Bent Functions, Their Generalizations and Relatives

Xiang-dong Hou
Department of Mathematics and Statistics
University of South Florida, Tampa, 33620

Abstract

A function $f : \mathbb{Z}_p^{2n} \to \mathbb{Z}_p$ is called a *bent* function if $\sum_{x\in\mathbb{Z}_2^{2n}}(-1)^{f(x)+\langle x,y\rangle} = \pm 2^n$ for all $y \in \mathbb{Z}_2^{2n}$. Bent functions arise from coding theory, cryptography, and combinatorics in various contexts. In coding theory, bent functions appear as boolean functions at the largest Hamming distance from the first order Reed-Muller code of length 2^{2n}. In cryptography, bent functions are ideal candidates for S-boxes. In combinatorics, bent functions are the indicator functions of Hadamard difference sets in $\mathbb{Z}_2^{2n}$. The notion of bent functions has been generalized for different purposes. This talk is aimed at providing a limited overview of bent functions and their generalizations and relatives. We will survey the known results, the old questions that remain open, and the new challenges that emerge.