Partially APN Functions with APN-like Polynomial Representations

Pante Stanica
(joint work with L. Budaghyan, N. Kaleyski, C. Riera)

Department of Applied Mathematics
Naval Postgraduate School
Monterey, CA 93943, USA; pstanica@nps.edu
*Also associated to IMAR (Institute of Mathematics of the Romanian Academy)

Some Notations & Definitions I

- $\mathbb{F}_{2^n}$ is the finite field with 2^n elements, often identified with the vector space of tuples $\mathbb{F}_2^n$
- Boolean functions: $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$
- $\mathcal{B}_n$ = the set of all Boolean functions on n variables.
- The *Walsh–Hadamard transform* of $f \in \mathcal{B}_n$ is

$$\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n(u \cdot x)},$$

  $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function, given by $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.
- $\mathcal{W}_f$ satisfies *Parseval's relation* $\sum_{a \in \mathbb{F}_{2^n}} \mathcal{W}_f(a)^2 = 2^{2n}$.

Some Notations & Definitions II

- $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a vectorial Boolean, or (n, m)-function;
- When $m = n$, F can be uniquely represented as a univariate polynomial $F(x) = \sum_{i=0}^{2^n-1} a_i x^i,\ a_i \in \mathbb{F}_{2^n}$ (using the natural identification of $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$);
- Walsh transform $\mathcal{W}_F(a, b)$ is the Walsh-Hadamard transform of its component fcts. $\mathrm{Tr}_1^m(bF(x))$ at a, i.e.,

$$\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^m(bF(x)) + \mathrm{Tr}_1^n(ax)}, a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}.$$

- F is called an *almost perfect nonlinear* (*APN*) function if $\#\{x \in \mathbb{F}_{2^n} : F(x + a) + F(x) = b\} \leq 2$.

Characterizations of the APN property: F be an (n, n)-function

(i) $$\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^4(a,b) \geq 2^{3n+1}(3\cdot 2^{n-1}-1); \text{ “}=\text{” iff } F \text{ is APN;}$$

(ii) if F is APN & $F(0)=0$, then
$$\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b) = 2^{2n+1}(3\cdot 2^{n-1}-1);$$

(iii) (Rodier Condition) F is APN 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 surface $(x+y)(x+z)(y+z)=0$.

Partial APN functions

Definition

Let $x_0 \in \mathbb{F}_{2^n}$. We call an (n, n)-function F a *(partial) x_0-APN function* (pAPN) if all u, v with $F(x_0) + F(u) + F(v) + F(x_0 + u + v) = 0$ are on the curve $(x_0 + u)(x_0 + v)(u + v) = 0$.

- Our proposal for the partial APN concept comes from a study of the conjecture of Budaghyan, Carlet, Helleseth, Li, Sun, which claims that for $n \geq 3$ an APN function modified at a point cannot remain APN.

Connection to the partial APN property?

$$F'(x) = \begin{cases} F(x) & \text{if } x \neq x_0 \\ y_1 & \text{if } x = x_0. \end{cases}$$

Theorem (Budaghyan-Kaleyski-Kwon-Riera-S. 2018)

If F is APN and its (x_0, y_1)-modification F' with $y_1 \neq F(x_0)$ is x_0-APN, then F' is APN.

In light of this, the conjecture of Budaghyan et al. can be strengthened:

Conjecture (Budaghyan-Kaleyski-Kwon-Riera-S. 2018)

An (x_0, y_1)-modification of an APN function with $y_1 \neq F(x_0)$ is not x_0-APN.

Partial APN – necessary and sufficient condition

In case you wonder... or not

Theorem (Budaghyan-Kaleyski-Kwon-Riera-S. 2018)

Let F be an (n, n)-function and $x_0 \in \mathbb{F}_{2^n}$. Then F is x_0-APN iff

$$\sum_{a,b \in \mathbb{F}_{2^n}} \mathcal{W}_F^3(a, b)(-1)^{\mathrm{Tr}_1^n(ax_0 + bF(x_0))} = 2^{2n+1}(3 \cdot 2^{n-1} - 1).$$

Code associated to a pAPN function I

- There is a connection between a partial APN function and the code associated to it;
- [Carlet-Charpin-Zionviev '98] Let $F(x) = \sum_{j=0}^{2^n-1} \gamma_j x^j$ on $\mathbb{F}_{2^n}$, $F(0) = 0$, and $\mathcal{C}_F$ be the $[2^n - 1, k, d]$ linear code generated by the matrix

$$C_F = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^n-2} \\ F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{2^n-2}) \end{pmatrix},$$

  (with entries viewed in the vector space $\mathbb{F}_2^n$).
- Codewords of $\mathcal{C}_F$: $Tr(a\,x) + Tr(b\,F(x))$, $a, b \in \mathbb{F}_{2^n}$;

Code associated to a pAPN function II

- The minimum distance of $\mathcal{C}_F$ is $3 \leq d \leq 5$;
- Further:
  1. $d = 5$ if and only if F is APN;
  2. $d = 4$ iff there exist *distinct* nonzero x, y, z, w s.t. $x + y + z + w = 0$ & $F(x) + F(y) + F(z) + F(w) = 0$;
  3. $d = 3$ iff there exist *distinct* x, y, z s.t. $x + y + z = 0$ & $F(x) + F(y) + F(z) = 0$;
- Thus, if F with $F(0) = 0$ is x_0-APN, but not APN, then $\mathcal{C}_F$ has distance either 3, or 4;
  1. E.g., $F(x) = x^3 + \mathrm{Tr}_1^5(x^7)$ is $0, 1$-APN on $\mathbb{F}_{2^5}$; $\mathcal{C}_f$ has $d = 4$;
  2. E.g., $F(x) = x^3 + x^{127}$ on $\mathbb{F}_{2^6}$ is x_0-APN for for 64 values on $\mathbb{F}_{2^7}$; $\mathcal{C}_f$ has $d = 3$;

The pAPN spectrum (size) is a CCZ invariant

Theorem (Budaghyan-Kalyesky-Riera-S. '19)

The size of the pAPN spectrum is preserved under the CCZ equivalence. More precisely, if $\mathcal{A}$ is the CCZ isomorphism, and denoting the respective pAPN spectra of F, G by S_F, S_G, then, if $x_0 \in S_F$, and $(\tilde{x}_0, G(\tilde{x}_0)) = \mathcal{A}(x_0, F(x_0))$, we have that $\tilde{x}_0 \in S_G$.

Monomial partial APN functions

Theorem (Budaghyan-Kaleyski-Kwon-Riera-S. 2018)

Let $\mathbb{F}_{2^n}$ be the extension field of $\mathbb{F}_2$ corresponding to the primitive polynomial f of degree n and let ζ be one of the (primitive) roots of f. Then (with $\binom{a}{b}_2 :\equiv \binom{a}{b} \pmod 2$):

- (i) *Let $F(x) = x^m$ over $\mathbb{F}_{2^n}$. Then F is APN if and only if F is 0-APN and x_1-APN for some $x_1 \in \mathbb{F}_{2^n}^*$.*
- (ii) *if $F(x) = x^m$ over $\mathbb{F}_{2^n}$, then F is 0-APN if and only if for $1 \le i \le 2^n - 1$, the minimal polynomial of ζ^i, $\prod_{j \in C_i}(X - \zeta^j) \nmid \sum_{k=1}^{mi-1} \binom{mi}{k}_2 X^{mi-k-1}$, where $C_i = \{(i \cdot 2^j) \pmod{2^n - 1) : j = 0, 1, \ldots\}$ is the unique cyclotomic coset of i modulo $2^n - 1$;*

General Gold, Kasami, Niho, Bracken-Leander, etc. I

Theorem (Budaghyan-Kaleyski-Riera-S. 2019)

(☺) *Let* $F(x) = x^{2^d-1}$ *over* $\mathbb{F}_{2^n}$, *where* $\gcd(d-1, n) = 1$, *then* F *is* 0*-APN;*

(3) $F(x) = x^\ell$ *with* $\ell = 3 \cdot 2^k$ *are the only power functions which are* 0*-APN over any extension of* $\mathbb{F}_2$. *All other power functions are* 0*-APN over infinitely many extensions of* $\mathbb{F}_2$. *They are also not* 0*-APN over infinitely many dimensions.*

(5) *Let* $f_1(x) = x^{2^t+1}$ *be the Gold function on* $\mathbb{F}_{2^n}$ *(APN when* $\gcd(t, n) = 1$*). Then* f_1 *is not* x_0*-APN for any* $x_0 \in \mathbb{F}_{2^n}$, *if* $\gcd(n, t) = d > 1$.

General Gold, Kasami, Niho, Bracken-Leander, etc. II

Theorem (Budaghyan-Kaleyski-Riera-S. 2019)

(17) *Let* $f_2(x) = x^{2^r - 2^t + 1}$, $r > s$ *(gen. Kasami). Then,* f_2 *is* 0*-APN iff* $\gcd(t, n) = \gcd(r - t, n) = 1$. *Moreover, if* $d = \gcd(t, r - t, n) > 1$, *then* f_2 *is not* ζ^k*-APN, where* ζ *is a* $(2^n - 1)$*-primitive root of unity, and* $k \equiv 0 \pmod{\frac{2^n-1}{2^d-1}}$.

(257) *Let* $f_3(x) = x^{2^r + 2^t - 1}$, $r > t$, *be the generalization of the Niho function* $x \to x^{2^{2t} + 2^t - 1}$ *over* $\mathbb{F}_{2^n}$ *(known to be APN for* $n = 2r + 1$, $2t = r$, *or* $n = 2t + 1$, $2r = 3t + 1$*). Then* f_3 *is* 0*-APN iff* $\gcd(r, n) = \gcd(t, n) = 1$. *(For* $t = 2$, *this includes* $f(x) = x^{2^r + 3}$, *the Welch function; known to be APN for* $n = 2r + 1$*).*

General Gold, Kasami, Niho, Bracken-Leander, etc. III

Theorem (Budaghyan-Kaleyski-Riera-S. 2019)

(65537) *Let* $f_4(x) = x^{2^{2t}+2^t+1}$ *(gen. Bracken-Leander) over* $\mathbb{F}_{2^{2n}}$. *If* t *is odd, then* f_4 *is not* 0*-APN. If* $n = 2t$ *and* t *is even, then* f *is* 0*-APN.*

4967297) *Let* $f_5(x) = x^{2^n-2^s}$. *Then,* f_5 *is* 0*-APN if and only if* $\gcd(n, s+1) = 1$. *In particular, for* $s = 1$, $f_5(x) = x^{-1}$ *is the inverse function (extended to* $\mathbb{F}_{2^n}$ *by setting* $0^{-1} = 0$*) which is known to be APN for* n *odd.*

Theorem (Budaghyan-Kaleyski-Riera-S. 2019)

Let $F(x) = x^{2^n-1} + x^{2^n-2}$ *be on* $\mathbb{F}_{2^n}$. *Then* F *is* 1*-APN, but not* 0*-APN, for all* $n \geq 3$. *Further,* F *is differentially* 4*-uniform.*

Go2Tks

Non pAPN (hence non APN) functions I

In a series of papers (2009–), Rodier et al. found several classes of functions that are never APN for infinitely many extensions of $\mathbb{F}_2$. We continued this work and extended some of Rodier's classes.

Theorem (Budaghyan-Kaleyski-Kwon-Riera-S. 2018)

- *Let L be a linear poly on $\mathbb{F}_{2^n}$, g primitive in $\mathbb{F}_{2^n}$ and $d \geq 1$. Let $F(x) = L\left(x^{2^d+1}\right) + \mathrm{Tr}_1^n(x^3)$, $G(x) = L\left(x^{2^{d+1}+2^d+1}\right) + \mathrm{Tr}_1^n(x^3)$. If $\gcd(d,n) > 1$, then neither F nor G is 0-APN.*
- *Let L_1, L_2 be linear on $\mathbb{F}_{2^n}$. If $\gcd(d,r,n) > 1$, then $L_1(x^{2^d+1}) + L_2(x^{2^r+1})$ is not 0-APN. Further $x^{2^d+1} + \mathrm{Tr}_1^n(x^{2^r+1})$ is not 0-APN if $\gcd(d,n) > 1$ and $\gcd(2^r+1, 2^n-1) = 1$, or $\gcd(d,r,n) > 1$. If $\gcd(d,s,n) > 1$, then $L_1\left(x^{2^{d+1}+2^d+1}\right) + L_2\left(x^{2^{s+1}+2^s+1}\right)$ is not 0-APN.*

Non pAPN (hence non APN) functions II

Theorem (Leander-Rodier, 2011)

If $n \geq 2$ and d is a nonzero integer which is not a power of 2, then the function

$$F(x) = x^{2^n-2} + \beta x^d$$

over $\mathbb{F}_{2^n}$ is not APN for $d \leq 29$ and any $\beta \in \mathbb{F}_{2^n}^*$.

Theorem (Budaghyan-Kaleyski-Kwon-Riera-S. 2018)

Let $a > b$ be positive integers. Assuming that one of x^a and x^b are 0-APN on $\mathbb{F}_{2^n}$ and $\gcd(a-b, 2^n-1) = 1$, the polynomial $x^a + \beta x^b$ is not 0-APN for any $\beta \in \mathbb{F}_{2^n}^*$.

pAPN and Dillon polynomial I

- Dillon suggested investigating functions of the form (n even)

$$F(x) = x(Ax^2+Bx^q+Cx^{2q})+x^2(Dx^q+Ex^{2q})+Gx^{3q}, q = 2^{n/2},$$

as candidates for APN or differentially 4-uniform functions.

- We took $q = 2^k$ and $q = 2^k + 1$, for arbitrary k, and investigated the pAPN property.
- Below we give a sample (for $q = 2^k + 1$, since if $q = 2^k$ they are all quadratic and the proofs are simpler).

pAPN and Dillon polynomial II

Theorem (Budaghyan-Kaleyski-Kwon-Riera-S. 2019)

Let $1 \le k \le n-1$. The following statements hold:

(1) $F_1(x) = Ax^3 + Cx^{2^{k+1}+3}$ *(respectively,* $F_2(x) = Ax^3 + Cx^{2^k+3}$*) is not* 0*-APN.*

(2) *The functions* $F_3(x) = Ax^3 + Gx^{2^{k+1}+2^k+3}$ *is not* 0*-APN if n is odd; if n is even, then F_3 is* 0*-APN if and only if* $\left(\frac{A}{G}\right)^{2^{-k}} \notin \mathbb{F}_{2^2}^*$.

(3) *Under* $\gcd(2^k+1, 2^n-1) = 1$*, which happens if n is odd, or* $n \equiv 2 \pmod 4$ *and k is even, then* $F_4(x) = Bx^{2^k+2} + Cx^{2^{k+1}+3}$ *is not* 0*-APN.*

(5) $F_5(x) = Bx^{2^k+2} + Dx^{2^k+3}$ *is never* 0*-APN.*

pAPN and Dillon polynomial III

Theorem (Budaghyan-Kaleyski-Kwon-Riera-S. 2019)

(8) *Under* $\gcd(2^{k+1}+1, 2^n-1) = 1$ *(which happens if n is odd, or $n \equiv 2 \pmod 4$ and k is odd), then* $F_6(x) = Bx^{2^k+2} + Gx^{2^{k+1}+2^k+2+1}$ *is not* 0*-APN.*

(13) $F_7(x) = Cx^{2^{k+1}+3} + Dx^{2^k+3}$, $F_8(x) = Cx^{2^{k+1}+3} + Ex^{2^{k+1}+4}$, $F_9(x) = Cx^{2^{k+1}+3} + Gx^{2^{k+1}+2^k+2+1}$, $F_{10}(x) = Dx^{2^k+3} + Gx^{2^{k+1}+2^k+2+1}$ *are never* 0*-APN.*

(21) *Under* $\gcd(2^k+1, 2^n-1) = 1$*, which happens if n is odd, or $n \equiv 2 \pmod 4$ and k is even, then* $F_{11}(x) = Dx^{2^k+3} + Ex^{2^{k+1}+4}$ *is not* 0*-APN.*

(34) *Under* $gcd(k, n) = 1$, $F_{12}(x) = Ex^{2^{k+1}+4} + Gx^{2^{k+1}+2^k+2+1}$ *is not* 0*-APN.*

Power functions $F(x) = x^i$ over $\mathbb{F}_{2^n}$ that are 0-APN, but not APN

n	Exponents i	Δ_F
1-5	-	-
6	27	12
7	7,21,31,55	6
	19,47	4
8	15,45	14
	21,111	4
	51	50
	63	6
9	7, 21, 35, 61, 63, 83, 91, 111, 117, 119, 175	6
	41, 187	8
	45, 125	4
10	15, 27, 45, 75, 111, 117, 147, 189, 207, 255	6
	21, 69, 87, 237, 375	4
	231, 363, 495	42
	105, 351	10
	93	92
	447	12
	51	8
11	7, 11, 15, 21, 29, 31, 37, 47, 49, 51, 53, 55, 67, 71, 73, 75, 81, 83, 85, 99, 101 103, 111, 113, 121, 125, 127, 137, 139, 149, 153, 155, 157, 159, 167, 171, 173 179, 181, 185, 187, 189, 191, 201, 203, 205 ,213, 215, 217, 219, 221, 223, 229 247, 255, 293, 295, 301, 307, 309, 311, 317, 319, 331, 333, 335, 339, 341, 343 347, 351, 359, 371, 373, 375, 379, 381, 383, 423, 427, 443, 469, 471, 475, 477 479, 491, 493, 495, 507, 511, 687, 727, 731, 735, 751, 763, 767, 879, 887, 959, 991	6
	19, 25, 27, 39, 41, 45, 61, 77, 87, 91, 105, 119, 123, 141, 147, 163, 165, 175 199, 211, 233, 235, 237, 239, 349, 363, 415, 429, 431, 439, 501, 503, 699, 895	8
	23, 69, 115, 207, 253, 299, 437, 759	22
	79, 109, 183, 251, 367, 463, 695, 703	4
	59, 93, 169, 243, 303, 509	10
	89, 445	88
	245, 447	16
12	27, 111, 153, 171, 279, 297, 423, 621, 747, 927, 1503, 1791	12
	75, 243, 255, 285, 615, 885, 951, 1455	14
	87, 213, 237, 339, 381, 591, 759	8
	327, 363, 447, 489, 699, 957, 1371	6
	63, 189, 441, 693	62
	69, 201, 717, 831	10
	45, 405, 495	44
	819	818
	315	314

Theorem (Pante Stanica: http://faculty.nps.edu/pstanica)

Thank you for your attention!

Proof.

None required, but questions are welcome! □