Magic action of o-polynomials and EA-equivalence of Niho bent functions

Diana Davidova*

Boolean functions of n variables are binary functions over the vector space F_2^n of all binary vectors of length n. Bent functions, introduced by Rothaus [1] in 1976, are Boolean functions of even number of variables n, that are maximally nonlinear in the sense that their nonlinearity, the minimum Hamming distance to all linear functions, is optimal. Bent functions have attracted a lot of research interest in mathematics because of their relation to difference sets and to designs, and in the applications of mathematics to computer science because of their relations to coding theory and cryptography. In general, bent functions are considered up to EA-equivalence, that is, functions within one class can be obtained from each other by composition from the left side by an affine permutation and by adding an affine Boolean function.

It is proven in [2] that so-called, Niho bent functions, introduced in [3], define $o-$polynomials and, conversely, every $o-$polynomial defines a Niho bent function. As further observed in the same paper, the projective equivalence of $o-$polynomials defines, for Niho bent functions, an equivalence relation called o-equivalence and, in general, the two o-equivalent Niho bent functions defined from an o-polynomial F and its inverse F^{-1} are $EA-$inequivalent. The study of $o-$equivalence was further continued in [4]. In that paper a group of transformations of order 24 preserving projective equivalence and introduced in [5] was in focus and it was discovered that there are two more transformations preserving $o-$equivalence but providing $EA-$inequivalent bent functions.

In our work we study so-called magic action, a transformation of $o-$polynomials preserving projective equivalence introduced in [6]. We check whether this transformation provides further new EAinequivalent bent functions.

References

[1] O. S. Rothaus, "On "bent" functions", J. Combin. Theory Ser. A, vol.20, no.3, pp.300-305, May 1976.

[2] C. Carlet, M.Mesnager, "On Dillon's class $\mathcal{H}$ of bent functions, Niho bent functions and $o-$polynomials, J.Combin Theory Ser A., vol.118,no.8, pp. 2392-2410, nov. 2011.

[3] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, "Construction of bent functions via Niho power functions", J. Combin. Theory Ser. A, vol. 113, no. 5, pp. 779-798, 2006.

[4] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, "On $o-$equivalence of Niho Bent functions",WAIFI 2014, Lecture Notes in Comp. Sci. 9061, pp. 155-168,2015

[5] W. Cherowitzo, "Hyperovals in Desarguesian planes of even order", Ann. DiscreteMath., 37 (1988), pp. 87-94.

[6] C. M. O'Keefe, T. Penttila, "Automorphisms groups of generalized quadrangles via an unusual action of $P\Gamma L(2, 2^h)$", Europ.J.Combinatorics, 2002, vol.23, pp.213-232.

*Uniersity of Bergen, e-mail: Diana.Davidova@uib.no