S©MR ISSN 1813-3304

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

Том 15, стр. 1842–1849 (2018) УДК 519.7
DOI 10.33048/semi.2018.15.148 MSC 94A60,06E30,68R01,05B40

MAXIMAL METRICALLY REGULAR SETS

A.K. OBLAUKHOV

Abstract. Metrically regular sets form an interesting subclass of all subsets of an arbitrary finite discrete metric space M. Let us denote $\widehat{S}$ the set of points which are at maximal possible distance from the subset S of the space M. Then S is called *metrically regular*, if the set of vectors which are at maximal possible distance from $\widehat{S}$ coincides with S. The problem of investigating metrically regular sets appears when studying *bent functions*, set of which is metrically regular in the Boolean cube with the Hamming metric. In this paper the method of obtaining metrically regular sets from an arbitrary subset of the metric space is presented. Smallest metrically regular sets in the Boolean cube are described, and it is proven that metrically regular sets of maximal cardinality in the Boolean cube have covering radius 1 and are complements of minimal covering codes of radius 1. Lower bound on the sum of cardinalities of a pair of metrically regular sets, each being metric complement of the other, is given.

Keywords: metrically regular set, metric complement, Boolean cube, minimal covering code, bent function.

1. Introduction

Metrically regular sets were first introduced in the book [3] as a part of the Boolean cube $\mathbb{F}_2^n = \{0,1\}^n$ with the Hamming metric. However, metrically regular sets can be well-defined in any finite discrete space M with a metric d admitting values from the set D. Metrically regular sets form an interesting subclass of all

Oblaukhov, A.K., Maximal metrically regular sets.

The work was supported by the Russian Foundation for Basic Research (projects no. 17-41-543364, 18-07-01394), by the Russian Ministry of Science and Education (the 5-100 Excellence Programme and the Project no. 1.12875.2018/12.1), by the program of fundamental scientific researches of the SB RAS no.I.5.1. (project no. 0314-2016-0017).

Received March, 23, 2018, published December, 30, 2018.

subsets of such metric space. Because the metric d is bounded, we can define the notion of a *metric complement* of a set — set of points which are at maximal possible distance from a given set. The metric complement of a set A is denoted by $\widehat{A}$. And, unlike with the case of the regular complementation operation, obtaining metric complement of the set $\widehat{A}$ will not necessarily yield us the set A again. But if it does, such set A is called a *metrically regular set.*

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 work a pair consisting of a metrically regular set A and its metric complement $B = \widehat{A}$ will often be referred to as "a pair of metrically regular sets A, B".

It is straightforward from Neumaier's definition [8] of completely regular codes that they are metrically regular (but the converse is not true). Metric regularity of linear subspaces of the Boolean cube is also investigated in the paper [1].

The problem of investigating metrically regular sets appeared when studying *bent functions* [4]. A Boolean function f in even number of variables is called *bent function* if it is at maximal possible distance from the set of affine functions. Thus, the set of bent functions $\mathcal{B}_n$ is a metric complement of the set of affine functions $\mathcal{A}_n$ in the Boolean cube $\mathbb{F}_2^{2^n}$ It is known that the set of affine functions is also a metric complement of the set of bent functions and therefore both sets are metrically regular [2].

Bent functions are often used in cryptography due to their high nonlinearity [9]. Many problems related to bent functions are still unsolved; in particular, the gap between the best known lower and upper bound on the number of bent functions is extremely large. In the search for better upper and lower bounds it is natural to investigate metrically regular sets with maximal or minimal cardinality.

In this work a method of obtaining a pair of metrically regular sets from an arbitrary subset of the metric space is presented.

Proposition. *Let X be an arbitrary subset of a finite metric space M. Let us denote $X_0 = X$, $X_{k+1} = \widehat{X}_k$ for $k \geqslant 0$. Then there exists a number $M \leq |D| - 1$ such that X_m is a metrically regular set for any $m \geqslant M$.*

Smallest metrically regular sets in the Boolean cube are discovered to contain only one vector. It is proven that for any metrically regular set in the Boolean cube there exists a metrically regular superset with covering radius 1. It is proven that any minimal covering code of radius 1 is a metrically regular set. Consequently, the general problem of finding largest metrically regular sets is proven to be equal to the problem of finding the smallest covering code of radius 1, which is a known open problem of the coding theory.

Lower bound on the sum of sizes of two sets which form a pair of metrically regular sets with covering radius r is obtained.

Theorem. *Let A,$B \subseteq M$ be a pair of metrically regular sets at distance $r \in D$ from each other of sizes N_1 and N_2 respectively, and let C_k be the size of the largest sphere of radius $k \in D$ in M. Then*

$$N_1 + N_2 \geqslant \frac{2|M|}{1 + \sum\limits_{\substack{k \in D \\ k < r}} C_k}.$$

2. Definitions and examples

Let M be a finite discrete metric space with a metric $d(\cdot,\cdot)$ admitting 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 set and let $y \in M$ be an arbitrary point. The distance from the point 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

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

Set X with the covering radius r is also sometimes called a *covering code* [5] of radius r.

Consider the set $Y = \{y \in\ M|d(y, X) = \rho(X)\}$ of all vectors at maximal possible distance from the set X. This set is called the *metric complement* [1] of X and is denoted by $\widehat{X}$. If $\widehat{\widehat{X}} = X$ then the set X is said to be *metrically regular* [3].

Throughout the paper we will consider a specific metric space $\mathbb{F}_2^n = \{0,1\}^n$ of binary vectors of length n with the Hamming metric. The *Hamming distance* between two vectors in this space is defined as the number of coordinates in which these vectors differ.

Let us consider some simple examples 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 $\widehat{X} = \{x \oplus \mathbf{1}\}$, consisting only of the opposite vector (here $\oplus$ denotes coordinate-wise XOR operation on vectors, and $\mathbf{1}$ is the vector consisting of all ones). 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., $X = \{y \in \mathbb{F}_2^n|d(x, y) \leqslant r\}$. Then the vector $x \oplus \mathbf{1}$ will be at distance $n - r$ from this set, while any other vector will be closer than that. So in this case, the covering radius of X is equal to $n - r$ and its metric complement is the set $\widehat{X} = \{x \oplus \mathbf{1}\}$ and $\widehat{\widehat{X}} = \{x\}$. This shows us that unless $r = 0$, ball of radius r is not a metrically regular set.

(3) An $(n-k)$-face is a set of all vectors with fixed values at chosen k coordinates. Let X be an $(n-k)$-face with values $a_1, a_2, \ldots, a_k$ at coordinates $i_1, \ldots, i_k$ respectively, where $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n$. For every vector $y \in \mathbb{F}_2^n$, there exists a vector x in the face X coinciding with y in all coordinates which are not fixed. Therefore, the distance from y to X is determined only by those coordinates of y that are fixed in the face. It is easy to see that $\rho(X) = k$ and $\widehat{X}$ is an $(n - k)$-face with opposite values in the same coordinates which are fixed in X. It follows that $\widehat{\widehat{X}} = X$, so any face is a metrically regular set.

Note that if A, B is a pair of metrically regular sets at distance r from each other, an arbitrary point x at distance k from the set A is not necessarily at distance $r-k$ from the set B. If, for example, A is the set of linear Boolean functions in even number of variables n, while B is the set of inverted linear functions, then these sets are metrical complements of each other at distance 2^{n-1} (thus they form a pair of metrically regular sets), but any bent function in n variables is at distance of at least $2^{n-1} - 2^{\frac{n}{2}-1}$ from either of these sets. This implies that the union of a pair of metrically regular sets with covering radii r is not necessarily a covering code of radius $\lfloor \frac{r}{2} \rfloor$.

3. Convergence to metrically regular sets

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. Does this process stabilize? If so, how and when? Proposition 1 answers these question.

Proposition 1. *Let X be an arbitrary subset of the space M. Let us denote $X_0 = X$, $X_{k+1} = \widehat{X}_k$ for $k \geqslant 0$. Then there exists a number $M \leq |D| - 1$ such that X_m is a metrically regular set for any $m \geqslant M$.*

Proof. Let $\rho(X)$ be equal to r. It is obvious that any point from the set X is at distance at least r from the set $\widehat{X}$. This means that $\rho(\widehat{X}) \geq r = \rho(X)$. Therefore,

$$\rho(X_0) \leq \rho(X_1) \leq \ldots \leq \rho(X_k) \leq \ldots \tag{1}$$

Because $\rho(X_k)$ admits not more than $|D|-1$ nonzero values, there exists a number N such that $\rho(X_N) = \rho(X_{N+1})$. Let us choose the smallest N satisfying this condition. Then, as was pointed out at the beginning of the proof, points of the set X_N are at distance of at least $\rho(X_N)$ from the set X_{N+1}. But we know that $\rho(X_{N+1})$ is equal to $\rho(X_N)$, hence all vectors of X_N are exactly at distance $\rho(X_N)$ from the set X_{N+1}, which means that $X_N \subseteq \widehat{X_{N+1}} = X_{N+2}$.

Note that $X_N \subseteq X_{N+2}$ implies $\rho(X_{N+2}) \leq \rho(X_N)$. Combining this with inequality 1, we can see that $\rho(X_{N+2})$ is in fact equal to $\rho(X_N)$. Using similar reasoning, we can prove that every $\rho(X_{N+k}), k > 0$ is equal to $\rho(X_N)$. So, if $\rho(X_{N+1}) = \rho(X_N)$ for some N, then $\rho(X_{N+k}) = \rho(X_N)$ for any $k > 0$. It follows that the smallest N at which such chain of equalities starts is not greater than $|D| - 2$.

Now we will use the following fact: if $A \subseteq B$ and $\rho(A) = \rho(B)$, then $\widehat{B} \subseteq \widehat{A}$. The interested reader may prove this statement. Since $\rho(X_{N+k}) = \rho(X_N)$ for all $k \geq 0$, and $\rho(X_N) = \rho(X_{N+1})$ implies $X_N \subseteq X_{N+2}$, we can also conclude that $X_{N+1} \subseteq X_{N+3}$. But using aforementioned fact we obtain $X_{N+3} = \widehat{X_{N+2}} \subseteq \widehat{X_N} = X_{N+1}$. Combining the two we see that the set X_{N+1} is equal to the set X_{N+3}, so X_{N+1} is a metrically regular set. By similar reasoning it is easy to prove that all sets X_m with $m \geq N + 1$ are metrically regular. If we denote $M := N + 1$, the number M fulfills the statement of the proposition. □

Proposition 1 tells us that if we take an arbitrary subset of the space M and iteratively apply the operation of metric complementation to it, eventually (after not more than $|D| - 1$ repetitions) we will stabilize on a pair of metrically regular sets.

Using this proposition, we can split the set $\mathcal{F}(M)$ of all subsets of M into equivalence classes, and call 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 (order of sets in the pair doesn't matter).

Proposition 1 can also be used for conducting experiments with metrically regular sets using computers.

4. Minimal and maximal metrically regular sets in the Boolean cube

Since affine and bent functions are subsets of the Boolean cube with the Hamming metric, let us consider the problem of finding the smallest and the largest metrically regular sets in this space. If x is a vector of $\mathbb{F}_2^n$, then the set $\{x\}$ of size 1 is metrically regular; therefore smallest metrically regular sets in the Boolean cube have cardinality 1. For largest metrically regular sets the solution doesn't come so easily, but we can reduce the general problem to the problem with fixed small covering radius.

Theorem 1. *Let A, B 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,$B \subseteq A^*$.*

Proof. Denote the distance between A and B as r. Consider the layer representation of $\mathbb{F}_2^n$ with respect to A: denote $A_k = \{x \in \mathbb{F}_2^n | d(x, A) = k\}$, k from 0 to r. Then $A_0 = A$, $A_r = B$. Denote

$$A^* = \bigcup_{\substack{0 \leqslant k \leqslant r,\\ k \text{ is even}}} A_k, \qquad B^* = \bigcup_{\substack{0 \leqslant k \leqslant r,\\ k \text{ is odd}}} A_k. \tag{2}$$

Note that A^* and B^* do not intersect and together cover the Boolean cube. Let us prove that $\widehat{A^*} = B^*, \widehat{B^*} = A^*$.

Let x be an arbitrary vector from B^*. Then there exists an odd number $m \geqslant 1$ such that $x \in A_m$. By definition of sets A_k, vector x is at distance 1 from $A_{m-1} \subseteq A^*$. Thus, every vector of B^* is at distance 1 from set A^*.

Let x be an arbitrary vector from A^*. Then there exists an even number m such that $x \in A_m$. If m is greater than 0, then by similar reasoning, vector x is at distance 1 from set B^*. Assume that $m = 0$, which means $x \in A$. Since $A = \widehat{B}$, there exists a path $x = x_0, x_1, \dots, x_{d-1}, x_d = y$ of length d from some vector $y \in B = A_d$ to vector $x \in A = A_0$. By definition of layer representation, an edge between sets A_i and A_j in case of $|i - j| > 1$ cannot exist. Therefore, each vector x_k from the path belongs to A_k, so the vector x_1 lies in $A_1 \subseteq B^*$. This means that $d(x, B^*) = 1$. Since x was chosen arbitrarily, every vector from A^* is also at distance 1 from set B^*.

Thus, $\widehat{A^*} = B^*$, $\widehat{B^*} = A^*$ (so A^* and B^* are metrically regular) and the covering radius of both is equal to 1. If r is odd, then $A \subseteq A^*$ and $B \subseteq B^*$, and if r is even, both A and B are contained in A^*. □

Theorem 1 tells us that for every metrically regular set in the Boolean cube there exists a metrically regular superset with maximal distance 1. Therefore the largest metrically regular set in the Boolean cube has maximal distance 1, and it is the metric (and usual) complement of the smallest metrically regular set with maximal distance 1.

5. Minimal covering codes

Recall that the *covering code* [5] of radius R is a subset of $\mathbb{F}_2^n$ with covering radius R.

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

Proof. Because C has covering radius 1, every vector of the Boolean cube is either in C or in its metric complement: $\mathbb{F}_2^n = C \cup \widehat{C}$. If $d(\widehat{C}) = 1$, then, similarly, $\mathbb{F}_2^n = \widehat{C} \cup \widehat{\widehat{C}}$, and therefore $C = \widehat{\widehat{C}}$, which means that C is metrically regular. Assume that $d(\widehat{C}) > 1$, so there exists a vector $y \in C$ such that $d(y, \widehat{C}) > 1$. This means that all neighbours (vectors at distance 1) of y are in C. But then the code $C \backslash \{y\}$ is also a covering code of radius 1, contradicting the minimality of C. □

It follows from the Proposition 2 that the smallest covering code of radius 1 is also the smallest metrically regular set with covering radius 1. Since a pair of metrically regular sets at distance 1 from each other covers the Boolean cube, the problem of finding the largest metrically regular set is equivalent to the problem of finding smallest covering code of radius 1. This is an open problem of coding theory [5].

But the set $\mathcal{B}_n$ has maximal distance $2^{n-1} - 2^{\frac{n}{2}-1}$. So let us now consider metrically regular sets at a fixed distance r from each other. Then, if $d \neq 1, n$, the problem of finding the largest and the smallest metrically regular set stands.

Conjecture 1. *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 for several minimal covering codes with $n = 2r + 3, n = 2r + 4$, where r equals 2 or 3, constructions of which can be found in [6, 7].

6. Bounds via sums

We see that the general problem of finding the smallest metrically regular set in the Boolean cube is trivial, while the general problem of finding the largest metrically regular set is reduced to the case when the covering radius of a set is equal to 1. But what about sizes of metrically regular sets at fixed distance from each other? We can estimate sizes of such sets nondirectly, by estimating the size of the union of two metrically regular sets. Here we return to the general finite metric space M with a metric $d(\cdot,\cdot)$ admitting values from the set D.

Theorem 2. *Let A,$B \subseteq M$ be a pair of metrically regular sets at distance $r \in D$ from each other of sizes N_1 and N_2 respectively, and let C_k be the size of the largest sphere of radius $k \in D$ in M. Then*

$$N_1 + N_2 \geqslant \frac{2|M|}{1 + \sum\limits_{\substack{k \in D \\ k < r}} C_k}.$$

Proof. Consider the layer representation of M with respect to A: denote $A_k = \{x \in M | d(x, A) = k\}$, $k \in D, k \leqslant r$. Then $A_0 = A$, $A_r = B$, and

$$|M| = \sum_{\substack{k \in D \\ k \leqslant r}} |A_k| = N_1 + N_2 + \sum_{\substack{k \in D \\ 0<k<r}} |A_k|. \tag{3}$$

Since every point of the space M has no more than C_k points at distance k from it,

$$|A_k| \leqslant C_k \cdot |A_0| \leqslant C_k \cdot N_1.$$

Using this bound with (3) we obtain

$$N_1 + N_2 = |M| - \sum_{\substack{k \in D \\ 0<k<r}} |A_k| \geqslant |M| - \sum_{\substack{k \in D \\ 0<k<r}} C_k \cdot N_1. \tag{4}$$

Similarly,

$$N_1 + N_2 \geqslant |M| - \sum_{\substack{k \in D \\ 0<k<r}} C_k \cdot N_2. \tag{5}$$

Adding inequalities (4) and (5), we obtain

$$2(N_1 + N_2) \geqslant 2|M| - (N_1 + N_2) \sum_{\substack{k \in D \\ 0<k<r}} C_k.$$

Grouping all terms with $N_1 + N_2$ and dividing by corresponding coefficient, we obtain the desired inequality. □

In the case when M is $\mathbb{F}_2^n$ with Hamming metric, we obtain the following bound.

Corollary 1. *Let $A,B \subseteq \mathbb{F}_2^n$ be a pair of metrically regular sets at distance r from each other of sizes N_1 and N_2 respectively. Then*

$$N_1 + N_2 \geqslant \frac{2^{n+1}}{1 + \sum\limits_{k=0}^{r-1} \binom{n}{k}}.$$

7. Conclusion

We can see that the general problem of searching for the smallest metrically regular set in the Boolean cube is trivial, while the problem of searching for the largest one can be reduced to a long standing open problem. However, in both cases the solution belongs to some (relatively) trivial class of metrically regular sets — either one-vector sets or sets with covering radius equal to 1. Therefore, to obtain more interesting results it is necessary to go from the general problem to the set of restricted subproblems — searching for the smallest or largest metrically regular set with fixed covering radius. Bound of the Theorem 2 provides first steps in this direction.

References

[1] A.K. Oblaukhov, *Metric complements to subspaces in the Boolean cube*, Journal of Applied and Industrial Mathematics, **10**:3 (2016), 397–403. MR3563718

[2] N. Tokareva, *Duality between bent functions and affine functions*, Discrete Mathematics, **312**:3 (2012), 666–670. MR2854814

[3] N. Tokareva, *Bent functions: results and applications to cryptography*, Academic Press, 2015. MR3362707

[4] O.S. Rothaus, *On "bent" functions*, Journal of Combinatorial Theory, Series A, **20**:3 (1976), 300–305. MR0403988

[5] G. Cohen et al., *Covering codes*, North-Holland Mathematical Library **54**, Amsterdam: North-Holland Publishing Co., 1997. MR1453577

[6] R.L. Graham, N. Sloane, *On the covering radius of codes*, IEEE Transactions on Information Theory, **31**:3 (1985), 385–401. MR0794436

[7] G. Cohen, A. Lobstein, N. Sloane, *Further results on the covering radius of codes*, IEEE Transactions on Information Theory, **32**:5 (1986), 680–694. MR0859092

[8] A. Neumaier, *Completely regular codes*, Discrete Mathematics, **106** (1992), 353–360. MR1181932

[9] T.W. Cusick, P. Stanica, *Cryptographic Boolean functions and applications*, Academic Press, 2017. MR3644644

Alexey Konstantinovich Oblaukhov
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: oblaukhov@gmail.com