Isometric mappings of the set of all Boolean functions into itself which preserve self-duality and the Rayleigh quotient

Aleksandr Kutsenko[*]

[*]Department of Mathematics and Mechanics, Novosibirsk State University

Bent functions are Boolean functions in even number of variables that are on the maximal possible Hamming distance from the set of all affine Boolean functions. For every bent function its dual bent function is uniquely defined. A bent functions is called *self-dual* if it coincides with its dual. It is said to be *anti-self-dual* if it is equal to the complement of its dual. A mapping of the set of all Boolean functions in n variables into itself is said to be isometric if it preserves the Hamming distance. It is known that any isometric mapping of the set of Boolean functions of n variables to itself preserving the class of bent functions is a combination of an affine transformation of coordinates and a shift by an affine function [4].

In the articles [1, 3] the restricted form af an affine transformation of coordinates and an affine shift which preserve self-duality was presented. In the paper [2] the mappings which preserve bentness and the Rayleigh quotient of a Boolean function were given. In the current work we generalize the known results within isometric mappings of Boolean functions into itself.

We prove that isometric mapping preserve self-duality if and only if it preserves anti-self-duality. The complete characterization of isometric mappings which preserve self-duality is obtained. Based on this result, the set of all isometric mappings which preserve the Rayleigh quotient of a Boolean function is found. From these results we receive all isometric mappings which preserve bentness and the Hamming distance between a bent functions and its dual.

Also all isometric mappings which are bijections between the sets of self-dual and anti-self-dual bent functions are found. Based on this result, the set of all isometric mappings which change the sign of the Rayleigh quotient of a Boolean function is deduced.

From the obtained results it follows that the approach to equivalence of (anti-)self-dual bent functions that is based on the restricted form of the affine equivalence from [1, 3] is the most general one within isometric mappings.

References

[1] Carlet C., Danielson L.E., Parker M.G., Solé. P. Self-dual bent functions, Int. J. Inform. Coding Theory, **1**, 384–399 (2010).

[2] Danielsen L.E., Parker M.G., Solé.P. The Rayleigh quotient of bent functions, Springer Lect. Notes in Comp. Sci. 5921, pp. 418–432. Springer, Berlin (2009).

[3] Feulner T., Sok L., Sole P., Wassermann A. Towards the Classification of Self-Dual Bent Functions in Eight Variables. Des. Codes Cryptogr. **68**(1), 395–406 (2013).

[4] Tokareva N. N. The group of automorphisms of the set of bent functions. Discrete Mathematics and Applications. **20**(5–6), 655–664 (2010).