Characterizations of differentially uniform functions by the Walsh transform and related cyclic difference set-like combinatorial structures

Claude Carlet, LAGA, University of Paris 8

Let n, m and δ be positive integers, with δ even. A function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is called differentially δ-uniform if, for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^m$, the equation $F(x) + F(x + a) = b$ has at most δ solutions. Differentially 2-uniform functions are called APN.
A characterization of differentially δ-uniform functions by the Walsh transform $W_F(u, v) = \sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)+u\cdot x}$ is known only for $\delta = 2$:

$$\sum_{u,v\in\mathbb{F}_2^n;v\neq 0} W_F^4(u, v) = 2^{3n+1}(2^n - 1).$$

We shall give characterizations for any $\delta \geq 4$ and new ones for $\delta = 2$. In particular:

- Every (n, n)-function F is APN if and only if:

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^m\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} W_F^2(u_1, v_1)W_F^2(u_2, v_2)W_F^2(u_1+u_2, v_1+v_2) = 2^{5n}(2^n-1)(2^n-2),$$

- Every $(n, n-1)$-function F is differentially 4-uniform if and only if:

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^m\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} W_F^2(u_1, v_1)W_F^2(u_2, v_2)W_F^2(u_1+u_2, v_1+v_2) = 2^{5n}(2^{n-1}-1)(2^{n-1}-2).$$

We shall introduce two notions on (n, n)-functions:

- componentwise APNness, for which the arithmetic mean of $W_F^4(u, v)$ when $u \in \mathbb{F}_2^n$ and v is fixed nonzero in $\mathbb{F}_2^n$ equals 2^{2n+1},
- componentwise Walsh uniformity, for which the arithmetic mean of $W_F^2(u_1, v_1)W_F^2(u_2, v_2)W_F^2(u_1 + u_2, v_1 + v_2)$ when $u_1, u_2 \in \mathbb{F}_2^n$ and v_1, v_2 are fixed nonzero and distinct in $\mathbb{F}_2^m$, equals 2^{3n}.

We shall study these notions, prove that quadratic and Kasami APN functions are componentwise Walsh uniform, as well as the inverse of one of the Gold functions, and deduce a new property of Kasami functions related to the difference set property proved by Dillon and Dobbertin in [New cyclic difference sets with Singer parameters, FFA 2004].