Quaternary bent functions and their derived boolean functions

Zoubida JADDA[1], Patrice PARRAUD[1], Soukayna QARBOUA[2]

[1] ESCC/CREC, UR Macclia,
(patrice.parraud,zoubida.jadda)@st-cyr.terre-net.defense.gouv.fr
[2] LMCA, Faculty of Sciences, University of Mohamed V Agdal, Rabat, Morocco,
qarboua.soukayna@gmail.com

The linear complexity of sequences is one of the important security measures for stream cipher systems. Recently, in the study of vectorized stream cipher systems, bent functions have been generalized to the alphabet $Z_q = Z/qZ$ and also studied by several authors. This generalization maps the classical definition of binary bent functions to generalized bent functions. Among all known constructions of generalized bent functions not a lot matter about their binary projection. We present in this paper a new construction of a family of m-variables quaternary ($\mathbb{Z}_4 = Z/4Z = \{0, 1, 2, 3\}$-valued) bent functions over Galois ring and cyclotomic classes using an intern function defined on a particular splitting of the Teichmüller set. Using a particular binary projection map we obtain a family of $2m$-variables boolean bent functions and a family of $2m + 1$-variables boolean functions with maximal nonlinerity equal to $4^m - 2^{m+1}$.