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

Diana Davidova
University 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

