Recent Results on Bent Functions

Claude Carlet
GREYC, Université de Caen and INRIA[1], France

Let n be a positive even integer. A Boolean function defined on the set V_n of all binary words of length n is called *bent* if the Walsh (i.e. discrete Fourier, Hadamard) transform $\widehat{f_\chi}(s) = \sum_{x \in V_n} (-1)^{f(x)+x \cdot s}$ of the real-valued function $f_\chi(x) = (-1)^{f(x)}$ has constant absolute value . Because of *Parseval's relation*: $\sum_{s \in V_n} \left(\widehat{f_\chi}(s)\right)^2 = 2^{2n}$, f is bent if and only if for any s, $\widehat{f_\chi}(s)$ is equal to $\pm 2^{\frac{n}{2}}$.

Equivalent definitions are the following:
- the support $\{x \in V_n \mid f(x) = 1\}$ is a difference set;
- f is at maximum Hamming distance from the Reed-Muller code of order 1;
- for any nonzero word s, the Boolean function $f(x) + f(x+s)$ is balanced (i.e. takes the values 0 and 1 equally often; the addition is in GF(2)).

The notion of bent function and the ability to produce large classes of bent functions are relevant to cryptography and to algebraic coding theory.

After having presented the recent constructions of bent functions and the characterizations of these functions in terms of finite geometries, we shall present some new directions in the attempt of classifying them and recent results on the generalizations of the notion to functions over residue class rings.

[1]INRIA, Projet Codes, Domaine de Voluceau, BP 105, 78153 Le Chesnay Cedex, France
Claude.Carlet@inria.fr