Finite Fields and Their Applications 72 (2021) 101835

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On construction and (non)existence of c-(almost) perfect nonlinear functions

Daniele Bartoli [a], Marco Calderini [b,*]

[a] *Department of Mathematics and Computer Sciences, University of Perugia, Italy*
[b] *Department of Informatics, University of Bergen, Norway*

ARTICLE INFO

Article history:
Received 11 August 2020
Received in revised form 9 December 2020
Accepted 19 February 2021
Available online xxxx
Communicated by Pascale Charpin

MSC:
11T06
06E30
94A60

Keywords:
c-differential uniformity
Perfect nonlinear
Almost perfect nonlinear
Exceptional APcN

ABSTRACT

Functions with low differential uniformity have relevant applications in cryptography. Recently, functions with low c-differential uniformity attracted lots of attention. In particular, so-called APcN and PcN functions (generalization of APN and PN functions) have been investigated. Here, we provide a characterization of such functions via quadratic polynomials as well as non-existence results.

1. Introduction

Perfect nonlinear (PN) and *almost perfect nonlinear* (APN) functions and in general functions with low differential uniformity over finite fields have been widely investigated

* Corresponding author.
E-mail addresses: daniele.bartoli@unipg.it (D. Bartoli), marco.calderini@uib.no (M. Calderini).

https://doi.org/10.1016/j.ffa.2021.101835

due to their applications in cryptography. Indeed, differential cryptanalysis [5,6] is an important cryptanalytic approach targeting symmetric-key primitives. In order to be resistant against such types of attacks, cryptographic functions used in the substitution box (S-box) in the cipher are required to have a differential uniformity as low as possible (see [10] for a survey on differential uniformity of vectorial Boolean functions). In [7], the authors introduce a different type of differential, useful for ciphers that utilize modular multiplication as a primitive operation. Consequently, a new concept called multiplicative differential (and the corresponding c-differential uniformity) has been introduced [20].

Definition 1.1. [20, Definition 1] Given a p-ary (n,m)-function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, and $c \in \mathbb{F}_{p^m}$, the (multiplicative) c-derivative of f with respect to $a \in \mathbb{F}_{p^n}$ is the function

$$ {}_cD_af(x) = f(x+a) - cf(x), \qquad \forall x \in \mathbb{F}_{p^n}. $$

For an (n,n)-function f, and $a, b \in \mathbb{F}_{p^n}$, let

$$ {}_c\Delta_f(a,b) := |\{x \in \mathbb{F}_{p^n} \ : \ f(x+a) - cf(x) = b\}|, $$

and

$$ {}_c\Delta_f := \max\{{}_c\Delta_f(a,b) \ : \ a,b \in \mathbb{F}_{p^n}, (a,c) \neq (0,1)\}, $$

where $|S|$ is the cardinality of the set S. The quantity ${}_c\Delta_f$ is called c-differential uniformity of f. Note that for $c = 1$, the above definitions coincide with the usual derivative of f and its differential uniformity.

If ${}_c\Delta_f \leq \delta \in \mathbb{N}$, we say that f is differentially (c,δ)-uniform. In the special cases $\delta = 1$ and $\delta = 2$, such functions are also called PcN and APcN functions. It is worth noting that PcN functions (namely β-planar functions) have been investigated and partially classified in [4].

Clearly, the case $c = 1$ (APN and PN functions) has been widely investigated in the literature; see [8,9,16–18,23,28,29,37] and [11,14,15,19,26,27,31,44] for known APN and PN functions. PN functions are also called *planar*. APN and PN functions are of central interest in design theory, coding theory, and cryptography.

Very recently, power functions with low c-differential uniformity, and the c-differential uniformity of some known APN functions in odd characteristic have been studied in [34]. Also in [25], the authors focus on monomial functions and study their c-differential uniformity for $c = -1$.

In this paper, we further investigate the construction and existence of some APcN and PcN functions. First, in Section 2, we collect some preliminary results and definitions that we will use in the rest of the paper. In Section 3, we first give a characterization of APcN and PcN quadratic functions, which, in particular, gives us a correspondence between planar DO polynomials and APcN maps. Then, we show that, using the AGW criterion [1] and its generalization [33], it is possible to construct several classes of APcN and PcN

functions. In the last section, we give some nonexistence results for some exceptional monomial APcN and PcN functions using connections with algebraic curves and Galois theory tools.

2. Preliminaries

Let $q = p^n$ be a fixed prime power. We denote by $\mathbb{F}_q$ and $\overline{\mathbb{F}_q}$ the field with q elements and its algebraic closure. The multiplicative group of $\mathbb{F}_q$ will be denoted by $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. In the following we will focus on functions defined from $\mathbb{F}_q$ to itself, i.e. p-ary (n, n)-functions. Any function $f : \mathbb{F}_q \to \mathbb{F}_q$ can be represented uniquely by an element of the polynomial ring $\mathbb{F}_q[x]$ of degree less than q.

For $f \in \mathbb{F}_q[x]$:

- f is *linear* if $F(x) = \sum_i a_i x^{p^i}$ (also known as linearized polynomials).
- f is *affine* if it differs from a linear polynomial by a constant.
- f is a *Dembowski-Ostrom (DO)* polynomial if $F(x) = 2\sum_{0 \le i \le j < n} a_{ij} x^{p^i + p^j}$, with $i < j$ if $p = 2$.
- f is *quadratic* if it differs from a DO polynomial by an affine polynomial.

The *trace function* from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is given by the linear polynomial

$$Tr_q^{q^n}(x) = \sum_{i=0}^{n-1} x^{q^i}.$$

A polynomial f is a *permutation polynomial (PP)* over $\mathbb{F}_q$, if $x \mapsto f(x)$ is a bijection from $\mathbb{F}_q$ to itself, and it is a *complete permutation polynomial (CPP)* over $\mathbb{F}_q$, if both $f(x)$ and $f(x) + x$ are PPs.

The AGW criterion, introduced in [1], is a useful method in the construction of PPs and CPPs; see for instance [32,41–43]. The AGW criterion, in the additive case, is given by the following proposition.

Proposition 2.1 *(Proposition 5.4 [1]). Let p be a prime and $q = p^m$ for some integer $m > 0$. Let $\phi(x)$ and $\psi(x)$ be two $\mathbb{F}_q$-linear polynomials over $\mathbb{F}_q$ seen as endomorphisms of $\mathbb{F}_{q^n}$, and let $g \in \mathbb{F}_{q^n}[x]$ and $h \in \mathbb{F}_{q^n}[x]$ such that $h(\psi(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q^*$. Then*

$$f(x) = h \circ \psi(x)\phi(x) + g \circ \psi(x)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if the following two conditions hold:

(i) $\ker(\phi) \cap \ker(\psi) = \{0\}$;
(ii) $h(x)\phi(x) + \psi(g(x))$ *permutes* $\psi(\mathbb{F}_{q^n})$.

As immediate consequence, in Theorem 5.10 in [1] the authors provided the following general framework of PPs.

Theorem 2.2 *([1]). Let p be a prime and $q = p^m$ for some integer $m > 0$. Let $\phi(x)$ be an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$ seen as endomorphism of $\mathbb{F}_{q^n}$, and let $g \in \mathbb{F}_{q^n}[x]$ and $h \in \mathbb{F}_{q^n}[x]$ such that $h(x^q - x) \subseteq \mathbb{F}_q^*$. Then*

$$f_1(x) = h(x^q - x)\phi(x) + Tr_q^{q^n}(g(x^q - x))$$

and

$$f_2(x) = h(x^q - x)\phi(x) + g(x^q - x)^{(q^n-1)/(q-1)}$$

are permutation polynomials of $\mathbb{F}_{q^n}$ if and only if $\ker(\phi) \cap \mathbb{F}_q = \{0\}$ and $h(x)\phi(x)$ permutes $J = \{x^q - x : x \in \mathbb{F}_{q^n}\}$.

In [33], Mesnager and Qu extended the AGW criterion for constructing 2-to-1 map. If q is even, a 2-to-1 map over $\mathbb{F}_q$ is a function such that any $b \in \mathbb{F}_q$ has either 2 or 0 preimages. If q is odd, for all but one $b \in \mathbb{F}_q$, it has either 2 or 0 preimages, and the exception element has exactly one preimage.

For $q = 2^m$, using ϕ a 2-to-1 map over $\mathbb{F}_q$ and that permutes $J = \{x^q + x : x \in \mathbb{F}_{q^n}\}$ it is possible to construct 2-to-1 maps of same type as in Theorem 2.2. More specifically, we have the following result.

Theorem 2.3 *(Theorem 15 [33]). Let $q = 2^m$, $\phi(x)$ be an $\mathbb{F}_q$-linear polynomial seen as an endomorphism of $\mathbb{F}_{q^n}$. Let $g, h \in \mathbb{F}_{q^n}[x]$ be such that $h(x^q + x) \in \mathbb{F}_q^*$ for any $x \in \mathbb{F}_{q^n}$. Assume*

$$f_1(x) = h(x^q + x)\phi(x) + Tr_q^{q^n}(g(x^q + x))$$

and

$$f_2(x) = h(x^q + x)\phi(x) + g(x^q + x)^{(q^n-1)/(q-1)}.$$

If ϕ is 2-to-1 over $\mathbb{F}_q$ and $h(x)\phi(x)$ permutes $J = \{x^q + x : x \in \mathbb{F}_{q^n}\}$, then both f_1 and f_2 are 2-to-1 over $\mathbb{F}_{q^n}$.

In the second part of this work, Section 4, we deal with exceptional power APcN and PcN maps.

Definition 2.4. Let $c \in \mathbb{F}_q$ be fixed. Let $f(x) \in \mathbb{F}_q[x]$ be a APcN (PcN) function over $\mathbb{F}_{q^r}$ for infinitely many r. Then, f is said exceptional APcN (PcN).

Results on exceptional APN and PN functions can be found in [2,13] and the references therein.

We use Galois theory tools to provide non-existence results for APcN and PcN monomials. We recall here the Galois theoretical part of our approach which deals with totally split places. This method was successfully used also in [3,21,35,36].

We will make use of the following results.

Theorem 2.5. *[40, Theorem 3.9] Let r be a prime and G be a primitive group of degree $n = s + k$ with $k \geq 3$. If G contains an element of degree and order s (i.e. an s-cycle), then G is either alternating or symmetric.*

The proof of the following result can be found in [24].

Lemma 2.6. *Let $L : K$ be a finite separable extension of function fields, let M be its Galois closure and $G := Gal(M : K)$ be its Galois group. Let P be a place of K and $\mathcal{Q}$ be the set of places of L lying above P. Let R be a place of M lying above P. Then we have the following:*

1. *There is a natural bijection between $\mathcal{Q}$ and the set of orbits of $H := \mathrm{Hom}_K(L, M)$ under the action of the decomposition group $D(R|P) = \{g \in G \,|\, g(R) = R\}$.*
2. *Let $Q \in \mathcal{Q}$ and let H_Q be the orbit of $D(R|P)$ corresponding to Q. Then $|H_Q| = e(Q|P)f(Q|P)$ where $e(Q|P)$ and $f(Q|P)$ are ramification index and relative degree, respectively.*
3. *The orbit H_Q partitions further under the action of the inertia group $I(R|P)$ into $f(Q|P)$ orbits of size $e(Q|P)$.*

The following can also be deduced by [30]; its proof can be found in [3].

Theorem 2.7. *Let p be a prime number, m a positive integer, and $q = p^m$. Let $L : F$ be a separable extension of global function fields over $\mathbb{F}_q$ of degree n, M be the Galois closure of $L : F$, and suppose that the field of constants of M is $\mathbb{F}_q$. There exists an explicit constant $C \in \mathbb{R}^+$ depending only on the genus of M and the degree of $L : F$ such that if $q > C$ then $L : F$ has a totally split place.*

3. A characterization of APcN and PcN functions

It is well-known that a DO polynomial is planar if and only if it is 2-to-1 (see [12, Theorem 3]). The following result gives a characterization of APcN and PcN quadratic polynomials for $c \in \mathbb{F}_p \setminus \{1\}$.

Let $f : \mathbb{F}_q \to \mathbb{F}_q$. We say that f is at most a 2-to-1 function if for any $b \in \mathbb{F}_q$ we have $|f^{-1}(b)| \leq 2$.

Theorem 3.1. *Let p be a prime. Let f be a quadratic polynomial over $\mathbb{F}_{p^m}$ for some integer m. Then, for any $c \in \mathbb{F}_p \setminus \{1\}$ we have the following.*

(i) *f is at most 2-to-1 if and only if f is APcN. Moreover, if f is a DO polynomial, then f is APcN if and only if f is planar.*
(ii) *f is a PP if and only if f is PcN.*

Proof. (i) Let f be a quadratic polynomial, that is $f(x) = \sum_{i,j} a_{i,j} x^{p^i+p^j} + \sum_i b_i x^{p^i}$. We can note that for any γ we have

$$f(x+\gamma) = f(x) + f(\gamma) + \sum_{i,j} a_{i,j}(x^{p^i}\gamma^{p^j} + x^{p^j}\gamma^{p^i}).$$

Let $c \in \mathbb{F}_p \setminus \{1\}$. Then

$$\begin{aligned} f(x+\gamma) - cf(x) =& (1-c)\left(f(x) + \sum_{i,j} a_{i,j}\left[x^{p^i}\left(\frac{\gamma}{1-c}\right)^{p^j} + x^{p^j}\left(\frac{\gamma}{1-c}\right)^{p^i}\right]\right. \\ &\left. + f\left(\frac{\gamma}{1-c}\right) - f\left(\frac{\gamma}{1-c}\right)\right) + f(\gamma) \\ =& (1-c) f\left(x + \frac{\gamma}{1-c}\right) + f(\gamma) - (1-c) f\left(\frac{\gamma}{1-c}\right). \end{aligned} \tag{1}$$

Thus, since f is at most 2-to-1 so is $f(x+\gamma) - cf(x)$, which implies that f is APcN, and vice versa.

If f is a DO polynomial we have $f(x) = f(-x)$. Therefore, the fact that f is at most 2-to-1 implies that f is 2-to-1, and so it is a planar function.

(ii) This follows directly from (1). □

Corollary 3.2. *Let p be a prime, and f be a DO polynomial over $\mathbb{F}_{p^m}$, with m a positive integer. Then, f is exceptional planar if and only if f is exceptional APcN for any $c \in \mathbb{F}_p \setminus \{1\}$.*

Remark 3.3. Let $q = p^h$. If the quadratic function f is of type

$$f(x) = \sum_{i,j} a_{i,j} x^{q^i+q^j} + \sum_i b_i x^{p^i},$$

then the results above can be extended to any $c \in \mathbb{F}_q \setminus \{1\}$.

Up to now, all known planar functions are DO polynomials, but the case of $x^{\frac{3^k+1}{2}}$ defined over $\mathbb{F}_{3^n}$ with k odd and $\gcd(k,n) = 1$. From Theorem 3.1, we have that these

known planar functions are also APcN. Moreover, in [34] it has been proved that the planar function $x^{\frac{3^k+1}{2}}$ is APcN for $c = -1$.

The result (i) of Theorem 3.1 cannot be extended to a general planar quadratic function. Indeed, the planarity of a function f is invariant by adding a linear (affine) polynomial to f, while the c-differential uniformity is not. So, if we consider a planar DO polynomial, adding a linear function we could obtain a function which is no more 2-to-1 and thus which is no APcN.

Example 3.4. The function $x^2 + x^3$ is planar over $\mathbb{F}_{3^2}$ but it is not APcN for any $c \neq 1$.

Remark 3.5. In [39], the authors introduced and studied c-differential bent functions. In their work, they also relaxed the definition of perfect c-nonlinearity excluding the case of the derivative in the zero direction. In particular, they defined PcN function any f such that $f(x+\gamma) - cf(x)$ is a permutation for any $\gamma \in \mathbb{F}_q^*$, and *strictly PcN* if in addition f is a permutation.

For $p = 2$, even if we exclude the derivative in the zero direction, a PcN function has to be a PP. Indeed, let f be PcN and suppose that there exist x_1 and $x_2 = x_1 + \gamma$ such that $f(x_1) = f(x_1 + \gamma)$. Since f is PcN,

$$f(x+\gamma) + cf(x) = (c+1)f(x) + f(x+\gamma) + f(x)$$

is a PP. But

$$f(x_1+\gamma) + cf(x_1) = (c+1)f(x_1) = (c+1)f(x_2) = f(x_2+\gamma) + cf(x_2),$$

which is a contradiction.

It would be interesting to understand if this is the case also for $p > 2$.

3.1. Some PcN and APcN polynomials from the AGW criterion

In the following we will show that from the AGW criterion and its generalization [33] (for the case $p = 2$) we can obtain PcN and APcN functions.

Theorem 2.2 gives us the possibility of constructing PPs of the form

$$f_1(x) = h(x^q - x)\phi(x) + Tr_q^{q^n}(g(x^q - x))$$

and

$$f_2(x) = h(x^q - x)\phi(x) + g(x^q - x)^{(q^n-1)/(q-1)},$$

where g can be any polynomial over $\mathbb{F}_{q^n}$. This is implied by the fact that $x^q - x$ annihilates both $Tr_q^{q^n}(g(x))$ and $g(x)^{(q^n-1)/(q-1)}$ for any x. We can immediately construct some PcN polynomials.

Theorem 3.6. *Let f_1 and f_2 be PPs as in Theorem 2.2 with $h \equiv b \in \mathbb{F}_q^*$. Then f_1 and f_2 are PcN for any $c \in \mathbb{F}_q \setminus \{1\}$.*

Proof. Let $c \in \mathbb{F}_q \setminus \{0,1\}$. Consider for instance the permutation f_1. Then, f_1 is PcN if and only if

$$f_1(x+\gamma) - cf_1(x) = b(1-c)\phi(x) + Tr_q^{q^n}(g(x^q - x + \gamma^q - \gamma)) - cTr_q^{q^n}(g(x^q - x)) + b\phi(\gamma)$$

is a PP for any γ. Denoting by $\psi(x) = x^q - x$, and by $g'(x) = g(x + \gamma^q - \gamma)$, from the AGW criterion (Proposition 2.1) we have that this is a PP if and only if

$$b(1-c)\phi(x) + \psi(Tr_q^{q^n}(g'(x)) - cTr_q^{q^n}(g(x)))$$

permutes $J = \{x^q - x : x \in \mathbb{F}_{q^n}\}$. Now, $\psi(Tr_q^{q^n}(g(x)) - cTr_q^{q^n}(g(x))) = 0$ and thus $b(1-c)\phi(x)$ permutes J since f_1 is a PP. The same holds for f_2. □

Another type of PPs, which are also PcN, can be constructed in the following way.

Theorem 3.7. *Let p be a prime and $q = p^m$ for some integer $m > 0$. Let $g(x) \in \mathbb{F}_{q^2}[x]$ be any polynomial such that $g(J) \subseteq J$ where $J = \{x^q - x : x \in \mathbb{F}_{q^2}\}$ and $\phi(x)$ be an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$. Let $s > 0$ be an even integer. Then, for any $b \in \mathbb{F}_q^*$*

$$f(x) = b\phi(x) + (g(x^q - x))^s$$

is a PP if and only if $\phi(x)$ induces a permutation over J.

Proof. From the AGW criterion (Proposition 2.1) we have that f is a PP if and only if

$$(g(x))^{qs} - (g(x))^s + b\phi(x)$$

permutes J.

Note that for any $y \in J$ we have $Tr_q^{q^2}(y) = 0$ and thus $y^q = -y$. Since s is even, for any $y \in J$ we have $y^s \in \mathbb{F}_q$. Indeed,

$$y^{sq} = (-y)^s = y^s.$$

Then, since $g(J) \subseteq J$ we have that

$$(g(x))^{qs} - (g(x))^s = 0,$$

for any $x \in J$. Thus, f is a PP if and only if $\phi(x)$ permutes J. □

Example 3.8. An easy example of function g such that $g(J) \subseteq J$ is given by $g(x) = x + \delta$ with $\delta \in J$.

Theorem 3.7 can be generalized (with a similar proof) to functions f of type

$$f(x) = b\phi(x) + \sum_i (g_i(x^q - x))^{s_i},$$

where s_i's are even, and g_i's are such that $g_i(J) \subseteq J$.

Corollary 3.9. *Let p be a prime and $q = p^m$ for some integer $m > 0$. Let t be a positive integer. Let $g_1, ..., g_t \in \mathbb{F}_{q^2}[x]$ be such that $g_i(J) \subseteq J$ for all $1 \leq i \leq t$, where $J = \{x^q - x : x \in \mathbb{F}_{q^2}\}$, and $\phi(x)$ an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$. Let $s_1, ..., s_t$ be even integers. Then, for any $b \in \mathbb{F}_q^*$*

$$f(x) = b\phi(x) + \sum_i (g_i(x^q - x))^{s_i},$$

is a PP if and only if $\phi(x)$ induces a permutation over J.

Remark 3.10. Note that the polynomials in Theorem 2.2 and 3.7, considering $\phi(x) = x$, are also CPPs when $b \neq 0, -1$.

As for the case of the functions f_1 and f_2 of Theorem 2.2, also the functions satisfying Theorem 3.7 are PcN when $c \in \mathbb{F}_q \setminus \{1\}$.

Theorem 3.11. *Let p be a prime and $q = p^m$ for some integer $m > 0$. Let $f(x)$ be a PP as in Theorem 3.7. Then $f(x)$ is PcN for any $c \in \mathbb{F}_q \setminus \{1\}$.*

Proof. We have that

$$f(x + \gamma) - cf(x) = b(1 - c)\phi(x) + (g'(x^q - x))^s - c(g(x^q - x))^s + b\phi(\gamma),$$

where $g'(x) = g(x + \gamma^q - \gamma)$. Note that since J is an $\mathbb{F}_q$-vector space, $g'(J) \subseteq J$. Now as in Theorem 3.7, this is a permutation if and only if $\phi(x)$ permutes J. This condition is satisfied since f is a PP. □

Remark 3.12. In even characteristic, PN functions (i.e. PcN function with $c = 1$) do not exist. As pointed out in [20], PcN functions, for $c \neq 1$, exist also for the case $p = 2$. Indeed, trivially, any PP is PcN for $c = 0$ and any linear permutation is PcN for any $c \neq 1$. Theorems 3.6 and 3.11 provide non-trivial PcN functions for $p = 2$.

A similar argument can be done for the case of APcN maps using the results of [33]. As for the PcN case we can obtain APcN maps for any $c \in \mathbb{F}_q \setminus \{1\}$ using functions as in Theorem 2.3. In particular, for n odd, we can obtain the following APcN maps.

Theorem 3.13. *Let n and m be two positive integers with n odd. Let $q = 2^m$ and $\phi(x)$ be an $\mathbb{F}_q$-linear polynomial which is 2-to-1 over $\mathbb{F}_q$ and that permutes $J = \{x^q + x : x \in \mathbb{F}_{q^n}\}$. Let $g \in \mathbb{F}_{q^n}[x]$ and $b \in \mathbb{F}_q^*$. Then,*

$$f_1(x) = b\phi(x) + Tr_q^{q^n}(g(x^q + x)) \text{ and } f_2(x) = b\phi(x) + g(x^q + x)^{(q^n-1)/(q-1)}$$

are APcN functions for any $c \in \mathbb{F}_q \setminus \{1\}$.

Proof. Let us consider $f_1(x)$. For any γ we have

$$\begin{aligned} f_1(x+\gamma) + cf_1(x) =& b\phi(x) + b\phi(\gamma) + Tr_q^{q^n}(g(x^q + x + \gamma^q + \gamma)) \\ &+ cb\phi(x) + Tr_q^{q^n}(cg(x^q + x)) \\ =& b(c+1)\phi(x) + Tr_q^{q^n}(g'(x^q + x)) + b\phi(\gamma), \end{aligned}$$

where $g'(x) = g(x+\gamma^q+\gamma)+cg(x)$. Then, $f_1(x+\gamma)+cf_1(x)$ is 2-to-1 from Theorem 2.3.

For f_2 the claim follows in a similar way. □

Example 3.14. For constructing APcN functions as in Theorem 3.13, we can consider, for example, the 2-to-1 function ϕ over $\mathbb{F}_q$ defined by $\phi(x) = x^{2^i} + x$ with $\gcd(i, m) = 1$.

Indeed, since $\gcd(i, m) = 1$ we have that $\ker(\phi) = \mathbb{F}_2$, implying that ϕ is 2-to-1 over $\mathbb{F}_q$. Moreover ϕ permutes J. Suppose that there exist $x_1, x_2 \in J$ such that $\phi(x_1) = \phi(x_2)$ then $\phi(x_1 + x_2) = 0$. Since J is a vector subspace, we have $x_1 + x_2 \in J \cap \ker(\phi) = \{0\}$, recall that n is odd and $Tr_q^{q^n}(1) = 1$.

Remark 3.15. Note that, when n is even, it is not possible to construct ϕ that is a 2-to-1 map over $\mathbb{F}_q$ and permutes J since $\mathbb{F}_q \subseteq J$. Indeed $\mathbb{F}_{q^2}$ is a subfield of $\mathbb{F}_{q^n}$ and, denoting by $\psi(x) = x^q + x$, we have $\psi(\mathbb{F}_{q^2}) = \mathbb{F}_q$.

So, for n even, it is not possible to construct APcN functions as in Theorem 3.13.

4. Non-existence results for APcN and PcN monomials

In this section we provide non-existence results for exceptional APcN (and PcN) monomials. In what follows, we will consider exponents d such that $p \nmid d(d-1)$, and we denote p^h by q, for some integer h, and by s the smallest positive integer such that $d - 1 \mid (p^s - 1)$.

Let us consider $f(x) = x^d$ defined over $\mathbb{F}_q$. The monomial $f(x)$ is APcN, $c \neq 1$, if and only if

$$\forall a, b \in \mathbb{F}_q \Longrightarrow (x + a)^d - cx^d = b \text{ has at most two solutions.} \tag{2}$$

For $a = 0$, the condition above implies that x^d is at most a 2-to-1 function. That is $\gcd(d, q - 1) \leq 2$.

When $a \neq 0$, Condition (2) can be simplified to

$$\forall b \in \mathbb{F}_q \Longrightarrow (x+1)^d - cx^d = b \text{ has at most two solutions.} \tag{3}$$

A standard tool, when dealing with APN or PN functions is to consider the curve $\mathcal{C}_{f,c}$ of affine equation

$$\mathcal{C}_{f,c} \ : \ \frac{(X+1)^d - (Y+1)^d - c(X^d - Y^d)}{X-Y} = 0. \tag{4}$$

We refer to [4] for and the references therein for an introduction to basic concepts about curves over finite fields.

Note that Condition (3) implies the existence of at most $q/2$ values b_i for which $(x+1)^d - cx^d = b_i$ has two solutions. Therefore, there are at most $q/2$ pairs $\{x_i, y_i\}$, $x_i \neq y_i$, $x_i, y_i \in \mathbb{F}_q$, such that x_i and y_i satisfy $(x_i+1)^d - cx_i^d = b_i = (y_i+1)^d - cy_i^d$. Thus, $\mathcal{C}_{f,c}$ possesses at most q $\mathbb{F}_q$-rational points. If q is large enough with respect to d, the existence of more than one absolutely irreducible component of $\mathcal{C}_{f,c}$ defined over $\mathbb{F}_q$ would imply, by Hasse-Weil bound, the existence of roughly $2q$ $\mathbb{F}_q$-rational points, a contradiction.

First, we will provide sufficient conditions on c and d for which $\mathcal{C}_{f,c}$ is absolutely irreducible. In particular, we provide upper bounds on the number of singular points of $\mathcal{C}_{f,c}$. To this end we will consider, for simplicity, the curve $\mathcal{D}_{f,c} : (X+1)^d - (Y+1)^d - c(X^d - Y^d) = 0$. Singular points of $\mathcal{C}_{f,c}$ are a subset of the singular points of $\mathcal{D}_{f,c}$.

Theorem 4.1. *Let $\xi \in \overline{\mathbb{F}_q}$ be a primitive $(d-1)$-root of unity. Suppose that*

$$\nexists \ \ i,j,k \in \{0,\dots,d-2\}, i \neq 0, \ \textit{such that} \ \sqrt[d-1]{c} \neq \frac{1-\xi^i}{\xi^k - \xi^j}. \tag{5}$$

Then, $\mathcal{D}_{f,c}$ contains no singular points off $X = Y$. In particular, this is true if $\sqrt[d-1]{c} \notin \mathbb{F}_{p^s}$.

Proof. Since $p \nmid d$, $\mathcal{D}_{f,c}$ does not possess singular points at infinity. Note that there are no singular points lying on $X = 0$ or $Y = 0$. Affine singular points (x_0, y_0), $x_0 \neq y_0$, satisfy

$$\begin{cases} (\frac{x_0+1}{x_0})^{d-1} = c \\ (\frac{y_0+1}{y_0})^{d-1} = c \\ (\frac{x_0}{y_0})^{d-1} = 1 \end{cases}. \tag{6}$$

Let $\xi \in \overline{\mathbb{F}_q}$ be a primitive $(d-1)$-root of unity and denote by $c_0 = \sqrt[d-1]{c}$. Therefore, $y_0 = \xi^i x_0$, $y_0 = 1/(c_0\xi^j - 1)$, $x_0 = 1/(c_0\xi^k - 1)$, for some $i,j,k \in \{0,\dots,d-2\}$ and $i \neq 0$. Each triple (i,j,k) provides a pair (x_0, y_0) satisfying (6). Thus,

$$c_0\xi^k - 1 = \xi^i(c_0\xi^j - 1). \tag{7}$$

By our hypothesis $\xi \in \mathbb{F}_{p^s}$. Equation (7) yields

$$c_0(\xi^k - \xi^{i+j}) = 1 - \xi^i.$$

Since $i \neq 0$, we have a contradiction. So, no pairs (x_0, y_0) satisfy (6) and there are no singular points. □

Note that, under the hypothesis of Theorem 4.1 the number of singular points of $\mathcal{C}_{f,c}$ is at most $d/2$. A deeper analysis shows that

$$\begin{aligned}&(X+1+a)^d - (Y+1+a)^d - c((X+a)^d - (Y+a)^d)\\ &= d[(a+1)^{d-1} - ca^{d-1}](X-Y) + \binom{d}{2}[(a+1)^{d-2} - ca^{d-2}](X^2 - Y^2) + \cdots\end{aligned}$$

and therefore points (a, a) are double points of $\mathcal{D}_{f,c}$ and then simple points of $\mathcal{C}_{f,c}$. So, $\mathcal{C}_{f,c}$ possesses no singular points and hence it is absolutely irreducible.

Theorem 4.2. *Suppose that c satisfies Condition (5). Then, $\mathcal{C}_{f,c}$ is absolutely irreducible.*

We want to prove that if q is large enough there exists $t_0 \in \mathbb{F}_q$ such that the equation $(x+1)^d - cx^d = t_0$ has more than two solutions, i.e. x^d is not exceptional PcN nor APcN. To this end we will investigate the geometric and the algebraic Galois groups of the polynomial $F_{c,d}(t, x) = (x+1)^d - cx^d - t$.

More in details, consider $G_{c,d}^{arith} = \mathrm{Gal}(F_{c,d}(t, x) : \mathbb{F}_q(t))$ and $G_{c,d}^{geom} = \mathrm{Gal}(F_{c,d}(t, x) : \overline{\mathbb{F}}_q(t))$. They are both subgroups of $\mathcal{S}_d$, the symmetric group over d elements. Our aim is to prove that $G_{c,d}^{geom} = \mathcal{S}_d$. This would force that $G_{c,d}^{geom} = \mathcal{S}_d = G_{c,d}^{arith}$, since $G_{c,d}^{geom} \leq G_{c,d}^{arith}$ and therefore by Chebotarev density Theorem [30], one obtains the existence of a specialization $t_0 \in \mathbb{F}_q$ for which $F_{c,d}(t_0, x)$ splits into d pairwise distinct linear factors $(x - x_i)$ defined over $\mathbb{F}_q$ and therefore $(x+1)^d - cx^d$ cannot be a permutation or 2-to-1 and x^d is not PcN nor APcN.

Lemma 4.3. *Let c satisfy Condition (5). The geometric Galois group $G_{c,d}^{geom}$ coincides with $\mathcal{S}_d$.*

Proof. First we prove that the geometric Galois group of $F_{c,d}(t, x) = (x+1)^d - cx^d - t \in \mathbb{F}_q[x]$ is primitive (i.e. it does not act on a nontrivial partition of the underlying set). Let M be the splitting field of $F_{c,d}(t, x)$ and G be the Galois group of $F_{c,d}(t, x)$ over $\mathbb{F}_q(t)$. Let x be a root of $F_{c,d}(t, x)$ and consider the extension $\mathbb{F}_q(x) : \mathbb{F}_q(t)$. Clearly, $t = (x+1)^d - cx^d = f_{c,d}(x)$ by definition. As a consequence of Lüroth's Theorem, f is indecomposable (i.e. it cannot be written as a composition of two non-linear polynomials) if and only if G is a primitive group; see [22, Proposition 3.4].

To this end, suppose that $f_{c,d}(x) = h_1(h_2(x))$, for some $h_1(x), h_2(x) \in \overline{\mathbb{F}_q}[x]$, with $\deg(h_1(x)), \deg(h_2(x)) \in [2, \dots, d/2]$. Then

$$(h_2(X) - h_2(Y)) \mid (f_{c,d}(X) - f_{c,d}(Y)) = (h_1(h_2(X)) - h_1(h_2(Y))).$$

By Theorem 4.2, $\mathcal{C}_{f,c}$ is absolutely irreducible and then $h_2(X) - h_2(Y) = X - Y$, which contradicts $\deg(h_2(x)) > 1$. Therefore $\mathrm{Gal}(F_{c,d}(t,x) : \overline{\mathbb{F}}_q(t))$ is primitive.

Now we prove that there exists $t_0 \in \overline{\mathbb{F}_q}$ such that $(x+1)^d - cx^d = t_0$ has exactly $d-1$ roots in $\overline{\mathbb{F}_q}$. Elements $t_0 \in \overline{\mathbb{F}_q}$ for which $(x+1)^d - cx^d = t_0$ has a repeated root x_0 are such that

$$(x_0+1)^{d-1} - cx_0^{d-1} = 0, \qquad t_0 = cx_0^{d-1}.$$

Suppose that there exists another repeated root $y_0 \neq x_0$ of $(x+1)^d - cx^d = t_0$. Then

$$\begin{cases} (x_0+1)^{d-1} - cx_0^{d-1} = 0 \\ x_0^{d-1} = y_0^{d-1} \\ (y_0+1)^{d-1} - cy_0^{d-1} = 0, \end{cases}$$

which is equivalent to (6). So each t_0 has at most one repeated root. Note that a repeated root x_0 is at most a double root of $(x+1)^d - cx^d = t_0$ since otherwise $(x_0+1)^{d-2} = cx_0^{d-2}$ and a contradiction easily arises from $(x_0+1)^{d-1} = cx_0^{d-1}$. Therefore each root of $(x+1)^{d-1} - cx^{d-1}$ (they are pairwise distinct) provides a $t_0 = (x_0+1)^d - cx_0^d$ such that the equation $(x+1)^d - cx^d = t_0$ has exactly $d-1$ roots in $\overline{\mathbb{F}_q}$.

Let r be such that the element t_0 obtained above belongs to $\mathbb{F}_{q^r}$. This means that $(x+1)^d - cx^d - t_0$ has exactly one factor of multiplicity 2 and all the others of multiplicity 1. Let now M be the splitting field of $F_{c,d}(t,x)$ over $\mathbb{F}_{q^r}(t)$. Let R be a place of M lying above t_0. Now, using Lemma 2.6 we obtain that the decomposition group $D(R \mid t_0)$ has a cycle of order exactly 2 and fixes all the other elements of $H = \mathrm{Hom}_{\mathbb{F}_{q^r}(t)}(\mathbb{F}_q(x), M)$, where x is a root in $\overline{\mathbb{F}_q(t)}$ of $F_{c,d}(t,X)$ (H can be simply thought as the set of roots of $F_{c,d}(t,X)$ in $\overline{\mathbb{F}_q(t)}$). Now pick any element $g \in D(R \mid t_0)$ that acts non-trivially on H. This element has to be a transposition, which in turn forces $\mathrm{Gal}(F_{c,d}(t,x) : \mathbb{F}_{q^{ru}}(t))$ to contain a transposition for any $u \in \mathbb{N}$ and therefore in particular that $\mathrm{Gal}(F_{c,d}(t,x) : \overline{\mathbb{F}}_q(t))$ contains a transposition.

We already know that $\mathrm{Gal}(F_{c,d}(t,x) : \overline{\mathbb{F}}_q(t))$ is primitive. Now using Theorem 2.5 with $s = 2$ we conclude that both $\mathcal{S}_d = \mathrm{Gal}(F_{c,d}(t,x) : \overline{\mathbb{F}}_q(t))$ and $\mathrm{Gal}(F_{c,d}(t,x) : \mathbb{F}_q(t)) = \mathcal{S}_d$. □

Theorem 4.4. *Let c satisfy Condition (5). Then x^d is not exceptional PcN nor APcN.*

Proof. Consider $F = \mathbb{F}_q(t)$ and $L = F(z)$, where z is a root of $F_{c,d}(t,x) \mid \overline{\mathbb{F}}_q(t)$. Lemma 4.3 tells us that the field of constants of the Galois closure of $L : F$ is trivial, as the geometric Galois group of $F_{c,d}(t,x)$ is equal to the arithmetic one. Let C be

the constant in Theorem 2.7. Using now Theorem 2.7 we have that if $q > C$ there exists a specialization $t_0 \in \mathbb{F}_q$ such that $F_{c,d}(t,x)$ is totally split and therefore $f_{c,d}(x) = t_0$ has d solutions in $\mathbb{F}_q$. The claim follows. □

Finally, we list a couple of open problems.

Open Problem 4.5. Non-existence results for PN or APN functions have been obtained using a number of different methods. It would be interesting to check whether such methods apply also to PcN and APcN for $c \neq 1$.

Open Problem 4.6. If $p = 2$, as already mentioned, no PN functions exist. A different definition of planar functions was given by Zhou [45]: a function $f : \mathbb{F}_q \to \mathbb{F}_q$ is *pseudo-planar* if, for each nonzero $\epsilon \in \mathbb{F}_q$, the function

$$x \mapsto \widehat{f}_\epsilon(x) := f(x+\epsilon) + f(x) + \epsilon x \tag{8}$$

is a permutation of $\mathbb{F}_q$. As shown by Zhou [45] and Schmidt and Zhou [38], pseudo-planar functions have similar properties and applications as their counterparts in odd characteristic. It is natural to extend such a definition to different c. We call a function $f(x)$ *pseudo-PcN* if for all $c, \epsilon \in \mathbb{F}_q$, $\epsilon \neq 0$,

$$f(x+\epsilon) + cf(x) + \epsilon x$$

is a permutation of $\mathbb{F}_q$. Can these functions have the same applications as "normal" PcN or APcN?

Acknowledgment

The research of D. Bartoli was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The research of M. Calderini was supported by Trond Mohn Foundation.

References

[1] A. Akbary, D. Ghioca, Q. Wang, On constructing permutations of finite fields, Finite Fields Appl. 17 (1) (2011) 51–67.
[2] D. Bartoli, Hasse-Weil type theorems and relevant classes of polynomial functions, in: Proceedings of 28th British Combinatorial Conference, in: London Mathematical Society Lecture Note Series, Cambridge University Press, to appear.
[3] D. Bartoli, G. Micheli, Algebraic constructions of complete m-arcs, arXiv:2007.00911.
[4] D. Bartoli, M. Timpanella, On a generalization of planar functions, J. Algebraic Comb. 52 (2019) 187–213.
[5] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, J. Cryptol. 4 (1) (1991) 3–72.
[6] E. Biham, A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer, 1993.

[7] N. Borisov, M. Chew, R. Johnson, D. Wagner, Multiplicative differentials, in: J. Daemen, V. Rijmen (Eds.), Fast Software Encryption, FSE 2002, in: Lecture Notes in Computer Science, vol. 2365, Springer, Berlin, Heidelberg, 2002.
[8] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, I. Villa, Constructing APN functions through isotopic shifts, IEEE Trans. Inf. Theory 66 (8) (2020) 5299–5309.
[9] L. Budaghyan, C. Carlet, G. Leander, Two classes of quadratic APN binomials inequivalent to power functions, IEEE Trans. Inf. Theory 54 (9) (2008) 4218–4229.
[10] C. Carlet, Boolean Functions for Cryptography and Coding Theory, Cambridge University Press, Cambridge, 2020.
[11] R.S. Coulter, R.W. Matthews, Planar functions and planes of Lenz-Barlotti class II, Des. Codes Cryptogr. 10 (1997) 167–184.
[12] R.S. Coulter, R.W. Matthews, On the number of distinct values of a class of functions over a finite field, Finite Fields Appl. 17 (2011) 220–224.
[13] M. Delgado, The state of the art on the conjecture of exceptional APN functions, Note Mat. 37 (1) (2017) 41–51.
[14] P. Dembowski, T.G. Ostrom, Planes of order n with collineation groups of order n^2, Math. Z. 193 (1968) 239–258.
[15] C. Ding, J. Yuan, A new family of skew Paley-Hadamard difference sets, J. Comb. Theory, Ser. A 113 (2006) 1526–1535.
[16] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: a new case for n divisible by 5, in: Finite Fields and Applications, Augsburg, Germany, 1999, pp. 113–121.
[17] H. Dobbertin, Almost perfect nonlinear power functions on GF(2n): the Welch case, IEEE Trans. Inf. Theory 45 (4) (1999) 1271–1275.
[18] H. Dobbertin, Almost perfect nonlinear power functions on GF(2n): the Niho case, Inf. Comput. 151 (1–2) (1999) 57–72.
[19] H. Dobbertin, D. Mills, E.N. Muller, A. Pott, W. Willems, APN functions in odd characteristic, Discrete Math. 267 (2003) 95–112.
[20] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity, IEEE Trans. Inf. Theory (2020).
[21] A. Ferraguti, G. Micheli, Full classification of permutation rational functions and complete rational functions of degree three over finite fields, Des. Codes Cryptogr. 88 (2020) 867–886.
[22] M. Fried, R.E. MacRae, On the invariance of chains of fields, Ill. J. Math. 13 (1969) 165–171.
[23] R. Gold, Maximal recursive sequences with 3-valued recursive crosscorrelation function, IEEE Trans. Inf. Theory 14 (1) (1968) 154–156.
[24] R.M. Guralnick, T.J. Tucker, M.E. Zieve, Exceptional covers and bijections on rational points, Int. Math. Res. Not. (2007) rnm004.
[25] S.U. Hasan, M. Pal, Co. Riera, P. Stănică, On the c-differential uniformity of certain maps over finite fields, Des. Codes Cryptogr. (2020).
[26] T. Helleseth, C. Rong, D. Sandberg, New families of almost perfect nonlinear power mappings, IEEE Trans. Inf. Theory 45 (2) (1999) 475–485.
[27] T. Helleseth, D. Sandberg, Some power mappings with low differential uniformity, Appl. Algebra Eng. Commun. Comput. 8 (1997) 363–370.
[28] H. Janwa, R.M. Wilson, Hyperplane sections of Fermat varieties in $\mathbb{P}^3$ in char. 2 and some applications to cyclic codes, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, in: Lecture Notes in Computer Science, vol. 673, Springer-Verlag, Berlin, Germany, 1993, pp. 180–194.
[29] T. Kasami, The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes, Inf. Control 18 (1971) 369–394.
[30] M. Kosters, A short proof of a Chebotarev density theorem for function fields, Math. Commun. 22 (2) (2017) 227–233.
[31] E. Leducq, New families of APN functions in characteristic 3 or 5, in: Arithmetic, Geometry, Cryptography and Coding Theory, in: Contemporary Mathematics, vol. 574, AMS, 2012, pp. 115–123.
[32] Z. Li, M. Wang, J. Wu, X. Zhu, Some new forms of permutation polynomials based on the AGW criterion, Finite Fields Appl. 61 (2020) 101584.
[33] S. Mesnager, L. Qu, On two-to-one mappings over finite fields, IEEE Trans. Inf. Theory 65 (12) (2019) 7884–7895.
[34] S. Mesnager, C. Riera, P. Stănică, H. Yan, Z. Zhou, Investigations on c-(almost) perfect nonlinear functions, arXiv:2010.10023.
[35] G. Micheli, Constructions of locally recoverable codes which are optimal, IEEE Trans. Inf. Theory 66 (1) (2020) 167–175.

[36] G. Micheli, On the selection of polynomials for the dlp quasi-polynomial time algorithm for finite fields of small characteristic, SIAM J. Appl. Algebra Geom. 3 (2) (2019) 256–265.
[37] K. Nyberg, Differentially uniform mappings for cryptography, in: Advances in Cryptography, EUR OCRYPT93, in: Lecture Notes in Computer Science, vol. 765, Springer-Verlag, New York, 1994, pp. 55–64.
[38] K.-U. Schmidt, Y. Zhou, Planar functions over fields of characteristic two, J. Algebraic Comb. 40 (2014) 503–526.
[39] P. Stănică, S. Gangopadhyy, A. Geay, C. Riera, A. Tkachenko, C-differential bent functions and perfect nonlinearity, arXiv:2006.12535.
[40] H. Wielandt, Finite Permutation Groups, Academic Press, New York, 1964.
[41] X. Xu, X. Feng, X. Zeng, Complete permutation polynomials with the form $(x^{p^m}-x+\delta)^s+ax^{p^m}+bx$ over $\mathbb{F}_{p^n}$, Finite Fields Appl. 57 (2019) 309–343.
[42] P. Yuan, C. Ding, Permutation polynomials over finite fields from a powerful lemma, Finite Fields Appl. 17 (2011) 560–574.
[43] P. Yuan, C. Ding, Further results on permutation polynomials over finite fields, Finite Fields Appl. 27 (2014) 88–103.
[44] Z. Zha, X. Wang, Almost perfect nonlinear power functions in odd characteristic, IEEE Trans. Inf. Theory 57 (7) (2011) 4826–4832.
[45] Y. Zhou, $(2^n, 2^n, 2^n, 1)$-relative difference sets and their representations, J. Comb. Des. 21 (2013) 563–584.