of the Reed — Muller code of order $m-2$ is also easy to establish as follows [11].

The Reed — Muller code of order $m-2$ has covering radius 2 [12]. By definition, it consists of all Boolean functions of degree at most $m-2$. Since all functions of degree $m$ have odd weights, and all functions of smaller degree have even weights, functions of degree $m$ are at distance 1 from $\mathcal{RM}(m-2,m)$, while functions of degree $m-1$ are at distance 2, and therefore

$$\widehat{\mathcal{RM}}(m-2,m) = \mathcal{RM}(m-1,m) \setminus \mathcal{RM}(m-2,m).$$

Since $\mathcal{RM}(m-2,m)$ is linear, $\rho(\widehat{\mathcal{RM}}(m-2,m)) = \rho(\mathcal{RM}(m-2,m)) = 2$ and thus functions of degree $m$ are at distance 1 from $\widehat{\mathcal{RM}}(m-2,m)$. It follows that $\widehat{\widehat{\mathcal{RM}}}(m-2,m) = \mathcal{RM}(m-2,m)$ and therefore the following holds:

**Theorem 11.** Codes $\mathcal{RM}(k,m)$ for $k \geqslant m-2$ are metrically regular.

Codes of order $m-3$ are harder to handle. In 1979, A. M. McLoughlin [23] has proved that

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

This result is reestablished by G. Cohen et al. in [12] using a method of syndrome matrices, different from the method in [23]. This method allows the author of [11] not only to obtain the 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.

In the case of even number $m$ of variables, the metric complement can be described as follows:

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

where

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

while, for $m$ odd, the description is as follows:

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

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

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

Then, the metric regularity of $\mathcal{RM}(m-3,m)$ is proved by establishing that no functions other that those contained in $\mathcal{RM}(m-3,m)$ preserve the metric complement under addition (once again utilizing Proposition 6).

The author then considers the code $\mathcal{RM}(2,6)$. Using a proper ordering of the values in the value vectors of functions, this code can be presented in the following manner:

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

Since both $\mathcal{RM}(2,5)$ and $\mathcal{RM}(1,5)$ were shown to be metrically regular, this constructions is useful and allows the author to establish the metric regularity of the code $\mathcal{RM}(2,6)$ as well. The proof of this result heavily relies on the fact that $\mathcal{RM}(2,6)$ attains the upper bound on the covering radius provided by the $(\mathbf{u}, \mathbf{u}+\mathbf{v})$ construction, i.e., $\rho(\mathcal{RM}(2,6)) = \rho(\mathcal{RM}(2,5)) + \rho(\mathcal{RM}(1,5))$ [24].

Thus, the metric regularity of the codes $\mathcal{RM}(1,5)$, $\mathcal{RM}(2,6)$ and of the codes $\mathcal{RM}(k,m)$ for $k \geqslant m-3$ has been established. Factoring in the result by N. Tokareva [6], which proves the metric regularity of $\mathcal{RM}(1,m)$ for even $m$, this covers 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 $\mathcal{RM}(1,7)$ [25, 26] and $\mathcal{RM}(2,7)$ [27]. Given these results, the following conjecture is formulated [11].

**Conjecture 2.** All Reed — Muller codes $\mathcal{RM}(k,m)$ are metrically regular.

## 7. Conclusion

In the paper, the main published results concerning metric complements and metric regularity are presented. Metric regularity of partition sets of functions is established. General problem of finding smallest metrically regular sets is found to be trivial, while finding the largest is shown to be as hard as finding the smallest covering code of radius 1. For fixed covering radius, a lower bounds on the sum of sizes of metrically regular sets constituting a pair is obtained. Using the notion of strongly metrically regular set, iterative constructions of metrically regular sets are described and the number of sets which can be obtained using these constructions is calculated. Two families of "large" (relative to the size of $\mathbb{F}_2^n$) metrically regular sets with fixed covering radius are constructed, giving the idea of how big the largest metrically regular sets can be. Characterizations of the first and the second metric complements of linear codes are given. Metric regularity of the Reed — Muller codes $\mathcal{RM}(1,m)$ for $m$ even, $\mathcal{RM}(k,m)$ for $k=0$, $k \geqslant m-3$ and of the codes $\mathcal{RM}(1,5)$ and $\mathcal{RM}(2,6)$ is established.

REFERENCES

1. *Tokareva N.* Duality between bent functions and affine functions. Discrete Mathematics, 2012, vol. 312, no. 3, pp. 666–670.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Academic Press, 2015. 220 p.
3. *Rothaus O. S.* On "bent" functions. J. Combin. Theory. Ser. A, 1976, vol. 20, no. 3, pp. 300–305.
4. *Cusick T. W. and Stănică P.* Cryptographic Boolean Functions and Applications. Academic Press, 2017. 288 p.
5. *Mesnager S.* Bent Functions: Fundamentals and Results. Springer International Publishing, 2016. 544 p.
6. *Tokareva N. N.* The group of automorphisms of the set of bent functions. Discrete Math. Appl., 2010, vol. 20, no. 5–6, pp. 655–664.

7. *Stănică P., Sasao T., and Butler J. T.* Distance duality on some classes of Boolean functions. J. Combin. Math. Combin. Computing, 2018, vol. 107, pp. 181–198.
8. *Oblaukhov A. K.* Maximal metrically regular sets. Siberian Electronic Math. Reports, 2018, vol. 15, pp. 1842–1849.
9. *Oblaukhov A.* A lower bound on the size of the largest metrically regular subset of the Boolean cube. Cryptogr. Commun., 2019, vol. 11, no. 4, pp. 777–791.
10. *Oblaukhov A. K.* Metric complements to subspaces in the Boolean cube. J. Appl. Industr. Math., 2016, vol. 10, no. 3, pp. 397–403.
11. *Oblaukhov A.* `https://arxiv.org/abs/1912.10811` — On metric regularity of Reed — Muller codes, 2020.
12. *Cohen G., Honkala I., Litsyn S., and Lobstein A.* Covering Codes. Elsevier, 1997, vol. 54.
13. *Cohen G., Lobstein A., and Sloane N.* Further results on the covering radius of codes. IEEE Trans. Inform. Theory, 1986, vol. 32, no. 5, pp. 680–694.
14. *Graham R. L. and Sloane N.* On the covering radius of codes. IEEE Trans. Inform. Theory, 1985, vol. 31, no. 3, pp. 385–401.
15. *Tokareva N., Gorodilova A., Agievich S., et al.* Mathematical methods in solutions of the problems presented at the Third International Students' Olympiad in Cryptography. Prikladnaya Diskretnaya Matematika, 2018, no. 40, pp. 34–58.
16. *Neumaier A.* Completely regular codes. Discrete Math., 1992, vol. 106, pp. 353–360.
17. *Kutsenko A.* Metrical properties of self-dual bent functions. Designs, Codes Cryptography, 2020, vol. 88, no. 1, pp. 201–222.
18. *Kolomeec N. A. and Pavlov A. V.* Svoystva bent-funktsiy, nakhodyashchikhsya na minimal'nom rasstoyanii drug ot druga [Properties of bent functions which are at minimal distance from each other]. Prikladnaya Diskretnaya Matematika, 2009, no. 4(6), pp. 5–20. (in Russian)
19. *Kolomeets N. A.* Enumeration of the bent functions of least deviation from a quadratic bent function. J. Appl. Industr. Math., 2012, vol. 6, no. 3, pp. 306–317.
20. *Kolomeec N. A.* Verkhnyaya otsenka chisla bent-funktsiy na rasstoyanii $2^k$ ot proizvol'noy bent-funktsii ot 2k peremennykh [Upper bound on the number of bent functions which are at distance $2^k$ from an arbitrary bent function]. Prikladnaya Diskretnaya Matematika, 2014, no. 3(25), pp. 28–39. (in Russian)
21. *Kolomeec N.* The graph of minimal distances of bent functions and its properties. Designs, Codes Cryptography, 2017, vol. 85, no. 3, pp. 395–410.
22. *Berlekamp E. and Welch N.* Weight distributions of the cosets of the $(32, 6)$ Reed — Muller code. IEEE Trans. Inform. Theory, 1972, vol. 18, no. 1, pp. 203–207.
23. *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 J. Appl. Math., 1979, vol. 37, no. 2, pp. 419–422.
24. *Schatz J.* The second order Reed — Muller code of length 64 has covering radius 18. IEEE Trans. Inform. Theory, 1981, vol. 17, no. 4, pp. 529–530.
25. *Mykkeltveit J.* The covering radius of the $(128, 8)$ Reed — Muller code is 56. IEEE Trans. Inform. Theory, 1980, vol. 26, no. 3, pp. 359–362.
26. *Hou X. D.* Covering radius of the Reed — Muller code $R(1, 7)$ — a simpler proof. J. Combin. Theory. Ser. A, 1996, vol. 74, no. 2, pp. 337–341.
27. *Wang Q.* The covering radius of the Reed — Muller code $RM(2, 7)$ is 40. Discrete Math., 2019, vol. 342, no. 12, Article 111625.