Metrically regular subsets of the Boolean cube*

Alexey Oblaukhov[1,2]

[1]Sobolev Institute of Mathematics, Novosibirsk, Russia
[2]Novosibirsk State University, Novosibirsk, Russia
E-mail: oblaukhov@gmail.com

The talk is devoted to the problem of investigating metrically regular subsets of the Boolean cube. Let us recall some definitions. Given a subset $X \subseteq \mathbb{F}_2^n$ of the Boolean cube, its *metric complement* $\widehat{X}$ is a set of all binary vectors which are at the maximal possible distance from the set X. Then, if the set $\widehat{\widehat{X}}$ coincides with X, the set X is called *metrically regular*.

The problem of studying metrically regular sets was first posed in [1] when studying bent functions. A Boolean function f in even number of variables is called *bent function*, if it is at the maximal possible distance from the set of affine functions. Thus, the set of bent functions $\mathcal{B}_n$ is the metric complement of the set of affine functions $\mathcal{A}_n$. It is known that the set of affine functions is also the metric complement of the set of bent functions and therefore both sets are metrically regular.

Metric complements and metrically regular sets have been actively studied by the author. Particularly, in paper [3], metric complements to linear subspaces (linear codes) of the Boolean cube are studied, while paper [4] deals with metrically regular sets of maximal and minimal cardinality. Several metrically regular classes of Boolean functions are also studied in [2].

In this work, metric regularity of different classes of commonly used codes (both linear and non-linear) is investigated. In particular, metric regularity of certain Reed-Muller codes has been proven (as was mentioned above, Tokareva proved that codes $RM(1, n)$ (affine functions) are metrically regular for even n). It is also conjectured that any Reed-Muller code $RM(r, n)$ is metrically regular.

References

[1] Tokareva N. *Bent functions: results and applications to cryptography.* Acad. Press. Elsevier. 2015. 230 pages.

[2] Stănică P., Sasao T., Butler J. T. *Distance Duality on Some Classes of Boolean Functions.* Journal of Combinatorial Mathematics and Combinatorial Computing. 2018. V. 107. P. 181–198

[3] Oblaukhov A. K. *Metric complements to subspaces in the Boolean cube.* Journal of Applied and Industrial Mathematics. 2016. V. 10. No. 3. P. 397–403.

[4] Oblaukhov A. K. *A lower bound on the size of the largest metrically regular subset of the Boolean cube.* Cryptography and Communications. 2018. Published online.

*The author was supported by the Russian Foundation for Basic Research (project no. 18-31-00479), 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).