ON DILLON'S CLASS H OF BENT FUNCTIONS, NIHO BENT FUNCTIONS AND O-POLYNOMIALS

CLAUDE CARLET AND SIHEM MESNAGER

Abstract. One of the classes of bent Boolean functions introduced by John Dillon in his thesis is family H. While this class corresponds to a nice original construction of bent functions in bivariate form, Dillon could exhibit in it only functions which already belonged to the well-known Maiorana-McFarland class. We first notice that H can be extended to a slightly larger class that we denote by $\mathcal{H}$. We observe that the bent functions constructed via Niho power functions, which four examples are known, due to Dobbertin et al. and to Leander-Kholosha, are the univariate form of the functions of class $\mathcal{H}$. We answer to the open question raised by Dobbertin et al. in JCT A 2006 on whether the duals of the Niho bent functions introduced in the paper are Niho bent as well, by explicitely calculating the dual of one of these functions. We observe that this Niho function also belongs to the Maiorana-McFarland class, which brings us back to the problem of knowing whether H (or $\mathcal{H}$) is a subclass of the Maiorana-McFarland completed class. We then show that the condition for a function in bivariate form to belong to class $\mathcal{H}$ is equivalent to the fact that a polynomial directly related to its definition is an o-polynomial and we deduce eight new cases of bent functions in $\mathcal{H}$ which are potentially new bent functions and most probably not affine equivalent to Maiorana-McFarland functions.

Keywords. Boolean function, Bent function, Maximum nonlinearity, Walsh-Hadamard transform, Partial Spread class, Niho function, O-polynomial.

1. Introduction

Bent functions [9, 29] are extremal objects in combinatorics and Boolean function theory. They have been studied for about 40 years; even more, under the name of difference sets in elementary Abelian 2-groups. The motivation for the study of these particular difference sets is mainly cryptographic (but bent functions play also a role in coding theory and sequences; and as difference sets they lead to designs). Symmetric cryptosystems using Boolean functions can be cryptanalyzed when these Boolean functions can be approximated by affine Boolean functions, that is, by functions of the form $\ell(x_1, \cdots, x_n) = a_0 + a_1x_1 + \cdots + a_nx_n = a_0 + a \cdot x$, where $x = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$, $a = (a_1, \cdots, a_n) \in \mathbb{F}_2^n$ and $a_0 \in \mathbb{F}_2$. The set of affine functions can be viewed as the Reed-Muller code of order 1 (see [22]), denoted by $R(1, n)$. We say that ℓ approximates a Boolean function f if the Hamming distance $d_H(f, \ell) = \#\{x \in \mathbb{F}_2^n \mid f(x) \neq \ell(x)\}$ between them is small. So, a Boolean function resists attacks by affine approximation if its distance to $R(1, n)$ (i.e. its minimum distance to all affine functions) is large. This distance is called the *nonlinearity* of the function. The maximal possible nonlinearity of n-variable Boolean functions, given by the so-called covering radius bound $2^{n-1} - 2^{n/2-1}$ (see for instance in [3] a

Date: November 7, 2010.

LAGA , UMR 7539, CNRS, Department of Mathematics, University of Paris XIII and University of Paris VIII, 2 rue de la liberté, 93526 Saint-Denis Cedex, France. *Email*: claude.carlet@inria.fr, mesnager@math.jussieu.fr.

survey on Boolean functions), can be achieved with equality for n even only.

A Boolean function f on $\mathbb{F}_2^n$ ($n = 2m$ even) is called bent if its nonlinearity equals $2^{n-1} - 2^{m-1}$ (hence its resistance to the attacks based on affine approximation is optimal). Equivalently, as shown in [9, 29], f is bent if and only if its Walsh transform $\widehat{\chi_f}$ defined at every $a \in \mathbb{F}_2^n$ by $\widehat{\chi_f}(a) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}$, where "$\cdot$" denotes any inner product in $\mathbb{F}_2^n$ (for instance the inner product defined above), takes values $\pm 2^m$ only (this characterization is independent of the choice of the inner product in $\mathbb{F}_2^n$, since any other inner product has the form $\langle x, s\rangle = x \cdot L(s)$, where L is an auto-adjoint linear automorphism, *i*.e. an automorphism whose associated matrix is symmetric). If f is bent, then the *dual function* $\widetilde{f}$ of f, defined on $\mathbb{F}_2^n$ by:

$$\widehat{\chi_f}(u) = 2^m(-1)^{\widetilde{f}(u)}$$

is also bent and its own dual is f itself.

As any Boolean functions, bent functions can be represented in a unique way by their algebraic normal form (ANF)

$$f(x) = \sum_{I\subseteq\{1,\cdots,n\}} a_I \left(\prod_{i\in I} x_i\right) ;\ a_I \in \mathbb{F}_2. \tag{1}$$

The global degree of their ANF (called their algebraic degree) is not large: it is upper bounded by m. For this reason (since a cryptographic Boolean function should have high algebraic degree, to allow resistance to the Berlekamp-Massey and Rønjom-Helleseth attacks [24, 28]) and also because bent functions are not balanced, that is, do not have an output uniformly distributed over $\mathbb{F}_2$, they are improper for being used as is in cryptosystems. But they can be used to build proper balanced functions, see [10].

Bent functions are often better viewed in their bivariate representation and can also be viewed in their univariate representation. The univariate representation of any Boolean function is defined as follows: we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ (which is an n-dimensional vector space over $\mathbb{F}_2$) and we consider then the input to f as an element of $\mathbb{F}_{2^n}$. An inner product in $\mathbb{F}_{2^n}$ is $x \cdot y = Tr_1^n(xy)$ where $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. There exists a unique univariate polynomial $\sum_{i=0}^{2^n-1} a_i x^i$ over $\mathbb{F}_{2^n}$ such that f is the polynomial function over $\mathbb{F}_{2^n}$ associated to it (this is true for every function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$). Then the algebraic degree of f equals the maximum 2-weight of the exponents with nonzero coefficients, where the 2-weight $w_2(i)$ of an integer i is the number of 1's in its binary expansion. Hence, in the case of a bent function, all exponents i whose 2-weights are larger than m have null coefficient a_i. Moreover, f being Boolean, its univariate representation can be written in the form $f(x) = \sum_{j\in\Gamma_n} Tr_1^{o(j)}(a_j x^j)$, where Γ_n is the set of integers obtained by choosing one element in each cyclotomic coset of 2 modulo $2^n - 1$, $o(j)$ is the size of the cyclotomic coset of 2 modulo $2^n - 1$ containing j and $a_j \in \mathbb{F}_{2^{o(j)}}$. This expression is unique. It can also be written under a non-unique form $Tr_1^n(P(x))$ where $P(x)$ is a polynomial over $\mathbb{F}_{2^n}$.

The bivariate representation of Boolean functions is defined as follows: we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ and we consider then the input to f as an ordered pair (x, y) of elements of $\mathbb{F}_{2^m}$. There exists a unique bivariate polynomial $\sum_{0\le i,j\le 2^m-1} a_{i,j}x^i y^j$ over $\mathbb{F}_{2^m}$ such that f is the bivariate polynomial function over $\mathbb{F}_{2^m}$ associated to it. Then the algebraic degree of f equals $\max_{(i,j)\,|\,a_{i,j}\neq 0}(w_2(i) + w_2(j))$. And f being Boolean, its bivariate representation can be written in the form $f(x, y) = Tr_1^m(P(x, y))$ where $P(x, y)$ is some polynomial over $\mathbb{F}_{2^m}$.

Clearly, if f is bent and ℓ is affine, then $f+\ell$ is bent. The automorphism group of the set of bent functions (i.e., the group of permutations π on $\mathbb{F}_2^n$ or $\mathbb{F}_{2^n}$ such that $f \circ \pi$ is bent for every bent function f) is the general affine group, that is, the group of linear automorphisms composed by translations. A class of bent functions is called a *complete class* if it is globally invariant under the action of the general affine group and under the addition of affine functions.
Any function f is bent if and only if, for any nonzero vector a, the Boolean function $D_a f(x) = f(x) + f(x+a)$ is balanced (i.e. has Hamming weight 2^{n-1}). For this reason, bent functions are also called *perfect nonlinear functions*. Equivalently, f is bent if and only if the $2^n \times 2^n$ matrix $H = [(-1)^{f(x+y)}]_{x,y\in\mathbb{F}_2^n}$ is a Hadamard matrix (*i*.e. satisfies $H \times H^t = 2^n I$, where I is the identity matrix), and if and only if the support of f is a *difference set*. Bent functions have also the property that, for every even positive integer w, the sum $\sum_{a\in\mathbb{F}_2^n} \widehat{\chi_f}^{\,w}(a)$ is minimum.
Bent functions are all known for $n \leq 8$, only (their determination for 8 variables [18, 19] has been achieved only recently) as well as their classification under the action of the general affine group. For $n \geq 10$, only classes of bent functions are known, which do not cover a large part of them, apparently. Determining all bent functions (or more practically, classifying them under the action of the general affine group) seems elusive. Several constructions of explicit bent functions are known which lead to infinite classes. We describe the main ones in the next section. The two most well-known are the Maiorana-McFarland class and the PSap class. Both were studied in Dillon's thesis [9] and have been later revisited in numerous papers. Another class, denoted by H, was introduced in [9] as well, but Dillon could not exhibit bent functions in it which were not in the Maiorana-McFarland class. The construction of the bent functions in this class is based on a nice observation that we shall recall in the next section. We shall also see that class H can be slightly extended into a class that we shall denote by $\mathcal{H}$. The definition given by Dillon of the functions in class H is in terms of their bivariate representation; class $\mathcal{H}$ is also defined in this representation. We shall observe that these classes, when viewed in their univariate representation, are the so-called Niho bent functions, which have been studied in several papers. In [14], Dobbertin et al. introduced three classes of Niho bent functions. The problem of knowing whether the duals of these functions are also Niho bent was left open. We calculate the bivariate representation of the second Dobbertin-et-al's function and the bivariate expression of its dual. We observe that the dual is not a Niho bent function, which allows replying negatively to the open question. Another open question (which is not addressed in [14], though) is: do these three functions belong to the completed Maiorana-McFarland class? We leave this question open. More generally, an important question is to determine whether all functions in class H (resp. $\mathcal{H}$) belong to the completed Maiorana-McFarland class. We reply negatively to this question by observing that the condition for a function with given bivariate representation to belong to $\mathcal{H}$ is equivalent to the fact that some polynomial is an o-polynomial over $\mathbb{F}_{2^m}$ (see below the definition of these polynomials). There exist currently 8 known infinite classes of o-polynomials over $\mathbb{F}_{2^m}$, up to the group of transformations which leave invariant the set of these polynomials; this leads us to 8 new classes of bent functions, which potentially do not all belong to the Maiorana-McFarland class.

In whole the paper, $E^\star = E \setminus \{0\}$ and $\#E$ will denote the cardinality of E, for any set E.

2. The two main known classes of bent functions

We recall that $n = 2m$. Several classes of bent functions have been introduced in [9, 29]. Some (like the $\mathcal{PS}$ class, recalled below) need conditions whose realizations are difficult to achieve, and so are more principles of constructions rather than explicit constructions. Others lead to explicit bent functions (given by their ANF or their polynomial univariate or bivariate representation). The two main ones of this last kind are the following:

1. The *Maiorana-McFarland class* $\mathcal{M}$ is the set of all the Boolean functions on $\mathbb{F}_2^n = \{(x, y); x, y \in \mathbb{F}_2^m\}$, of the form:

$$f(x, y) = x \cdot \pi(y) + g(y) \tag{2}$$

where π is any permutation on $\mathbb{F}_2^m$ and g any Boolean function on $\mathbb{F}_2^m$ ("$\cdot$" denotes here an inner product in $\mathbb{F}_2^m$). Any such function is bent. More precisely, the bijectivity of π is a necessary and sufficient condition for f being bent. The dual function $\widetilde{f}(x, y)$ equals: $y \cdot \pi^{-1}(x) + g(\pi^{-1}(x))$, where π^{-1} is the inverse permutation of π. The completed class of $\mathcal{M}$ (that is, the smallest possible complete class including $\mathcal{M}$) contains all the quadratic bent functions (that is, the bent functions of algebraic degree 2).

2. We define now the $\mathcal{PS}_{ap}$ *class*. For this, we first need to define the *Partial Spreads class* $\mathcal{PS}$. It is the set of all the sums (modulo 2) of the indicators of 2^{m-1} or $2^{m-1}+1$ "disjoint" m-dimensional subspaces of $\mathbb{F}_2^n$ ("disjoint" meaning that any two of these spaces intersect in 0 only, and therefore that their sum is direct and equals $\mathbb{F}_2^n$). J. Dillon denotes by $\mathcal{PS}^-$ (resp. $\mathcal{PS}^+$) the class of those bent functions for which the number of m-dimensional subspaces is 2^{m-1} (resp. $2^{m-1}+1$). All the elements of $\mathcal{PS}^-$ have algebraic degree m exactly, but not all those of $\mathcal{PS}^+$ (which contains for instance all the quadratic functions, if m is even). J. Dillon exhibits in [9] a subclass of $\mathcal{PS}^-$, denoted by $\mathcal{PS}_{ap}$, whose elements are defined in an explicit form: $\mathbb{F}_2^m$ is identified to the Galois field $\mathbb{F}_{2^m}$ (an inner product in this field being defined as $x \cdot y = Tr_1^m(xy)$, where $Tr_1^m(x) = \sum_{i=0}^{m-1} x^{2^i}$ is the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$). The elements of $\mathcal{PS}_{ap}$ are the functions of the form $f(x, y) = g\left(x\, y^{2^m-2}\right)$, *i.*e. $g\left(\frac{x}{y}\right)$ with $\frac{x}{y} = 0$ if $y = 0$, where g is any balanced Boolean function on $\mathbb{F}_2^m$ which vanishes at 0. The complements $g\left(\frac{x}{y}\right) + 1$ of these functions are the functions $g(\frac{x}{y})$ where g is balanced and does not vanish at 0; they belong to the class $\mathcal{PS}^+$. In both cases, the dual of $g(\frac{x}{y})$ is $g(\frac{y}{x})$.

3. Class $\mathcal{H}$ and Niho bent functions

3.1. **Classes H and $\mathcal{H}$ in bivariate form.** In his thesis [9], Dillon introduces a third family of bent functions whose expression is given but whose bentness is achieved under some non-obvious condition (so the class is less explicit than class $\mathcal{M}$ or class $\mathcal{PS}_{ap}$, but it happens to be more explicit than class $\mathcal{PS}$, the condition for H being easier to satisfy than for $\mathcal{PS}$, as we shall see). He defines these functions in bivariate form (but as we shall see, they can also be seen in univariate form). The functions of this family are defined as $f(x, y) = Tr_1^m(y + xG(yx^{2^m-2}))$, with $x, y \in \mathbb{F}_{2^m}$ where G is a permutation of $\mathbb{F}_{2^m}$ such that $G(x) + x$ does not vanish and, for every $\beta \in \mathbb{F}_{2^m}^\star$, the function $G(x) + \beta x$ is two-to-one (i.e. the pre-image by this function of any element of $\mathbb{F}_{2^m}$ is either a pair or the empty set). He denotes this family of bent functions by H.

The condition that $G(x)+x$ does not vanish is required only for H to be a sub-class of $\mathcal{PS}$ but is

not necessary for f to be bent. Similarly, the linear term $Tr_1^m(y)$ can be taken off if we are only interested in the bentness of the function. We have then $f(x,y) = \begin{cases} Tr_1^m\left(xG\left(\frac{y}{x}\right)\right) \text{ if } x \neq 0 \\ 0 \text{ if } x = 0 \end{cases}$.
Note that the restriction of g to the vectorspaces $\{(x, ax)\,;\, x \in \mathbb{F}_{2^m}\}$ where $a \in \mathbb{F}_{2^m}$ and $\{(0,y)\,;\, y \in \mathbb{F}_{2^m}\}$ are linear. More generally, any function whose restrictions to these vectorspaces are linear has the form:

$$g(x,y) = \begin{cases} Tr_1^m\left(xH\left(\frac{y}{x}\right)\right) \text{ if } x \neq 0 \\ Tr_1^m(\mu y) \text{ if } x = 0 \end{cases} \tag{3}$$

where $\mu \in \mathbb{F}_{2^m}$ and H is a mapping from $\mathbb{F}_{2^m}$ to itself. In the following proposition, we check (again, since this has been essentially done by Dillon) what is the necessary and sufficient condition on H and μ such that g is bent.

Proposition 1. *let g be a Boolean function function over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ defined by (3). Then g is bent if and only if, denoting $G(z) = H(z) + \mu z$, we have:*

$$G \text{ is a permutation on } \mathbb{F}_{2^m} \tag{4}$$

$$\text{For every } \beta \in \mathbb{F}_{2^m}^\star, \text{ the function } z \mapsto G(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m}. \tag{5}$$

Proof. For every $\alpha, \beta \in \mathbb{F}_{2^m}$, we have:

$$\widehat{\chi_g}(\alpha,\beta) = \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{g(x,y)+Tr_1^m(\alpha x+\beta y)} =$$
$$\sum_{x \in \mathbb{F}_{2^m}^\star, z \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(xH(z)+\alpha x+\beta xz)} + \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m((\beta+\mu)y)} =$$
$$\sum_{x \in \mathbb{F}_{2^m}, z \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(xH(z)+\alpha x+\beta xz)} - 2^m + 2^m \delta_\mu(\beta) =$$
$$2^m \,\#\{z \in \mathbb{F}_{2^m} \,/\, H(z) + \alpha + \beta z = 0\} - 2^m + 2^m \delta_\mu(\beta).$$

We denote by $N_{\alpha,\beta}$ the cardinality of the set $\{z \in \mathbb{F}_{2^m} \,/\, H(z) + \alpha + \beta z = 0\}$.
Then we have $\widehat{\chi_g}(\alpha,\beta) = \begin{cases} 2^m N_{\alpha,\mu} \text{ if } \beta = \mu \\ 2^m N_{\alpha,\beta} - 2^m \text{ if } \beta \neq \mu \end{cases}$, and Conditions (4) and (5) are necessary and sufficient for g being bent. □

Definition 1. We call $\mathcal{H}$ the extended class of H equal to the set of functions g defined by (3) and satisfying (4) and (5) (that is, satisfying (5), since we shall see below that Condition (5) implies Condition (4)).

Note that function g defined by (3) satisfies $g(x,y) + Tr_1^m(\mu y) = \begin{cases} Tr_1^m\left(xG\left(\frac{y}{x}\right)\right) \text{ if } x \neq 0 \\ 0 \text{ if } x = 0 \end{cases}$
and that changing $G(x)$ into $G(x)+\nu$ changes $g(x,y)$ into $g(x,y)+Tr_1^m(\nu x)$. Hence, we can assume without loss of generality (up to the addition of a linear function) that $\mu = 0$ and $G(0) = 0$.

We consider now the duals of the functions in class $\mathcal{H}$. Under the conditions of Proposition 1:
- if $\beta = \mu$ then we have $\widehat{\chi_g}(\alpha,\beta) = 2^m$ and the equation $H(z) + \beta z = G(z) + (\beta+\mu)z = \alpha$ has a solution
- and if $\beta \neq \mu$ then we have $\widehat{\chi_g}(\alpha,\beta) = 2^m$ if and only if the equation $H(z) + \beta z = G(z) + (\beta +$

$\mu)z = \alpha$ has solutions.
We deduce:

Proposition 2. *Let g be a bent function of the form (3) Then the dual function of g is defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ as:*
$\widetilde{g}(\alpha,\beta) = \begin{cases} 1 \text{ if the equation } H(z)+\beta z = G(z)+(\beta+\mu)z = \alpha \text{ has no solution in } \mathbb{F}_{2^m} \\ 0 \text{ otherwise} \end{cases}$

Remark 1. Since bent functions exist of the form (3), a natural question is: does there exist also semi-bent functions of the same form? Recall that a Boolean function is called semi-bent if its Walsh transform takes only the values 0 and $\pm 2^{m+1}$. Assume without loss of generality that $\mu = 0$ and that $G(0) = 0$. We remark that g is semi-bent if and only if $N_{\alpha,0} \in \{0,2\}$ and $N_{\alpha,\beta} \in \{1,3\}$ ($\beta \neq 0$). If $N_{\alpha,0} \in \{0,2\}$, $\widehat{\chi_g}(\alpha,0) \in \{0, 2^{m+1}\}$ and if $N_{\alpha,\beta} \in \{1,3\}$, $\widehat{\chi_g}(\alpha,\beta) \in \{0, 2^{m+1}\}$. This is impossible if $n > 2$ because of the Lemma 3 below. Therefore, there exists no semi-bent function of the form (3) for $n > 2$.

Lemma 3. *Let g be a Boolean function. If the Walsh transform values of g are all non-negative, then g is affine.*

Proof. According to Parseval's relation and since, by the inverse Fourier transform formula, we have $\sum_{\omega\in\mathbb{F}_2^n} \widehat{\chi_f}(\omega) = \pm 2^n$ (see e.g. [3]), we have: $\sum_{\omega\in\mathbb{F}_2^n} \widehat{\chi_g}^2(\omega) = 2^{2n} = (\sum_{\omega\in\mathbb{F}_2^n} \widehat{\chi_g}(\omega))^2$. This implies $\sum_{\omega\neq\omega'\in\mathbb{F}_2^n} \widehat{\chi_g}(\omega)\widehat{\chi_g}(\omega') = 0$ (relation valid for every Boolean function) and therefore, since the values of $\widehat{\chi_g}$ are non-negative: $\widehat{\chi_g}(\omega) = 0$ or $\widehat{\chi_g}(\omega') = 0$ for every $\omega \neq \omega'$. The Walsh transform of g takes therefore non-zero value at exactly one point and it is well-known that g is then affine (that is, has algebraic degree at most 1). □

3.1.1. *A first infinite class of functions in $\mathcal{H}$.* The Frobenius map $z \mapsto G(z) = z^2$ gives an example of functions G, which leads to a function in the class $\mathcal{H}$: $g(x,y) = Tr_1^m(y^2x^{2^m-2})$. More generally, one can get functions in the class $\mathcal{H}$ by considering the maps $z \mapsto G(z) = z^{2^i}$ where i is co-prime with m, since the equation $z^{2^i} + \beta z = \alpha$ is equivalent, denoting $\gamma = \beta^{\frac{1}{2^i-1}}$, to $\left(\frac{z}{\gamma}\right)^{2^i} + \frac{z}{\gamma} = \frac{\alpha}{\gamma^{2^i}}$. As observed by Dillon, the related bent functions are in the completed Maiorana-MacFarland's class; indeed they equal $g(x,y) = Tr_1^m(x^{2^j}yx^{2^m-1}) = Tr_1^m(yx^{2^j-1})$ ($j = m-i$).

3.1.2. *Stability of functions G satisfying Conditions (4) and (5).* Note that Condition (5) is equivalent to saying that for every $\beta \in \mathbb{F}_{2^m}^\star$, the function $z \mapsto \beta G(z) + z$ is 2-to-1. Let G be a function satisfying Conditions (4) and (5). Then

- the function $z \mapsto G^{-1}(z)$ satisfies Conditions (4) and (5), since denoting $G^{-1}(z)$ by z', the equation $G^{-1}(z) + \beta z = \alpha$ is equivalent to $G(z') + \frac{1}{\beta}z' = \frac{\alpha}{\beta}$.
- the function $z \mapsto G'(z) := \lambda G(z) + \lambda'$ with $\lambda \neq 0$ satisfies Conditions (4) and (5).
- the function $z \mapsto G'(z) := G(\lambda z + \lambda')$ with $\lambda \neq 0$ satisfies Conditions (4) and (5).
- the function $z \mapsto G'(z) := zG(z^{2^m-2})$ (with $G(0) = 0$) satisfies Conditions (4) and (5). Indeed (still assuming that $\beta \neq 0$) if $\alpha \neq 0$ then $zG(z^{2^m-2}) = \alpha$ is equivalent to $G(z^{2^m-2}) = \alpha z^{2^m-2}$ which has one solution since $G(z) + \alpha z = 0$ has two solutions and $z = 0$ is one of them, and the equation $zG(z^{2^m-2}) + \beta z = \alpha$ is equivalent to $G(z^{2^m-2}) + \alpha z^{2^m-2} = \beta$ and has therefore 0 or 2 solutions; and if $\alpha = 0$ then $zG(z^{2^m-2}) =$

$\alpha = 0$ is equivalent to $z = 0$ and the equation $zG(z^{2^m-2}) + \beta z = \alpha = 0$ is equivalent to $z = 0$ or $G(z^{2^m-2}) = \beta$ which has one (nonzero) solution.

- the function $z \mapsto G'(z) := (A^{-1} \circ G \circ A)(z)$ (where A is an affine automorphism of $\mathbb{F}_{2^m}$) satisfies Conditions (4) and (5). In particular, if A is the linear automorphism π such that $\pi(z) := z^{2^j}$ ($\pi^{-1}(z) = z^{2^{m-j}}$) then, $G'(z) = (G(z^{2^j}))^{2^{m-j}}$.

3.2. **Functions of class $\mathcal{H}$ in univariate form: Niho bent functions.** We identify now $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with $\mathbb{F}_{2^n}$ by considering a basis (α, β) of the $\mathbb{F}_{2^m}$-vector space $\mathbb{F}_{2^n}$ and identifying $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with $t = x\alpha + y\beta$. Then the vectorspaces $\{(x, ax)\,;\, x \in \mathbb{F}_{2^m}\}$ where $a \in \mathbb{F}_{2^m}$ and $\{(0, y)\,;\, y \in \mathbb{F}_{2^m}\}$ become the $2^m + 1$ multiplicative cosets of $\mathbb{F}_{2^m}^\star$ in $\mathbb{F}_{2^n}^\star$, added with 0. These cosets can be written $u\mathbb{F}_{2^m}^\star$ where u ranges over the multiplicative subgroup U of $\mathbb{F}_{2^n}^\star$ of order $2^m + 1$, if we want to have a unique representation of each of them. And if we allow repetition, they are the cosets $u\mathbb{F}_{2^m}^\star$ where $u \in \mathbb{F}_{2^n}^\star$. The necessary and sufficient condition for a bent function to belong to class $\mathcal{H}$ is then that its restriction to each vectorspace $u\mathbb{F}_{2^m}$, $u \in \mathbb{F}_{2^n}^\star$, is linear.

Lemma 4. *Let f be a Boolean function over $\mathbb{F}_{2^n}$ and $f(x) = \sum_{i=0}^{2^n-1} a_i x^i$ its univariate representation. Then the restrictions of f to the vectorspaces $u\mathbb{F}_{2^m}$, $u \in \mathbb{F}_{2^n}^\star$, are all linear if and only if the only exponents i such that $a_i \neq 0$ are congruent with powers of 2 modulo $2^m - 1$.*

Proof. The condition is clearly sufficient. Let us show that it is also necessary. We first notice that $a_0 = 0$. If the restriction of f to $u\mathbb{F}_{2^m}$ is linear for some u then there exists $\lambda_u \in \mathbb{F}_{2^m}$ such that $f(ux) = \sum_{i=1}^{2^n-1} a_i u^i x^{i[\mathrm{mod}\ 2^m-1]}) = Tr_1^m(\lambda_u x)$ for every $x \in \mathbb{F}_{2^m}^\star$. By uniqueness of the univariate representation of a Boolean function over $\mathbb{F}_{2^m}$, we deduce that for every $k \in \{0, \cdots, 2^m - 2\}$ which is different from a power of 2, we have $\sum_{\substack{1 \leq i \leq 2^n-1 \\ i \equiv k \ [\mathrm{mod}\ 2^m-1]}} a_i u^i = 0$. Hence, if the restrictions of f to the vectorspaces $u\mathbb{F}_{2^m}$, $u \in \mathbb{F}_{2^n}^\star$, are all linear then we have $\sum_{\substack{1 \leq i \leq 2^n-1 \\ i \equiv k \ [\mathrm{mod}\ 2^m-1]}} a_i u^i = 0$ for every $u \in \mathbb{F}_{2^n}^\star$ (and therefore for every $u \in \mathbb{F}_{2^n}$) and every $k \in \{0, \cdots, 2^m - 2\}$ which is different from a power of 2. This completes the proof, by uniqueness of the univariate representation of a function from $\mathbb{F}_{2^m}$ to itself. □

Note that this result extends to any function f from $\mathbb{F}_{2^n}$ to itself.

Bent functions whose restrictions to the vectorspaces $u\mathbb{F}_{2^m}$ are all linear have already been investigated in [14] and [20]. Since the exponents congruent with powers of 2 modulo $2^m - 1$ are called Niho exponents, we shall call these functions *Niho bent functions*. The name of Niho exponent comes from a theorem dealing with power functions by Niho [25], which has been later extended to linear combinations of such power functions in [14] (see also [20]), and which relates the value of the Walsh transform of such a sum to the number of solutions in U of some equation.

Four examples of infinite classes of Niho bent functions are known up to linear equivalence:

- The simplest one is the quadratic function $Tr_1^m\left(at^{2^m+1}\right)$, where $a \in \mathbb{F}_{2^m}^\star$.
- Three other examples are given in [14]. They are binomials of the form $f(t) = Tr_1^n(\alpha_1 t^{d_1} + \alpha_2 t^{d_2})$, $t \in \mathbb{F}_{2^n}$, where $2d_1 = 2^m + 1 \in \mathbb{Z}/(2^n - 1)\mathbb{Z}$ and $\alpha_1, \alpha_2 \in \mathbb{F}_{2^n}^\star$ are such that $(\alpha_1 + \alpha_1^{2^m})^2 = \alpha_2^{2^m+1}$. Equivalently, denoting $a = (\alpha_1 + \alpha_1^{2^m})^2$ and $b = \alpha_2$, we have $a = b^{2^m+1} \in \mathbb{F}_{2^m}^\star$ and $f(t) = Tr_1^m(at^{2^m+1}) + Tr_1^n(bt^{d_2})$ (note that if $b = 0$ and $a \neq 0$

then f is also bent but it belongs then to the class of quadratic Niho bent functions seen above). The values of d_2 are:
  - $d_2 = (2^m - 1)\,3 + 1$ (with the condition that, if m is congruent with 2 mod 4, then $b = \alpha_2$ is the fifth power of an element in $\mathbb{F}_{2^n}$; otherwise, b can be any nonzero element),
  - $4d_2 = (2^m - 1) + 4$ (with the condition that m is odd),
  - $6d_2 = (2^m - 1) + 6$ (with the condition that m is even).

  As observed in [14], these functions have respectively algebraic degrees m, 3 and $\frac{m}{2} + 1$.
- The second class in [14] has been generalized by Leander and Kholosha [20] into the functions: $Tr_1^n\big(\alpha t^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} t^{s_i}\big)$, $r > 1$ such that $gcd(r, m) = 1$, $\alpha \in \mathbb{F}_{2^n}$ such that $\alpha + \alpha^{2^m} = 1$, $s_i = (2^m - 1)\frac{i}{2^r} \mod (2^m + 1) + 1$, $i \in \{1, \cdots, 2^{r-1} - 1\}$.

4. On Dobbertin-et-al's Niho bent functions

Recall that, for any positive integer k, and r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$, denoted by Tr_r^k, is the mapping defined as: $\forall x \in \mathbb{F}_{2^k}, \quad Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}}$. The trace function Tr_r^k satisfies the transitivity property, that is, $Tr_1^k = Tr_1^r \circ Tr_r^k$.

It was left open in [14] to determine if the duals of the functions introduced there are also Niho bent (possibly up to affine equivalence). In the next proposition, we study how the mapping G related to the functions in the second class satisfies Conditions (4) and (5). We subsequently study the duals of these functions and give an answer to this question.

Proposition 5. *Let f be defined as*

$$\forall t \in \mathbb{F}_{2^n}, \quad f(t) = Tr_1^m(at^{2^m+1}) + Tr_1^n(bt^{(2^m-1)\frac{1}{4}+1}) \tag{6}$$

with m odd, $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_{2^n}^\star$ such that $b^{2^m+1} = a$. There exists v in $\mathbb{F}_{2^n}^\star$ such that $b^4 = a^2 v^{2^m-1}$. Let u be an element of $\mathbb{F}_{2^n}$ such that (u, v) is a basis of $\mathbb{F}_{2^n}$ as two-dimensional vector space over $\mathbb{F}_{2^m}$. The restriction of f to $v\mathbb{F}_{2^m}$ equals $Tr_1^m(\mu y)$ with $\mu = a^{1/2}v^{(2^m+1)/2} + Tr_m^n(bv^{(2^m-1)\frac{1}{4}+1})$. The mapping G such that $G(z) = H(z) + \mu z$ and

$$f(ux + vy) = \begin{cases} Tr_1^m\left(xH\left(\frac{y}{x}\right)\right) \text{ if } x \neq 0 \\ Tr_1^m(\mu y) \text{ if } x = 0 \end{cases}$$

can be characterised by $G^4(z) = a^2u^{2(2^m+1)} + Tr_m^n(b^4u^{2^m+3}) + Tr_m^n(v^{2^m}u)Tr_m^n(b^4u^2)z$ and satisfies Conditions (4) and (5).

Proof. There exists $v \in \mathbb{F}_{2^n}$ such that $b^4 = a^2v^{2^m-1}$ since $\left(\frac{b^4}{a^2}\right)^{2^m+1} = \frac{b^{4(2^m+1)}}{a^4} = 1$. Every element t of $\mathbb{F}_{2^n}$ can be uniquely written as $ux + vy$ with $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Note that $Tr_m^n(v^{2^m}t) = Tr_m^n(v^{2^m}ux) + Tr_m^n(v^{2^m+1}y) = Tr_m^n(v^{2^m}u)x$ since $v^{2^m+1} \in \mathbb{F}_{2^m}$ and thus $Tr_m^n(v^{2^m+1}y) = v^{2^m+1}yTr_m^n(1) = 0$. This implies that $Tr_m^n(v^{2^m}u) \neq 0$ (otherwise $Tr_m^n(v^{2^m}t) = 0$ for every $t \in \mathbb{F}_{2^n}^\star$ which is impossible (for instance take $t = v^{-2^m}\eta \neq 0$ with $Tr_m^n(\eta) = 1$ to get a contradiction)).
Now

$$f(ux+vy) = Tr_1^m(a(ux+vy)^{2^m+1}) + Tr_1^n(b(ux+vy)^{(2^m-1)\frac{1}{4}+1}).$$

For $x=0$:

$$\begin{aligned} f(vy) &= Tr_1^m(a(vy)^{2^m+1}) + Tr_1^n(b(vy)^{(2^m-1)\frac{1}{4}+1}) \\ &= Tr_1^m(av^{2^m+1}y^2) + Tr_1^n(bv^{(2^m-1)\frac{1}{4}+1}y) \\ &= Tr_1^m(\mu y), \text{with } \mu = a^{1/2}v^{(2^m+1)/2} + Tr_m^n(bv^{(2^m-1)\frac{1}{4}+1}) \end{aligned}$$

For $x \neq 0$:

$$\begin{aligned} f(ux+vy) &= Tr_1^m(a(u+vy/x)^{2^m+1}x^2) + Tr_1^n(b(u+vy/x)^{(2^m-1)\frac{1}{4}+1}x) \\ &= Tr_1^m(a^{\frac{1}{2}}(u+vy/x)^{\frac{2^m+1}{2}}x) + Tr_1^m(Tr_m^n(b(u+vy/x)^{(2^m-1)\frac{1}{4}+1})x)) \\ &= Tr_1^m\left(H(y/x)x\right) \end{aligned}$$

with

$$H(z) := a^{1/2}(u+vz)^{(2^m+1)/2} + Tr_m^n(b(u+vz)^{(2^m-1)\frac{1}{4}+1});\ z \in \mathbb{F}_{2^m}.$$

Taking the 4th power and using the fact that $z^{2^m} = z$, we get:

$$\begin{aligned} H^4(z) &= a^2(u^2+v^2z^2)^{(2^m+1)} + Tr_m^n(b^4(u+vz)^{2^m+3}) \\ &= a^2u^{2(2^m+1)} + a^2u^{2^{m+1}}v^2z^2 + a^2u^2v^{2^{m+1}}z^2 + a^2v^{2(2^m+1)}z^4 + Tr_m^n(b^4(u+vz)^{2^m+3}) \end{aligned}$$

Now, the trace function Tr_m^n is linear over $\mathbb{F}_{2^m}$ and,

$$(X+Y)^{2^m+3} = X^{2^m+3} + X^{2^m+2}Y + X^{2^m+1}Y^2 + X^{2^m}Y^3 + X^3Y^{2^m} + X^2Y^{2^m+1} + XY^{2^m+2} + Y^{2^m+3}.$$

Hence,

$$\begin{aligned} Tr_m^n(b^4(u+vz)^{2^m+3}) &= Tr_m^n(b^4u^{2^m+3}) + zTr_m^n(b^4u^{2^m+2}v) + z^2Tr_m^n(b^4u^{2^m+1}v^2) + z^3Tr_m^n(b^4u^{2^m}v^3) \\ &\quad + zTr_m^n(b^4u^3v^{2^m}) + z^2Tr_m^n(b^4u^2v^{2^m+1}) \\ &\quad + z^3Tr_m^n(b^4v^{2^m+2}) + z^4Tr_m^n(b^4v^{2^m+3}). \end{aligned}$$

We thus get that

$$\begin{aligned} H^4(z) + \mu^4z^4 &= H^4(z) + a^2v^{2(2^m+1)}z^4 + Tr_m^n(b^4v^{2^m+3})z^4 \\ &= a^2u^{2(2^m+1)} + a^2u^{2^{m+1}}v^2z^2 + a^2u^2v^{2^{m+1}}z^2 + a^2z^4v^{2(2^m+1)} \\ &\quad + Tr_m^n(b^4u^{2^m+3}) + zTr_m^n(b^4u^{2^m+2}v) + z^2Tr_m^n(b^4u^{2^m+1}v^2) + z^3Tr_m^n(b^4u^{2^m}v^3) \\ &\quad + zTr_m^n(b^4u^3v^{2^m}) + z^2Tr_m^n(b^4u^2v^{2^m+1}) \\ &\quad + z^3Tr_m^n(b^4uv^{2^m+2}) + z^4Tr_m^n(b^4v^{2^m+3}) \\ &\quad + a^2v^{2(2^m+1)}z^4 + Tr_m^n(b^4v^{2^m+3})z^4 \\ &= a^2u^{2(2^m+1)} + z[Tr_m^n(b^4u^{2^m+2}v) + Tr_m^n(b^4u^3v^{2^m})] \\ &\quad + z^2[a^2u^{2^{m+1}}v^2 + a^2u^2v^{2^{m+1}} + Tr_m^n(b^4u^{2^m+1}v^2) + Tr_m^n(b^4u^2v^{2^m+1})] \\ &\quad + z^3[Tr_m^n(b^4u^{2^m}v^3) + Tr_m^n(b^4uv^{2^m+2})] + Tr_m^n(b^4u^{2^m+3}) \end{aligned}$$

We have:

$$\begin{aligned} Tr_m^n(b^4u^{2^m+2}v) + Tr_m^n(b^4u^3v^{2^m}) &= Tr_m^n(b^4u^2(u^{2^m}v + uv^{2^m})) \\ &= Tr_m^n(b^4u^2(Tr_m^n(uv^{2^m}))) \\ &= Tr_m^n(v^{2^m}u)Tr_m^n(b^4u^2); \end{aligned}$$

$$\begin{aligned} a^2u^{2^{m+1}}v^2 + a^2u^2v^{2^{m+1}} + Tr_m^n(b^4u^{2^m+1}v^2) + Tr_m^n(b^4u^2v^{2^m+1}) &= \\ a^2(u^{2^{m+1}}v^2 + u^2v^{2^{m+1}}) + Tr_m^n(b^4(u^{2^m+1}v^2 + u^2v^{2^m+1})) &= \\ a^2(Tr_m^n(u^{2^{m+1}}v^2)) + Tr_m^n(b^4uvTr_m^n(v^{2^m}u)) &= \\ a^2Tr_m^n((v^{2^m}u)^2) + Tr_m^n(v^{2^m}u)Tr_m^n(b^4uv) &= \\ a^2(Tr_m^n(v^{2^m}u))^2 + Tr_m^n(v^{2^m}u)Tr_m^n(b^4uv) &= \\ Tr_m^n(v^{2^m}u)\big(a^2Tr_m^n(v^{2^m}u) + Tr_m^n(b^4uv)\big) &= 0 \end{aligned}$$

since $b^4 = a^2v^{2^m-1}$, and

$$\begin{aligned} Tr_m^n(b^4u^{2^m}v^3) + Tr_m^n(b^4uv^{2^m+2}) &= Tr_m^n(b^4v^2(u^{2^m}v + uv^{2^m})) \\ &= Tr_m^n(v^{2^m}u)Tr_m^n(b^4v^2) = 0 \end{aligned}$$

since $Tr_m^n(b^4v^2) = Tr_m^n(a^2v^{2^m+1}) = 0$ (indeed, $v^{2^m+1} \in \mathbb{F}_{2^m}$).
Then

$$G^4(z) = a^2u^{2(2^m+1)} + Tr_m^n(b^4u^{2^m+3}) + Tr_m^n(v^{2^m}u)Tr_m^n(b^4u^2)z.$$

Note now that $Tr_m^n(b^4u^2) \neq 0$. Indeed, otherwise $b^4u^2 \in \mathbb{F}_{2^m}$ and $b^4v^2 \in \mathbb{F}_{2^m}$ and thus $v/u \in \mathbb{F}_{2^m}$ contradicting the fact that $\{u, v\}$ is a basis.
Therefore, G is a permutation. Moreover, Condition (5) is equivalent to say that, for every $\rho \neq 0$,

$$L(z) = Tr_m^n(b^4u^2)z + \rho z^4$$

is 2-to-1. Note that L is linear : $L(z + z') = L(z) + L(z')$ and that

$$L(z) = 0 \iff z = 0 \text{ or } z = \left(\frac{Tr_m^n(b^4u^2)}{\rho}\right)^{1/3}.$$

We have used the fact that m is odd, the map $x \in \mathbb{F}_{2^m} \mapsto x^3$ is a permutation. Thus, the equation $L(z) = c$ has 0 or 2 solutions.
Therefore, Conditions (4) and (5) are fulfilled, implying that the function f is bent. □

Remark 2. We can see that function f belongs, up to affine equivalence, to the sub-class of $\mathcal{H}$ described in 3.1.1 (with $i = m - 2$). In particular, it belongs to the completed Maiorana-McFarland class (see e.g. [3])

Let us now compute the dual function of f. For that, and to simplify the calculation, we assume from now on that $b^4 \neq a^2$ and that $Tr_m^n(v) = 1$ (such v exists and is unique). Then we can take $u = v^{2^m}$ (indeed, v and v^{2^m} are linearly independent : suppose that there exists $z \in \mathbb{F}_{2^m}^\star$ such that $v^{2^m} = zv$; then $v^{2^m-1} = z$, that is, $(v^{2^m-1})^{2^m-1} = v^{2(1-2^m)} = 1$, a contradiction with $b^4 = a^2v^{2^m-1}$ and $b^4 \neq a^2$). Let us now define $g : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^n}$ as: $\forall (x, y) \in (\mathbb{F}_{2^m})^2, g(x, y) = f(vx + v^{2^m}y)$, where $b^4 = a^2v^{2^m-1}$. According to Proposition 2, we know the support of the

dual $\widetilde{g}$ of g: $\widetilde{g}(\alpha,\beta)=1$ if and only if the equation $H(z)+\beta z+\alpha=0$ has no solution in $\mathbb{F}_{2^m}$. Of course, the Walsh transforms of f and g are closely related:

Lemma 6. $\forall w\in\mathbb{F}_{2^n}$, $\widehat{\chi_f}(w)=\widehat{\chi_g}\big(Tr_m^n(vw),Tr_m^n(v^{2^m}w)\big)$

Proof. Every element w of $\mathbb{F}_{2^n}$ can be uniquely decomposed as $w=v\alpha+v^{2^m}\beta$, with $(\alpha,\beta)\in\mathbb{F}_{2^m}$ since $\{v,v^{2^m}\}$ is a basis of $\mathbb{F}_{2^n}$. Multiplying by v, we have $vw=v^2\alpha+v^{2^m+1}\beta$. Note now that $v^{2^m+1}\beta\in\mathbb{F}_{2^m}$ and that $Tr_m^n(v^2)=Tr_m^n(v)^2=1$. Thus, $Tr_m^n(vw)=\alpha$. Likewise, we can show that $Tr_m^n(v^{2^m}w)=\beta$. Furthermore, for $t=vx+v^{2^m}y$ with $(x,y)\in\mathbb{F}_{2^m}$, one has $Tr_1^n(wt)=Tr_1^m(Tr_m^n(vw)x+Tr_m^n(v^{2^m}w)y)=Tr_1^m(\alpha x+\beta y)$.
The Walsh transform of f is defined as :

$$\widehat{\chi_f}(w)=\sum_{t\in\mathbb{F}_{2^n}}(-1)^{f(t)+Tr_1^n(wt)}$$

Thus,

$$\widehat{\chi_f}(w)=\sum_{(x,y)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}}(-1)^{g(x,y)+Tr_1^m(\alpha x)+Tr_1^m(\beta y)}=\widehat{\chi_g}(\alpha,\beta).$$

□

Hence, according to Lemma 6 and to the observations preceding it, the dual function $\widetilde{f}$ of f satisfies $\widetilde{f}(w)=1$ if and only if the equation $H(z)+Tr_m^n(v^{2^m}w)z+Tr_m^n(vw)=0$ has no solution in $\mathbb{F}_{2^m}$ where, according to Proposition 5, $H(z)=G(z)+\mu z$ is given by:

$$H^4(z) \;=\; a^2u^{2(2^m+1)}+Tr_m^n(b^4u^{2^m+3})+Tr_m^n(v^{2^m}u)Tr_m^n(b^4u^2)z+(a^2v^{2(2^m+1)}+Tr_m^n(b^4v^{2^m+3}))z^4.$$

Let us simplify a little the above expression by noting that, for $u=v^{2^m}$ and $b^4=a^2v^{2^m-1}$:

$$Tr_m^n(b^4u^{2^m+3})=a^2Tr_m^n(v^{2^m-1+1+3\cdot2^m})=a^2Tr_m^n(v^{2^{m+2}})=a^2Tr_m^n(v)^{2^{m+2}}=a^2$$

$$Tr_m^n(v^{2^m}u)=Tr_m^n(v^{2^{m+1}})=Tr_m^n(v)^{2^{m+1}}=1$$

$$Tr_m^n(b^4v^{2^m+3})=a^2Tr_m^n(v^{2(2^m+1)})=a^2v^{2(2^m+1)}Tr_m^n(1)=0$$

Furthermore, note that $Tr_m^n(v)=1=v+v^{2^m}$ and then that $v^{-1}=1+v^{2^m-1}$ that is, $v^{2^m-1}=1+v^{-1}$. Therefore,

$$\begin{aligned}Tr_m^n(b^4u^2)=a^2Tr_m^n(v^{2^m-1}v^{2^{m+1}})&=a^2\big(Tr_m^n(v^{2^{m+1}})+Tr_m^n(v^{2^m}v^{2^m-1})\big)\\&=a^2\big(1+Tr_m^n(v^{2^m-1})+Tr_m^n(v^{2^m})\big)=a^2Tr_m^n(v^{2^m-1})\\&=a^2(Tr_m^n(1+v^{-1}))=a^2Tr_m^n(v^{-1}).\end{aligned}$$

We have also $\mu=a^{1/2}v^{(2^m+1)/2}+Tr_m^n(bv^{(2^m-1)\frac{1}{4}+1})=a^{1/2}(v^{(2^m+1)/2}+Tr_m^n(v^{(2^m+1)/2}))=a^{1/2}v^{(2^m+1)/2}$ (since $v^{(2^m+1)/2}\in\mathbb{F}_{2^m}$ and therefore $Tr_m^n(v^{(2^m+1)/2}))=0$).
We thus obtain that $H^4(z)=a^2(v^{2(2^m+1)}+1)+a^2Tr_m^n(v^{-1})z+a^2v^{2(2^m+1)}z^4$, that is:

$$H^4(z)=a^2\big(v^{2(2^m+1)}+1+Tr_m^n(v^{-1})z+v^{2(2^m+1)}z^4\big).$$

The support of the dual function of f is thus defined as:
$\widetilde{f}(a^{\frac{1}{2}}w)=1$ if and only if the equation $v^{\frac{2^m+1}{2}}+1+Tr_m^n(vw)+Tr_m^n(v^{-\frac{1}{4}})z^{\frac{1}{4}}+(v^{\frac{2^m+1}{2}}+Tr_m^n(v^{2^m}w))z=0$ has no solution in $\mathbb{F}_{2^m}$. Note that $\frac{2^m+1}{2}=(2^m-1)\frac{1}{2}+1$.

Now, we have the following Lemma

Lemma 7. *Let σ, ρ, τ be three elements of $\mathbb{F}_{2^m}$. Assume that $\sigma \neq 0$. Let $N = \{z \in \mathbb{F}_{2^m} \mid \sigma z + \rho z^{\frac{1}{4}} = \tau\}$. Then, $N = \begin{cases} 2 \text{ if } Tr_1^m(\frac{\tau}{\sigma} \cdot \frac{1}{\lambda}) = 0 \text{ where } \lambda = (\frac{\rho^4}{\sigma^4})^{\frac{1}{3}} \\ 0 \text{ otherwise.} \end{cases}$*

Proof. Rewrite the equation $\sigma z+\rho z^{\frac{1}{4}} = \tau$ as $\lambda\big((\frac{z}{\lambda})+\frac{\rho}{\sigma}\frac{1}{\lambda^{\frac{3}{4}}}(\frac{z}{\lambda})^{\frac{1}{4}}\big) = \frac{\tau}{\sigma}$. Choose λ such that $\lambda^{\frac{3}{4}} = \frac{\rho}{\sigma}$ (m being odd, the mapping $\lambda \mapsto \lambda^3$ is a permutation of $\mathbb{F}_{2^m}$ and therfore the mapping $\lambda \mapsto \lambda^{3/4}$ as well).
Then, $N = \{t \in \mathbb{F}_{2^m} \mid t + t^{\frac{1}{4}} = \frac{\tau}{\sigma} \cdot \frac{1}{\lambda}\}$.
The map $t \in \mathbb{F}_{2^m} \mapsto t+t^{\frac{1}{4}}$ is linear; its kernel is equal to $\mathbb{F}_2$ (since $t+t^{\frac{1}{4}} = 0 \iff t = 0$ or $t^{\frac{3}{4}} = 1 \iff t = 0$ or $t = 1$), hence its image E has dimension $m-1$ and equals then $\{\delta \in \mathbb{F}_{2^m} \mid Tr_1^m(\delta) = 0\}$ (indeed, for every element $\delta = t+t^{\frac{1}{4}}$ of E, one has $Tr_1^m(\delta) = Tr_1^m(t)+Tr_1^m(t)^{\frac{1}{4}} = 0$). This implies that N equals 2 if $Tr_1^m(\frac{\tau}{\sigma} \cdot \frac{1}{\lambda}) = 0$ and is null otherwise, proving the result.
□

We deduce:

Theorem 8. *Let $n = 2m$ with m odd and f be defined as*

$$\forall t \in \mathbb{F}_{2^n}, \quad f(t) = Tr_1^m(at^{2^m+1}) + Tr_1^n(bt^{(2^m-1)\frac{1}{4}+1})$$

where $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_{2^n}^\star$ are such that $b^{2^m+1} = a$ and $b^4 \neq a^2$. Let v be such that $Tr_m^n(v) = 1$ and $b^4 = a^2v^{2^m-1}$. Then the dual of f is such that

$$\widetilde{f}(a^{\frac{1}{2}}w) = Tr_1^m\left(\left(v^{\frac{2^m+1}{2}} + 1 + Tr_m^n(vw)\right)\left(\frac{Tr_m^n(v^{2^m}w) + v^{\frac{2^m+1}{2}}}{Tr_m^n(v^{-1})}\right)^{\frac{1}{3}}\right).$$

It has algebraic degree $\frac{m+3}{2}$. Hence, for $m > 3$, $\widetilde{f}$ is affinely inequivalent to the functions introduced in [14].

Proof. Applying Lemma 7 with $\sigma = Tr_m^n(v^{2^m}w) + v^{\frac{2^m+1}{2}}, \rho = Tr_m^n(v^{-\frac{1}{4}})$ and $\tau = v^{\frac{2^m+1}{2}} + 1 + Tr_m^n(vw)$, we deduce that $\widetilde{f}(a^{\frac{1}{2}}w) = 1$ if and only if

$$Tr_1^m\left(\frac{v^{\frac{2^m+1}{2}} + 1 + Tr_m^n(vw)}{Tr_m^n(v^{2^m}w) + v^{\frac{2^m+1}{2}}}\left(\frac{Tr_m^n(v^{2^m}w) + v^{\frac{2^m+1}{2}}}{Tr_m^n(v^{-1/4})}\right)^{\frac{4}{3}}\right) = 1$$

that is

$$\widetilde{f}(a^{\frac{1}{2}}w) = Tr_1^m\left(\left(v^{\frac{2^m+1}{2}} + 1 + Tr_m^n(vw)\right)\left(\frac{Tr_m^n(v^{2^m}w) + v^{\frac{2^m+1}{2}}}{Tr_m^n(v^{-1})}\right)^{\frac{1}{3}}\right).$$

For every element z of $\mathbb{F}_{2^m}$ we have $z^{1/3} = z^{1+4+4^2+4^3+\cdots+4^{\frac{m-1}{2}}}$. Hence, the vectorial function $\left(\frac{Tr_m^n(v^{2^m}w)+v^{\frac{2^m+1}{2}}}{Tr_m^n(v^{-1})}\right)^{\frac{1}{3}}$ has algebraic degree $\frac{m+1}{2}$. Since the functions $v^{\frac{2^m+1}{2}} + 1 + Tr_m^n(vw)$ and $Tr_m^n(v^{2^m}w) + v^{\frac{2^m+1}{2}}$ are affinely independent over $\mathbb{F}_{2^m}$, we deduce that the degree of the dual is $\frac{m+3}{2}$. Since the algebraic degree is affine invariant, and since for $m > 3$, $\frac{m+3}{2}$ is different from 3 and m, this proves that $\widetilde{f}$ is affinely inequivalent to the functions introduced in [14]. □

This gives an answer to the open question evoked in [14]: at least one of the duals of the functions introduced in this paper is affinely inequivalent to them.

Remark 3. Function $\widetilde{f}$ in Theorem 8 is affinely equivalent to the bivariate function $g(x,y) = xy^{1/3}$. The function $y \in \mathbb{F}_{2^m} \mapsto y^{1/3} \in \mathbb{F}_{2^m}$ is a permutation and $\widetilde{f}$ belongs then to the completed Maiorana-McFarland class (but we knew this already thanks to Remark 2, since the dual of a function in the completed Maiorana-McFarland class belongs to this same class (see e.g. [3])).

5. Functions in class $\mathcal{H}$ and o-polynomials

Since the function studied above in Proposition 5 and Thorem 8 belongs to the completed Maiorana-McFarland class and since we do not know whether the other known Niho bent functions are in this same class, we are brought back to the question of knowing whether functions can be exhibited in class $\mathcal{H}$ which are not in the completed Maiorana-McFarland class. We observe now that Condition (5) implies Condition (4) and is equivalent to the fact that G is an o-polynomial.

Definition 2. Let m be any positive integer. A permutation polynomial over $\mathbb{F}_{2^m}$ is called an o-polynomial if, for every $\gamma \in \mathbb{F}_{2^m}$, the function $z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} \text{ if } z \neq 0 \\ 0 \text{ if } z = 0 \end{cases}$ is a permutation of $\mathbb{F}_{2^m}$.

Note that some authors like Dobbertin in [11] add the condition "$G(0) = 0$, $G(1) = 1$" to the definition of o-polynomials; we do not include it since if it is not satisfied by an o-polynomial G, we can replace G by the o-polynomial $\frac{G(z)+G(0)}{G(1)+G(0)}$, which satisfies it.

Lemma 9. *Any function G from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ satisfies Condition (5) if and only if it is an o-polynomial.*

Proof. Recall first that any function from $\mathbb{F}_{2^m}$ to itself can be represented (in a unique way) as a polynomial over $\mathbb{F}_{2^m}$ of degree at most $2^m - 1$. For every $\gamma, \beta \in \mathbb{F}_{2^m}$, the equation $G(z) + \beta z = G(\gamma) + \beta\gamma$ is satisfied by γ. Thus, if Condition (5) is satisfied, then for every $\beta \in \mathbb{F}_{2^m}{}^\star$ and every $\gamma \in \mathbb{F}_{2^m}$, there exists exactly one $z \in \mathbb{F}_{2^m}^\star$ such that $G(z+\gamma) + \beta(z+\gamma) = G(\gamma) + \beta\gamma$, that is, $\frac{G(z+\gamma)+G(\gamma)}{z} = \beta$. Then, for every $\gamma \in \mathbb{F}_{2^m}$, the function $z \in \mathbb{F}_{2^m}^\star \mapsto \frac{G(z+\gamma)+G(\gamma)}{z} \in \mathbb{F}_{2^m}^\star$ is bijective, that is, G and the function $z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} \text{ if } z \neq 0 \\ 0 \text{ if } z = 0 \end{cases}$ are permutations. Hence, G is an o-polynomial. Conversely, if G is an o-polynomial, then for every $\gamma \in \mathbb{F}_{2^m}$, we have $\frac{G(z+\gamma)+G(\gamma)}{z} \neq 0$ for every $z \neq 0$ (note that there is no need to assume that G is a permutation for having this) and for every $\beta \neq 0$ there exists exactly one nonzero z such that $G(z+\gamma) + G(\gamma) = \beta z$. Then for every $c \in \mathbb{F}_{2^m}$, either the equation $G(z) + \beta z = c$ has no solution, or it has at least a solution γ and then exactly one second solution $z + \gamma$ ($z \neq 0$). This completes the proof. □

This property was partially observed by Maschietti [23] (for power functions and $b = 1$) as recalled by Dobbertin in [11]. Note that, according to the proof of Lemma 9, the property that for every $\gamma \in \mathbb{F}_{2^m}$, the function $z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} \text{ if } z \neq 0 \\ 0 \text{ if } z = 0 \end{cases}$ is a permutation of $\mathbb{F}_{2^m}$ implies that G is a permutation of $\mathbb{F}_{2^m}$.

The simplest example of an o-polynomial is the already seen Frobenius automorphism $G(z) = z^{2^i}$ where i is coprime with n. The other known examples are the following:

(1) $G(z) = z^6$ where m is odd;
(2) $G(z) = z^{3\cdot 2^k+4}$, where $m = 2k-1$ [15];
(3) $G(z) = z^{2^k+2^{2k}}$, where $m = 4k-1$ [15];
(4) $G(z) = z^{2^{2k+1}+2^{3k+1}}$, where $m = 4k+1$;
(5) $G(z) = z^{2^k} + z^{2^k+2} + z^{3\cdot 2^k+4}$, where $m = 2k-1$ [8];
(6) $G(z) = z^{\frac{1}{6}} + z^{\frac{3}{6}} + z^{\frac{5}{6}}$ where m is odd;
(7) $G(z) = \frac{\delta^2(z^4+z)+\delta^2(1+\delta+\delta^2)(z^3+z^2)}{z^4+\delta^2z^2+1} + z^{1/2}$, where $Tr_1^m(1/\delta) = 1$ and, if $m \equiv 2 \pmod 4$, then $\delta \notin \mathbb{F}_4$;
(8) $G(z) = \frac{1}{Tr_m^n(b)}\left(Tr_m^n(b^r)(z+1) + Tr_m^n((bz+b^{2^m})^r)(z+Tr_m^n(b)z^{1/2}+1)^{1-r}\right)+z^{1/2}$, where m is even, $r = \pm\frac{2^m-1}{3}$, $b \in \mathbb{F}_{2^{2m}}$, $b^{2^m+1} = 1$ and $b \neq 1$, where $Tr_m^n(x) = x + x^{2^m}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$.

Note that the corresponding functions $G'(z) := zG(z^{2^m-2}) = zG(1/z)$ are affinely independent from Frobenius. This provides potentially new n-variable bent functions:

- $f(x,y) = Tr_1^m(x^{-5}y^6)$, $x,y \in \mathbb{F}_{2^m}$ where m is odd;
- $f(x,y) = Tr_1^m(x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$, $x,y \in \mathbb{F}_{2^m}$, where $m = 2k-1$;
- $f(x,y) = Tr_1^m(x^{1-2^k-2^{2k}}y^{2^k+2^{2k}})$, $x,y \in \mathbb{F}_{2^m}$, where $m = 4k-1$;
- $f(x,y) = Tr_1^m(x^{1-2^{2k+1}-2^{3k+1}}y^{2^{2k+1}+2^{3k+1}})$, $x,y \in \mathbb{F}_{2^m}$, where $m = 4k+1$;
- $f(x,y) = Tr_1^m(x^{1-2^k}y^{2^k} + x^{-(2^k+1)}y^{2^k+2} + x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$, $x,y \in \mathbb{F}_{2^m}$, where $m = 2k-1$;
- $f(x,y) = Tr_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}} + x^{\frac{3}{6}}y^{\frac{3}{6}} + x^{\frac{1}{6}}y^{\frac{5}{6}})$, $x,y \in \mathbb{F}_{2^m}$, where m is odd;
- $f(x,y) = Tr_1^m\left(\left[\frac{\delta^2(x^{-3}+1)+\delta^2(1+\delta+\delta^2)(x^{-2}+x^{-1})}{x^{-4}+\delta^2x^{-2}+1} + x^{1/2}\right]\left[\frac{\delta^2(y^4+y)+\delta^2(1+\delta+\delta^2)(y^3+y^2)}{y^4+\delta^2y^2+1} + y^{1/2}\right]\right)$, $x,y \in \mathbb{F}_{2^m}$, where $Tr_1^m(1/\delta) = 1$ and, if $m \equiv 2 \pmod 4$, then $\delta \notin \mathbb{F}_4$;
- $f(x,y) = Tr_1^m\left(x\,[A(x)]\,[B(y)]\right)$, $x,y \in \mathbb{F}_{2^m}$, where m is even,

$$A(x) = \frac{1}{Tr_m^n(b)}\left(Tr_m^n(b^r)(x^{-1}+1) + Tr_m^n((bx^{-1}+b^{2^m})^r)(x^{-1}+Tr_m^n(b)x^{-1/2}+1)^{1-r}\right) + x^{-1/2}$$

$$B(y) = \frac{1}{Tr_m^n(b)}\left(Tr_m^n(b^r)(y+1) + Tr_m^n((by+b^{2^m})^r)(y+Tr_m^n(b)y^{1/2}+1)^{1-r}\right) + y^{1/2}$$

$r = \pm\frac{2^m-1}{3}$, $b \in \mathbb{F}_{2^{2m}}$, $b^{2^m+1} = 1$ and $b \neq 1$.

Conclusion

We have observed that the bent functions studied under the name of Niho bent functions are the univariate version of a (slightly extended) class of bent functions introduced 35 years ago by John Dillon, but which had not been further investigated because Dillon had not found examples of functions in his class which were not affinely equivalent to already known bent functions. We have replied to an open question raised by Dobbertin et al. on the duals of the three classes of Niho bent functions introduced by these authors, by calculating the dual of one of these three classes. We have found eight new infinite classes of bent functions whose bivariate expressions are explicit, by noticing that the condition for a function to be in this class is equivalent to the fact that a polynomial directly related to its definition is an o-polynomial. We leave open two problems: (1) Extend the calculation of the dual to the generalization of the class given by Leander and Kholosha and calculate the duals of the two other functions introduced by

Dobbertin et al. (2) Determine for each of the eight classes of Niho bent functions that we obtained if it is included in a known class of explicit bent functions such as $\mathcal{M}$ or $\mathcal{PS}_{ap}$.

References

[1] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy. On almost perfect nonlinear functions. *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 4160-4170, 2006.

[2] A. Canteaut, C. Carlet, P. Charpin and C. Fontaine. On cryptographic properties of the cosets of R(1,m), IEEE Transactions on Information Theory, Vol. 47,pp 1494-1513, 2005.

[3] C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pages 257-397, 2010.

[4] C. Carlet and P. Gaborit. Hyperbent functions and cyclic codes. *Journal of Combinatorial Theory*, Series A, Vol 113, no. 3, pages 466-482, 2006.

[5] C. Carlet. Generalized Partial Spreads, *IEEE Transactions on Information Theory*, vol. 41, no. 5, pp. 1482-1487, 1995.

[6] S. Chee and S. Lee and K. Kim. Semi-bent Functions Advances in Cryptology-ASIACRYPT94. Proc. 4th Int. Conf. on the Theory and Applications of Cryptology, Wollongong, Australia, 1994, Pieprzyk, J. and Safavi-Naini, R., Eds., Lect. Notes Comp. Sci. Vol. 917, pp 107-118, 1994.

[7] J. H. Cheon and S. Chee. Elliptic curves and resilient functions Lecture Notes in Computer Science, Vol. 2015 pp 386–397, 2000.

[8] W. Cherowitzo. α-flocks and hyperovals. *Geometriae Dedicata* 72, pp. 221-246, 1998.

[9] J. F. Dillon. *Elementary Hadamard Difference sets*. Ph. D. Thesis, Univ. of Maryland, 1974.

[10] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. *Proceedings of Fast Software Encryption, Second International Workshop*, Lecture Notes in Computer Science 1008, pp. 61-74, 1995.

[11] H. Dobbertin. Uniformly representable permutation polynomials. *Proceedings of Sequences and their Applications, SETA 01, Discrete Mathematics and Theoretical Computer Science*, Springer, pp. 1-22, 2002.

[12] H. Dobbertin and G. Leander. A survey of some recent results on bent functions Proceedings of SETA'04 SEquences ans Their Applications Lecture Notes in computer Science 3486, pp 1-29, 2005.

[13] H. Dobbertin, and G. Leander. Cryptographers Toolkit for Construction of 8-Bit Bent Functions Cryptology ePrint Archive, Report no. 2005/089. Available at http://eprint.iacr.org/2005/089 2005.

[14] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke and P. Gaborit. Construction of Bent Functions via Niho Power Functions. *Journal of Combinatorial Theory, Series A*, Volume 113, Issue 5, pp. 779-798, 2006.

[15] D. Glynn. Two new sequences of ovals in finite Desarguesian planes of even order. *Lecture Notes in Mathematics* 1036, pp. 217-229, 1983.

[16] G. Gong and K. Khoo. Additive autocorrelation of resilient boolean functions, Lecture Notes in Computer Science, Vol. 3006, pp. 275-290, 2004.

[17] Y. Laigle-Chapuy. Polynômes de permutation et applications en cryptographie. PhD Thesis, 2009.

[18] P. Langevin, G. Leander, P. Rabizzoni, P. Veron and J.-P. Zanotti. Web page http://langevin.univ-tln.fr/project/quartics/

[19] P. Langevin, P. Rabizzoni, P. Veron, J.-P. Zanotti. On the number of bent functions with 8 variables. *Proceedings of the conference BFCA 2006*, Publications des universités de Rouen et du Havre, pp. 125-136, 2007.

[20] G. Leander and A. Kholosha. Bent functions with 2^r Niho exponents. *IEEE Trans. Inform. Theory 52 (12)*, pp 5529–5532, 2006

[21] O.A Logachev, A. Salnikov, and V. Yashchenko. Boolean Functions in Coding Theory and Cryptology, Moscow: Mos. Tsentr Nepreryvnogo Mat. Obrazovaniya (MCCME), (2004).

[22] F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*, Amsterdam, North Holland. 1977.

[23] A. Maschietti. Difference sets and hyperovals. *Designs, Codes and Cryptography* 14, pp. 89-98, 1998.

[24] J. L. Massey. Shift-register analysis and BCH decoding. *IEEE Transactions on Information Theory*, vol. 15, pp. 122-127, 1969.

[25] Y. Niho. Multivalued cross-correlation functions between two maximal linear recursive sequences, PhD thesis, Univ. of Southern California, 1972.

[26] M.G. Parker and A. Pott. On Boolean Functions Which Are Bent and Negabent, Int. Work- shop on Sequences, Subsequences, and Consequences (SSC 2007), Los Angeles, USA, 2007. Revised Invited Papers, Golomb, S.W., Gong, G., Helleseth, T., and Song, H.-Y., Eds., Lect. Notes Comp. Sci. 4893 (2007), 9-23.

[27] C. Qu, J. Seberry, and J. Pieprzyk. Homogeneous Bent Functions, Discrete Appl. Math. 102 no. 1-2 , 133-139, 2000.

[28] S. Rønjom and T. Helleseth. A new attack on the filter generator. *IEEE Transactions on Information theory*, vol. 53, no. 5, pp. 1752-1758, 2007.

[29] O.S. Rothaus. On "bent" functions, J. Combin.Theory Ser A 20, pp. 300-305, 1976.

[30] A. M. Youssef and G. Gong. Hyper-Bent Functions, Advances in Crypology Eurocrypt'01, LNCS, Springer, pp. 406-419, 2001.

[31] Y. Zheng and X. M. Zhang. Relationships between bent functions and complementary plateaued functions, Lecture Notes in Computer Science, Vol. 1787, pp. 60-75, 1999.