Bent functions, semi-bent functions and o-polynomials

with S. Mesnager

Boolean functions are called bent when they lie at maximal distance to the first order Reed-Muller code $RM(1,n)$ (n even). This distance is called the nonlinearity of the function. Bent functions are characterized by the fact that their Walsh transform takes values $\pm 2^{n/2}$. play roles not only in coding theory but also in cryptography (where they can be used to design balanced functions with high nonlinearity), designs, difference sets in elementary Abelian 2-groups... Their study has been initiated in the 70's by Dillon and Rothaus in parallel with the design of the DES. One of the classes of bent Boolean functions introduced by John Dillon in his thesis is family H. While this class corresponds to a nice original construction of bent functions in bivariate form, Dillon could exhibit in it only functions which already belonged to the well-known Maiorana-McFarland class. After noticing that H can be extended to a slightly larger class that we shall denote by $\mathcal{H}$, we shall observe that the bent functions constructed via Niho power functions, which four examples are known, due to Dobbertin et al. and to Leander-Kholosha, are the univariate form of the functions of class $\mathcal{H}$. Their restrictions to the vector spaces $uF_{2^{n/2}}$, $u \in F_{2^n}^\star$, are linear. We shall answer to the open question raised by Dobbertin et al. on whether the duals of the Niho bent functions introduced in the paper are Niho bent as well. The fact that this Niho function also belongs to the Maiorana-McFarland class will bring us back to the problem of knowing whether H (or $\mathcal{H}$) is a subclass of the Maiorana-McFarland completed class. We shall then show that the condition for a function in bivariate form to belong to class $\mathcal{H}$ is equivalent to the fact that a polynomial directly related to its definition is an o-polynomial (a notion from discrete geometry) and deduce several new cases of bent functions in $\mathcal{H}$ which are potentially new bent functions and probably not affine equivalent to Maiorana-McFarland functions.

Semi-bent functions in n variables (n even) are those Boolean functions whose Walsh transforms take values in $\{0, \pm 2^{n/2}\}$. They do not have optimal nonlinearity but, contrarily to bent functions, they can be balanced, which is interesting from cryptographic viewpoint. We shall show how obtaining semi-bent functions from a function belonging to class $\mathcal{H}$ and a function from the so-called PSap class of bent functions.