Boolean Bent and Near-Bent Function Construction and 2 Error-Correcting Codes

Jose W. Velazquez*, Heeralal Janwa, University of Puerto Rico at Rio Piedras

A function $f : F_{2^r} \to F_{2^k}$ is called a vectorial Boolean function in r variables. Whenever $k = 1$ we call these functions Boolean functions. These function's nonlinearity property is a measure of the distance to the set of affine functions (the first order Reed-Muller codes). Almost Perfect Nonlinear (APN) functions of the form $f(x) = x^d$ have good cryptographic properties and have been studied by Janwa and Wilson (1993) and Janwa, McGuire and Wilson (1996) on the construction of 2 error-correcting codes. These functions are found to be APN whenever d corresponds to the Gold or Kasami-Welch exponents under certain conditions. The conditions found are similar to the conditions for the construction of the Gold and Kasami-Welch bent and near-bent Boolean functions. These bent and near-bent functions are defined as $Tr(\alpha x^d)$, $Tr(x^d)$ respectively, with d corresponding to the Gold or Kasami-Welch exponents. The functions have high nonlinearity, and are studied for their connections to error-correcting codes. In this work, we develop algorithms to construct these functions, compare our results to known theorems and expand results by Dillon and Dobbertin on the construction of Gold bent functions. Codes derived from these functions will be used to construct Low-Density-Parity-check (LDPC) codes with fast linear-time decoding via belief propagation in Bayesian networks to improve current NASA standards.

Keywords: Error-correction, Boolean Functions, Bent functions, Cyclic-Codes