
STEVEN WANG, Carleton University

On constructing bent functions from cyclotomic mappings

There have been many developments on construction of associate schemes using nonlinear functions such as p -ary bent functions. A Boolean function f in n variables with $f(0) = 0$ is bent if and only if the Cayley graph defined on \mathbb{Z}_2^n by the support of a Boolean function is a strongly regular with parameters $(2^{2n}, 2^{2n-1} + \epsilon 2^{n-1}, 2^{2n-2} + \epsilon 2^{n-1}, 2^{2n-2} + \epsilon 2^{n-1})$, $\epsilon = \pm 1$. We study a new method of constructing Boolean bent functions from cyclotomic mappings. As a result, several new explicit infinite families of bent functions and their duals are derived.