Metrically regular subsets of the Boolean cube

Alexey Oblaukhov

Novosibirsk State University

BFA, Florence, Italy
2019

Structure of the talk

1. Definitions and examples
2. Largest and smallest metrically regular sets
3. Strongly metrically regular sets
4. Linear codes and Reed-Muller codes

Definitions

Let $\mathbb{F}_2^n$ be the space of binary vectors of length n with Hamming metric. 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 y to X is defined as $d(y, X) = \min_{x \in X} d(y, x)$. The *covering radius* of the set X is

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

Definitions

Let $\mathbb{F}_2^n$ be the space of binary vectors of length n with Hamming metric. 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 y to X is defined as $d(y, X) = \min_{x \in X} d(y, x)$. The *covering radius* of the set X is

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

Consider the set $Y = \{y \in \mathbb{F}_2^n | d(y, X) = \rho(X)\}$ of all vectors at maximal distance from X. This set is called the *metric complement* [1] of X and denoted by $\widehat{X}$. If $\widehat{\widehat{X}} = X$ then the set X is called *metrically regular* [2].

[1] Oblaukhov A. K. Metric complements to subspaces in the Boolean cube, 2016.

[2] Tokareva N. N. Bent functions: results and applications to cryptography. Academic Press. 2015.

Examples

Let $x \in \mathbb{F}_2^n$ be an arbitrary vector and $\mathbf{1}$ be the all-ones vector. Let's consider some simple examples of metric complements:

Examples

Let $x \in \mathbb{F}_2^n$ be an arbitrary vector and $\mathbf{1}$ be the all-ones vector. Let's consider some simple examples of metric complements:

- Let $X = \{x\}$. Then $\widehat{X} = \{x \oplus \mathbf{1}\}$, and $\widehat{\widehat{X}} = X$, so X is metrically regular;

Examples

Let $x \in \mathbb{F}_2^n$ be an arbitrary vector and $\mathbf{1}$ be the all-ones vector. Let's consider some simple examples of metric complements:

- Let $X = \{x\}$. Then $\widehat{X} = \{x \oplus \mathbf{1}\}$, and $\widehat{\widehat{X}} = X$, so X is metrically regular;
- Let $X = \{x, x \oplus \mathbf{1}\}$. In this case, $\widehat{X} = S_{\lceil \frac{n}{2} \rceil}(x) \cup S_{\lfloor \frac{n}{2} \rfloor}(x)$, where $S_r(x)$ is a sphere of radius r centered at x. Then $\widehat{\widehat{X}} = \{x, x \oplus \mathbf{1}\} = X$;

Examples

Let $x \in \mathbb{F}_2^n$ be an arbitrary vector and $\mathbf{1}$ be the all-ones vector. Let's consider some simple examples of metric complements:

- Let $X = \{x\}$. Then $\widehat{X} = \{x \oplus \mathbf{1}\}$, and $\widehat{\widehat{X}} = X$, so X is metrically regular;
- Let $X = \{x, x \oplus \mathbf{1}\}$. In this case, $\widehat{X} = S_{\lceil \frac{n}{2} \rceil}(x) \cup S_{\lfloor \frac{n}{2} \rfloor}(x)$, where $S_r(x)$ is a sphere of radius r centered at x. Then $\widehat{\widehat{X}} = \{x, x \oplus \mathbf{1}\} = X$;
- Let $X = B_r(x) = \{y \in \mathbb{F}_2^n | d(x, y) \leqslant r\}$. Then $\widehat{X} = \{x \oplus \mathbf{1}\}$ and $\widehat{\widehat{X}} = \{x\}$, so unless $r = 0$, ball is not metrically regular;

Examples

Let $x \in \mathbb{F}_2^n$ be an arbitrary vector and $\mathbf{1}$ be the all-ones vector. Let's consider some simple examples of metric complements:

- Let $X = \{x\}$. Then $\widehat{X} = \{x \oplus \mathbf{1}\}$, and $\widehat{\widehat{X}} = X$, so X is metrically regular;
- Let $X = \{x, x \oplus \mathbf{1}\}$. In this case, $\widehat{X} = S_{\lceil \frac{n}{2} \rceil}(x) \cup S_{\lfloor \frac{n}{2} \rfloor}(x)$, where $S_r(x)$ is a sphere of radius r centered at x. Then $\widehat{\widehat{X}} = \{x, x \oplus \mathbf{1}\} = X$;
- Let $X = B_r(x) = \{y \in \mathbb{F}_2^n | d(x, y) \leqslant r\}$. Then $\widehat{X} = \{x \oplus \mathbf{1}\}$ and $\widehat{\widehat{X}} = \{x\}$, so unless $r = 0$, ball is not metrically regular;
- Any completely regular code is metrically regular.

Bent functions

The problem of investigating metrically regular sets appeared when studying *bent functions* (Rothaus, 1976).

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 $\mathcal{A}_n$. It is known that the set of bent functions is metrically regular [3].

Bent functions are often used in cryptography due to their high nonlinearity. 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.

[3] Tokareva N. Duality between bent functions and affine functions, 2012.

Other works

Several metrically regular classes of Boolean functions were also studied by Stănică et al. in [4].

They introduce partition set functions, which include symmetric functions, rotation symmetric functions, self-anti-dual-functions, linear structure functions, and degenerate functions.

It is shown that the set $\mathcal{S}$ of partition set functions associated with a partition on the domain $\mathbb{F}_2^n$ is a metrically regular set, along with its metric complement $\widehat{\mathcal{S}}$, which is explicitly described.

They also show that the distributions of weights in $\widehat{\mathcal{S}}$ is binomial and centered at 2^{n-1}, the point at which a function is perfectly balanced.

[4] Stanica P., Sasao T., Butler J. T. Distance Duality on Some Classes of Boolean Functions.

Iterative construction

Proposition 1

Let X be an arbitrary subset of $\mathbb{F}_2^n$. Let us denote $X_0 = X$, $X_{k+1} = \widehat{X}_k$ for $k \geqslant 0$. Then there exists a number $M \leqslant n$ such that X_m is a metrically regular set for any $m \geqslant M$.

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

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

Maximal and minimal metrically regular sets

In the search of better upper and lower bounds it is natural to investigate metrically regular sets with maximal or minimal cardinality.

If x is a vector of $\mathbb{F}_2^n$, then the set $\{x\}$ of size 1 is metrically regular, therefore the smallest metrically regular set has cardinality 1.

Maximal and minimal metrically regular sets

In the search of better upper and lower bounds it is natural to investigate metrically regular sets with maximal or minimal cardinality.

If x is a vector of $\mathbb{F}_2^n$, then the set $\{x\}$ of size 1 is metrically regular, therefore the smallest metrically regular set has cardinality 1.

However, for largest metrically regular sets the answer doesn't come so easily.

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 $A, B \subseteq A^*$.

Note that if A, B is a pair of metrically regular sets at distance 1 from each other, then $A \cup B = \mathbb{F}_2^n$.

Minimal covering codes

Covering code 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 covering code of radius 1 of minimal size, then C is metrically regular.

Minimal covering codes

Covering code 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 covering code of radius 1 of minimal size, then C is metrically regular.

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.

Thus the problem of finding the largest metrically regular set is equivalent to the problem of finding smallest covering code of radius 1.

Fixed distance

But most interesting sets have covering radius greater than 1.
Let us now consider metrically regular sets at a fixed distance r from each other. Then if $r \neq 1, n$, the problem of finding the largest and the smallest metrically regular set stands.

Fixed distance

But most interesting sets have covering radius greater than 1.
Let us now consider metrically regular sets at a fixed distance r from each other. Then if $r \neq 1, n$, 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.

Conjecture has been checked on some minimal codes for $n = 2r + 3$, $n = 2r + 4$, $r = 2, 3$, constructions of which can be found in [5,6].

[5] Graham R. L., Sloane N. On the covering radius of codes, 1985.

[6] Cohen G., Lobstein A., Sloane N. Further results on the covering radius of codes, 1986.

Sum of cardinalities

We can estimate sizes of metrically regular sets at fixed distance indirectly, by estimating the size of their union.

Theorem 2

Let A, B be a pair of metrically regular sets at distance r from each other of sizes M_1 and M_2 respectively. Then

$$M_1 + M_2 \geqslant \frac{2^{n+1}}{1 + \sum\limits_{k=0}^{r-1} \binom{n}{k}}.$$

Sum of cardinalities

We can estimate sizes of metrically regular sets at fixed distance indirectly, by estimating the size of their union.

Theorem 2

Let A, B be a pair of metrically regular sets at distance r from each other of sizes M_1 and M_2 respectively. Then

$$M_1 + M_2 \geqslant \frac{2^{n+1}}{1 + \sum\limits_{k=0}^{r-1} \binom{n}{k}}.$$

For instance, for $r = 2$ we obtain the following bound:

$$M_1 + M_2 \geqslant \frac{2^{n+1}}{n+2}.$$

Strongly metrically regular sets

Metrically regular sets are defined by their outstanding metric properties, but a lot of them possess even more regularity.

Let A, B be a pair of metrically regular sets with covering radius r. Sets A and B are called *strongly metrically regular*, if for any vector $x \in \mathbb{F}_2^n$ it holds

$$d(x, A) + d(x, B) = r.$$

In other words, any vector of Boolean cube belongs to some shortest path from the set A to the set B.

Alternative definition of strongly metrically regular sets

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:

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

where r is the covering radius of A.

Alternative definition of strongly metrically regular sets

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:

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

where r is the covering radius of A.

We can now formulate an equivalent definition of a strongly metrically regular set:

Sets A and B are *strongly metrically regular* if and only if for any k from 0 to r it holds $A_k = B_{r-k}$, where r is the covering radius of both sets.

Iterative constructions of strongly metrically regular sets

Let us now consider several methods of constructing new strongly metrically regular sets using existing ones.

Theorem 3

Let A, B be a pair of strongly metrically regular sets. Then $C = A \cup B$ is also a strongly metrically regular set.

This theorem can be generalized to obtain more iterative constructions of strongly metrically regular sets.

Iterative constructions of strongly metrically regular sets

Theorem 4

Let A, B be a pair of strongly metrically regular sets with 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 $r^* > 0$ such that all the following conditions are satisfied:

1. $(i_{k+1} - i_k)$ *is equal to* 1, $2r^*$ *or* $2r^* + 1$ $\forall k : 1 \leqslant k \leqslant s - 1$;
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. $i_1 = r^*$ *or* $i_1 = 0$, *and if* $i_1 = 0$, *then* $i_2 - i_1 > 1$;
4. $i_s = d - r^*$ *or* $i_s = d$, *and if* $i_s = d$, *then* $i_s - i_{s-1} > 1$;

The number r^* is the covering radius of C.

Number of sets obtained via Theorem 4

Let us calculate the number of sequences of indices satisfying conditions of the Theorem 4 for fixed pair of strongly metrically regular sets A, B and fixed parameter r.

Theorem 5

Let A, B be a pair of strongly metrically regular sets with covering radius r. Then the number $G_{r^*}(r)$ of different strongly metrically regular sets with covering radius r^* that can be obtained by applying Theorem 4 to the pair A, B can be calculated using the following recurrent formulas:

$$\begin{cases} G_{r^*}(r) = G_{r^*}(r - r^*) + G_{r^*}(r - r^* - 1), \ \text{if } r > r^* \\ G_{r^*}(r^*) = 2 \\ G_{r^*}(r) = 0, \ \text{if } 0 \leqslant r < r^* \end{cases}$$

Number of sets obtained via Theorem 4

In the case of $r^* = 1$ we can see that the recurrence for $G_1(r)$ is of the form

$$G_1(r) = G_1(r-1) + G_1(r-2), \text{ for } r > 1,$$

which coincides with the recurrence for Fibonacci numbers. Initial values for $G_1(r)$ are twice the initial values for Fibonacci sequence. Thus,

$$G_1(r) = 2F_r = \frac{2}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^r - \left(\frac{1-\sqrt{5}}{2}\right)^r\right)$$

where F_r is r-th Fibonacci number.

Number of sets obtained via Theorem 4

In the case of $r^* = 1$ we can see that the recurrence for $G_1(r)$ is of the form

$$G_1(r) = G_1(r-1) + G_1(r-2), \text{ for } r > 1,$$

which coincides with the recurrence for Fibonacci numbers. Initial values for $G_1(r)$ are twice the initial values for Fibonacci sequence. Thus,

$$G_1(r) = 2F_r = \frac{2}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^r - \left(\frac{1-\sqrt{5}}{2}\right)^r\right)$$

where F_r is r-th Fibonacci number.

Since $A = \{\mathbf{0}\}, B = \{\mathbf{1}\}, \mathbf{0}, \mathbf{1} \in \mathbb{F}_2^n$ is a pair of strongly metrically regular sets at distance n from each other, we can easily obtain $2F_n$ metrically regular sets with covering radius 1 from it.

Construction of a large set

Using Theorem 4, we can construct a family of relatively large metrically regular sets $\{Y_n^r\}$ $(n \geqslant 2r)$, where r denotes covering radius of the set, and n denotes dimension of the Boolean cube.

One can calculate exact sizes of the sets from this family, but the formula contains complex numbers. However, asymptotic behaviour of these sizes is known:

$$|Y_n^r| \sim \frac{2}{2r+1} 2^n.$$

Moreover, we can obtain real lower bound on these sizes:

$$|Y_n^d| \geqslant 2^n \left(\frac{2}{2r+1} - \frac{2}{\sqrt{n-s+1}} \right)$$

where s is the remainder of $n+1$ divided by $2r+1$.

Construction of a large set

We can construct another large family of sets $\{Z_n^r\}$ $(n \geqslant 2r)$.

If we take the set of vectors of the weight r in the Boolean cube of dimension $2r$, we will obtain a metrically regular set of size $\binom{2r}{r}$.

Extending this set into the Boolean cube of dimension n (by mapping every vector of $\mathbb{F}_2^{2r}$ to a face in $\mathbb{F}_2^n$), we get metrically regular set Z_n^r of size

$$|Z_n^r| = 2^{n-2r}\binom{2r}{r}.$$

Since $\binom{2r}{r} \sim \frac{2^{2r}}{\sqrt{\pi r}}$, sets Z_n^r are roughly $\frac{1}{\sqrt{\pi r}}$-th of the Boolean cube, when n, r are big enough.

Lower bound on the size of the largest metrically regular set

Combining constructions from two previous slides, we can formulate the following:

Theorem 6

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 s be the remainder of $n+1$ divided by $2r+1$. Then

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

Linear codes

Now let us touch upon linear codes.

Linear codes

Now let us touch upon linear codes.

Proposition 3

If $L \subseteq \mathbb{F}_2^n$ is a linear code of dimension k, then $\widehat{L}$ is a union of shifts $a \oplus L$, and $\rho(L) \leqslant n - k$.

Linear codes

Now let us touch upon linear codes.

Proposition 3

If $L \subseteq \mathbb{F}_2^n$ is a linear code of dimension k, then $\widehat{L}$ is a union of shifts $a \oplus L$, and $\rho(L) \leqslant n - k$.

Proposition 4

Let $L \subseteq \mathbb{F}_2^n$ be a linear code. Then $x \in \widehat{\widehat{L}}$ iff $\widehat{L}$ is invariant under the shift by x, i.e. $\widehat{L} = x \oplus \widehat{L}$.

Linear codes

Now let us touch upon linear codes.

Proposition 3

If $L \subseteq \mathbb{F}_2^n$ is a linear code of dimension k, then $\widehat{L}$ is a union of shifts $a \oplus L$, and $\rho(L) \leqslant n - k$.

Proposition 4

Let $L \subseteq \mathbb{F}_2^n$ be a linear code. Then $x \in \widehat{\widehat{L}}$ iff $\widehat{L}$ is invariant under the shift by x, i.e. $\widehat{L} = x \oplus \widehat{L}$.

Corollary 7

Let $L \subseteq \mathbb{F}_2^n$ be a linear code and assume that $\widehat{L}$ is an affine subspace, i.e. $\widehat{L} = a \oplus L_1$ for some linear code L_1. Then $\widehat{\widehat{L}} = L_1$.

Reed-Muller codes

It is known that the set of affine functions $\mathcal{A}_m$ (m even), which coincides with the Reed-Muller code of the first order $RM(1, m)$, is metrically regular.

Reed-Muller codes

It is known that the set of affine functions $\mathcal{A}_m$ (m even), which coincides with the Reed-Muller code of the first order $RM(1, m)$, is metrically regular.

Proposition 5

Reed-Muller codes $RM(r, m)$ are metrically regular for $r \geqslant m - 2$.

Reed-Muller codes

It is known that the set of affine functions $\mathcal{A}_m$ (m even), which coincides with the Reed-Muller code of the first order $RM(1, m)$, is metrically regular.

Proposition 5

Reed-Muller codes $RM(r, m)$ are metrically regular for $r \geqslant m - 2$.

Conjecture 2

All Reed-Muller codes $RM(r, m)$ are metrically regular.

Open problems

- Describe possible sizes of metrically regular sets within fixed distance and connections between sizes of two sets which form a pair;

Open problems

- Describe possible sizes of metrically regular sets within fixed distance and connections between sizes of two sets which form a pair;
- Find connection between code parameters of a set and its metric complement (in general case and in case of metrically regular sets);

Open problems

- Describe possible sizes of metrically regular sets within fixed distance and connections between sizes of two sets which form a pair;
- Find connection between code parameters of a set and its metric complement (in general case and in case of metrically regular sets);
- Obtain equivalence relations and classification of metrically regular sets;

Publications

[1] **Oblaukhov A. K.** Metric complements to subspaces in the Boolean cube // Journal of Applied and Industrial Mathematics. 2016. Vol. 10. №. 3. P. 397–403.
[2] **Oblaukhov A. K.** Maximal metrically regular subsets of the Boolean cube // Siberian Electronic Mathematical Reports. 2018.
[3] **Oblaukhov A. K.** A lower bound on the size of the largest metrically regular subset of the Boolean cube // Cryptography and Communications. 2018.

Thank you for your attention!