Relation between o-equivalence and EA-equivalence for Niho bent functions

Diana Davidova

Univesity of Bergen
Department of Informatics
e-mail:diana.davidova@uib.no

joint work with
Lilya Budaghyan, Claude Carlet, Tor Helleseth,
Ferdinand Ihringer and Tim Penttila

Boolean functions, and bent functions in particular, are considered up to so-called EA-equivalence, which is the most general known equivalence relation preserving bentness of functions [1, 2]. However, for a special type of bent functions, so-called Niho bent functions there is a more general equivalence relation called o-equivalence. The concept of o-equivalence is induced from the equivalence of o-polynomials and is studied in [3, 4, 5].

In the present work we identify all cases which can potentially lead to pairwise EA-inequivalent Niho bent functions derived from o-equivalence of any given Niho bent function. This allows us to determine all pairwise EA-inequivalent Niho bent functions arising from all known o-monomials via o-equivalence. For the case of o-polynomials (not necessarily o-monomials), we provide an explicit number of all pairwise EA-inequivalent Niho bent functions which can be derived from each of the known o-polynomials via o-equivalence.

In addition, we prove that every o-polynomial on F_{2^m} necessarily defines a vectorial Niho bent function from $F_{2^{2m}}$ to F_{2^m} (not just a Boolean bent Niho function as was previously known).

References

[1] L. Budaghyan and C. Carlet. CCZ-equivalence of single and multi output Boolean functions. *Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq'09*, Contemporary Math., AMS, v. 518, pp. 43-54, 2010.

[2] L. Budaghyan and C. Carlet. On CCZ-equivalence and its use in secondary constructions of bent functions. *Preproceedings of International Workshop on Coding and Cryptography WCC 2009*, pp. 19-36, 2009.

[3] 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.

[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] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, Tim Penttila, "Projective equivalence of ovals and EA-equivalence of Niho bent functions", Fourth Isree Conference, September 14-20, 2014.