C-differential bent functions and perfect nonlinearity

Pantelimon Stănică[1], Sugata Gangopadhyay[2], Aaron Geary[1], Constanza Riera[3], Anton Tkachenko[3]

[1] Applied Mathematics Department,
Naval Postgraduate School, Monterey, USA;
{pstanica, aaron.geary}@nps.edu

[2] Department of Computer Science and Engineering,
Indian Institute of Technology Roorkee, INDIA;
sugata.gangopadhyay@cs.iitr.ac.in

[3]Department of Computer Science,
Electrical Engineering and Mathematical Sciences,
Western Norway University of Applied Sciences,
5020 Bergen, Norway; {csr, atk}@hvl.no

October 3, 2021

Abstract

Drawing inspiration from Nyberg's paper [22] on perfect nonlinearity and the c-differential notion we defined in [7], in this paper we introduce the concept of c-differential bent functions in two different ways (thus extending Kumar et al. [11] classical definition). We further extend the notion of perfect c-nonlinear introduced in [7], also in two different ways, and show that, in both cases, the concepts of c-differential bent and perfect c-nonlinear are equivalent (under some natural restriction of the parameters). Some constructions of functions with these properties are also provided; one such construction provides a large class of PcN functions with respect to all c in some subfield of the field under consideration. We also show that both our classes of 0-differential bents are supersets of permutation polynomials, and that Maiorana-McFarland bent functions are not differential bent (of the first kind).

Keywords: Boolean and p-ary function, autocorrelation, c-differential bent, differential uniformity, perfect and almost perfect c-nonlinearity
MSC 2000: 06E30, 11T06, 94A60, 94C10.

1 Introduction and basic definitions

We will introduce here only some basic notations and definitions on Boolean and p-ary functions (where p is an odd prime); the reader can consult [2, 3, 6, 18, 26] for more on these objects.

For a positive integer n and p a prime number, we denote by $\mathbb{F}_p^n$ the n-dimensional vector space over $\mathbb{F}_p$, and by $\mathbb{F}_{p^n}$ the finite field with p^n elements, while $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$ will denote the multiplicative group. For $a \neq 0$, we often write $\frac{1}{a}$ to mean the inverse of a in the multiplicative group of the finite field under discussion. We use $\#S$ to denote the cardinality of a set S and $\bar{z}$, for the complex conjugate. We call a function from $\mathbb{F}_{p^n}$ (or $\mathbb{F}_p^n$) to $\mathbb{F}_p$ a *p-ary function* on n variables. For positive integers n and m, any map $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ (or, $\mathbb{F}_p^n \to \mathbb{F}_p^m$) is called a *vectorial p-ary function*, or (n, m)-*function*. When p is fixed, we write $\mathbb{V}_{n,p}$ for the vector space $\mathbb{F}_{p^n}$, or $\mathbb{F}_p^n$ under consideration, and $\mathcal{B}_{n,p}^m$, for the p-ary functions defined on $\mathbb{V}_{n,p}$ with values in $\mathbb{V}_{m,p}$. If $p = 2$ we write $\mathbb{V}_n$ and $\mathcal{B}_n^m$, and if $m = 1$, we will drop the superscript, altogether. When $m = n$, F can be uniquely represented as a univariate polynomial over $\mathbb{F}_{p^n}$ (using some identification, via a basis, of the finite field with the vector space) of the form $F(x) = \sum_{i=0}^{p^n-1} a_i x^i,\ a_i \in \mathbb{F}_{p^n}$, whose *algebraic degree* is then the largest Hamming weight of the exponents i with $a_i \neq 0$. To (somewhat) distinguish between the vectorial and single-component output, we shall use upper/lower case to denote the functions. For a p-ary function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, the *Walsh-Hadamard transform* is defined as the complex-valued function

$$\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x) - \mathrm{Tr}_n(ux)},\ u \in \mathbb{F}_{p^n},$$

where $\zeta_q = e^{\frac{2\pi i}{q}}$, for any q, and $\mathrm{Tr}_n : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the absolute trace function, given by $\mathrm{Tr}_n(x) = \sum_{i=0}^{n-1} x^{p^i}$ (we will denote it by Tr, if the dimension is clear from the context). For $f \in \mathcal{B}_{n,p}$, the map $\mathcal{F}_f(u) = \sum_{x \in \mathbb{V}_n} f(x) \zeta_p^{\mathrm{Tr}(ux)}$ is the Fourier transform of f. The (vectorial) Walsh transform $\mathcal{W}_F(a, b)$ of an (n, m)-function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ at $a \in \mathbb{F}_p^n, b \in \mathbb{F}_p^m$ is the Walsh-Hadamard transform of its component function $\mathrm{Tr}_m(bF(x))$ at a, that is,

$$\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(bF(x)) - \mathrm{Tr}_n(ax)}.$$

NB: If one wishes to work with vector spaces, then one can replace the Tr by any scalar product on that environment, for example, if $\mathbb{V}_{n,p} = \mathbb{F}_p^n$, the vector space of the n-tuples over $\mathbb{F}_p$ we use the conventional dot product $u \cdot x$ for $\mathrm{Tr}(ux)$.

In this paper, we will use both the absolute trace Tr_n and the relative trace $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}$, defined as $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{p^{mi}}$.

Given a p-ary function $f \in \mathcal{B}_{n,p}$, the derivative of f with respect to $a \in \mathbb{F}_{p^n}$ is the p-ary function $D_a f(x) = f(x+a) - f(x)$, for all $x \in \mathbb{F}_{p^n}$.

The sum

$$\mathcal{C}_{f,g}(z) = \sum_{x \in \mathbb{V}_n} \zeta_p^{f(x+z)-g(x)}$$

is the *crosscorrelation* of $f, g \in \mathcal{B}_{n,p}$ at $z \in \mathbb{V}_n$. The *autocorrelation* of $f \in \mathcal{B}_{n,p}$ at $u \in \mathbb{V}_n$ is $\mathcal{C}_{f,f}(u)$ above, which we denote by $\mathcal{C}_f(u)$.

For an (n,m)-function F, and $a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}$, we let $\Delta_F(a,b) = \#\{x \in \mathbb{F}_{p^n} : F(x+a) - F(x) = b\}$. We call the quantity $\delta_F = \max\{\Delta_F(a,b) : a, b \in \mathbb{F}_{p^n}, a \neq 0\}$ the *differential uniformity* of F. If $\delta_F = \delta$, then we say that F is differentially δ-uniform. If $m = n$ and $\delta = 1$, then F is called a *perfect nonlinear* (*PN*) function, or *planar* function. If $m = n$ and $\delta = 2$, then F is called an *almost perfect nonlinear* (*APN*) function. It is well known that PN functions do not exist if $p = 2$. While most of the literature deals with (n,n)-functions when it comes to differential uniformity, we see no reason why the concept (beyond its uses in S-boxes, of course) cannot be considered for all (n,m)-functions.

In [7] we defined a multiplier differential and the corresponding difference distribution table (in any characteristic). For an (n,m)-function F, $a \in \mathbb{F}_{p^n}$ 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

$$_cD_aF(x) = F(x+a) - cF(x), \text{ for all } x \in \mathbb{F}_{p^n}.$$

We let the entries of the c-Difference Distribution Table (c-DDT) be defined by $_c\Delta_F(a,b) = \#\{x \in \mathbb{F}_{p^n} : F(x+a) - cF(x) = b\}$. We call the quantity

$$\delta_{F,c} = \max\{{}_c\Delta_F(a,b) \,|\, a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m} \text{ and } a \neq 0 \text{ if } c = 1\}$$

the *c-differential uniformity* of F (while we previously worked with (n,n)-functions, there is no reason why we should not consider general (n,m)-functions in this definition). We extend here for general n and m the concepts that, in [7], were defined for $m = n$:

If $\delta_{F,c} = \delta$, then we say that F is differentially (c,δ)-uniform (or that F has c-uniformity δ, or for short, F *has δ-uniform c-DDT*). If $\delta = 1$, then

F is called a *perfect c-nonlinear* (*PcN*) function (certainly, for $c = 1$, they only exist for odd characteristic p; however, as proven in [7], there exist PcN functions for $p = 2$, for all $c \neq 1$). If $\delta = 2$, then F is called an *almost perfect c-nonlinear* (*APcN*) function. When we need to specify the constant c for which the function is PcN or APcN, then we may use the notation c-PN, or c-APN. It is easy to see that if F is an (n, n)-function, that is, $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, then F is c-PN if and only if ${}_cD_aF$ is a permutation polynomial.

The rest of the paper is organized as follows. Section 2 and 3 introduce our two types of crosscorrelations/autocorrelations and define (naturally) the concepts of perfect c-nonlinear and c-differential bent functions in the context of (n, m)-functions, and show that c-differential bent functions correspond to perfect c-nonlinear functions (we use indices $1, 2$ to specify which type of bentness or perfect nonlinearity we refer to). Characterizations and some constructions of both concepts are provided. Section 4 concludes the paper.

2 The first crosscorrelation: c-differential bent$_1$ and perfect$_1$ c-nonlinear functions

In this section we extend the PcN notion to allow arbitrary p-ary (n, m)-functions. We shall recover some results shown in [7, 20] as particular cases.

As for the regular differentials, for $F \in \mathcal{B}^m_{n,p}$ and fixed $c \in \mathbb{V}_m$, we define the *c-crosscorrelation* at $u \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}$ by

$$ {}_c\mathfrak{C}_{F,G}(u, b) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(b(F(x+u)-cG(x)))} $$

and the corresponding *c-autocorrelation* at $u \in \mathbb{F}_{p^n}$, ${}_c\mathfrak{C}_F = {}_c\mathfrak{C}_{F,F}$. Surely, ${}_c\mathfrak{C}_{F,G}(u, b) = \mathcal{C}_{\mathrm{Tr}_m(bF),\mathrm{Tr}_m(bcG)}(u)$ and ${}_c\mathfrak{C}_F(u, b) = \mathcal{C}_{\mathrm{Tr}_m(bF),\mathrm{Tr}_m(bcF)}(u)$ (b can only be $0, 1$ when $m = 1$). We want to emphasize the c-differentials, which is going to be relevant later as it relates to the perfect c-nonlinear concept. (We do not want to complicate more the notation by using indices here, since it will be obvious which concept we refer to, because this autocorrelation has two input variables, while the second concept has only one input variable.)

Nyberg [22] extended the notion of perfect nonlinearity and called a function perfect nonlinear if its derivatives are balanced (i.e. they take every value the same number of times). Thus, the function's (non-trivial) autocorrelation must be zero. Likewise, we now extend the definition of PcN, in the following way.

Definition 2.1. *For arbitrary positive integers m, n, and F an (n, m)-function and $c \in \mathbb{F}_{p^m}$ fixed, we say that F is* perfect$_1$ c-nonlinear (PcN) *if its c-autocorrelation ${}_c\mathfrak{C}_F(u, b) = 0$, for all $u \in \mathbb{F}_{p^n}^*$, $b \in \mathbb{F}_{p^m}^*$. A* strictly perfect$_1$ c-nonlinear *is a function F for which all ${}_c\mathfrak{C}_F(u, b) = 0$, for all $u \in \mathbb{F}_{p^n}$, $b \in \mathbb{F}_{p^m}^*$ (obviously, strictly perfect$_1$ c-nonlinear functions do not exist for $c = 1$).*

NB: We removed $b = 0$ from the domain, since in that case the autocorrelation of any function is constant, p^n.

Surely, if the c-derivatives are balanced, that is, if ${}_cD_aF(x) = F(x+a) - cF(x)$, at every fixed $a \neq 0$, assumes the same value $y \in \mathbb{F}_{p^m}$ for exactly p^{n-m} values of $x \in \mathbb{F}_{p^n}$, then F is perfect$_1$ c-nonlinear (similarly, at every fixed a for strictly perfect$_1$ c-nonlinear functions). Later we show that a function is perfect$_1$ c-nonlinear if and only if the traces of the c-differentials are balanced. It is clear that PcN functions (for $m = n$) are strictly perfect$_1$ c-nonlinear functions, and of course, one wonders about the converse (again, for $n = m$). If all the traces of multiples of c-differentials are balanced and so, for all $u \neq 0$, the sum

$$\sum_{x \in \mathbb{F}_{p^n}} \chi_b\left({}_cD_uF(x)\right) = 0,$$

for all $b \neq 0$, where $\chi_b(x) = \chi(bx)$ and χ is the canonical additive character of $\mathbb{F}_{p^m}$, then, by [13, Theorem 7.7], ${}_cD_uF(x)$ must be a permutation, hence F is PcN.

A known result for classical Boolean functions, was extended in [24] for generalized Boolean functions (that is, functions defined from $\mathbb{V}_n$ into $\mathbb{Z}_q$, where $q = 2^k$), and a corresponding result connecting our definition of c-crosscorrelation to the Walsh transforms of general p-ary functions, holds, as well.

Lemma 2.2. *Let p be a prime number and m, n be nonzero positive integers. If $F, G \in \mathcal{B}_{n,p}^m$ and $c \in \mathbb{F}_{p^m}$, then for all $b \in \mathbb{F}_{p^m}$, we have*

$$\begin{aligned} &\sum_{u \in \mathbb{F}_{p^n}} {}_c\mathfrak{C}_{F,G}(u, b)\zeta_p^{-\mathrm{Tr}_n(\alpha u)} = \mathcal{W}_F(\alpha, b)\overline{\mathcal{W}_G(\alpha, bc)}, \text{ for all } \alpha \in \mathbb{F}_{p^n}, \\ &{}_c\mathfrak{C}_{F,G}(u, b) = p^{-n} \sum_{x \in \mathbb{F}_{p^n}} \mathcal{W}_F(x, b)\overline{\mathcal{W}_G(x, bc)}\zeta^{\mathrm{Tr}_n(ux)}, \text{ for all } u \in \mathbb{F}_{p^n}. \end{aligned} \tag{1}$$

In particular, if $F = G$, then

$$\sum_{u\in\mathbb{F}_{p^n}} {}_c\mathfrak{C}_F(u,b)\zeta_p^{-\mathrm{Tr}_n(\alpha u)} = \mathcal{W}_F(\alpha,b)\overline{\mathcal{W}_F(\alpha,bc)}$$

$${}_c\mathfrak{C}_F(u,b) = p^{-n}\sum_{x\in\mathbb{F}_{p^n}} \mathcal{W}_F(x,b)\overline{\mathcal{W}_F(x,bc)}\zeta_p^{\mathrm{Tr}_n(ux)}.$$

Proof. We start with

$$\begin{aligned}
&\sum_{u\in\mathbb{F}_{p^n}} {}_c\mathfrak{C}_{F,G}(u,b)\zeta_p^{-\mathrm{Tr}(ux)} = \sum_{u\in\mathbb{F}_{p^n}}\sum_{z\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(b(F(z+u)-cG(z))}\zeta_p^{\mathrm{Tr}_n(-ux)}\\
=&\sum_{u\in\mathbb{F}_{p^n}}\sum_{z\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(b(F(z+u)-cG(z))}\zeta_p^{-\mathrm{Tr}((z+u)x)+\mathrm{Tr}_n(zx)}\\
=&\sum_{z\in\mathbb{F}_{p^n}} \zeta_p^{-\mathrm{Tr}_m(bcG(z))}\zeta_p^{\mathrm{Tr}_n(zx)}\sum_{u\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(bF(z+u))}\zeta_p^{-\mathrm{Tr}_n((z+u)x)}\\
\overset{w:=z+u}{=}&\sum_{z\in\mathbb{F}_{p^n}} \zeta_p^{-\mathrm{Tr}_m(bcG(z))}\zeta_p^{\mathrm{Tr}(zx)}\sum_{w\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(bF(w))}\zeta_p^{-\mathrm{Tr}_n(wx)}\\
=&\mathcal{W}_F(x,b)\overline{\mathcal{W}_G(x,bc)}.
\end{aligned}$$

For the second identity, we reverse the argument, and obtain

$$\begin{aligned}
&p^{-n}\sum_{x\in\mathbb{F}_{p^n}} \mathcal{W}_F(x,b)\overline{\mathcal{W}_G(x,bc)}\zeta^{\mathrm{Tr}_n(ux)}\\
=&p^{-n}\sum_{x\in\mathbb{F}_{p^n}}\sum_{z,w\in\mathbb{F}_{p^n}} \zeta_p^{-\mathrm{Tr}_m(bcG(z))}\zeta_p^{\mathrm{Tr}_n(zx)}\zeta_p^{\mathrm{Tr}_m(bF(w))}\zeta_p^{-\mathrm{Tr}_n(wx)}\zeta^{\mathrm{Tr}_n(ux)}\\
=&p^{-n}\sum_{z,w\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(b(F(w)-cG(z))}\sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n((u+z-w)x)}\\
=&\sum_{z\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(b(F(u+z)-cG(z))} = {}_c\mathfrak{C}_F(u,b).
\end{aligned}$$

The claimed consequences are immediate. □

We know that the bent notion exists from any group A to another group B [23], defined via character theory. There are many generalizations of the bent concept and we mention here [9, 10, 11, 14, 15, 16, 17, 19, 21, 24, 25, 28, 29]. We define yet another bent concept below, for $m \leq n$, that takes into account the differential type used.

Definition 2.3. *We say that a function $F \in \mathcal{B}_{n,p}^m$ is* c-differential bent$_1$ *if $\mathcal{W}_F(x,b)\overline{\mathcal{W}_F(x,bc)} = {}_c\mathfrak{C}_F(0,b)$, for all $x \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}^*$.*

We know that a p-ary function $F : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is bent if the complex absolute value of the Walsh transforms is constant, namely, $|\mathcal{W}_F(x)|^2 = \mathcal{W}_F(x)\overline{\mathcal{W}_F(x)} = \mathcal{C}_F(0) = p^n$, for all $x \in \mathbb{F}_{p^n}$. Surely, the definition was extended to vectorial p-ary functions by imposing the constant absolute values for all (nontrivial) component functions, $\mathrm{Tr}_m(bF), b \in \mathbb{F}_{p^m}^*$. Replacing $c = 1$ in our definition, we recover the original definition.

Below, we will show that a function $F \in \mathcal{B}_{n,p}^m$ is c-differential bent$_1$ if the traces of all of its c-differentials, ${}_cD_aF$ with $a \neq 0$, are balanced, thereby extending Nyberg's result [22] on perfect nonlinearity being equivalent to bentness for functions defined from $\mathbb{F}_{p^n}$ into $\mathbb{F}_p$. We can also regard it as an extension of the PcN property we defined (for $n = m$) in [7].

Theorem 2.4. *Let $1 \leq m \leq n$ be integers, p prime, and $F \in \mathcal{B}_{n,p}^m$, $1 \neq c \in \mathbb{F}_{p^m}$. Then F is perfect$_1$ c-nonlinear if and only if F is c-differential bent$_1$. Moreover, F is strictly perfect$_1$ c-nonlinear if and only if $\mathcal{W}_F(x,b)\overline{\mathcal{W}_F(x,bc)} = 0$, for all $x \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}^*$.*

Proof. We first assume that F is perfect$_1$ c-nonlinear, and so, ${}_c\mathfrak{C}_F(u,b) = 0$, for all $u \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_{p^m}^*$. From Lemma 2.2, for an arbitrary $b \in \mathbb{F}_{p^m}^*$, we compute

$$\begin{aligned}\mathcal{W}_F(x,b)\overline{\mathcal{W}_F(x,bc)} &= \sum_{u\in\mathbb{F}_{p^n}} {}_c\mathfrak{C}_F(u,b)\zeta_p^{-\mathrm{Tr}_n(ux)}\\ &= {}_c\mathfrak{C}_F(0,b) + \sum_{0\neq u\in\mathbb{F}_{p^n}} \zeta_p^{-\mathrm{Tr}_n(ux)}\,{}_c\mathfrak{C}_F(u,b)\\ &= {}_c\mathfrak{C}_F(0,b),\end{aligned}$$

where we used the assumption that the c-autocorrelations ${}_c\mathfrak{C}_F(u,b)$ are zero, except, possibly, at $u = 0$.

For the reciprocal, we assume that F is c-differential bent$_1$, that is, $\mathcal{W}_F(x,b)\overline{\mathcal{W}_F(x,bc)} = {}_c\mathfrak{C}_F(0,b)$, $b \neq 0$. Then, for any $b \in \mathbb{F}_{p^m}^*$ and $u \in \mathbb{F}_{p^n}^*$,

$$\begin{aligned}{}_c\mathfrak{C}_F(u,b) &= p^{-n}\sum_{x\in\mathbb{F}_{p^n}} \mathcal{W}_F(x,b)\overline{\mathcal{W}_F(x,bc)}\zeta_p^{\mathrm{Tr}_n(ux)}\\ &= p^{-n}\,{}_c\mathfrak{C}_F(0,b)\sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(ux)} = 0,\end{aligned}$$

where we used the same property that the exponential sum of a balanced function (in this case $\mathrm{Tr}(ux)$, for $u \neq 0$) is zero. This proves the first claim. The second claim follows easily using the equations above. □

We now discuss some of the differential properties of a perfect$_1$ c-nonlinear function.

Theorem 2.5. *Let m, n be positive integers, p a prime integer, $F \in \mathcal{B}^m_{n,p}$, and $c \in \mathbb{F}_{p^m}$ fixed. Then F is a perfect$_1$ c-nonlinear function (c-differential bent$_1$) if and only if, for all $b \neq 0, u \neq 0$ fixed, $x \mapsto \mathrm{Tr}_m(b(F(x+u) - cF(x))$ is balanced.*

Proof. With $c \in \mathbb{F}_{p^n}$ constant, for every $u \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}$, $0 \leq j \leq p-1$, we let $S^{u,b}_{j,c} = \{x \in \mathbb{F}_{p^n} \mid \mathrm{Tr}_m(b(F(x+u) - cF(x))) = j\}$. We will use below that the order of the cyclotomic polynomial of index p^m is $\phi(p^m) = p^{m-1}(p-1)$.

First, recall that the p^k-cyclotomic polynomial is $\phi_{p^k}(x) = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}}$. In particular, we deduce that $\zeta_p^{p-1} = -(1 + \zeta_p + \cdots + \zeta_p^{p-2})$. If $u \in \mathbb{F}^*_{p^n}, b \in \mathbb{F}^*_{p^m}$, and F is perfect$_1$ c-nonlinear, then

$$\begin{aligned} 0 = {}_c\mathfrak{C}_F(u,b) &= \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(b(F(x+u) - cF(x)))} \\ &= \sum_{j=0}^{p-1} |S^{u,b}_{j,c}| \zeta_p^j = \sum_{j=0}^{p-2} \left(|S^{u,b}_{j,c}| - |S^{u,b}_{p-1,c}| \right) \zeta_p^j. \end{aligned}$$

The extension $\mathbb{Q} \overset{p-1}{\hookrightarrow} \mathbb{Q}(\zeta_p)$ has degree $p-1$ and the elements in following set $\left\{ \zeta_p^j \mid 0 \leq j \leq p-2 \right\}$ are linearly independent in $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$, therefore the coefficients in the displayed expression are zero, that is, that for all $0 \leq j \leq p-2$, $|S^{u,b}_{j,c}| = |S^{u,b}_{p-1,c}|$. Summarizing, for any $0 \leq j \leq p-1$, the cardinality of the set $S^{u,b}_{j,c}$ is independent of j, and so, for all $c, b, u \neq 0$ fixed, the function $x \mapsto \mathrm{Tr}_m(b(F(x+u) - cF(x))$ is balanced.

If $x \mapsto \mathrm{Tr}_m(b(F(x+u) - cF(x))$ is balanced, by reversing the argument, we find that f is perfect$_1$ c-nonlinear. □

As a consequence, we can easily characterize the 0-differential bent$_1$ functions.

Corollary 2.6. *Let $F \in \mathcal{B}^m_{n,p}$. The following statements are equivalent:*

(*i*) *F is a 0-differential bent$_1$ (perfect$_1$ 0-nonlinear) function;*

(*ii*) *$\mathcal{W}_F(0, b) = 0$, for all $b \neq 0$;*

(*iii*) *(Under $m = n$) F is a permutation polynomial.*

Proof. When $c = 0$, for $u \neq 0$ fixed, the map $x \mapsto \mathrm{Tr}_m(b(F(x+u))$ is balanced if and only if $x \mapsto \mathrm{Tr}_m(b(F(x))$ is balanced (since $x \mapsto x+u$ is a bijection on the input set $\mathbb{F}_{p^n}$). Under $m = n$, using [13, Theorem 7.7], this is equivalent to F being a permutation polynomial. □

Thus, if $m = n$ and F is a permutation of $\mathbb{F}_{p^n}$, then F is 0-differential bent_1 (since in this case, F is PcN for $c = 0$ [7]). We give below another example of c-differential bent_1 functions on $\mathbb{F}_{p^n}$, for all $c \neq 1$. Let $F(x) = x^{p^k}$ be a linearized monomial on $\mathbb{F}_{p^n}$. We compute the trace of arbitrary components of its derivative, obtaining

$$\begin{aligned}\mathrm{Tr}_n(b\,({}_cD_aF(x))) &= \mathrm{Tr}_n\left(b(x^{p^k} + a^{p^k} - cx^{p^k}\right)\\ &= \mathrm{Tr}_n\left((1-c)x^{p^k}\right) + \mathrm{Tr}_n(a)\\ &= \mathrm{Tr}_n\left((1-c)^{p^{-k}}x\right) + \mathrm{Tr}_n(a),\end{aligned}$$

which is balanced, if $c \neq 1$. Thus, any linearized monomial is a (strictly) $\mathrm{perfect}_1$ c-nonlinear function, for all $c \neq 1$. In fact, given any linearized polynomial L, for which $\mathrm{Tr}_n\left((1-c)^{p^{-k}}L(x)\right)$ is balanced, then L is a (strictly) $\mathrm{perfect}_1$ c-nonlinear function, for all $c \neq 1$. Thus, this class of $\mathrm{perfect}_1$ c-nonlinear functions is a superclass of linearized polynomials L whose trace $\mathrm{Tr}_n((1-c)^{p^{-k}}L(x))$ is balanced, and, furthermore, when $c = 0$, is a superclass of permutation polynomials.

Surely, the question is whether there are other examples. We ran a SageMath code and found some (strictly) $\mathrm{perfect}_1$ c-nonlinear (c-differential bent_1) functions on small dimensions that are not linearized polynomials. For instance, $F(x) = x^3$ is $\mathrm{perfect}_1$ 0-nonlinear on $\mathbb{F}_{2^3}$; $F(x) = x^5$ is (strictly) $\mathrm{perfect}_1$ 0-nonlinear on $\mathbb{F}_{2^3}$ and (strictly) $\mathrm{perfect}_1$ $\{0,2\}$-nonlinear on $\mathbb{F}_{3^3}$; $F(x) = x^{21}$ is $\mathrm{perfect}_1$ c-nonlinear for all $c \neq 1$ in $\mathbb{F}_{3^4}$; $F(x) = x^{15}$ is (strictly) $\mathrm{perfect}_1$ $\{0,2\}$-nonlinear on $\mathbb{F}_{3^3}$. From our first two examples (and several more of that type), we see that the Gold function is not always 0-differential bent for small values of n, and so, we wondered what happens, in general. The answer is provided by [7, 20] for the Gold function. However, we can show a more general result, which, as a consequence, implies also the behavior of the Gold function. We could not adapt the methods from [7] to show the theorem, so we provide here an alternative method that proves quite useful to show several results at once.

Theorem 2.7. *Let p be a prime number, n a positive integer and $F(x) = x^d$, a monomial function. If $\gcd(d, p^n - 1) = 1$, then F is 0-differential bent_1. If $\gcd(d, p^n - 1) = 2$, then F is not 0-differential bent_1.*

Proof. If $\gcd(d, p^n - 1) = 1$, then,

$$\sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(\alpha x^d)} = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(\alpha x)} = 0, \text{ if } \alpha \neq 0,$$

using the fact that $x \to x^d$ is a permutation if $\gcd(d, p^n - 1) = 1$, so if x covers $\mathbb{F}_{p^n}$, then x^d does the same, therefore showing the first claim.

To show the second claim, by Corollary 2.6, if F were 0-differential bent$_1$, then $\sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(\alpha F(x))} = 0$. Assuming $\gcd(d, p^n - 1) = 2$, then we have the identity between the following Gaussian sums

$$\sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(\alpha x^d)} = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(\alpha x^2)}$$

(we use here the fact that under $\gcd(d, p^n - 1) = 2$, then $\{x^d \,|\, x \in \mathbb{F}_{p^n}\} = \{x^2 \,|\, x \in \mathbb{F}_{p^n}\}$, which can be seen by making the change of variable $x \mapsto x^{d/\gcd(d, p^n-1)}$). We could use [13, Theorems 5.33 & 5.15], or simply [8, Corollary 3 (Sidelnikov)] and infer that

$$\sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(\alpha x^2)} = \begin{cases} \eta(\alpha)(-1)^{n-1} p^{n/2} & \text{if } p \equiv 1 \pmod 4 \\ \eta(\alpha)(-1)^{n-1} i^n p^{n/2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

From this last identity, we see that we cannot have $\sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(\alpha x^2)} = 0$, if $\alpha \neq 0$, and so, F cannot be 0-differential bent$_1$. □

The following are some important corollaries (we use [7, Lemma 9]: if $p = 2$, then $\gcd(2^k + 1, 2^n - 1) = 1$ and, if $p > 2$, then $\gcd\left(p^k + 1, p^n - 1\right) = 2$, when $\frac{n}{\gcd(n,k)}$ odd; also, when n is even, k is odd, $\gcd(n, k) = 1$, then $\gcd\left(\frac{3^k+1}{2}, 3^n - 1\right) = 2$). Note that Corollary 2.8 is also a consequence of [7, Theorem 10 (ii)] and [20].

Corollary 2.8. *Let n, k be positive integers with $\frac{n}{\gcd(n,k)}$ odd and $F(x) = x^{p^k+1}$ be defined on $\mathbb{F}_{p^n}$, p an odd prime. Then F is not 0-differential bent$_1$. If $p = 2$, then F is 0-differential bent$_1$.*

The Gold function is not the only function for which we have this type of result. The Coulter-Matthews [5] PN function is yet another example of a function that is not 0-differential bent$_1$ (hence not perfect$_1$ 0-nonlinear), under some conditions, and it is 0-differential bent$_1$, under some other conditions (see [7, 20] for a general result on the function $x \mapsto x^{\frac{p^k+1}{2}}$ and its differential uniformity).

Corollary 2.9. *Let $n = 2m \geq 2$, k odd,* $\gcd(n,k) = 1$ *(so,* $\gcd\left(\frac{3^k+1}{2}, 3^n - 1\right) = 2$*). Then $F(x) = x^{\frac{3^k+1}{2}}$ is not 0-differential bent$_1$. If n, k are such that* $\gcd\left(\frac{3^k+1}{2}, 3^n - 1\right) = 1$*, then $F(x) = x^{\frac{3^k+1}{2}}$ is 0-differential bent$_1$.*

We can generate classes of (n,m)-functions that are c-differential bent$_1$ in the following way. We take G to be a PcN function on $\mathbb{F}_{p^n}$ with respect to $c \in \mathbb{F}_{p^m}$, a proper subfield of $\mathbb{F}_{p^n}$ (that is, $m < n$, $m \,|\, n$). We then define $F(x) = \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}(G(x))$. First, observe that since $c \in \mathbb{F}_{p^m}$, then $\mathrm{Tr}_n({}_cD_aG(x)) = \mathrm{Tr}_m({}_cD_aF(x))$. Now, if ${}_cD_aG$ is a permutation (using our assumption), then ${}_cD_aF = \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}({}_cD_aG)$ is balanced, and so is $b\,({}_cD_aF)$, for $b \neq 0$. We now use the fact that multiplication by $b \neq 0$ simply shuffles the output. What we mean is that with notations, $\mathrm{Ker}(\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}) = \{x \in \mathbb{F}_{p^n} \,|\, \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}(x) = 0\}$, and $A_i = \{x \in \mathbb{F}_{p^n} \,|\, \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}(x) = \alpha^i\}$, where $\mathbb{F}_{p^m} = \{0, \alpha^i \,|\, 0 \leq i \leq p^m - 2\}$ (α is a primitive element of $\mathbb{F}_{p^m}$), then, writing $b = \alpha^{i_0}$, the partition corresponding to $b\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}$ is now $A_0, A_{i+i_0 \pmod{p^m-1}}$. Using this and the transitivity of the traces, then $\mathrm{Tr}_m(b\,({}_cD_aF))$ is also balanced. We record this in the next proposition.

Proposition 2.10. *Let $m \,|\, n$, $m < n$, and p prime. If G is PcN on $\mathbb{F}_{p^n}$ with respect to $c \in \mathbb{F}_{p^m}$, then $F(x) = \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}(G(x))$ is c-differential bent$_1$.*

It is obvious that not all c-differential bent$_1$ functions from $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ come from traces of permutations on $\mathbb{F}_{p^n}$ (we can see that by taking a trace function F of a PcN G, as above, and then interchanging output points with the same trace output value). More precisely, we take $\mathbb{F}_{p^m} = \{0, \alpha^i \,|\, 0 \leq i \leq p^m - 2\}$ (α is a primitive element of $\mathbb{F}_{p^m}$) and random A_i, A_j, $i \neq j$, as above. We now define $H(x) = F(x)$, unless $x \in A_1 \cup A_2$, when $H(x) = \alpha^j$, if $x \in A_i$ and $H(x) = \alpha^i$, if $x \in A_i$.

Classical (binary) bent functions do not transfer easily in this generalized bent context. To argue that claim, we next show that Maiorana-McFarland bents cannot be c-differential bent$_1$ for $c \neq 1$.

Proposition 2.11. *Let $n = 2m$. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be a (bent) Maiorana-McFarland (n,m)-function defined by*

$$F(x,y) = x\pi(y), \text{ for all } x, y \in \mathbb{F}_{2^m}, \tag{2}$$

where $\pi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is a permutation. Then F cannot be c-differential bent$_1$ for $c \neq 1$.

Proof. As is customary, we identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_{2^m}^2 = \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. The Walsh-Hadamard transform of F at $((u,v),b) \in \mathbb{F}_{2^m}^2 \times \mathbb{F}_{2^m}^*$ is

$$\begin{aligned} W_F((u,v),b) &= \sum_{x\in\mathbb{F}_{2^m}} \sum_{y\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_m(bF(x,y))+\mathrm{Tr}_m(ux)+\mathrm{Tr}_m(vy)} \\ &= \sum_{x\in\mathbb{F}_{2^m}} \sum_{y\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_m(bx\pi(y))+\mathrm{Tr}_m(ux)+\mathrm{Tr}_m(vy)}. \end{aligned} \tag{3}$$

Then

$$\begin{aligned} &W_F((u,v),b)W_F((u,v),bc) \\ &= \sum_{\substack{x_1\in\mathbb{F}_{2^m}\\ y_1\in\mathbb{F}_{2^m}}} \sum_{\substack{x_2\in\mathbb{F}_{2^m}\\ y_2\in\mathbb{F}_{2^m}}} (-1)^{\mathrm{Tr}_m(x_1(\pi_b(y_1)+u))+\mathrm{Tr}_m(x_2(\pi_{bc}(y_2)+u))+\mathrm{Tr}_m(v(y_1+y_2))} \\ &= \sum_{\substack{y_1\in\mathbb{F}_{2^m}\\ y_2\in\mathbb{F}_{2^m}}} (-1)^{\mathrm{Tr}_m(v(y_1+y_2))} \sum_{x_1\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_m(x_1(\pi_b(y_1)+u))} \\ &\qquad \times \sum_{x_2\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_m(x_2(\pi_{bc}(y_2)+u))} \\ &= 2^{2m} \sum_{\substack{y_1\in\mathbb{F}_{2^m}\\ y_2\in\mathbb{F}_{2^m}}} (-1)^{\mathrm{Tr}_m(v(y_1+y_2))} \delta_0(\pi_b(y_1)+u))\delta_0(\pi_{bc}(y_2)+u)) \\ &= 2^{2m}(-1)^{\mathrm{Tr}_m(v(\pi_b^{-1}(u)+\pi_{bc}^{-1}(u)))}, \end{aligned}$$

where $\pi_b(x) = b\pi(x)$ and $\pi_{bc}(x) = bc\pi(x)$, for all $x \in \mathbb{F}_{2^m}$. Since the product of the Walsh coefficients is not independent of u, v for $c \neq 1$, our claim is shown. □

We now give a class of Dembowski-Ostrom (bilinear) polynomials on $\mathbb{F}_{2^n}$ that are c-differential bent$_1$ for all $c \neq 1$ (PcN) in some subfield of $\mathbb{F}_{p^n}$, from the known class of (bilinear) DO polynomials of [1]. The next theorem provides a new class of PcN functions.

Theorem 2.12. *Let k be a divisor of the positive integer n such that $k \geq 2$, n/k is odd, and $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}$ be the relative trace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^k}$ (recall that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{2^{ki}}$). Then, for any $a \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2$, the polynomials*

$$F(x) = x\left(\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(x) + ax\right)$$

are c-differential bent$_1$ (PcN) on $\mathbb{F}_{2^n}$, for all $1 \neq c \in \mathbb{F}_{p^k}$.

Proof. For easy writing, we shall use Tr for $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}$ in the proof. The case of $c = 0$ is contained in [1], though, our proof will provide an argument for all $c \neq 1$ at once. To show our claim, it will be sufficient to show that, for $c \neq 1$ fixed, the c-differentials ${}_cD_uF$ are permutations on $\mathbb{F}_{p^n}$. We will use the well-known fact (and easy to show by expanding the trace and using the "freshman identity" $(A+B)^p = A^p + B^p$ in characteristic p) that $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^k}}(x^p) = \left(\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^k}}(x)\right)^p$. First, since a and $\mathrm{Tr}(x)$ are in $\mathbb{F}_{2^k}$, we have

$$\mathrm{Tr}(F(x)) = \mathrm{Tr}(x\mathrm{Tr}(x)) + \mathrm{Tr}(ax^2) = \mathrm{Tr}(x)^2 + a\mathrm{Tr}(x)^2 = (1+a)\mathrm{Tr}(x)^2,$$

and

$$\begin{aligned}\mathrm{Tr}(F(x+u) + cF(x)) &= (1+a)\mathrm{Tr}(x+u)^2 + (1+a)c\mathrm{Tr}(x)^2 \\ &= (1+a)\left((1+c)\mathrm{Tr}(x)^2 + \mathrm{Tr}(u)^2\right).\end{aligned}$$

By absurd, we assume that for some fixed u, there exist $x \neq y$ in $\mathbb{F}_{2^n}$ such that ${}_cD_uF(x) = {}_cD_uF(y)$. Thus, applying the relative trace Tr to the identity $F(x+u) + cF(x) = F(y+u) + cF(y)$, we obtain

$$(1+a)\left((1+c)\mathrm{Tr}(x)^2 + \mathrm{Tr}(u)^2\right) = (1+a)\left((1+c)\mathrm{Tr}(y)^2 + \mathrm{Tr}(u)^2\right).$$

Since $a \neq 1$ and $c \neq 1$, we then get $\mathrm{Tr}(x) = \mathrm{Tr}(y)$. Going back to $F(x+u) + cF(x) = F(y+u) + cF(y)$, we get

$$\begin{aligned}&(x+u)(Tr(x+u) + a(x+u)) + cx(Tr(x) + ax) \\ =&(y+u)(Tr(y+u) + a(y+u)) + cy(Tr(y) + ay),\end{aligned}$$

which, by labeling $T = \mathrm{Tr}(x) = \mathrm{Tr}(y)$ and $t = \mathrm{Tr}(u)$, becomes

$$\begin{aligned}&(x+u)(T+t) + ax^2 + au^2 + cxT + acx^2 \\ =&(y+u)(T+t) + ay^2 + au^2 + cyT + acy^2.\end{aligned}$$

Simplifying, we obtain

$$(x+y)((1+c)T + t) = a(c+1)(x+y)^2,$$

and since $x \neq y$, $a \neq 0$, $c \neq 1$, we infer that $x + y = \frac{(1+c)T+t}{a(c+1)} \in \mathbb{F}_{2^k}$. But then $0 = 2T = \mathrm{Tr}(x+y) = (x+y)\mathrm{Tr}(1) = \frac{n}{k}(x+y) = x+y$, since $\frac{n}{k}$ is odd, implying that $x = y$, a contradiction. □

Remark 2.13. *We used SageMath to search for c-differential bent$_1$ functions, in small dimensions n. For example, we found that the bilinear Dembowski-Ostrom permutation polynomials of* [1] *(the Gold case was already treated earlier in our paper), $F_a(x) = x^{2^k+1} + ax^{2^{n-k}+1}$, where $d = \gcd(n,k)$, $\frac{n}{d}$ is odd and $a \neq g^{t(2^d-1)}$ for all integers t; or $G_a(x) = x^{2^{2k}+1} + a^{2^k+1}x^{2^k+1} + ax^2$, $n = 3k$, and $a \neq g^{t(2^k-1)}$ for all integers t, are all c-differential bent$_1$ functions. More precisely, F_α (α is a primitive element in the finite field $\mathbb{F}_{2^n}$ under discussion) is $\{0, \alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+\alpha+1\}$-differential bent$_1$ (PcN) on $\mathbb{F}_{2^5}$ (we took here the primitive polynomial x^5+x^2+1); G_α is $\{0, \alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+\alpha+1\}$-differential bent$_1$ (PcN) on $\mathbb{F}_{2^6}$ (with the primitive polynomial $x^6+x^4+x^3+x+1$).*

It is not surprising that one cannot extend this theorem to the odd characteristic. Kyureghyan and Özbudak [12] showed that if p is odd, $q = p^n$, and $n \geq 5$, then $F(x) = x(\mathrm{Tr}_n(x) - ax)$ cannot be planar (that is, for all $a \neq 0$, $F(x+a)-F(x)$ is a permutation), and if $a = 1, 2$, then it is planar on $\mathbb{F}_{q^3}$ (the necessity of this last result was shown in [1]); in [27] it was proved that the above function is also not planar for $n \geq 4$.

We next ask the question whether one can characterize the differential bentness of any DO polynomial and we have such an attempt below. Suppose that $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ (arbitrary). The c-autocorrelation of F at $u \in \mathbb{F}_{p^n}$ and $b \in \mathbb{F}_{p^m}$ is

$$\begin{aligned} {}_c\mathfrak{C}_F(u,b) &= \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(b(F(x+u)-cF(x)))} \\ &= \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(b(F(x+u)-F(x)+F(x)-cF(x)))} \\ &= \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(b(F(x+u)-F(x)))}\zeta_p^{\mathrm{Tr}_m(b(1-c)(F(x)))}. \end{aligned} \tag{4}$$

Using the above observation, we can characterize some cases when Dembowski-Ostrom (DO) polynomials are (or are not) c-differential bent$_1$ (we do not see an easy way to modify our method [7] to show such a result, so we use a different technique).

For an (n,n)-function $F \in \mathcal{B}^n_{n,p}$, we let $\Omega_{F,i} = \{x \,|\, \mathrm{Tr}_n(F(x)) = i\}$ be the i-support of F, $0 \leq i \leq p-1$. For a Dembowski-Ostrom polynomial $F(x) = \sum_{i,j=0}^{n-1} a_{ij}x^{p^i+p^j}$, we let $L_u(x) = A_{n-1}x + A^p_{n-2}x^p + \cdots + A_1^{p^{n-2}}x^{p^{n-2}} +$

$A_0^{p^{n-1}} x^{p^{n-1}}$ be the *linearized companion polynomial* at $u \in \mathbb{F}_{p^n}^*$, where $A_i = \sum_{k=0}^{n-1} u^{p^k}(a_{ik} + a_{ki})$.

Theorem 2.14. *Let $n \geq 2$, $c \in \mathbb{F}_{p^n}$ fixed, and $F(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i+p^j}$ be a Dembowski-Ostrom polynomial on $\mathbb{F}_{p^n}$, p prime. The following statements hold*:

(*i*) *If, for some $u \in \mathbb{F}_{p^n}^*$, there exists $b \in \mathbb{F}_{p^n}^*$ such that $L_u(b) = 0$, where $A_i = \sum_{k=0}^{n-1} u^{p^k}(a_{ik} + a_{ki})$, and $\sum_{i=1}^{p-1} \#\Omega_{b(1-c)F,i} < p^{n-1}$, then F is not c-differential bent$_1$.*

(*ii*) *If for $u, b \in \mathbb{F}_{2^n}^*$, when either $L_u(b) \neq 0$ and $\sum_{i=1}^{p-1} \zeta_p^i \sum_{x \in \Omega_{b(1-c)F,i}} \zeta_p^{\mathrm{Tr}_m(bD_uF(x))} = 0$, or, $L_u(b) = 0$ and $\sum_{i=1}^{p-1} \zeta_p^i \sum_{x \in \Omega_{b(1-c)F,i}} \zeta_p^{\mathrm{Tr}_m(bD_uF(x))} = (-1)^{bF(u)} p^n$, then F is c-differential bent$_1$.*

Proof. From (4), we infer

$$\begin{aligned}
{}_c\mathfrak{C}_F(u,b) &= \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(b(F(x+u)-F(x)))} \zeta_p^{\mathrm{Tr}_n(b(1-c)(F(x)))} \\
&= \sum_{i=0}^{p-1} \zeta_p^i \sum_{x \in \Omega_{b(1-c)F,i}} \zeta_p^{\mathrm{Tr}_n(b(F(x+u)-F(x)))} \\
&= \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(bD_uF(x))} - \sum_{i=1}^{p-1} (1-\zeta_p^i) \sum_{x \in \Omega_{b(1-c)F,i}} \zeta_p^{\mathrm{Tr}_n(bD_uF(x))}.
\end{aligned}$$

Surely, for u fixed,

$$\begin{aligned}
D_uF(x) &= \sum_{i,j=0}^{n-1} a_{ij}(x+u)^{p^i+p^j} + \sum_{i,j=0}^{n-1} a_{ij} x^{p^i+p^j} \\
&= \sum_{i,j=0}^{n-1} a_{ij} \left(u^{p^i} x^{p^j} + u^{p^j} x^{p^i} + u^{p^i+p^j} \right) \\
&= \sum_{i=0}^{n-1} \left(\sum_{k=0}^{n-1} u^{p^k}(a_{ik} + a_{ki}) \right) x^{p^i} + \sum_{i,j=0}^{n-1} u^{p^i+p^j}.
\end{aligned}$$

We let $A_i = \sum_{k=0}^{n-1} u^{p^k}(a_{ik} + a_{ki})$ and $A = \sum_{i,j=0}^{n-1} u^{p^i+p^j}$. We now use [13, Theorem 5.34], which states that for a polynomial $f(x) = A_r x^{p^r} + A_{r-1}x^{p^{r-1}} + \cdots + A_1 x^p + A_0 x + A$,

$$\sum_{x\in\mathbb{F}_{p^n}} \chi_b(f(x)) = \begin{cases} \chi_b(A)p^n & \text{if } bA_r + b^p A_{r-1}^p + \cdots + b^{p^{r-1}} A_1^{p^{r-1}} + b^{p^r} A_0^{p^r} = 0 \\ 0 & \text{otherwise,} \end{cases}$$

where χ is a nontrivial additive character of $\mathbb{F}_{p^n}$ and $\chi_b(y) = \chi(by)$. In our case, $\chi(y) = \zeta_p^{\mathrm{Tr}_n(y)}$ and so,

$$\begin{aligned} \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(bD_uF(x))} &= \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n\left(b\sum_{i=0}^{n-1} A_i x^{p^i}\right)} \\ &= \begin{cases} \zeta_p^{bF(u)} p^n & \text{if } L_u(b) = 0 \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

If the i-support of $\mathrm{Tr}_n(b(1-c)F(x))$ satisfies $\sum_{i=1}^{p-1} \#\Omega_{b(1-c)F,i} < p^{n-1}$, we therefore find that for b satisfying $bA_{n-1} + b^p A_{n-2}^p + \cdots + b^{p^{n-2}} A_1^{p^{n-2}} + b^{p^{n-1}} A_0^{p^{n-1}} = 0$, then

$$\begin{aligned} &\left| \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(bD_uF(x))} - \sum_{i=1}^{p-1}(1-\zeta_p^i) \sum_{x\in\Omega_{b(1-c)F,i}} \zeta_p^{\mathrm{Tr}_n(bD_uF(x))} \right| \\ &\geq \left|\zeta_p^{bF(u)}\right| p^n - \left|\sum_{i=1}^{p-1}(1-\zeta_p^i)\right| \sum_{i=1}^{n-1} \#\Omega_{b(1-c)F,i} > 0, \end{aligned}$$

where we used the fact that $p = \sum_{i=1}^{p-1}(1-\zeta_p^i)$, and the first claim is shown.

With a similar approach, the second claim follows easily, since the autocorrelation is zero under the imposed conditions. The theorem is shown. □

Remark 2.15. *We can impose different conditions on the DO polynomial F such that F becomes c-differential bent$_1$, but they all become too technical and we prefer to just give the idea above.*

When $p = 2$, the theorem above takes a slightly simpler form.

Corollary 2.16. *Let $n \geq 2$, $c \in \mathbb{F}_{2^n}$ fixed, and $F(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{2^i+2^j}$ be a Dembowski-Ostrom polynomial on $\mathbb{F}_{2^n}$. The following statements hold*:

(*i*) *If, for some* $u \in \mathbb{F}_{2^n}^*$, *there exists* $b \in \mathbb{F}_{2^n}^*$ *such that* $L_u(b) = 0$, *where* $A_i = \sum_{k=0}^{n-1} u^{p^k}(a_{ik} + a_{ki})$, *and* $|\Omega_{b(1-c)F,1}| < 2^{n-1}$, *then* F *is not* c*-differential bent*$_1$.

(*ii*) *If for* $u, b \in \mathbb{F}_{2^n}^*$, $L_u(b) \neq 0$ *and* $\sum_{x \in \Omega_{b(1-c)F,1}} (-1)^{\mathrm{Tr}_m(bD_uF(x))} = 0$, *or, if* $L_u(b) = 0$ *and* $\sum_{x \in \Omega_{b(1-c)F,1}} (-1)^{\mathrm{Tr}_m(bD_uF(x))} = (-1)^{bF(u)} 2^{n-1}$, *then* F *is* c*-differential bent*$_1$.

3 A second crosscorrelation: c-differential bent$_2$ and perfect$_2$ c-nonlinearity

In this section, we take a novel route and define a (semi-vectorial) Walsh transform (and a crosscorrelation below) by identifying *only* the output domain (via some basis, generated by the primitive element α) with $\mathbb{Z}_{p^m}$, using the invertible map $\sigma : \mathbb{F}_{p^m} \to \mathbb{Z}_{p^m}$, $\sigma(a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}) = a_0 + a_1 p + \cdots + a_{m-1}p^{m-1}$ (the invertibility comes from the unique representation of an integer in base p). We now define the (semi-vectorial) *Walsh transform* by (we avoid writing $\sigma(F)$ and just use F below, with the understanding that the exponent of $\zeta_{p^m}^{F(x)}$ has the meaning that we regard it in $\mathbb{Z}_{p^m}$)

$$\mathcal{H}_F(a) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_{p^m}^{F(x)} \zeta_p^{-\mathrm{Tr}_n(ax)}.$$

As for the regular differentials, for $f \in \mathcal{B}_{n,p}^m$ and fixed $c \in \mathbb{V}_m$, we define the *c-crosscorrelation* at $z \in \mathbb{F}_{p^n}$ by

$${}_c\mathcal{C}_{F,G}(z) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_{p^m}^{F(x+z)-cG(x)}$$

and the corresponding *c-autocorrelation* at $z \in \mathbb{F}_{p^n}$, ${}_c\mathcal{C}_F = {}_c\mathcal{C}_{F,F}$. Surely, if $m = 1$, ${}_c\mathcal{C}_{F,G} = \mathcal{C}_{F,cG}$ and ${}_c\mathcal{C}_F = \mathcal{C}_{F,cF}$. The proof of the following lemma is similar to the one of Lemma 2.2, so we omit it.

Lemma 3.1. *Let* p *be a prime number and* m, n *be nonzero positive integers. If* $F, G \in \mathcal{B}_{n,p}^m$ *and* $c \in \mathbb{F}_{p^m}$, *then*

$$\begin{aligned} \sum_{u \in \mathbb{F}_{p^n}} {}_c\mathcal{C}_{F,G}(u)\zeta_p^{-\mathrm{Tr}(\alpha u)} &= \mathcal{H}_F(\alpha)\overline{\mathcal{H}_{cG}(\alpha)}, \alpha \in \mathbb{F}_{p^n} \\ {}_c\mathcal{C}_{F,G}(u) &= p^{-n} \sum_{x \in \mathbb{F}_{p^n}} \mathcal{H}_F(x)\overline{\mathcal{H}_{cG}(x)}\zeta^{\mathrm{Tr}(ux)}, u \in \mathbb{F}_{p^n}. \end{aligned} \tag{5}$$

In particular, if $F = G$, then

$$\sum_{u\in\mathbb{F}_{p^n}} {}_c\mathcal{C}_F(u)\zeta_p^{-\mathrm{Tr}(\alpha u)} = \mathcal{H}_F(\alpha)\overline{\mathcal{H}_{cF}(\alpha)}$$

$${}_c\mathcal{C}_F(u) = p^{-n}\sum_{x\in\mathbb{F}_{p^n}} \mathcal{H}_F(x)\overline{\mathcal{H}_{cF}(x)}\zeta_p^{\mathrm{Tr}(ux)}.$$

As before, we define a perfect nonlinear and bent property that takes into account this type of autocorrelation and differential.

Definition 3.2. *For $m \le n$, we say that a function $F \in \mathcal{B}_{n,p}^m$ is* c-differential bent$_2$ *if $\mathcal{H}_F(x)\overline{\mathcal{H}_{cF}(x)} = {}_c\mathcal{C}_F(0)$ $\forall x \in \mathbb{F}_{2^n}$.*

Definition 3.3. *We say that F is* perfect$_2$ c-nonlinear *if its c-autocorrelation ${}_c\mathcal{C}_F(u) = 0$, $u \in \mathbb{F}_{p^n}^*$. If, in addition, ${}_c\mathcal{C}_F(0) = 0$, then F is* strictly perfect$_2$ c-nonlinear*.*

Below, we will show that a function $F \in \mathcal{B}_{n,p}^m$ is c-differential bent$_2$ if and only if F is perfect$_2$ c-nonlinear ($m \le n$), thereby extending Nyberg's result [22], in this context, as well. If F is a PcN (n, n)-function (as we defined it in [7]), then F is strictly perfect$_2$ c-nonlinear, since $F(x+u)-cF(x)$ is a permutation and ${}_c\mathcal{C}_F(u) = 0$. However, the reciprocal may not be true, in general, since a sum of powers of roots of unity being zero does not imply our uniform distribution of the exponents.

Theorem 3.4. *Let $1 \le m \le n$ be integers, p prime, and $F \in \mathcal{B}_{n,p}^m$, $1 \ne c \in \mathbb{F}_{p^m}$. Then F is perfect$_2$ c-nonlinear if and only if F is c-differential bent$_2$. In particular, F is strictly perfect$_2$ c-nonlinear if and only if $\mathcal{H}_F(x)\overline{\mathcal{H}_{cF}(x)} = 0$.*

Proof. We first assume that F is perfect$_2$ c-nonlinear, and so, ${}_c\mathcal{C}_F(u) = 0$, for all $u \in \mathbb{F}_{p^n}^*$. It is easy to see that, by using Lemma 3.1,

$$\mathcal{H}_F(x)\overline{\mathcal{H}_{cF}(x)} = \sum_{u\in\mathbb{F}_{p^n}} {}_c\mathcal{C}_F(u)\zeta_p^{-\mathrm{Tr}(ux)} = {}_c\mathcal{C}_F(0).$$

For the reciprocal, we assume that F is c-differential bent$_2$. Then, for any $0 \ne u \in \mathbb{F}_{p^n}$,

$${}_c\mathcal{C}_F(u) = p^{-n}\sum_{x\in\mathbb{F}_{p^n}} \mathcal{H}_F(x)\overline{\mathcal{H}_{cF}(x)}\zeta_p^{\mathrm{Tr}(ux)}$$

$$= p^{-n}{}_c\mathcal{C}_F(0) \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(ux)} = 0,$$

where we used the property that the exponential sum of a balanced function (in this case $x \mapsto \mathrm{Tr}(ux)$, $u \neq 0$) is zero. □

As for the 0-differential bent$_1$, we can easily characterize 0-differential bent$_2$ functions.

Corollary 3.5. *Let $F \in \mathcal{B}_{n,p}^m$, with integers m, n, both greater than 1. Then F is a 0-differential bent$_2$ (perfect$_2$ 0-nonlinear) function if and only if $\mathcal{H}_F(0) = 0$.*

Proof. For $c = 0$, ${}_c\mathcal{C}_F(0) = \mathcal{H}_F(0)$. Since F is a 0-differential bent$_2$, then $\mathcal{H}_F(a)\overline{\mathcal{H}_{\mathbf{0}}(a)} = {}_0\mathcal{C}_F(0) = \mathcal{H}_F(0)\ \forall a \in \mathbb{F}_{2^n}$. However, $\mathcal{H}_{\mathbf{0}}(a) = \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{-\mathrm{Tr}_n(ax)}$, which is 0, if $a \neq 0$, and p^n if $a = 0$. Thus, ${}_0\mathcal{C}_F(0) = \mathcal{H}_F(0) = 0$. Conversely, assuming $\mathcal{H}_F(0) = 0$, the identity $\mathcal{H}_F(a)\overline{\mathcal{H}_{\mathbf{0}}(a)} = 0$ will hold for all $a \neq 0$ (if $a \neq 0$, then $\mathcal{H}_F(a)$ is arbitrary). If $a = 0$, then $\mathcal{H}_F(0) = \sum_{x\in\mathbb{F}_{p^n}} \zeta_{p^m}^{F(x)} = \mathcal{H}_F(0) = 0$. □

By the previous corollary, however, we find that if $m = n$, and F is a permutation on $\mathbb{F}_{p^n}$, then F is always going to be 0-differential bent$_2$ (since $\mathcal{H}_F(0) = 0$, if F is a permutation). Surely, if F is a permutation, then F is clearly a 0-differential bent$_2$ (perfect$_2$ 0-nonlinear) function. Moreover, if L is a linearized permutation polynomial on $\mathbb{F}_{p^n}$, then L is a perfect$_2$ c-nonlinear function, for all $c \neq 1$. To check that, we compute the autocorrelation of L, and get

$${}_c\mathcal{C}_L(a) = \sum_{x\in\mathbb{F}_{p^n}} \zeta_{p^n}^{(1-c)L(x)+L(a)} = 0,$$

for all $c \neq 1$, when L is a permutation. Thus, one can regard the set of c-differential bent$_2$ functions as a superclass of linearized permutation polynomials. We summarize this discussion below.

Proposition 3.6. *If L is a linearized permutation polynomial on $\mathbb{F}_{p^n}$, then L is c-differential bent$_2$ (perfect$_2$ c-nonlinear function), for all $c \neq 1$. If $m = n$, and F is a permutation on $\mathbb{F}_{p^n}$, then F is 0-differential bent$_2$ (perfect$_2$ 0-nonlinear function).*

By SageMath, we get other polynomials. For example, $F(x) = x^3$ is perfect$_2$ 0-nonlinear on $\mathbb{F}_{2^3}$; $F(x) = x^3 + x^5$ is perfect$_2$ 0-nonlinear on $\mathbb{F}_{2^3}$.

A general way of providing examples of (n, m)-functions that are c-differential bent$_1$, is to take a function G on $\mathbb{F}_{p^n}$ that is perfect c-nonlinear (and so, ${}_cD_aF$ is a permutation) for c in a proper subfield $\mathbb{F}_{p^m}$ of $\mathbb{F}_{p^n}$ and apply the relative trace $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}$ to it, obtaining $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ (for some m, which is a divisor of n) defined by $F(x) = \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}(G(x))$. We now provide the argument. Since G is PcN with respect to c, then $G(x+a)-cG(x)$ is a permutation on $\mathbb{F}_{p^n}$, and $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}(G(x+a)-cG(x))$ is therefore balanced on $\mathbb{F}_{p^m}$. Now, using the fact that $c \in \mathbb{F}_{p^m}$, we obtain that $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}(G(x+a)-cG(x)) = {}_cD_aF(x)$, and so, ${}_cD_aF$ is balanced on $\mathbb{F}_{p^m}$. We record this as a proposition.

Proposition 3.7. *Let $m \,|\, n$, $m < n$, and p prime. If G is PcN on $\mathbb{F}_{p^n}$ with respect to $c \in \mathbb{F}_{p^m}$, then $F(x) = \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}(G(x))$ is c-differential bent$_2$.*

We now discuss some of the differential properties of a perfect$_2$ c-nonlinear function.

Theorem 3.8. *Let m, n be positive integers and p a prime number, $F \in \mathcal{B}^m_{n,p}$ and, for all $0 \le j \le p^m - 1$, we let $S^u_{j,c} = \{x \in \mathbb{F}_{p^n} \,|\, F(x+u) - cF(x) = j\}$. Then F is a perfect$_2$ c-nonlinear function (c-differential bent$_2$) if and only if its output values satisfy $|S^u_{j+p^{m-1}\ell,c}| = |S^u_{j+p^{m-1}(p-1),c}|$, for all $0 \le j \le p^{m-1} - 1$, and $0 \le \ell \le p-1$.*

Proof. To show our claim, we order $\mathbb{F}_{p^m} = \{\alpha_0 = 0, \alpha_1 = 1, \alpha_2, \ldots, \alpha_{p^m-2}\}$, such that $\sigma(u_j) = j \in \mathbb{Z}_{p^m}$ (the bijective map σ was defined in the beginning of this section). We will use below that the order of the cyclotomic polynomial of index p^k is $\phi(p^k) = p^{k-1}(p-1)$, for all $k > 0$.

If $p = 2$ and $u \neq 0$, since $\zeta_{2^m}^{2^{m-1}+j} = -\zeta_{2^m}^j$, then

$$0 = {}_c\mathcal{C}_F(u) = \sum_{x \in \mathbb{F}_{2^n}} \zeta_{2^m}^{F(x+u)-cF(x)} = \sum_{j=0}^{2^m-1} |S^u_{j,c}| \zeta_{2^m}^j = \sum_{j=0}^{2^{m-1}-1} \left(|S^u_{j,c}| - |S^u_{j+2^{m-1},c}| \right) \zeta_{2^m}^j,$$

which will render $|S^u_{j,c}| = |S^u_{j+2^{m-1},c}|$, since $\left\{ \zeta_{2^m}^j \,|\, 0 \le j \le 2^{m-1} - 1 \right\}$ forms a basis for the cyclotomic field $\mathbb{Q}(\zeta_{2^m})$.

If $p > 2$ and $u \neq 0$, then $\zeta_{p^m}^{\ell p^{m-1}+j} = \zeta_p^\ell \zeta_{p^m}^j$, for $0 \le \ell \le p-1$, and

$$0 = {}_c\mathcal{C}_F(u) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_{p^m}^{F(x+u)-cF(x)} = \sum_{j=0}^{p^m-1} |S^u_{j,c}| \zeta_{p^m}^j = \sum_{j=0}^{p^{m-1}-1} \left(\sum_{\ell=0}^{p-1} \zeta_p^\ell |S^u_{j+p^{m-1}\ell,c}| \right) \zeta_{p^m}^j.$$

The extension $\mathbb{Q}(\zeta_p) \overset{p^{m-1}}{\hookrightarrow} \mathbb{Q}(\zeta_{p^m})$ has degree p^{m-1} and the following set $\left\{\zeta_{p^m}^j \,|\, 0 \le j \le p^{m-1}-1\right\}$ forms a basis of $\mathbb{Q}(\zeta_{p^m})$ over $\mathbb{Q}(\zeta_p)$, therefore the coefficients in the displayed expression are zero. That is, for all $0 \le j \le p^{m-1}-1$, $\sum_{\ell=0}^{p-1} \zeta_p^\ell |S^u_{j+p^{m-1}\ell,c}| = 0$. Again, using that the set $\left\{\zeta_p^j \,|\, 0 \le j \le p-2\right\}$ forms a basis for the cyclotomic field $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ and that $\zeta_p^{p-1} = -(1 + \zeta_p + \cdots + \zeta_p^{p-2})$, we get

$$\sum_{\ell=0}^{p-1} \zeta_p^\ell \left(|S^u_{j+p^{m-1}\ell,c}| - |S^u_{j+p^{m-1}(p-1),c}| \right) = 0, \text{ for all } 0 \le j \le p^{m-1}-1,$$

from which we infer that $|S^u_{j+p^{m-1}\ell,c}| = |S^u_{j+p^{m-1}(p-1),c}|$, for $0 \le j \le p^{m-1}-1$, and $0 \le \ell \le p-1$. If the previous condition will hold, by reversing the argument, we find that F is perfect$_2$ c-nonlinear. □

4 Concluding remarks

In this paper we define two different cross/autocorrelations for vectorial p-ary (n,m)-functions and the corresponding concepts of perfect c-nonlinear and c-differential bent functions in this context. We show that c-differential bent functions correspond to perfect c-nonlinear functions, thus extending Nyberg's classical result [22]. Observe that if $m = 1$, the two c-differential bent concepts coincide with the classical bent notion [11], so the new definitions can be regarded as generalizations in two different directions. We only concentrated here on a few classes of functions (Maiorana-McFarland, Gold, Coulter-Matthews and Dembowski-Ostrom polynomials) and investigated their c-differential bent properties (mostly, for the first bent type). It would be interesting to check other classes of functions for their c-differential bent$_1$ or bent$_2$ properties.

References

[1] A. Blokhuis, R.S. Coulter, M. Henderson, C.M. O'Keefe, *Permutations amongst the Dembowski-Ostrom polynomials*, Finite Fields and Applications: Proc. of the Fifth Internat. Conf. on Finite Fields and Applications (D. Jungnickel and H. Niederreiter, eds.), 2001, pp. 37–42.

[2] L. Budaghyan, Construction and Analysis of Cryptographic Functions, Springer-Verlag, 2014.

[3] C. Carlet, Boolean Functions for Cryptography and Coding Theory, Cambridge University Press, Cambridge, 2021.

[4] R. S. Coulter, M. Henderson, *On a conjecture on planar polynomials of the form* $X(\mathrm{Tr}_n(X) - uX)$, Finite Fields Appl. 21 (2013), 30–34.

[5] R. S. Coulter, R. W. Matthews, *Planar functions and planes of Lenz-Barlotti class* II, Des. Codes Cryptogr. 10 (1997), 167–184.

[6] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications (Ed. 2), Academic Press, San Diego, CA, 2017.

[7] P. Ellingsen, P. Felke, C. Riera P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity*, IEEE Trans. Inf. Theory 66:9 (2020), 5781–5789.

[8] T. Helleseth and A. Kholosha, *Monomial and quadratic bent functions over the finite fields of odd characteristic*, IEEE Trans. Inform. Theory 52:5 (2006), 2018–2032.

[9] S. Hodžić, W. Meidl, E. Pasalic, *Full characterization of generalized bent functions as (semi)-bent spaces, their dual and the Gray image*, IEEE Trans. Inform. Theory 64 (2018), 5432– 5440.

[10] S. Hodžić, E. Pasalic, *Generalized bent functions – Some general construction methods and related necessary and sufficient conditions*, Cryptogr. Commun. 7 (2015), 469–483.

[11] P. V. Kumar, R. A. Scholtz, L, R. Welch, *Generalized bent functions and their properties*, J. Combin. Theory – Series A 40(1) (1985), 90–107.

[12] G. Kyureghyan, F. Özbudak, *Planarity of products of two linearized polynomials*, Finite Fields Appl. 18 (6) (2012), 1076–1088.

[13] R. Lidl, H. Niederreiter, Finite Fields (Ed. 2), Encycl. Math. Appl., vol.20, Cambridge Univ. Press, Cambridge, 1997.

[14] T. Martinsen, W. Meidl, S. Mesnager, P. Stănică, *Decomposing generalized bent and hyperbent functions*, IEEE Trans. Inf. Theory 63:12 (2017), 7804–7812.

[15] T. Martinsen, W. Meidl, A. Pott, P. Stănică, *On symmetry and differential properties of generalized Boolean functions*, Proc. of WAIFI 2018: Arithmetic of Finite Fields, LNCS 11321 (2018), 207–223.

[16] T. Martinsen, W. Meidl, P. Stănică, *Generalized bent functions and their Gray images*, Proc. of WAIFI 2016: Arithmetic of Finite Fields, LNCS 10064 (2017), 160–173.

[17] T. Martinsen, W. Meidl, P. Stănică, *Partial Spread and Vectorial Generalized Bent Functions*, Designs, Codes & Cryptogr. 85:1 (2017), 1–13.

[18] S. Mesnager, Bent functions: fundamentals and results, Springer Verlag, 2016.

[19] S. Mesnager, C. Riera, P. Stănică, *Multiple characters transforms and generalized Boolean functions*, Cryptogr. Commun. 11:6 (2019), 1247–1260.

[20] S. Mesnager, C. Riera, P. Stănică, H. Yan, Z. Zhou, *Investigation on c-(almost) perfect nonlinear functions*, IEEE Trans. Inform. Theory 67:10 (2021), 6916–6925.

[21] S. Mesnager, C. Tang, Y. Qi, L. Wang, B. Wu, and K. Feng, *Further Results on Generalized Bent Functions and Their Complete Characterization*, IEEE Trans. Inform. Theory 64:7 (2018), 5441–5452.

[22] K. Nyberg, *Perfect nonlinear S-boxes*, In D.W. Davies (ed.), Adv. Crypt – EUROCRYPT '91, LNCS 547, pp. 378–386, 1991.

[23] A. Pott, *Nonlinear functions in abelian groups and relative difference sets*, Optimal discrete structures and algorithms (ODSA 2000), Discrete Appl. Math. 138 (2004), 177–193.

[24] P. Stănică, T. Martinsen, S. Gangopadhyay, B. K. Singh, *Bent and generalized bent Boolean functions*, Des. Codes & Cryptogr. 69 (2013), 77–94.

[25] C. Tang, C. Xiang, Y. Qi, K. Feng. *Complete characterization of generalized bent and 2^k-bent Boolean functions*, IEEE Trans. Inf. Theory 63:7 (2017), 4668–4674.

[26] N. Tokareva, Bent Functions, Results and Applications to Cryptography, Academic Press, San Diego, CA, 2015.

[27] M. Yanga, S. Zhu, K. Feng, *Planarity of mappings $x(\mathrm{Tr}(x) - \frac{\alpha}{2}x)$ on finite fields*, Finite Fields Appl. 23 (2013), 1–7.

[28] F. Zhang, S. Xia, P. Stănică, Y. Zhou, *Further results on constructions of generalized bent Boolean functions*, Inf. Sciences - China. 59 (2016), 1–3.

[29] Z. Zha, X. Wang, *Almost Perfect Nonlinear Power Functions in Odd Characteristic*, IEEE Trans. Inf. Theory 57:7 (2011) (1999), 4826–4832.