Partially APN Functions with APN-like Polynomial Representations

Pante Stănică*

(joint work with Lilya Budaghyan, Nikolay Kaleyski, Constanza Riera)

*Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943-5212, U.S.A.

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. We call a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ a *Boolean function* on n variables and denote the set of all such functions by $\mathcal{B}_n$. For a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ we define the *Walsh-Hadamard transform* to be the integer valued function $\mathcal{W}_f(u) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ux)}$, where $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function, $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

An (n, m)-*function* (often called a *vectorial Boolean function* if there is no need to explicitly specify the dimensions n and m) is a map $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. When $m = n$, it can be represented as a univariate polynomial over $\mathbb{F}_{2^n}$ (using the natural identification of the finite field $\mathbb{F}_{2^n}$ with the vector space $\mathbb{F}_2^n$) of the form $F(x) = \sum_{i=0}^{2^n-1} a_i x^i,\ a_i \in \mathbb{F}_{2^n}$. The algebraic degree of the function is then the largest Hamming weight of an exponent i, with $a_i \neq 0$. For an (n, m)-function F, we define the Walsh transform $W_F(a, b)$ to be the Walsh-Hadamard transform of its component function $\mathrm{Tr}_1^m(bF(x))$ at a, that is, $W_F(a, b) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^m(bF(x))+\mathrm{Tr}_1^n(ax)}$.

For an (n, n)-function F, and $a, b \in \mathbb{F}_{2^n}$, we let $\Delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} : F(x+a)+F(x) = b\}|$. We call the quantity $\Delta_F = \max\{\Delta_F(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\}$ the *differential uniformity* of F. If $\Delta_F \leq \delta$, then we say that F is differentially δ-uniform. If $\delta = 2$, then F is an *almost perfect nonlinear* (*APN*) function. There are several equivalent characterizations of APN-ness. For example, F is APN if and only if $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^4(a, b) = 2^{3n+1}(3 \cdot 2^{n-1} - 1)$, if and only if $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a, b) = 2^{2n+1}(3 \cdot 2^{n-1} - 1)$ (under $F(0) = 0$), if and only if all the points x, y, z satisfying $F(x) + F(y) + F(z) + F(x + y + z) = 0$, belong to the curve $(x + y)(x + z)(y + z) = 0$ (we call this last one, the Rodier condition).

Along with S. Kwon, we previously introduced a notion of partial APN-ness in an attempt to resolve a conjecture on the upper bound on the algebraic degree of APN functions. For a fixed $x_0 \in \mathbb{F}_{2^n}$, we call an (n, n)-function a (*partial*) x_0-*APN function* (which we typically refer to as simply x_0-APN, or just partially APN) if all points, x, y, satisfying $F(x_0) + F(x) + F(y) + F(x_0 + x + y) = 0$ (Rodier equation) belong to the curve $(x_0 + x)(x_0 + y)(x + y) = 0$.

Certainly, an APN function is x_0-APN for any point x_0. An alternative way to express the fact that a given function F is x_0-APN is to say that for any $a \neq 0$ the equation $F(x+a)+F(x) = F(x_0 + a) + F(x_0)$ has only two solutions x, namely x_0 and $x_0 + a$.

Here, we theoretically and experimentally investigate the partial APN-ness of monomial functions, which are known to be APN under certain conditions, and removing those constraints, we find when they can be partially APN. We also show that the binomial $F(x) = x^{2^n-1} + x^{2^n-2}$ over $\mathbb{F}_{2^n}$ is 1-APN but not 0-APN for $n \geq 3$. We further derive some conditions under which a polynomial of the form $F(x) = x(Ax^2 + Bx^q + Cx^{2q}) + x^2(Dx^q + Ex^{2q}) + Gx^{3q}$ for $q = 2^k$ with $1 \leq k \leq n - 1$ is (not) partial APN (this class of polynomials was suggested by Dillon as containing potential APN or differentially 4-uniform functions). Since every APN function is 0-APN as well, some of the results we obtain can be seen as non-existence results for APN functions.