Received: 24 December 2022 | Revised: 1 August 2023 | Accepted: 8 August 2023

DOI: 10.1002/jcd.21916

RESEARCH ARTICLE

WILEY

P℘N functions, complete mappings and quasigroup difference sets

Nurdagül Anbar[1] | **Tekgül Kalaycı**[1] | **Wilfried Meidl**[1,2] | **Constanza Riera**[3] | **Pantelimon Stănică**[4]

[1]Faculty of Engineering and Natural Sciences, Sabancı University, MDBF, Istanbul, Turkey

[2]Institut für Mathematik, Alpen-Adria-Universität Klagenfurt, Klagenfurt, Austria

[3]Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, Bergen, Norway

[4]Department of Applied Mathematics, Naval Postgraduate School, Monterey, California, USA

Correspondence
Pantelimon Stănică, Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943-5216, USA.
Email: pstanica@nps.edu

Funding information
NPS Foundation; Research Council of Norway; Türkiye Bilimsel ve Teknolojik Arastirma Kurumu; Austrian Science Fund, Grant/Award Number: FWF Project P 35138

Abstract

We investigate pairs of permutations F, G of $\mathbb{F}_{p^n}$ such that $F(x+a)-G(x)$ is a permutation for every $a \in \mathbb{F}_{p^n}$. We show that, in that case, necessarily $G(x)=\wp(F(x))$ for some complete mapping $-\wp$ of $\mathbb{F}_{p^n}$, and call the permutation F a perfect $\wp$ nonlinear (P℘N) function. If $\wp(x)=cx$, then F is a PcN function, which have been considered in the literature, lately. With a binary operation on $\mathbb{F}_{p^n}\times\mathbb{F}_{p^n}$ involving $\wp$, we obtain a quasigroup, and show that the graph of a P℘N function F is a difference set in the respective quasigroup. We further point to variants of symmetric designs obtained from such quasigroup difference sets. Finally, we analyze an equivalence (naturally defined via the automorphism group of the respective quasigroup) for P℘N functions, respectively, for the difference sets in the corresponding quasigroup.

KEYWORDS

c-differential uniformity, difference sets, permutations, quasigroups, symmetric designs

1 | INTRODUCTION

Let F be a function from the finite field $\mathbb{F}_{p^n}$ with p^n elements, into the finite field $\mathbb{F}_{p^m}$ with p^m elements. Here, and throughout the paper, m, n denote positive integers. The derivative D_aF of F in direction $a \in \mathbb{F}_{p^n}$ is the function defined by

$$D_aF(x) = F(x + a) - F(x).$$

For every $a \in \mathbb{F}_{p^n}$, $b \in \mathbb{F}_{p^m}$, we define $\delta_F(a, b) = |\{x \in \mathbb{F}_{p^n} : D_aF(x) = b\}|$, and $\delta_F = \max\{\delta_F(a, b) : a \in \mathbb{F}_{p^n}^* = \mathbb{F}_{p^n}\setminus\{0\}, b \in \mathbb{F}_{p^m}\}$. The function F is called *differentially δ-uniform*, if for all $a \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_{p^m}$, we have $\delta_F(a, b) \le \delta$. The value δ_F is called the *differential uniformity* of F.

A low differential uniformity is crucial for functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ used in cryptography to thwart differential attacks [2].

In the case $n = m$, and if and only if the characteristic p is odd, there exist some functions F, called *planar functions*, for which every derivative D_aF, $a \neq 0$, is a permutation, that is, $\delta_F = 1$. More general, a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is called *perfect nonlinear (PN)* or a *bent function*, if the derivative D_aF is balanced for every nonzero $a \in \mathbb{F}_{p^n}$, that is, for every $a \in \mathbb{F}_{p^n}^*$, $b \in \mathbb{F}_{p^m}$, the equation $D_aF(x) = b$ has exactly p^{n-m} solutions. Whereas such functions exist in odd characteristic for all integers n and $m \le n$, if $p = 2$, then n must be even and $m \le n/2$ (see [16]).

Perfect nonlinear functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ have rich connections to objects from several areas like coding theory, geometry and combinatorics. Bent functions correspond to relative difference sets, divisible designs, planar functions yield projective planes, and if they are quadratic, commutative semifields. Boolean bent functions correspond to difference sets. For these reasons, perfect nonlinear functions have been intensively investigated over the last decades [4], not only for characteristic 2 where substantial motivation comes from cryptography, but also for odd characteristic p [14].

Given a function F from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$, the concept of a c-differential

$$_cD_aF(x) = F(x + a) - cF(x), c \in \mathbb{F}_{p^m}^*, \tag{1}$$

has been introduced in Ellingsen et al. [5].

A function F from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is called *perfect c-nonlinear (PcN)* (also *c-differential bent*), if $_cD_aF$ is balanced for all $a \in \mathbb{F}_{p^n}$. (In the classical case, when $c = 1$, $a = 0$ is exempted.)

As motivation for this definition, in several articles it is pointed to possible variants of the differential attack. However, there is not yet such an attack, since the principal idea of the differential attack, canceling the key in the sum of two outputs of the S-box, does not seem to work if $c \neq 1$. However, we make some observations in the last section, where we point to future research, which may help in circumventing that. Further research is required, surely, but as it turns out, there are instances in higher order differentials when the round keys may disappear.

Further, many interesting connections to various kinds of difference sets, projective planes, and so on, that we see for the conventional derivative ($c = 1$), are not clear when $c \neq 1$. Hence, one objective of this article is to endow the c-differential with some further meaning, and relate the concept to combinatorial objects. For this purpose, we first extend the concept of the c-differential, and consider, for functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, more general, differentials of the form

$$_{\wp}D_aF(x) = F(x + a) - \wp(F(x)), \tag{2}$$

for a permutation $\wp$ of $\mathbb{F}_{p^m}$. The c-differential in (1) corresponds then to the permutation $\wp(x) = cx$; in the classical case, $\wp$ is the identity.

We call a function F from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ a P$\wp$N function if $_{\wp}D_aF$ is balanced for every $a \in \mathbb{F}_{p^n}$. Note that it is a requirement that $m \le n$, though we are most interested in the case of $n = m$. Observe that, given a permutation F, we can write any permutation G as $G(x) = \wp(F(x))$ for

some permutation $\wp$. Therefore in Equation (2) for $m = n$, we consider pairs of permutations F, G (though not obvious now, Proposition 3.2 implies that F must be a permutation if ${}_{\wp}D_a F(x)$ is a permutation for every a) of $\mathbb{F}_{p^n}$ such that

$$F(x + a) - G(x)$$

is a permutation for every $a \in \mathbb{F}_{p^n}$. This may lead to some interesting questions on permutation polynomials and, as we will see, complete mappings. Notably, as for perfect nonlinear functions, we can assign such permutations F to some variants of difference sets, namely difference sets in corresponding *quasigroups*.

We remark that the definition of the $\wp$-differential is independent from the representation of the n-dimensional vector space over $\mathbb{F}_p$, which throughout this article will be identified with the (additive group of the) finite field $\mathbb{F}_{p^n}$.

Recall that the (algebraic) degree of a function on $\mathbb{F}_{p^n}$ is the maximum p-ary weight of the exponents in its polynomial representation, where the p-ary weight of an integer j is the sum of the coefficients in the base p representation of j. Hence, an affine function has all exponents of the form p^k (for some integers k) or 0, a quadratic function has (additionally) exponents of the form $p^k + p^\ell$, $k \leq \ell$.

The article is organized as follows. We start in Section 2 with some basic considerations of quasigroups, orthomorphisms and their relations to combinatorial designs. In Section 3, we describe some properties of $\wp$ and F for P$\wp$N functions F. We show that if for two permutations F, G of $\mathbb{F}_{p^n}$ for which $F(x + a) - G(x)$ is a permutation for every $a \in \mathbb{F}_{p^n}$, then $G(x) = \wp(F(x))$ for an orthomorphism $\wp$ (i.e., for a complete mapping $-\wp$). In Section 4, we confirm that such pairs of nonlinear permutations F, G exist for orthomorphisms $\wp$ other than $\wp(x) = cx$. (As we will see, linear permutations F are trivial examples of P$\wp$N functions for every orthomorphism $\wp$.)

In Section 5, we describe the quasigroup difference sets, which we can assign to a P$\wp$N function. We then analyze the incidence structure obtained from the development of the (quasigroup) difference set which we get from a P$\wp$N function for a linear orthomorphism $\wp$. Note that $\wp(x) = cx$ form a special class of linear orthomorphisms. We remark that there are now several examples of PcN functions in the literature, many of them for $c = -1$. The incidence structure has an interpretation as a generalization of a design obtained from a difference set in a group.

In Section 6, we analyze the equivalence for P$\wp$N functions. Naturally, the automorphism group of the quasigroup which comprises the corresponding difference set has to be considered. We will show that equivalence for P$\wp$N functions is included in EA-equivalence.

In Section 7, we discuss the above-mentioned observation related to differential attacks, and point to some perspectives for future research.

2 | COMPLETE MAPPINGS, ORTHOMORPHISMS AND LATIN SQUARES

We collect in this section some results on complete mappings and orthomorphisms and their connection to combinatorial objects, that may make our results more clear. For more information, we recommend [10], or any other book on algebraic designs that the reader prefers.

We recall that a set Q with a binary operation $\star$ is called a *quasigroup*, if, for all a, b in Q, the equations $a \star x = b$ and $y \star a = b$ have a unique solution $(x, y) \in Q^2$ (this is sometimes

called the *Latin square property*). Quasigroups do not necessarily have an identity. If the identity element exists a quasigroup is called a *loop*. Trivially, every group is a loop.

All *complete mappings*, respectively *orthomorphisms*, relevant for this article are permutations of a vector space, which we may represent with (the additive group of) a finite field. However one can define a complete mapping more general on an algebraic structure $(Q, \star)$ (for instance also a group or a quasigroup) as a bijective map ρ on Q such that $f(x) = \rho(x) \star x$ is also a bijective map on Q.

A *Latin square* (notion coming from Euler) is an $n \times n$ square matrix using n (the order of the Latin square) different elements, none of them occurring twice within any row or column of the matrix. A *transversal* of a Latin square of order n is a set of n entries, one in each row and each column, such that no two of the cells contain the same symbol.

Though the complete mappings relevant for this article are all complete mappings of a finite field, we also point to a connection of complete mappings of quasigroups with transversals of Latin squares given by a result of Johnson, Dulmage and Mendelsohn from 1961 [10, chapter 1]: If Q is a quasigroup with a complete mapping, then its multiplication table is a Latin square with a transversal. Conversely, if L is a Latin square having a transversal, then at least one of the quasigroups which have L as a multiplication table has a complete mapping. Finding classes of complete mappings on (abelian) groups (for instance, $\mathbb{F}_{p^n}$) is still an ongoing research. While we do not attempt to be all-inclusive here (as i.e., not the purpose of the paper), we mention, for example, the complete mappings on a finite field in [11, 12].

3 | PROPERTIES OF P$\wp$N FUNCTIONS

So far, research concentrated on P$\wp$N permutations F of $\mathbb{F}_{p^n}$, where $\wp(x) = cx$, $c \neq 1$, in which case F is called a PcN function.

Differently from PN functions, which can only exist for p odd, and for which, except for the Coulter–Matthews functions, all known examples are quadratic functions (and correspond to commutative semifields), quite some examples of PcN functions, $c \neq 1$, are known (though, not too many for even characteristic):

- Every linearized permutation of $\mathbb{F}_{p^n}$ is PcN for every $c \in \mathbb{F}_{p^n} \setminus \{1\}$.
- Every quadratic permutation of $\mathbb{F}_{p^n}$ is PcN for every $c \in \mathbb{F}_p \setminus \{1\}$, see [1].
- Further examples are given in the list in Appendix B.

We first extend a result of [1] to functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$.

Proposition 3.1. *Let p be an odd prime, $c \neq 1$ in the prime field $\mathbb{F}_p$, and let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a quadratic function, where $m|n$. Then F is balanced if and only if F is PcN.*

Proof. We first show that a quadratic function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ can be written as $F(x) = \mathrm{Tr}_m^n(G(x))$ for a quadratic function G on $\mathbb{F}_{p^n}$. Let $y \in \mathbb{F}_{p^m}$ such that $F(x_y) = y$ for some $x_y \in \mathbb{F}_{p^n}$. Then there exists an element $z_y \in \mathbb{F}_{p^n}$ such that $\mathrm{Tr}_m^n(z_y) = y$. Consider the function G on $\mathbb{F}_{p^n}$ such that $G(x_y) = z_y$. Then $F(x_y) = \mathrm{Tr}_m^n(G(x_y)) = \mathrm{Tr}_m^n(z_y) = y$, which implies that $F(x) = \mathrm{Tr}_m^n(G(x))$. Since F is a quadratic function and the relative trace function is linear, G is quadratic.

As $F(x) = \mathrm{Tr}_m^n(G(x))$, $F(x)$ is PcN if and only if $F(x+a) - cF(x) = \mathrm{Tr}_m^n(G(x+a) - cG(x))$ is balanced for every $a \in \mathbb{F}_{p^n}$. By [1, equation 1], for a quadratic function G on $\mathbb{F}_{p^n}$ and $c \neq 1$ in the prime field $\mathbb{F}_p$, we have

$$G(x+a) - cG(x) = \alpha G\left(x + \frac{a}{\alpha}\right) + \beta,$$

where $\alpha = 1 - c \in \mathbb{F}_p^*$, and $\beta = G(a) - \alpha G\left(\frac{a}{\alpha}\right) \in \mathbb{F}_{p^n}$. Therefore, $F(x)$ is PcN if and only if $F(x+a) - cF(x) = \mathrm{Tr}_m^n\left(\alpha G\left(x + \frac{a}{\alpha}\right) + \beta\right)$ is balanced, which clearly holds if and only if $\mathrm{Tr}_m^n(G(x)) = F(x)$ is balanced. □

In the next proposition, we obtain some first results on P$\wp$N functions F from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ with $\wp$ not necessarily of the form $\wp(x) = cx$.

Proposition 3.2. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a P$\wp$N function, with $\wp(x) \neq x$. Then F is balanced and $\wp(x) - x$ is a permutation of $\mathbb{F}_{p^m}$. In particular, for a permutation $\wp$ of $\mathbb{F}_{p^n}$, a P$\wp$N function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and the function $\wp(x) - x$ are always permutations.*

Proof. Since F is P$\wp$N, the function $F(x+a) - \wp(F(x))$ is balanced for all $a \in \mathbb{F}_{p^n}$. In particular, in the case $a = 0$, the function

$$F(x) - \wp(F(x)) = (x - \wp(x)) \circ F(x)$$

is balanced. Therefore, $x - \wp(x)$ is onto. This implies that $x - \wp(x)$ is a permutation of $\mathbb{F}_{p^m}$. Since $x - \wp(x)$ is a permutation, $((x - \wp(x)) \circ F(x))^{-1}(b) = F^{-1}(c)$, where $c - \wp(c) = b$. Therefore, the balancedness of $(x - \wp(x)) \circ F(x)$ implies that F is balanced. □

Remark 3.3. By Proposition 3.2, $\wp(x)$ and $\wp(x) - x$ being permutations is a necessary requirement for being P$\wp$N, if $\wp(x) \neq x$. We recall that a permutation $\wp$ for which $\wp(x) - x$ is also a permutation is called an orthomorphism. Note that, for a general prime p, $\wp$ is an orthomorphism if and only if $-\wp$ is a complete mapping. (Observe that, if $p = 2$, being an orthomorphism is equivalent to being a complete mapping). We also note that if $\wp$ is an orthomorphism then we could also consider $\wp(x) - x$ as a complete mapping, since $\wp(x) = \wp(x) - x + x$ implies that both $\wp(x) - x$ and $\wp(x)$ are permutations.

We can reformulate Proposition 3.2 for permutations as follows.

Corollary 3.4. *Let F, G be permutations of $\mathbb{F}_{p^n}$ such that $F(x+a) - G(x)$ is a permutation for every $a \in \mathbb{F}_{p^n}$. Then $G(x) = \wp(F(x))$ for some orthomorphism $\wp$ of $\mathbb{F}_{p^n}$.*

Remark 3.5. F is P$\wp$N for some orthomorphism $\wp$ if and only if F is P$\wp_c$N for the orthomorphism $\wp_c(x) = \wp(x) + c, c \in \mathbb{F}_{p^n}$. Hence we will always suppose that $\wp(0) = 0$.

Remark 3.6. In multivariate representation, a linear orthomorphism is an invertible matrix A, for which $A - I$ is also invertible.

The converse of Proposition 3.2 does not hold in general, but as we show in the next proposition, it does hold for linear functions F. This confirms that for every orthomorphism $\wp$, we have P$\wp$N functions, namely at least the linear ones.

Proposition 3.7. *Let $\wp$ be an orthomorphism of $\mathbb{F}_{p^m}$, that is, $\wp(x)$ and $\wp(x) - x$ are permutations of $\mathbb{F}_{p^m}$. A linear function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is P$\wp$N if and only if F is balanced. In particular, if $n = m$, then a linear function F on $\mathbb{F}_{p^n}$ is P$\wp$N if and only if F is a permutation.*

Proof. By Proposition 3.2, it is enough to show that if F is balanced, then F is P$\wp$N. As F is linear, for $a \in \mathbb{F}_{p^n}$ we have

$$F(x + a) - \wp(F(x)) = F(x) + F(a) - \wp(F(x)) = (x - \wp(x)) \circ F(x) + F(a).$$

Hence, $F(x + a) - \wp(F(x))$ is balanced if and only if $(x - \wp(x)) \circ F(x)$ is balanced. As $x - \wp(x)$ is a permutation and $F(x)$ is balanced, we obtain the assertion. □

This result can be extended to affine functions F, if $\wp$ is linearized.

Proposition 3.8. *Let $\wp$ be a linearized orthomorphism of $\mathbb{F}_{p^m}$. An affine function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is P$\wp$N if and only if F is balanced. In particular, if $n = m$, then an affine function F on $\mathbb{F}_{p^n}$ is P$\wp$N if and only if F is a permutation.*

Proof. Again, by Proposition 3.2, it is enough to show that if F is balanced, then F is P$\wp$N. We can write $F(x) = L(x) - \alpha$, where L is a linearized function, and $\alpha \in \mathbb{F}_{p^m}$. As L is linear, for $a \in \mathbb{F}_{p^n}$ we have

$$\begin{aligned} F(x + a) - \wp(F(x)) &= L(x) + L(a) - \alpha - (\wp(L(x)) - \wp(\alpha)) \\ &= (x - \wp(x)) \circ L(x) + L(a) - \alpha + \wp(\alpha). \end{aligned}$$

Hence, $F(x + a) - \wp(F(x))$ is balanced if and only if $(x - \wp(x)) \circ L(x)$ is balanced. As $x - \wp(x)$ is a permutation and $L(x)$ is balanced (note that L is balanced if and only if F is balanced), we obtain the assertion. □

4 | ORTHOMORPHISMS OTHER THAN $\wp(x) = cx$

As every linear permutation is P$\wp$N for every orthomorphism $\wp$, and every quadratic permutation is P$\wp$N for $\wp(x) = cx$, $c \in \mathbb{F}_p \setminus \{0, 1\}$, one may conclude that P$\wp$N functions are not very rare objects (for odd characteristic). In the meantime also several examples of nonlinear and not quadratic PcN functions are known for several values of c, see the tables in Appendix B.

However, if we only slightly change the orthomorphism cx to another linearized monomial $\wp(x) = cx^{p^j}$, the situation becomes quite different. With examples for small field size, one can computationally confirm that, in general, the simplest quadratic permutation of $\mathbb{F}_{2^n}$, the Gold function $F(x) = x^{2^k+1}$, $\gcd(2^n - 1, 2^k + 1) = 1$, is not P$\wp$N. In the following proposition, it is shown that for sufficiently large finite fields, the function x^{2^k+1} is never P$\wp$N for $\wp(x) = cx^{2^j}$.

This supports the assumption that for orthomorphisms other than $\wp(x) = cx$, P$\wp$N functions are harder to find.

Proposition 4.1. *For a divisor j of n, let $\wp(x) = cx^{2^j}$, where c is not a $(2^j - 1)$th power in $\mathbb{F}_{2^n}$. For every j, k, the Gold function $F(x) = x^{2^k+1}$ is not P$\wp$N for all sufficiently large n, with* $\gcd(2^n - 1, 2^k + 1) = 1$.

Proof. First note that $\wp$ is an orthomorphism since c is not a $(2^j - 1)$th power (which always exists as j divides n). We can suppose that $\gcd(2^n - 1, 2^k + 1) = 1$ since otherwise x^{2^k+1} is not a permutation.

To show that F is not P$\wp$N for all sufficiently large n, observe that

$$\begin{aligned} F(x + a) + \wp(F(x)) &= (x + a)^{2^k+1} + cx^{2^j(2^k+1)} \\ &= cx^{2^j(2^k+1)} + x^{2^k+1} + ax^{2^k} + a^{2^k}x + a^{2^k+1}. \end{aligned}$$

That is, $F(x + a) + \wp(F(x))$ is a permutation of $\mathbb{F}_{2^n}$ if and only if

$$H(x) = F(x + a) + \wp(F(x)) + a^{2^k+1} = cx^{2^j(2^k+1)} + x^{2^k+1} + ax^{2^k} + a^{2^k}x$$

is a permutation of $\mathbb{F}_{2^n}$. We will show that for sufficiently large n, there exists $a \in \mathbb{F}_{2^n}^*$ such that $H(x)$ has a nonzero root in $\mathbb{F}_{2^n}$, which gives the desired conclusion. Set $x = ay \neq 0$. Then we have

$$H(ay) = ca^{2^j(2^k+1)}y^{2^j(2^k+1)} + a^{2^k+1}y^{2^k+1} + a^{2^k+1}y^{2^k} + a^{2^k+1}y.$$

Hence $H(ay) = 0$ if and only if

$$a^{(2^j-1)(2^k+1)} = c^{-1}\frac{y^{2^k+1} + y^{2^k} + y}{y^{2^j(2^k+1)}}. \tag{3}$$

Recall that a^{2^k+1} is a permutation of $\mathbb{F}_{2^n}$ and $y \neq 0$. Hence, by setting $z = a^{2^k+1}$, Equation (3) holds if and only if

$$z^{2^j-1} = c^{-1}\frac{y^{2^k} + y^{2^k-1} + 1}{y^{2^j(2^k+1)-1}}. \tag{4}$$

Let F be the function field of the curve defined by Equation (4), that is, $F = \mathbb{F}_{2^n}(y, z)$ with $z^{2^j-1} = c^{-1}\left(y^{2^k} + y^{2^k-1} + 1\right)/y^{2^j(2^k+1)-1}$. Since $2^j - 1$ is a divisor of $2^n - 1$, $F/\mathbb{F}_{2^n}(y)$ is a Kummer extension of degree $2^j - 1$. For the properties of Kummer extensions, we refer to [20, proposition 3.7.3]. Note that $p(T) = T^{2^k} + T^{2^k-1} + 1$ is a separable polynomial. Therefore, any zero of $y^{2^k} + y^{2^k-1} + 1$ is totally ramified in $F/\mathbb{F}_{2^n}(y)$. This implies that $\mathbb{F}_{2^n}$ is the full constant field of F. Hence, Equation (4) defines an absolutely irreducible curve $\mathcal{X}$ over $\mathbb{F}_{2^n}$, see [20, corollary 3.6.8]. Then the Hasse–Weil bound [20, theorem 5.2.3] implies that $\mathcal{X}$ has a sufficiently large number of rational points for all sufficiently large values of n. Together with Bezout's theorem, we conclude

that there exists a rational point $(y, z) \in \mathcal{X}$ satisfying $yz \neq 0$. As $z = a^{2^k+1}$ and $y = ax$, this shows the existence of $a \in \mathbb{F}_{2^n}^*$ for which $G(x)$ has a nonzero root in $\mathbb{F}_{2^n}$. □

Remark 4.2. One can show that Proposition 4.1 applies at least for $n > 2(j + k)$. For the proof we refer to Appendix A.

There is a rich literature on construction of complete mappings, respectively, orthomorphisms, see Remark 3.3. We refer to [11, 12, 17, 21] and references therein. This potentially may provide a large variety of P℘N functions and quasigroup difference sets in a large variety of quasigroups (see next section). It appears to be hard to find (all) P℘N functions for a given class of orthomorphisms different from cx. In the remainder of this section, we provide a sporadic example for a complete mappping with Niho exponent in [12], and two infinite (nonlinear) classes of P℘N functions, one for characteristic 2 and one for odd characteristic.

Example 4.3. For an odd prime p, positive integers k, m, q, with $q = p^m$ and $\gcd(k, q + 1) = 1$, let $a, b \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. In [12], it is shown that $F(x) = ax^{kpq(q-1)+1} + bx^{kq(q-1)+1} + ax^{pk(q-1)+1} + bx^{k(q-1)+1} + (c^q + c)x$ is a complete mapping of $\mathbb{F}_{q^2}$ if $a = -b$, $\mathrm{Tr}_1^m\left(\frac{c^q+c}{a}\right) \neq 0$ and $\mathrm{Tr}_1^m\left(\frac{c^q+c+1}{a}\right) \neq 0$.

In the case, $m = 2$, $p = 3$, $k = 1$, $a = \alpha^{10}$, $b = \alpha^{50}$, $c = \alpha^5$, where $\alpha^4 + 2\alpha^3 + 2 = 0$, we confirm by MAGMA that the conditions are satisfied, hence $F(x) = ax^{217} - bx^{73} + ax^{25} - bx^9 + (c^9 + c)x$ is a complete mapping of $\mathbb{F}_{3^4}$, and that F is P℘N for the orthomorphism $\wp(x) = -F(x)$.

We continue with the two infinite (nonlinear) classes of P℘N functions. The first class is motivated by a complete mapping given in [11].

For a prime p and positive integers n, m with $n = 2m$, let $a, b \in \mathbb{F}_{p^n}^*$ with $a + b, a + b + 1 \in \mathbb{F}_{p^m}^*$, and $h(x) \in \mathbb{F}_{p^n}[x]$. Then $F(x) = ax^{p^m} + bx + h(x^{p^m} - x)$ is a complete mapping of $\mathbb{F}_{p^n}$ if and only if both $h(x)^{p^m} - h(x) + (b - a^{p^m})x$ and $h(x)^{p^m} - h(x) + (b - a^{p^m} + 1)x$ are bijective on $S = \{x^{p^m} - x \mid x \in \mathbb{F}_{p^n}\}$.

Our first class is obtained from F given as above with $p = 2$, $h(x) = x^3$ and $a = 0$, that is, $F(x) = bx + (x^{2^m} + x)^3$. Since in [11], $a = 0$ is excluded, in the proof of Theorem 4.4 below, we first show that $bx + (x^{2^m} + x)^3$ is a complete mapping.

Theorem 4.4. *Let $n = 2m$, m odd, $b \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ and let $F(x) = bx + (x^{2^m} + x)^3$. Then F is P℘N for the orthomorphism $\wp(x) = F(x) = bx + (x^{2^m} + x)^3$ of $\mathbb{F}_{2^n}$.*

Proof. We first show that F is a permutation polynomial of $\mathbb{F}_{2^n}$. Let ζ be an element satisfying $\zeta^2 + \zeta + 1 = 0$. Then $\{1, \zeta\}$ forms a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^m}$. Note that $\mathbb{F}_4 = \mathbb{F}_2(\zeta)$, that is, $\zeta^3 = 1$ and $\zeta^{2^m} = (\zeta^{2^{m-1}-1}\zeta)^2 = \zeta^2 = \zeta + 1$, as m is odd, and hence $3 \mid 2^{m-1} - 1$. Writing $x \in \mathbb{F}_{2^n}$ as $x = y + \zeta z$ for some unique $y, z \in \mathbb{F}_{2^m}$, we have the following equalities.

$$\begin{aligned} F(x) = bx + (x^{2^m} + x)^3 &= b(y + \zeta z) + ((y + \zeta z)^{2^m} + y + \zeta z)^3 \\ &= by + \zeta bz + (\zeta^{2^m} + \zeta)^3 z^3 \\ &= by + z^3 + \zeta bz, \end{aligned}$$

where we used $\zeta^{2^m} + \zeta + 1 = 0$ in the second equality. We immediately see that F is onto, hence a permutation. In fact for given $u + v\zeta$, we have $F(y + z\zeta) = u + v\zeta$ with $z = v/b$ and $y = (u + z^3)/b$ $(z = v/b)$. As readily seen, F is an orthomorphism as $\bar{b}\,x + (x^{2^m} + x)^3$ is a permutation for $\bar{b} = b + 1 \notin \{0, 1\}$.

It remains to show that $F(x + a) + F(F(x))$ is a permutation polynomial of $\mathbb{F}_{2^n}$ for all $a \in \mathbb{F}_{2^n}$. We have

$$\begin{aligned}
&F(x + a) + F(F(x))\\
&= b(x + a) + (x^{2^m} + x + a^{2^m} + a)^3 + F(bx + (x^{2^m} + x)^3)\\
&= b(x + a) + (x^{2^m} + x)^3 + (x^{2^m} + x)^2(a^{2^m} + a)\\
&\quad + (x^{2^m} + x)(a^{2^m} + a)^2 + (a^{2^m} + a)^3 + b(bx + (x^{2^m} + x)^3)\\
&\quad + \left((bx + (x^{2^m} + x)^3)^{2^m} + (bx + (x^{2^m} + x)^3)\right)^3\\
&= bx + ba + (x^{2^m} + x)^3 + (x^{2^m} + x)^2(a^{2^m} + a)\\
&\quad + (x^{2^m} + x)(a^{2^m} + a)^2 + (a^{2^m} + a)^3 + b^2x + b(x^{2^m} + x)^3\\
&\quad + \left(b^{2^m}x^{2^m} + (x^{2^m} + x)^3 + bx + (x^{2^m} + x)^3\right)^3.
\end{aligned}$$

We can ignore the constant term $ba + (a^{2^m} + a)^3$, set $a^{2^m} + a = c \in \mathbb{F}_{2^m}$, and show that

$$H(x) = (b + b^2)x + (b + 1)(x^{2^m} + x)^3 + c(x^{2^m} + x)^2 + (c^2 + b)(x^{2^m} + x)$$

is a permutation polynomial, where $H(x) = F(x + a) + F(F(x)) + ba + (a^{2^m} + a)^3$. Substituting $x = y + \zeta z$ into $H(x)$, and using the fact that $x^{2^m} + x = (y + \zeta z)^{2^m} + y + \zeta z = z$, we obtain

$$H(y + \zeta z) = (b + b^2)y + (b + 1)z^3 + cz^2 + (c^2 + b)z + \zeta(b + b^2)z.$$

Given $u, v \in \mathbb{F}_{2^m}$, we uniquely obtain $z = v/(b + b^2)$ and then y from $H(y + z\zeta) = u + v\zeta$. Note that $b + b^2 \neq 0$. Consequently, H is onto, hence it is a permutation. □

Remark 4.5. We observe that the function F given in Theorem 4.4 stays P℘N for any extension $\mathbb{F}_{2^{kn}}$ of $\mathbb{F}_{2^n}$ of odd degree k. In other words, F stays P℘N for infinitely many extensions $\mathbb{F}_{2^n}$. We call such a function F an exceptional P℘N function.

We now provide a class of P℘N functions on $\mathbb{F}_{p^n}$ for odd characteristic p.

Theorem 4.6. *Let m, k be positive integers, $n = 2m$, and q a power of an odd prime p. Let $F(x) = (x^{q^m} - x)^{2k} - x \in \mathbb{F}_{q^n}[x]$. Then F is a P℘N function with respect to the orthomorphism $\wp(x) = F(x)$.*

Proof. In [25] it is shown (with our notations) that if $\delta^{q^m} = -\delta$ and L is a p-linearized polynomial, then a polynomial of the form $G(x) = (x^{q^m} - x + \delta)^{2k} + L(x)$ is a

permutation polynomial on $\mathbb{F}_{q^n}$ if and only if L is a permutation polynomial. Taking $L(x) = -x$ and $\delta = 0$, it follows that $F = \wp$ is a permutation polynomial.

We next compute

$$\begin{aligned}
F(F(x)) &= \left((F(x)^{q^m} - F(x)\right)^{2k} - F(x) \\
&= \left(\left((x^{q^m} - x)^{2k} - x\right)^{q^m} - (x^{q^m} - x)^{2k} + x\right)^{2k} - (x^{q^m} - x)^{2k} + x \\
&= \left((x^{q^m} - x)^{2kq^m} - x^{q^m} - (x^{q^m} - x)^{2k} + x\right)^{2k} - (x^{q^m} - x)^{2k} + x \\
&= \left(\left(x^{q^{2m}} - x^{q^m}\right)^{2k} - x^{q^m} - (x^{q^m} - x)^{2k} + x\right)^{2k} - (x^{q^m} - x)^{2k} + x \\
&= \left((x - x^{q^m})^{2k} - x^{q^m} - (x^{q^m} - x)^{2k} + x\right)^{2k} - (x^{q^m} - x)^{2k} + x \\
&= x,
\end{aligned}$$

that is, F is self-invertible. Therefore, we have

$$F(x + a) - \wp(F(x)) = \left(x^{q^m} - x - a^{q^m} + a\right)^{2k} - (x + a) - x.$$

It will be sufficient to show that $H_a(x) = (x^{q^m} - x - a^{q^m} + a)^{2k} - 2x$ is a permutation. Taking $\delta = a^{q^m} - a$, $L(x) = -2x$ and observing that $\delta^{q^m} = -\delta$, for all a, using again the same result in [25], we infer that H_a is a permutation. □

Remark 4.7. We emphasize that by Example 4.3 and Theorem 4.6, the existence on nontrivial P$\wp$N functions is also guaranteed for nonquadratic orthomorphisms. We expect that one can find P$\wp$N functions also for several other classes of orthomorphisms respectively complete mappings in the literature. As a next, most likely difficult step, one could attempt to classify *all* orthomorphisms $\wp$ which permit nontrivial P$\wp$N functions, respectively some classes of nontrivial difference sets in their corresponding quasigroup (see the following section).

5 | P$\wp$N FUNCTIONS, DIFFERENCE SETS, AND DESIGNS

Let G be a group of order $\mu\nu$ with a normal subgroup N of order ν. A k-subset D of G is called a (μ, ν, k, λ) *relative difference set, relative to* N, if every element of $G\backslash N$ can be written as a difference of two elements in D in exactly λ ways, and there is no representation of this form for any nonzero element in N. A relative difference set is a generalization of a (ν, k, λ) *d*ifference set, which we can see as a relative difference set with trivial $N = \{0\}$ (and hence $\nu = 1$, $\nu = \mu\nu = \mu$).

The set of all translates $\{D + a : a \in G\}$ of a subset D in a group G, is called the *development* of D. If D is a (μ, ν, k, λ) relative difference set, then the development of D gives rise to a *divisible design* (the points are the elements of the group, the blocks are the translates $D + a$). We refer to [9] for further information on divisible designs. If D is a difference set ($\nu = 1$), then we obtain a symmetric design, where every two distinct points are simultaneously on exactly λ blocks, and every two blocks intersect in exactly λ points.

The definition of a bent function via balanced conventional derivatives has an equivalent version in terms of relative difference sets. A function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is bent if and only if the graph of F, $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_{p^n}\}$, is a (p^n, p^m, p^n, p^{n-m}) relative difference set in $\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$ relative to $\{0\} \times \mathbb{F}_{p^m}$.

Bent functions hence give also rise to divisible designs. We remark that for a planar function, the divisible design can be transformed into a projective plane, see [18, section 3.3].

The objective of this section is to relate P$\wp$N functions with the quasigroup difference sets. We then analyze the incidence structure obtained from the development of the (quasigroup) difference set, which we get from a P$\wp$N function for a linear orthomorphism $\wp$. The developments of these sets exhibit then properties comparable to those of designs.

5.1 | P$\wp$N functions and quasigroup difference sets

For a permutation $\wp$ of $\mathbb{F}_{p^m}$, we define the binary operation $+_\wp$ on the set $\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$ as

$$(x_1, y_1) +_\wp (x_2, y_2) = (x_1 + x_2, y_1 + \wp(y_2)).$$

Consequently, $(\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}, +_\wp)$ becomes a quasigroup.

We extend the definition of a difference set in finite groups to finite quasigroups. Note that for calculating the set of all differences in a subset D of $(Q, \star)$, it is only required that $(Q, \star)$ is a quasigroup.

Definition 5.1. Let D be a k-subset of a quasigroup Q of order v. Then D is called a (v, k, λ) quasigroup difference set in Q, if every element of Q can be written as a difference of two elements in D in exactly λ ways.

Remark 5.2. There is a slight difference between the definition of a difference set in a group and in a quasigroup. For a difference set D in a group G, all but the zero element (which not necessarily exists in a quasigroup) can be written as a difference of elements in D in λ ways. Clearly, in a group, the element 0 can be written as a difference of two elements of D in exactly $|D| = k$ ways. As a consequence, whereas the parameters of a difference set in a group satisfy $k(k-1) = (v-1)\lambda$, for a quasigroup difference set we have $k^2 = v\lambda$.

We can use any permutation $\wp$ to define a quasigroup, as given above. Our objective is to relate P$\wp$N functions to difference sets in such a quasigroup. By this we intend to point to some similarities to perfect nonlinear functions. In light of Proposition 3.2, we restrict ourselves to $\wp$ being an orthomorphism.

Theorem 5.3. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a function and $\wp$ a permutation of $\mathbb{F}_{p^m}$. Then the graph $\mathcal{G}_F$ of F is a (p^{n+m}, p^n, p^{n-m}) difference set in $(\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}, +_\wp)$ if and only if F is P$\wp$N. In particular, for the case $m = n$, the graph $\mathcal{G}_F$ is a $(p^{2n}, p^n, 1)$ difference set in $(\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}, +_\wp)$ if and only if F is P$\wp$N.*

Proof. First note that in a quasigroup $(Q, \star)$, a is the difference of b and c, if c is the unique solution of $a \star x = b$. In our quasigroup, (a, b) is then the difference of (x_1, y_1) and (x_2, y_2) if $a + x_2 = x_1$ and $b + \wp(y_2) = y_1$, that is, $a = x_1 - x_2$ and $b = y_1 - \wp(y_2)$.

For a fixed $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$, we determine the number of possibilities to write (a, b) as a difference (in the quasigroup) of two distinct elements in $\mathcal{G}_F$, that is, $(a, b) = (x_1 - x_2, F(x_1) - \wp(F(x_2)))$. This is exactly the number of x, such that $(a, b) = (a, F(x + a) - \wp(F(x)))$. If F is a P$\wp$N function, the number is exactly p^{n-m} for all $a \in \mathbb{F}_{p^n}$ and $b \in \mathbb{F}_{p^m}$, that is, $\mathcal{G}_F$ of F is a (p^{n+m}, p^n, p^{n-m}) difference set in $(\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}, +_\wp)$.

Conversely, suppose that $\mathcal{G}_F$ is a (v, k, λ) difference set in $(\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}, +_\wp)$. By Remark 5.2, we have $v = p^{n+m}$, $k = p^n$ and $\lambda = p^{n-m}$. That is, $\mathcal{G}_F$ is a (p^{n+m}, p^n, p^{n-m}) difference set in $(\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}, +_\wp)$. For the above-mentioned reason, this holds if and only if $F(x + a) - \wp(F(x)) = b$ has exactly p^{n-m} solutions in $\mathbb{F}_{p^n}$ for any $a \in \mathbb{F}_{p^n}$ and $b \in \mathbb{F}_{p^m}$. This implies that F is P$\wp$N. □

5.2 | P$\wp$N functions and designs

Whereas the difference set is defined with the group operation, for the design (which is simply an incidence relation between blocks and points) constructed from the difference set, the structure of the group is not relevant. We attempt to assign a class of incidence structure to the quasigroup difference sets obtained with P$\wp$N functions. As one may expect, the independence of the number of solutions for ${}_\wp D_a F(x) = b$ from a and b, again transfers to a property (in terms of λ) that pairs of points of the incidence structure satisfy simultaneously. For simplicity, we consider the case of linearized orthomorphisms $\wp(x)$. There are several examples for such functions known in the case $\wp(x) = -x$, see the list in Appendix B.

The development of the graph of F in the quasigroup $(\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}, +_\wp)$ consists of the sets $(x, F(x)) +_\wp (u, v) = (x + u, F(x) + \wp(v))$, $x \in \mathbb{F}_{p^n}$. Since $\wp(v)$ runs through $\mathbb{F}_{p^m}$ if v does, this equals the set of the conventional translates $(x, F(x)) + (u, v)$.

Theorem 5.4. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a P$\wp$N function, where $\wp$ is linear. Then the development of the graph of F yields an incidence structure with $v = p^n \times p^m$ points and v blocks, with the following properties:*

(i) *Every block contains $k = p^n$ points (elements of $\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$), and every point is on exactly k blocks.*
(ii) *The block set separates into a class of $r = p^n$ single blocks $B_1, ..., B_r$ and a class of $2s = (p^m - 1)p^n$ paired blocks $B_{r+1}, \overline{B}_{r+1}, ..., B_{r+s}, \overline{B}_{r+s}$. For every pair of points, the number of blocks among $B_1, ..., B_r$ which contain both elements simultaneously, and the number of pairs of blocks among $B_{r+1}, \overline{B}_{r+1}, ..., B_{r+s}, \overline{B}_{r+s}$, for which one element of the pair of points is in B_{r+i} and the other one is in $\overline{B}_{r+i}$, always add to p^{n-m}.*
(iii) *The point set separates into a class of r single points $P_1, ..., P_r$ and a class of $2s$ paired points $P_{r+1}, \overline{P}_{r+1}, ..., P_{r+s}, \overline{P}_{r+s}$. For every pair of blocks, the number of points among $P_1, ..., P_r$, which are on both blocks, and the number of pairs of points among $P_{r+1}, \overline{P}_{r+1}, ..., P_{r+s}, \overline{P}_{r+s}$, for which one point of the pair is in one of the two blocks, the other point is in the other block, always add to p^{n-m}.*

Proof. We first show (i). By definition, every block has k points. For a given point $(x_1, y_1) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$, we pick an element $(x, F(x))$ of the graph of F. Then

$(x_1, y_1) = (x, F(x)) + (u, v)$ for a unique $(u, v) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$, and (x_1, y_1) is a point of $\mathcal{G}_F + (u, v)$. Since there are k choices for an element of the graph, (x_1, y_1) is on k blocks.

Next, we look at (ii). We now divide the blocks into two classes. The first class consists of the p^n blocks of the form $\mathcal{G}_F + (u, 0)$, $u \in \mathbb{F}_{p^n}$. In the second class, the set of the remaining blocks, we form $p^n(p^m - 1)/2$ pairs of the form $\mathcal{G}_F + (u, v)$, $\mathcal{G}_F + (u, \wp^{-1}(v))$. Note that $\wp^{-1}(v) = v$ if and only if $\wp(v) = v$, that is, $-\wp(v) + v = 0$. Since $-\wp(v) + v$ is a permutation of $\mathbb{F}_{p^m}$, this holds if and only if $v = 0$. Hence, $(u, v) = (u, \wp^{-1}(v))$ happens if and only if $(u, v) = (u, 0)$.

Suppose that $(x_1, y_1) \in \mathcal{G}_F + (u, v)$ and $(x_2, y_2) \in \mathcal{G}_F + (u, \wp^{-1}(v))$. That is, $(x_1, y_1) = (d_1, F(d_1)) + (u, v)$ and $(x_2, y_2) = (d_2, F(d_2)) + (u, \wp^{-1}(v))$ for some $d_1, d_2 \in \mathbb{F}_{p^n}$. In other words, by the linearity of $\wp$ we have

$$\begin{aligned} u &= x_1 - d_1 = x_2 - d_2, \text{and} \\ v &= y_1 - F(d_1) = \wp(y_2) - \wp(F(d_2)). \end{aligned} \tag{5}$$

Then by setting $a = d_1 - d_2$, we have

$$(x_1, y_1) -_{\wp} (x_2, y_2) = (x_1 - x_2, y_1 - \wp(y_2)) = (a, F(a + d_2) - \wp(F(d_2))).$$

Since F is P$\wp$N, for $a \in \mathbb{F}_{p^n}$ the equation $F(a + d_2) - \wp(F(d_2)) = b$ has p^{n-m} solutions. In particular, the number d_2, equivalently, the number of u, satisfying Equation (5) is p^{n-m}. As we remarked, if $v = 0$, then the pairs lie in the same block $\mathcal{G}_F + (u, 0)$; otherwise they lie in the distinct blocks, namely, $\mathcal{G}_F + (u, v)$, $\mathcal{G}_F + (u, \wp^{-1}(v))$.

Finally, we show (iii). The class of single points is given by the points $(x, 0)$, $x \in \mathbb{F}_{p^n}$. The remaining points form s pairs (x, y), $(x, \wp^{-1}(y))$. Similarly, note that $\wp^{-1}(y) = y$ if and only if $y = 0$, that is, for nonzero $y \in \mathbb{F}_{p^n}$, the pairs (x, y), $(x, \wp^{-1}(y))$ are distinct.

Fix arbitrarily two (distinct) blocks $\mathcal{G}_F + (u_1, v_1)$, $\mathcal{G}_F + (u_2, v_2)$. We are interested in the number of $(x, y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$, such that (x, y) is in $\mathcal{G}_F + (u_1, v_1)$ and $(x, \wp^{-1}(y))$ is in $\mathcal{G}_F + (u_2, v_2)$. By the linearity of $\wp$, this is equivalent to

$$\begin{aligned} x &= d_1 + u_1 = d_2 + u_2, \text{and} \\ y &= F(d_1) + v_1 = \wp(F(d_2)) + \wp(v_2) \end{aligned} \tag{6}$$

for some $d_1, d_2 \in \mathbb{F}_{p^n}$. Set $a = u_2 - u_1$ and $b = \wp(v_2) - v_1$. Hence, we are looking for the number of elements d_2 satisfying $F(d_2 + a) - \wp(F(d_2)) = b$. Since F is P$\wp$N, the equation has p^{n-m} solutions, that is, there are p^{n-m} elements d_2 satisfying the equation. In other words, the number of elements $x \in \mathbb{F}_{p^n}$ satisfying Equation (6) is p^{n-m}. If $y \neq 0$, that is, $F(d_2) + v_2 \neq 0$, then the pairs (x, y), $(x, \wp^{-1}(y))$ lie in the distinct blocks $\mathcal{G}_F + (u_1, v_1)$, $\mathcal{G}_F + (u_2, v_2)$; otherwise $(x, 0)$ lies in both. □

Remark 5.5. As for the conventional symmetric designs, by the properties (i), (ii), (iii) in Theorem 5.4, the dual of the incidence structure, that is, the incidence structure obtained by changing the roles of points and blocks, has the same properties.

Remark 5.6. A design (which we obtain with the development of a difference set in a group) is an incidence structure as given in Theorem 5.4, for which all blocks (points) belong to the first class.

6 | EQUIVALENCE FOR P$\wp$N FUNCTIONS

Recall that if G, H are abelian groups and f, g are functions defined from G to H, then we say that f, g are *extended affine equivalent* (EA-equivalent) [3, 19] if there exist two automorphisms $\phi_1 \in \mathrm{Aut}(G)$, $\phi_2 \in \mathrm{Aut}(H)$ (the automorphism group of G, respectively, H), and $\psi \in \mathrm{Hom}(G, H)$ (the group of homomorphisms from G to H), $c_1 \in G, c_2 \in H$ such that $g(x) = \phi_2(f(\phi_1(x) + c_1)) + \psi(x) + c_2$. If $\psi = 0$, we recover the *affine equivalence*.

Clearly, the P$\wp$N property is not invariant under the classical (extended) affine equivalence, using automorphisms of the elementary abelian group.

Since P$\wp$N functions are meaningful seen as maps from the elementary abelian group $(\mathbb{F}_{p^n}, +)$ to the quasigroup $(\mathbb{F}_{p^m}, \star)$ with $y_1 \star y_2 = y_1 + \wp(y_2)$, for the equivalence transformations that preserve the P$\wp$N property, one apparently has to look at the automorphism group corresponding to the quasigroup operation.

Two functions $F_1, F_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ are *$\wp$-affine equivalent*, if $F_2 = \mathcal{A}_2(F_1(\mathcal{A}_1(x)))$, where

$$\mathcal{A}_1(x) = \mathcal{L}_1(x) + \alpha_1$$

for some linearized permutation $\mathcal{L}_1$ of $\mathbb{F}_{p^n}$ and $\alpha_1 \in \mathbb{F}_{p^n}$ (as for conventional affine equivalence), and

$$\mathcal{A}_2(x) = \mathcal{L}_2(x) + \wp(\overline{\alpha_2}) = \mathcal{L}_2(x) + \alpha_2$$

for some $\overline{\alpha_2} \in \mathbb{F}_{p^m}$, with $\wp(\overline{\alpha_2}) = \alpha_2$, and a permutation $\mathcal{L}_2$ of $\mathbb{F}_{p^m}$ satisfying $\mathcal{L}_2(y_1 + \wp(y_2)) = \mathcal{L}_2(y_1) + \wp(\mathcal{L}_2(y_2))$ for all $y_1, y_2 \in \mathbb{F}_{p^m}$. Then the graphs of F_1, F_2 are equivalent as subsets of the quasigroup $(\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}, +_\wp)$.

Lemma 6.1. *Let $\wp$ be a permutation of $\mathbb{F}_{p^m}$ (an orthomorphism) with $\wp(0) = 0$, and let $\mathcal{L}$ be a permutation of $\mathbb{F}_{p^m}$, such that $\mathcal{L}(y_1 + \wp(y_2)) = \mathcal{L}(y_1) + \wp(\mathcal{L}(y_2))$ for all $y_1, y_2 \in \mathbb{F}_{p^m}$. Then $\mathcal{L}$ is a linear permutation.*

Proof. Let $\mathcal{L}(y_1 + \wp(y_2)) = \mathcal{L}(y_1) + \wp(\mathcal{L}(y_2))$. For the unique y_2 for which $\mathcal{L}(y_2) = 0$ we have $y_1 + \wp(y_2) = y_1$, hence $\wp(y_2) = 0$, that is, $y_2 = 0$ and $\mathcal{L}(0) = 0$. Setting $y_1 = 0$, we then infer that $\mathcal{L}(\wp(y_2)) = \wp(\mathcal{L}(y_2))$ for every y_2. Consequently, $\mathcal{L}(y_1 + \wp(y_2)) = \mathcal{L}(y_1) + \wp(\mathcal{L}(y_2)) = \mathcal{L}(y_1) + \mathcal{L}(\wp(y_2))$ for all $y_1, y_2 \in \mathbb{F}_{p^m}$. Since we can write every y_3 as $\wp(y_2)$, we infer that $\mathcal{L}(y_1 + y_3) = \mathcal{L}(y_1) + \mathcal{L}(y_3)$ for all $y_1, y_3 \in \mathbb{F}_{p^m}$. □

In light of Lemma 6.1, F_1 and $F_2 = \mathcal{A}_2(F_1(\mathcal{A}_1(x)))$ are *$\wp$-linear equivalent*, if $\mathcal{A}_1, \mathcal{A}_2$ defined as above are linearized permutations, that is, $\alpha_1 = 0$ and $\alpha_2 = 0$.

With Lemma 6.1 we can completely describe $\wp$-affine (respectively linear) equivalence.

Theorem 6.2. *$F_1, F_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ are $\wp$-affine equivalent if and only if $F_2(x) = \mathcal{A}_2(F_1(\mathcal{A}_1(x)))$, where $\mathcal{A}_i = \mathcal{L}_i + \alpha_i$, $\alpha_1 \in \mathbb{F}_{p^n}$, $\alpha_2 \in \mathbb{F}_{p^m}$, $\mathcal{L}_1$ a linearized permutation of $\mathbb{F}_{p^n}$ and $\mathcal{L}_2$ a linearized permutation of $\mathbb{F}_{p^m}$ such that $\mathcal{L}_2(\wp(x)) = \wp(\mathcal{L}_2(x))$ for all $x \in \mathbb{F}_{p^m}$. In particular, $F_2(x) = \mathcal{A}_2(F_1(\mathcal{A}_1(x)))$ is P$\wp$N if and only if F_1 is P$\wp$N.*

We observe that $\wp$-affine equivalence is included in conventional affine equivalence.

Example 6.3. Let $\wp(x) = cx$, then the condition $\wp(\mathcal{L}(x)) = \mathcal{L}(\wp(x))$ reduces to $c\mathcal{L}(x) = \mathcal{L}(cx)$. If c is not in the prime field $\mathbb{F}_p$, this is a restriction on the linear permutation $\mathcal{L}$.

Recall that for every orthomorphism $\wp$, every linear permutation (respectively linear balanced function) is P$\wp$N. Clearly, two linear permutations are $\wp$-linear equivalent. Consequently, the linear permutations form one $\wp$-linear equivalence class of P$\wp$N functions on $\mathbb{F}_{p^n}$. As representative of the equivalence class, we may choose $F(x) = x$. The quasigroup difference set corresponding to a linear permutation is hence equivalent as a subset of $(\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}, +_\wp)$ to $\{(x, x) : x \in \mathbb{F}_{p^n}\}$. Note that a similar statement can be made for affine permutations and equivalence under the condition $\wp$ linearized.

On the other hand, two quadratic permutations as P$\wp$N functions, if we just restrict to $\wp(x) = cx$, $c \in \mathbb{F}_p$, $c \neq 1$, are in general not $\wp$-affine equivalent.

7 | PERSPECTIVES FOR FUTURE RESEARCH

In this paper, for the first time, we find a connection between the c-differential uniformity (cDU) and combinatorial designs. In particular, we show that the graph of a PcN function corresponds to a difference set in a quasigroup. Difference sets give rise to symmetric designs, which are known to construct optimal self complementary codes. Some types of designs can be also used in secret sharing and visual cryptography. We extend the PcN function to any orthomorphism $\wp$, not restricted to $x \mapsto cx$, and that enables us to define an equivalence relation among perfect $\wp$-nonlinear functions. We also provide an idea for a possible extension of the differential attack.

Lately there has been considerable progress in constructing PcN functions, in particular, but not only, in characteristic two. We refer to the table in the appendix and the corresponding references. In this article, we give two families of P$\wp$N functions for $\wp(x)$ other than cx. It is to be expected that many more classes of PcN ($c \neq 1$; recall that for $c = 0$, PcN functions are simply permutations), and more general, P$\wp$N functions can be found with moderate effort, though, perhaps not in the binary case, where there is only *one* known nontrivial monomial PcN class (some only for $c = -1$), and about nine polynomials ones (constructed via some switching of a linearized polynomial). Thus, in odd characteristic, this is somewhat opposite to the situation for planar functions. In view of the above, at this point, other more general questions should be asked.

To give a complete description of all P$\wp$N functions for some given orthomorphism $\wp$, and in this way to describe (up to equivalence) all difference sets of this type in the corresponding quasigroup, may be interesting. Another interesting question is also whether nonlinearized P$\wp$N functions exist for all orthomorphisms $\wp$, or whether for some orthomorphisms, the corresponding quasigroup has only $\{(x, x) : x \in \mathbb{F}_{p^n}\}$ as a difference set (arising from a graph of a function).

Some questions may arise from the connection to permutation polynomials. Are there interesting permutation polynomials among ${}_\wp D_a(F(x))$? (equivalence questions would have to be addressed.) Are there (other) properties, which are specific to the permutations ${}_\wp D_a(F(x))$?

We conclude this article with an observation about a higher order c-differential attack, that may help circumvent the key addition non-cancellation in an extension of the differential attack.

We consider a round function (S-box) F of a cipher (operating over a finite field of any characteristic p) with a postwhitening key K_1. Computing the c-differential of $F + K_1$ at c_1, we get

$$_{c_1}D_a(F + K_1)(x) = F(x + a) + K_1 - c_1(F(x) + K_1) =: G(x).$$

As in the case of higher order differential cryptanalysis, we continue with another round key K_2 and obtain

$$\begin{aligned} _{c_2}D_b(G + K_2)(x) &= G(x + b) - c_2G(x) + (1 - c_2)K_2 \\ &= F(x + a + b) - c_1F(x + b) - c_2F(x + a) + c_1c_2F(x) \\ &\quad + (1 - c_2)(1 - c_1)K_1 + (1 - c_2)K_2. \end{aligned}$$

Thus if either $c_2 = 1$ (hence, the second derivative is the classical one), or $c_2 \neq 1$ and the round key constants are related by $K_2 = -(1 - c_1)K_1$, the round keys will disappear and we get

$$\begin{aligned} _{c_2}D_b(_{c_1}D_a(F + K_1) + K_2)(x) &= {}_{c_1}D_aF(x + b) - c_2 \cdot {}_{c_1}D_aF(x) \\ &= {}_{c_2}D_b(_{c_1}D_a(F))(x). \end{aligned}$$

What that means is that the keyspace has to avoid round keys, like K_1, K_2, whose quotients $1 + K_2/K_1$ cannot be a constant c_1 such that the c_1-differential uniformity of F is rather high. In [7], it is shown that the second order cDU with respect to c (i.e., $c_1 = c_2 = c$) is at least the value of the cDU of F. Perhaps, it is worth investigating some of the known good cryptographic functions with respect to a sequence of derivatives, and investigate their higher order cDU, as in [7], since, as we see above, there are instances where the key addition disappears.

ACKNOWLEDGMENTS

Nurdagül Anbar and Tekgül Kalaycı are supported by TÜBİTAK Project under Grant 120F309. Wilfried Meidl is supported by the FWF Project P 35138. Constanza Riera is supported by Research Council of Norway under Grants 311646. Pantelimon Stănică is partially supported by a grant from the NPS Foundation.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no data sets were generated or analyzed during the current study.

ORCID


Pantelimon Stănică http://orcid.org/0000-0002-8622-7120

REFERENCES

1. D. Bartoli and M. Calderini, *On construction and (non) existence of c-(almost) perfect nonlinear functions*. Finite Fields Appl. **72** (2021), 101835.
2. E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*. J. Cryptol. **4** (1991), no. 1, 3–72.

3. C. Carlet, P. Charpin, and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*. Des. Codes Cryptogr. **15** (1998), 125–156.
4. C. Carlet and S. Mesnager, *Four decades of research on bent functions*. Des. Codes Cryptogr. **78** (2016), 5–50.
5. P. Ellingsen, P. Felke, C. Riera, P. Stănică, and A. Tkachenko, *C-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity*. IEEE Trans. Inform. Theory. **66** (2020), 5781–5789.
6. K. Garg, S. U. Hasan, and P. Stănică, *Several classes of permutation polynomials and their differential uniformity properties*. https://arxiv.org/pdf/2212.01931.pdf
7. A. Geary, M. Calderini, C. Riera, and P. Stănică, *Higher order c-differentials*, Proc. Int. Conf. on Security and Privacy Springer (ICSP 2021) (P. Stănică, S. Mesnager, and S. K. Debnath, eds.), Springer, Cham, Communications and Information Science 1497, 2021, pp. 3–15.
8. S. U. Hasan, M. Pal, C. Riera, and P. Stănică, *On the c-differential uniformity of certain maps over finite fields*. Des. Codes Cryptogr. **89** (2021), 221–239.
9. D. Jungnickel, *On automorphism groups of divisible designs*. Canadian J. Math. **34** (1982), 257–297.
10. A. D. Keedwell, and J. Dénes, *Latin squares and their applications*, 2nd ed., Elsevier, 2015.
11. L. Li, C. Li, C. Li, and X. Zeng, *New classes of complete permutation polynomials*. Finite Fields Appl. **55** (2019), 177–201.
12. L. Li, Q. Wang, Y. Xu, and X. Zeng, *Several classes of complete permutation polynomials with Niho exponents*. Finite Fields Appl. **72** (2021), Paper No. 101831, 31pp.
13. C. Li, C. Riera, and P. Stănică, *Low c-differentially uniform functions via an extension of Dillon's switching method*. Boolean Functions and Applications 2022, Paper #1. https://arxiv.org/pdf/2204.08760.pdf
14. W. Meidl, *A survey on p-ary and generalized bent functions*. Cryptogr. Commun. **14** (2022), no. 4, 737–782.
15. S. Mesnager, C. Riera, P. Stănică, H. Yan, and Z. Zhou, *Investigation on c-(almost) perfect nonlinear functions*. IEEE Trans. Inf. Theory. **67** (2021), no. 10, 6916–6925.
16. K. Nyberg, *Perfect nonlinear S-boxes*, Advances in cryptology-EUROCRYPT '91 (Brighton, 1991), Lecture Notes in Computer Science, vol. **547**, Springer, Berlin, 1991, pp. 378–386.
17. E. Pasalic, N. Cepak, and Y. Wei, *Infinite classes of vectorial plateaued functions, permutations and complete permutations*. Discrete Appl. Math. **215** (2016), 177–184.
18. A. Pott, *Almost perfect and planar functions*. Des. Codes Cryptogr. **78** (2016), 141–195.
19. A. Pott and Y. Zhou, *CCZ and EA equivalence between mappings over finite Abelian groups*. Des. Codes Cryptogr. **66** (2013), 99–109.
20. H. Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics. vol. 254, Springer Verlag, 2009.
21. B. Sun, K. Li, J. Guo, and L. Qu, *New constructions of complete permutations*. IEEE Trans. Inform. Theory. **67** (2021), no. 11, 7561–7567.
22. X. Wang, D. Zheng, and L. Hu, *Several classes of PcN power functions over finite fields*. Discrete Appl. Math. **15** (2022), no. 322, 171–182.
23. Y. Wu, N. Li, and X. Zeng, *New PcN and APcN functions over finite fields*. Des. Codes Cryptogr. **89** (2021), 2637–2651.
24. H. Yan, *On* (-1)*-differential uniformity of ternary APN power functions*. Cryptogr. Commun. **2** (2022), 357–369.
25. P. Yuan and C. Ding, *Further results on permutation polynomials over finite fields*. Finite Fields Appl. **27** (2014), 88–103.
26. Z. Zha and L. Hu, *Some classes of power functions with low c-differential uniformity over finite fields*. Des. Codes Cryptogr. **89** (2021), 1193–1210.

How to cite this article: N. Anbar, T. Kalaycı, W. Meidl, C. Riera, and P. Stănică, *PℊN functions, complete mappings and quasigroup difference sets*, J. Combin. Des. (2023), 1–24. https://doi.org/10.1002/jcd.21916

APPENDIX A

Proposition A.1. *Proposition 4.1 applies for all $n > 2(j + k)$.*

Proof. To show the statement on a sufficient condition on the size of n, we can study geometric properties of the curve given in Equation (4), namely $z^{2^j-1} = c^{-1}\frac{y^{2^k}+y^{2^k-1}+1}{y^{2^j(2^k+1)-1}}$, and its function field. Let F be the function field defined by Equation (4). As we observed, $F/\mathbb{F}_{2^n}(y)$ is a Kummer extension of degree $2^j - 1$. Ramified places are determined by the zeros and the poles of $\left(y^{2^k} + y^{2^k-1} + 1\right)/y^{2^j(2^k+1)-1}$ and their multiplicities. Since the zeros of $y^{2^k} + y^{2^k-1} + 1$ are simple, they are totally ramified. Moreover, $\gcd(2^j - 1, 2^j(2^k + 1) - 1) = 1$ implies that the zero of y is totally ramified. Note that the multiplicity of the pole of y is $(2^j - 1)(2^k + 1)$, that is, it is divisible by the degree of the extension. Hence, the pole of y is not ramified. Then by the Hurwitz genus formula, the genus $g(F)$ satisfies

$$2g(F) - 2 = (2^j - 1)(-2) + (2^j - 2)(2^k + 1),$$

that is, $2g(F) = (2^j - 2)(2^k - 1)$. Hence the number $N(F)$ of rational places of F satisfies

$$N(F) \geq 2^n + 1 - (2^j - 2)(2^k - 1)2^{n/2}. \tag{A1}$$

Now we investigate the geometric properties of the curve $\mathcal{X}$ defined by Equation (4), that is, $f(y, z) = cz^{2^j-1}y^{2^j(2^k+1)-1} + y^{2^k} + y^{2^k-1} + 1$. There are two rational points of $\mathcal{X}$ lying at infinity, namely $(0 : 1 : 0)$ of multiplicity $2^j(2^k + 1) - 1$ corresponding to the unique rational place lying above the zero of y and $(1 : 0 : 0)$ of multiplicity $2^j - 1$ corresponding to the places lying over the pole of y. Hence, there are at most 2^j rational places corresponding to the points at infinity. Recall that an affine point (α, β) is a singular point of $\mathcal{X}$ if and only if $f(\alpha, \beta) = (\partial f(y, z)/\partial y)(\alpha, \beta)) = (\partial f(y, z)/\partial z)(\alpha, \beta)) = 0$, where $\partial f(y, z)/\partial y$ and $\partial f(y, z)/\partial z$ are the partial derivatives of f with respect to y and z, respectively. Since $\partial f(y, z)/\partial y = cz^{2^j-1}y^{2^j(2^k+1)-2} + y^{2^k-2}$ and $\partial f(y, z)/\partial z = cz^{2^j-2}y^{2^j(2^k+1)-1}$, the curve $\mathcal{X}$ has no affine singular points. It is a well-known fact that each non-singular rational point corresponds to a unique rational place. From the above argument and Equation (A1), we conclude that the number $N(\mathcal{X})$ of rational affine points of $\mathcal{X}$ satisfies

$$N(\mathcal{X}) \geq 2^n - (2^j - 2)(2^k - 1)2^{n/2} - (2^j - 1).$$

Moreover, the line defined by y intersects $\mathcal{X}$ only at infinity, and the line defined by z intersects $\mathcal{X}$ at most at 2^k affine rational points. Hence, the number N of rational points (y, z) with $yz \neq 0$ satisfies $N \geq 2^n - (2^j - 2)(2^k - 1)2^{n/2} - (2^j - 1) - 2^k$, which gives the desired result. □

APPENDIX B

We include here two tables, which are taken from [13] and updated, containing some of the known classes with low c-differential uniformity (cDU) (we make the choice to include only the

TABLE B1 ${}_c\Delta_F$ of various classes of functions x^d, $c \neq 1$.

d	$\mathbb{F}_{p^n}$	${}_c\Delta_F$	Conditions	Ref
2	$p > 2$	2 (APcN)	None	[5]
$\frac{3^k+1}{2}$	$p = 3$	1 (PcN)	$c = -1$, $\frac{2n}{\gcd(k,2n)}$ is odd	[5]
$p^n - 2$	any p	1 (PcN)	$c = 0$	[5]
$2^n - 2$	$p = 2$	2 (APcN)	$c \neq 0$, $\mathrm{Tr}_n(c) = \mathrm{Tr}_n(1/c) = 1$	[5]
$2^n - 2$	$p = 2$	3	$c \neq 0$, $\mathrm{Tr}_n(c) = 0$ or $\mathrm{Tr}_n(1/c) = 0$	[5]
$p^n - 2$	$p > 2$	2 (APcN)	$c \neq 0$, $(c^2 - 4c) \notin [\mathbb{F}_{p^n}]^2$, $(1 - 4c) \notin [\mathbb{F}_{p^n}]^2$, or $c = 4, 4^{-1}$	[5]
$p^n - 2$	$p > 2$	3	$c \neq 0, 4, 4^{-1}$, $(c^2 - 4c) \in [\mathbb{F}_{p^n}]^2$ or $(1 - 4c) \in [\mathbb{F}_{p^n}]^2$	[5]
$2^k + 1$	$p = 2$	$\frac{2^{\gcd(2k,n)}-1}{2^{\gcd(k,n)}-1}$	$c \in \mathbb{F}_{2^{\gcd(n,k)}} \setminus \{1\}$, $\frac{n}{\gcd(n,k)} \geq 3 (n \geq 3)$	[15]
$2^k + 1$	$p = 2$	$2^{\gcd(n,k)} + 1$	$c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^{\gcd(n,k)}}$	[15]
$p^k + 1$	any p	$\gcd(p^k + 1, p^n - 1)$	$c \in \mathbb{F}_{p^{\gcd(n,k)}}$	[15]
$\frac{p^k+1}{2}$	$p > 2$	$p^{\gcd(n,k)} + 1$	$c = -1$	[15]
$\frac{p^n+1}{2}$	$p > 2$	≤ 4	$c \neq \pm 1$	[15]
$\frac{p^n+1}{2}$	$p > 2$	≤ 2	$c \neq \pm 1$, $\eta\left(\frac{1-c}{1+c}\right) = 1 p^n \equiv 1 \pmod 4$[	[15]
$\frac{2p^n-1}{3}$	any	≤ 3	$p^n \equiv 2 \pmod 3$	[15]
$\frac{p^n+3}{2}$	$p > 3$	≤ 3	$c = -1$, $p^n \equiv 3 \pmod 4$	[15]
$\frac{p^n+3}{2}$	$p > 3$	≤ 4	$c = -1$, $p^n \equiv 1 \pmod 4$	[15]
$\frac{p^n-3}{2}$	$p > 2$	≤ 4	$c = -1$	[15]

(Continues)

TABLE B1 (Continued)

d	$\mathbb{F}_{p^n}$	${}_c\Delta_F$	Conditions	Ref
$\frac{3^n+3}{2}$	$p=3$	2 (APcN)	$c=-1$, n even	[15]
$\frac{3^n-3}{2}$	$p=3$	6	$c=-1$, $n=0 \pmod 4$	[15]
$\frac{3^n-3}{2}$	$p=3$	4	$c=-1$, $n\neq 0 \pmod 4$	[15]
$\frac{3^n-3}{2}$	$p=3$	2 (APcN)	$c=0$,	[15]
$\frac{3^n+1}{4}(\frac{3^k+1}{4})^{-1}$	$p=3$	1 (PcN)	n,k odd, $c=-1$, $\gcd(n,k)=1$	[26]
$\frac{5^n-1}{2}+(\frac{5^k+1}{2})^{-1}$	$p=5$	1 (PcN)	n,k odd, $c=-1$, $\gcd(n,k)=1$	[26]
$\frac{p^n+1}{2}(p^k+1)^{-1}$	$p>2$	≤ 6	d even, $c=-1$, $p^n\equiv 3 \pmod 4$	[26]
$\frac{p^n+1}{2}(p^k+1)^{-1}$	$p>2$	≤ 3	d odd, $c=-1$, $p^n\equiv 3 \pmod 4$	[26]
$\frac{p^n+1}{4}+\frac{p^n-1}{2}$	$p>2$	≤ 3	$c=-1$, $p^n\equiv 7 \pmod 8$	[26]
$\frac{p^n-1}{2}+p^k+1$	$p>2$	≤ 3	$c=-1$, $\frac{n}{\gcd(n,k)}$ odd, $p^n\equiv 3 \pmod 4$	[26]
$\frac{p^n-1}{2}+p^k+1$	$p>2$	≤ 6	$c=-1$, $\frac{n}{\gcd(n,k)}$ odd, $p^n\equiv 1 \pmod 4$	[26]
$\frac{p^l+1}{2}$	$p>2$	1 (PcN)	$c=-1$, $l=0$ or l even and n odd, or l,n both even together with $t_2\geq t_1+1$, where $n=2^{t_1}u$ and $l=2^{t_2}$ such that $2\nmid u,v$	[8]
$\frac{p^l+1}{2}$	$p>2$	$\frac{p+1}{2}$	$c=-1$, $\gcd(l,2n)=1$, $p\equiv 1 \pmod 4$ or $p\equiv 3 \pmod 8$	[8]
$\frac{5^l+1}{2}$	$p=5$	3	$c=-1$, $\gcd(l,2n)=1$	[8]
$\frac{3^l+1}{2}$	$p=3$	2 (APcN)	$c=-1$, $\gcd(l,2n)=1$	[8]
$p^4+(p-2)p^2+p(p-1)+1$	$p>2$	1 (PcN)	$c=-1$, $n=5$	[8]

TABLE B1 (Continued)

d	$\mathbb{F}_{p^n}$	${}_c\Delta_F$	Conditions	Ref
$\frac{p^5+1}{p+1}$	$p>2$	1 (PcN)	$c=-1$, $n=5$	[8]
$(p-1)p^6+p^5+(p-2)p^3+(p-1)p^2+p$	$p>2$	1 (PcN)	$c=-1$, $n=7$	[8]
$\frac{p^7+1}{p+1}$	$p>2$	1 (PcN)	$c=-1$, $n=7$	[8]
$\frac{3^n+7}{2}$	$p=3$	≤2 (APcN)	$c=-1$, n odd	[23]
$\frac{3^{\frac{n+1}{2}}-1}{2}$	$p=3$	≤2 (APcN)	$c=-1$, $n\equiv 1 \pmod 4$	[24]
$\frac{3^{\frac{n+1}{2}}-1}{2}+\frac{3^n-1}{2}$	$p=3$	≤2 (APcN)	$c=-1$, $n\equiv 3 \pmod 4$	[24]
$\frac{3^{n+1}-1}{8}$	$p=3$	≤2 (APcN)	$c=-1$, $n\equiv 1 \pmod 4$	[24]
$\frac{3^{n+1}-1}{8}+\frac{3^n-1}{2}$	$p=3$	≤2 (APcN)	$c=-1$, $n\equiv 3 \pmod 4$	[24]
$(3^{\frac{n+1}{4}}-1)(3^{\frac{n+1}{2}}+1)$	$p=3$	≤4	$c=-1$, $n\equiv 3 \pmod 4$	[24]
$\frac{3^n+1}{4}+\frac{3^n-1}{2}$	$p=3$	≤4	$c=-1$, n odd	[24]
$d^{-1} \pmod{p^n-1}$	any p	1 (Pc′N)	x^d is PcN, $c'=c^d$	[22]
$\{2^j, 2^j(2^k+1), k,j\geq 0\}$	$p=2$	1 (PcN)		[22]
odd $2(p^k+1)^{-1} \pmod{p^n-1}$, $k\geq 0$	$p>2$	1 (PcN)	$c=-1$	[22]
$\frac{p^n+1}{2}\left(\frac{p^k+1}{2}\right)^{-1}$	$p>2$	1 (PcN)	$c=-1$, $v_2(k)=v_2(n)$, $p^n\equiv 1 \pmod 4$	[22]

TABLE B2 ${}_c\Delta_F$ of various classes of functions $F(x)$, $c \neq 1$.

$F(x)$	$\mathbb{F}_{p^n}$	${}_c\Delta_F$	Conditions	Ref
$x^{10} - ux^6 - u^2x^2$	$p = 3$	≥ 2	$u \in \mathbb{F}_{3^n}$	[5]
$L(x)\left(\sum_{i=1}^{l-1} L(x)^{\frac{p^n-1}{l}i} + u\right)$	any p	≤ 2 (APcN)	L an $\mathbb{F}_p$-linearized polynomial, $l \mid (p^n - 1)$, $u \neq 1, (1-l) \bmod p, 1 - \frac{l}{(1-c)(u+l-1)}, 1 + \frac{l}{(1-c)(u-1)} \in D_0$	[23]
$(x^{p^k} - x)^{\frac{q-1}{2}+1} + a_1x + a_2x^{p^k} + a_3x^{p^{2k}}$	$p = 3$	≤ 2 (APcN)	$c = -1$, $0 \leq i \leq 2$, $a_1, a_2, a_3 \in \mathbb{F}_3$, $a_1 + a_2 + a_3 \neq 0$	[23]
$f(x)(\mathrm{Tr}_n(x) + 1) + f(x + \gamma)\mathrm{Tr}_n(x)$	$p = 2$	1 (PcN)	$f(x)$ is PcN, $\gamma \in \mathbb{F}_{p^n}^*$	[23]
$L(x) + L(\gamma)(\mathrm{Tr}_n(x))^{q-1}$	any p	1 (PcN)	L an $\mathbb{F}_q$-linearized polynomial, $\gamma \in \mathbb{F}_q^*$, $\mathrm{Tr}_n(\gamma) = 0$	[23]
$u\phi(x) + g((\mathrm{Tr}_n(x))^q) - g(\mathrm{Tr}_n(x))$	any p	1 (PcN)	ϕ an $\mathbb{F}_q$-linearized polynomial, $u \in \mathbb{F}_q^*$, $\ker(\phi) \cap \ker(\mathrm{Tr}_n) = \{0\}$, $g \in \mathbb{F}_{q^n}[x]$	[23]
$u(x^q - x) + g(\mathrm{Tr}_n(x))$	any p	1 (PcN)	$g \in \mathbb{F}_{q^n}[x]$ a permutation of $\mathbb{F}_q$, $u \in \mathbb{F}_q^*$, $p \nmid n$	[23]
$F(x) + u\mathrm{Tr}_n(vF(x))$	any p	1 (PcN)	F is PcN, $\mathrm{Tr}_n(-uv) \neq 1$	[13]
$L_1(x) + L_1(\gamma)\mathrm{Tr}_n(L_2(x))$	any p	1 (PcN)	$\mathrm{Tr}_n\left(\frac{L_1(\gamma)}{1-c}\right) = 0$, $\mathrm{Tr}_n(\gamma) = 0$	[13]
$L(x) + \prod_{i=1}^{s}(\mathrm{Tr}_n\left(x^{2^{k_i}+1} + \delta_i\right))^{g_i}$	$p = 2$	≤ 2 (APcN)	$1 \leq k_i \leq n - 1$	[13]
$L(x) + \prod_{i=1}^{s}(\alpha_i\mathrm{Tr}_{nq^n/q^m}\left(x^{2^{k_i}+1} + \delta_i\right))^{g_i}$	$p = 2$	≤ 2 (APcN)	$g_i \geq 1$, $\delta_i \in \mathbb{F}_{2^n}$, $\alpha_i \in \mathbb{F}_{2^m*}$, $1 \leq k_i \leq n - 1$	[13]
$L(x) + u\sum_{i=1}^{t}(\mathrm{Tr}_{nq^n/q^m}(x)^{k_i} + \delta_i)^{s_i}$	any p	1 (PcN)	$pm \mid n$, $1 \leq t \in \mathbb{Z}_{>0}$, $u \in \mathbb{F}_{p^m*}$, $\delta_i \in \mathbb{F}_{p^m}$, $1 \leq k_i, s_i \leq p^n - 1$, L linearized permutation, $c \in \mathbb{F}_{p^m} \setminus \{1\}$	[13]
$(x^{2^m} + x + \delta)^{2^{2m}+1} + x$	$p = 2$	1 (PcN)	$n = 3m$, $c \in \mathbb{F}_{2^m} \setminus \{1\}$, $\delta \in \mathbb{F}_{2^n}$	[6]
$(x^{2^m} + x + \delta)^{2^{2m}+1} + x$	$p = 2$	2 (APcN)	$n = 3m$, $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, $\mathrm{Tr}_m^{3m}(\delta) = 1$	[6]
$(x^{2^m} + x + \delta)^{2^{2m}+1} + x$	$p = 2$	≤ 4	$n = 3m$, $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, $\mathrm{Tr}_m^{3m}(\delta) \neq 1$	[6]
$(x^{2^m} + x + \delta)^{2^{2m-1}+2^{m-1}} + x$	$p = 2$	1 (PcN)	$n = 3m$, $m \not\equiv \pm 1 \pmod 3$, $c \in \mathbb{F}_{2^m} \setminus \{1\}$, $\delta \in \mathbb{F}_{2^n}$	[6]
$(x^{2^m} + x + \delta)^{2^{2m-1}+2^{m-1}} + x$	$p = 2$	2 (APcN)	$n = 3m$, $m \not\equiv \pm 1 \pmod 3$, $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, $\mathrm{Tr}_m^{3m}(\delta) = 0$	[6]

TABLE B2 (Continued)

$F(x)$	$\mathbb{F}_{p^n}$	${}_c\Delta_F$	Conditions	Ref
$(x^{2^m}+x+\delta)^{2^{2m-1}+2^{m-1}}+x$	$p=2$	≤ 4	$n=3m$, $m \not\equiv \pm 1 \pmod 3$, $c \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, $\mathrm{Tr}_m^{3m}(\delta)\neq 0$	[6]
$(x^{3^m}-x+\delta)^{3^{2^{m-1}}+2\cdot 3^{m-1}}+x$	$p=3$	1 (PcN)	$n=2m$, $c \in \mathbb{F}_{3^m}\backslash\{1\}$, $\delta \in \mathbb{F}_{2^n}$, or $c \in \mathbb{F}_{3^n}\backslash\mathbb{F}_{3^m}$, $\mathrm{Tr}_m^{2m}(\delta)=0$	[6]
$(x^{3^m}-x+\delta)^{3^{2^{m-1}}+2\cdot 3^{m-1}}+x$	$p=3$	3	$n=2m$, $c \notin \mathbb{F}_{3^m}$, $\mathrm{Tr}_m^{2m}(\delta)\neq 0$	[6]
$(x^{p^m}-x+\delta)^{p^{m+1}+1}+x$	$p>2$	1 (PcN)	$n=2m$, $c \in \mathbb{F}_{p^m}\backslash\{1\}$, $\mathrm{Tr}_m^{2m}(\delta)=0$, or $\mathbb{F}rac\mathrm{Tr}_m^{2m}(\delta)-1\mathrm{Tr}_m^{2m}(\delta)$ is a $(p-1)$-th power	[6]
$(x^{p^m}-x+\delta)^{p^{m+1}+1}+x$	$p>2$	p	$n=2m$, $c \in \mathbb{F}_{p^n}\backslash\mathbb{F}_{p^m}$, $\mathrm{Tr}_m^{2m}(\delta)=0$, or $\frac{\mathrm{Tr}_m^{2m}(\delta)-1}{\mathrm{Tr}_m^{2m}(\delta)}$ is a $(p-1)$th power	[6]

ones whose cDU is less than 4, unless it is a well-known function, or is another case of a function with low cDU). We note that over the binary fields, there are not too many classes of PcN functions.

We use v_2 as the 2-valuation of the input, that is the largest power of 2 dividing the input; the inverse is taken in the sense of modulo $p^n - 1$ for the respective prime p. Table B1 lists the exponent of some monomials x^d. Table B2 lists the known polynomials with low cDU (here, $l > 1$ is a divisor of $p^n - 1$ and g is a primitive element of $\mathbb{F}_{p^n}$, and D_0 is the multiplicative subgroup of $\mathbb{F}_{p^n}$ generated by g).