On Dillon's class H of Niho bent functions and o-polynomials

Claude Carlet and Sihem Mesnager
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@univ-paris8.fr, smesnager@univ-paris8.fr

This extended abstract is a reduced version of the paper (Carlet and Mesnager 2011). We refer to this paper for the proofs and for complements.

Bent functions (Dillon 1974; Rothaus 1976) 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 $\ell(x_1,\ldots,x_n)=a_0+a_1x_1+\cdots+a_nx_n=a_0+a\cdot x$, where $x=(x_1,\ldots,x_n)\in\mathbb{F}_2^n$, $a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n$ and $a_0\in\mathbb{F}_2$. The Hamming distance $d_H(f,\ell)=\#\{x\in\mathbb{F}_2^n\mid f(x)\neq\ell(x)\}$ between them is then small. A Boolean function resists attacks by affine approximation if 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 in (Carlet 2010) a 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 (Dillon 1974; Rothaus 1976), 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 $\pm2^m$ only (this characterization is independent of the choice of the inner product in $\mathbb{F}_2^n$. 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)

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

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 (Massey 1969; Ronjom and Helleseth 2007)) 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 (Dobbertin 1995).

Bent functions are often better viewed in their bivariate representation and can also be viewed in their univariate representation: 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 $\sum_{i=0}^{2^n-1}a_ix^i$ 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. Moreover, f being Boolean, its univariate representation can be written in the form $f(x)=\sum_{j\in\Gamma_n}Tr_1^{o(j)}(a_jx^j)$, 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 $\sum_{0 \leq i,j \leq 2^m-1} a_{i,j} x^i y^j$ 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 $\mathbb{F}_{2^m}$.

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 (Carlet 2010). The corresponding notion of equivalence between functions is called *affine equivalence*. Also, if f is bent and ℓ is affine, then $f+\ell$ is bent. 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. The corresponding notion of equivalence is called *extended affine equivalence*, in brief, *EA-equivalence*.

Bent functions are all known for $n \leq 8$, only (their determination for 8 variables (Langevin et al. ; 2007) 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.

The two main known classes of explicit bent functions

We recall that $n = 2m$. Several classes of bent functions have been introduced in (Dillon 1974; Rothaus 1976). 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 representation, univariate or bivariate). The two main ones of this last kind are the following:

1. The *Maiorana-McFarland class* $\mathcal{M}$ is the set of all the n-variable Boolean functions of the form:

$$f(x,y) = x \cdot \pi(y) + g(y);\ x, y \in \mathbb{F}_2^m \qquad (2)$$

where "$\cdot$" denotes an inner product in $\mathbb{F}_2^m$, π is any permutation on $\mathbb{F}_2^m$ and g is any Boolean function on $\mathbb{F}_2^m$. Any such function is bent (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 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 recall now the definition of the $\mathcal{PS}_{ap}$ *class*. We first define the more general *Partial Spreads class* $\mathcal{PS}$: it equals the union of $\mathcal{PS}^-$ and $\mathcal{PS}^+$, where $\mathcal{PS}^-$ (respectively, $\mathcal{PS}^+$) is the set of all the sums (modulo 2) of the indicators of 2^{m-1} (respectively, $2^{m-1}+1$) pairwise supplementary m-dimensional subspaces of $\mathbb{F}_2^n$. All the elements of $\mathcal{PS}^-$ have algebraic degree m exactly, but not all those of $\mathcal{PS}^+$ (for instance, if m is even, then all quadratic functions are in $\mathcal{PS}^+$). J. Dillon exhibits in (Dillon 1974) a subclass of $\mathcal{PS}^-$, denoted by $\mathcal{PS}_{ap}$, whose elements can be defined explicitly: $\mathbb{F}_2^m$ is identified to the Galois field $\mathbb{F}_{2^m}$; an inner product in this field can be 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 the convention $\frac{1}{0}=0$, 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 $g(\frac{y}{x})$. See more in (Carlet 2010).

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

Classes H and $\mathcal{H}$ in bivariate form

In his thesis (Dillon 1974), Dillon introduces a third family of bent functions whose expression is given but whose bentness is achieved under some non-obvious condition. 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 $\mathcal{P}S$ 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 f 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:

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

where $\mu \in \mathbb{F}_{2^m}$ and ψ 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 ψ and μ such that g is bent.

Proposition 1. *(Carlet and Mesnager 2011) Let g be a Boolean function over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ defined by* (3)*. Then g is bent if and only if, denoting $G(z) = \psi(z) + \mu z$, we have:*

$$G \text{ is a permutation on } \mathbb{F}_{2^m}; \quad (4)$$

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

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 the 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 $G(0) = 0$.

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 class; indeed, denoting $j = m-i$, we have then $g(x,y) = Tr_1^m(x\,(yx^{2^m-2})^{2^i}) = Tr_1^m(x^{2^j}yx^{2^m-2}) = Tr_1^m(yx^{2^j-1})$.

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

1. 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 $G(z')+\frac{1}{\beta}z' = \frac{\alpha}{\beta}$.
2. the function $z \mapsto G'(z) := (L^{-1} \circ G \circ L)(z)$ where $L(z) = z^{2^j}$ is a field automorphism of $\mathbb{F}_{2^m}$, that is $G'(z) = (G(z^{2^j}))^{2^{m-j}}$, satisfies Conditions (4) and (5).
3. the function $z \mapsto G'(z) := \lambda G(z) + \lambda'$ with $\lambda \neq 0$ satisfies Conditions (4) and (5).
4. the function $z \mapsto G'(z) := G(\lambda z + \lambda')$ with $\lambda \neq 0$ satisfies Conditions (4) and (5).
5. the function $z \mapsto G'(z) := zG(z^{2^m-2})$ if $G(0) = 0$ and more generally the function $z \mapsto G'(z) := zG(z^{2^m-2}) + zG(0)$ for any value of $G(0)$ satisfies Conditions (4) and (5). Indeed (restricting ourself without loss of generality to the case $G(0) = 0$ - by replacing G by $G + G(0)$ - and 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.

Contrarily to the others, transformation (1) does not produce EA-equivalent functions, in general. We shall say that two functions G are *o-equivalent* (the reason why we choose such term will come below) if one can be obtained from the other by a sequence of the transformations $G \mapsto G'$ above. This gives a notion of equivalence of functions in class $\mathcal{H}$ which is not a sub-equivalence of the EA-equivalence of bent functions and is not a super-equivalence either.

The general $\mathbb{F}_{2^m}$-linear equivalence between the corresponding bent functions (when one equals the other composed on the right by an $\mathbb{F}_{2^m}$-linear automorphism over $\mathbb{F}_{2^n}$) is included in this notion of o-equivalence.

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 (u, v) 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:

$$t = xu + yv.$$

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 $\omega\mathbb{F}_{2^m}^\star$ where ω 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 $\omega\mathbb{F}_{2^m}^\star$ where $\omega \in \mathbb{F}_{2^n}^\star$. The necessary and sufficient condition for a bent function to belong to class $\mathcal{H}$ is then that its restriction to each vectorspace $\omega\mathbb{F}_{2^m}$, $\omega \in \mathbb{F}_{2^n}^\star$, is linear.

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

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

Bent functions whose restrictions to the vectorspaces $\omega\mathbb{F}_{2^m}$ are all linear have already been investigated in (Dobbertin et al. 2006) and (Leander and Kholosha 2006). Since the exponents congruent with powers of 2 modulo $2^m - 1$ are called Niho exponents, we shall call these functions *Niho bent functions*.

Five examples of infinite classes of Niho bent functions are known up to affine 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 (Dobbertin et al. 2006). 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).
- The second class in (Dobbertin et al. 2006) has been extended by Leander and Kholosha (Leander and Kholosha 2006) into the functions: $Tr_1^n\left(\alpha t^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} t^{s_i}\right)$, $r > 1$ such that $gcd(r, m) = 1$, $\alpha \in \mathbb{F}_{2^n}$ such that $\alpha + \alpha^{2^m} = 1$, $s_i = (2^m - 1)\frac{i}{2^r} + 1 \pmod{2^m + 1}$, $i \in \{1, \ldots, 2^{r-1} - 1\}$.

On an open question about Dobbertin-et-al's Niho bent functions

Recall that, for any positive integers 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: $Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}}, \forall x \in \mathbb{F}_{2^k}$. 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 (Dobbertin et al. 2006) to determine if the duals of the functions introduced there are affinely equivalent to these Niho bent functions.

Theorem 3. *(Carlet and Mesnager 2011) 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 $b^4 = a^2 v^{2^m-1}$. Then the dual of f is such that $\widetilde{f}(a^{\frac{1}{2}}w) = Tr_1^m\big(\big(v^{\frac{2^m+1}{2}} + 1 + Tr_m^n(v^{2^m}w)\big)\big(\frac{Tr_m^n(vw)+v^{\frac{2^m+1}{2}}}{Tr_m^n(v^{-1})}\big)^{\frac{1}{3}}\big)$. It has algebraic degree $\frac{m+3}{2}$. Hence, for $m > 3$, $\widetilde{f}$ is EA-inequivalent to the functions introduced in (Dobbertin et al. 2006).

The paper (Carlet, Helleseth, Kholosha and Mesnager) extends the calculation of the dual to the generalization of the class given by Leander and Kholosha.

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

Since the function studied above in Theorem 3 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 G over $\mathbb{F}_{2^m}$ is called an o-polynomial (an oval 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 $\mathbb{F}_{2^m}$.

Lemma 4. *(Carlet and Mesnager 2011) 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.*

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

1. $G(z) = z^6$ where m is odd (Segre 1962);
2. $G(z) = z^{3\cdot 2^k+4}$, where $m = 2k-1$ (Glynn 1983);
3. $G(z) = z^{2^k+2^{2k}}$, where $m = 4k-1$ (Glynn 1983);
4. $G(z) = z^{2^{2k+1}+2^{3k+1}}$, where $m = 4k+1$ (Glynn 1983);
5. $G(z) = z^{2^k} + z^{2^k+2} + z^{3\cdot 2^k+4}$, where $m = 2k-1$ (Cherowitzo 1998);
6. $G(z) = z^{\frac{1}{6}} + z^{\frac{1}{2}} + z^{\frac{5}{6}}$ where m is odd (Payne 1985); note that $G(z) = D_5\left(z^{\frac{1}{6}}\right)$, where D_5 is the Dickson polynomial of index 5 (R. Lidl and Turnwald 1993);
7. $G(z) = \frac{\delta^2(z^4+z)+\delta^2(1+\delta+\delta^2)(z^3+z^2)}{z^4+\delta^2 z^2+1} + z^{1/2}$, where $Tr_1^m(1/\delta) = 1$ and, if $m \equiv 2 \pmod 4$, then $\delta \notin \mathbb{F}_4$ (Cherowitzo et al. 1996);
8. $G(z) = \frac{1}{Tr_m^n(v)}\left[Tr_m^n(v^r)(z+1) + Tr_m^n\left[(vz + v^{2^m})^r\right]\left(z + Tr_m^n(v)z^{1/2} + 1\right)^{1-r}\right] + z^{1/2}$, where m is even, $r = \pm\frac{2^m-1}{3}$, $v \in \mathbb{F}_{2^{2m}}$, $v^{2^m+1} = 1$ and $v \neq 1$ (W.E. Cherowitzo and Penttila 2003).

We indicate now the bent functions we can obtain with the 6 first o-polynomials (we do not do the same for the two last o-polynomials since the situation with them needs to be clarified and since the expression of these bent functions would be complex - they are probably simpler in univariate form):

1. for m odd and $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = Tr_1^m(x^{-5}y^6)$;
   - $f(x,y) = Tr_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}})$.
2. for $m = 2k-1$ and $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = Tr_1^m(x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$;
   - $f(x,y) = Tr_1^m(x^{-3\cdot(2^{k-1}-1)}y^{3\cdot 2^{k-1}-2})$ (since the inverse of $3\cdot 2^k + 4$ [mod 2^m-1] equals $3\cdot 2^{k-1} - 2$; indeed, $(3\cdot 2^k+4)(3\cdot 2^{k-1}-2) = 9 - 8 = 1$ [mod 2^m-1]).
3. for $m = 4k-1$ and $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = Tr_1^m(x^{1-2^k-2^{2k}}y^{2^k+2^{2k}})$;
   - $f(x,y) = Tr_1^m(x^{2^{3k-1}-2^{2k}+2^k}y^{1-2^{3k-1}+2^{2k}-2^k})$ (since the inverse of $2^k + 2^{2k}$ [mod 2^m-1] equals $1 - 2^{3k-1} + 2^{2k} - 2^k$; indeed, $(2^k+2^{2k})(1-2^{3k-1}+2^{2k}-2^k) = 2^{m+1}-1$).
4. for $m = 4k+1$ and $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = Tr_1^m(x^{1-2^{2k+1}-2^{3k+1}}y^{2^{2k+1}+2^{3k+1}})$;
   - $f(x,y) = Tr_1^m(x^{2^{3k+1}-2^{2k+1}+2^k}y^{1-2^{3k+1}+2^{2k+1}-2^k})$ (since the inverse of $2^{2k+1}+2^{3k+1}$ [mod 2^m-1] equals $2^m - 2^{3k+1} + 2^{2k+1} - 2^k$).
5. for $m = 2k-1$ and $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = Tr_1^m(x^{1-2^k}y^{2^k} + x^{-(2^k+1)}y^{2^k+2} + x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$;
   - $f(x,y) = Tr_1^m\big(y\big(y^{2^k+1}x^{-(2^k+1)} + y^3x^{-3} + yx^{-1}\big)^{2^{k-1}-1}\big)$, since we have $G^{-1}(z) = z\big(z^{2^k+1} + z^3 + z\big)^{2^{k-1}-1}$ (see Lemma 5 below).
6. for m odd and $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = Tr_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}} + x^{\frac{1}{2}}y^{\frac{1}{2}} + x^{\frac{1}{6}}y^{\frac{5}{6}})$;
   - $f(x,y) = Tr_1^m\big(x\big[D_{\frac{1}{5}}\big(\frac{y}{x}\big)\big]^6\big)$ where $D_{\frac{1}{5}}$ is the Dickson polynomial of index $\frac{1}{5}$, the inverse of 5 modulo $2^{2m}-1$ (see (R. Lidl and Turnwald 1993) or Remark 2 below); note that $\frac{1}{5} = 2^{2m} - 2^{2m-1} + 2^{2m-3} - 2^{2m-5} + ... + 2^7 - 2^5 + 2^3 - 2$ [mod $2^{2m}-1$].

Lemma 5. *Let k be any positive integer and $m = 2k-1$. The inverse of function $z \in \mathbb{F}_{2^m} \mapsto z^{2^k} + 2^{2^k+2} + z^{3\cdot 2^k+4} \in \mathbb{F}_{2^m}$ equals: $z\big(z^{2^k+1} + z^3 + z\big)^{2^{k-1}-1}$.*

Remark 1. Another way for eliminating z' between the two equations $z^{2^k} + 2^{2^k+2} + z^{3\cdot 2^k+4} = t$ and $z + z'z + z'^2z^3 = t'$ is to use the resultant of the two polynomials in z' equal to $z' + z^2z' + z^4z'^3 + t$ et $z + z'z + z'^2z^3 + t'$ where z is considered as a parameter. But this leads to a more complex equation $z^3tt' + z^2t(t+1)t' + z(tt' + (t+1)^2(t'+1)) + (t+1)t'^2 = 0$.

Remark 2. Let us recall why the inverse of D_α equals D_β with $\beta\alpha \equiv 1 \pmod{2^n-1}$ for every α coprime with 2^n-1. Recall that $D_\alpha(D_\beta(y + \frac{1}{y})) = y^{\alpha\beta} + (\frac{1}{y})^{\alpha\beta}$ for every $y \in \mathbb{F}_{2^n}^\star$. Since every element $x \in \mathbb{F}_{2^m}^\star$ can be written as $x = c + \frac{1}{c}$ with $c \in \mathbb{F}_{2^n}$, we have $D_\alpha(D_\beta(x)) = D_\alpha(D_\beta(c + \frac{1}{c})) = c^{\alpha\beta} + (\frac{1}{c})^{\alpha\beta} = c + \frac{1}{c} = x$, proving that $D_\beta = D_\alpha^{-1}$ (note that $D_\alpha(0) = D_\beta(0) = 0$).

References

Carlet, C., Helleseth, T., Kholosha, A. and Mesnager, S. On the duals of bent functions with 2^r niho exponents. IEEE International Symposium on Information Theory, ISIT 2011.

Carlet, C., and Mesnager, S. 2011. On Dillon's class H of bent functions, Niho bent functions and o-polynomials. *Journal of Combinatorial Theory Series A* 118:2392–2410.

Carlet, C. 2010. 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, pp. 257–397. Preliminary version available at http://www-roc.inria.fr/secret/Claude.Carlet/chap-fcts-Bool-corr.pdf.

Cherowitzo, W.; Penttila, T.; Pinneri, I.; and Royle, G. F. 1996. Flocks and ovals. *Geometriae Dedicata* 60(1):17–37.

Cherowitzo, W. 1998. α-flocks and hyperovals. *Geometriae Dedicata* 72:221–246.

Dillon, J. F. 1974. *Elementary Hadamard Difference sets*. Ph.D. Dissertation, Univ. of Maryland.

Dobbertin, H.; Leander, G.; Canteaut, A.; C. Carlet, P. F.; and Gaborit, P. 2006. Construction of bent functions via niho power functions. *Journal of Combinatorial Theory, Series A* 113:779–798.

Dobbertin, H. 1995. Construction of bent functions and balanced boolean functions with high nonlinearity. In *Proceedings of Fast Software Encryption, Second International Workshop*, volume 1008 of *Lecture Notes in Computer Science*, 61–74.

Glynn, D. 1983. Two new sequences of ovals in finite desarguesian planes of even order. *Lecture Notes in Mathematics* 1036:217–229.

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

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

Leander, G., and Kholosha, A. 2006. Bent functions with 2^r niho exponents. *IEEE Trans. Inform. Theory* 52(12):5529–5532.

Massey, J. L. 1969. Shift-register analysis and bch decoding. *IEEE Transactions on Information Theory* 15:122–127.

Payne, S. E. 1985. A new infinite family of generalized quadrangles. *Congr. Numer.* 49:115–128.

Lidl, R., Mullen, G. L., and Turnwald, G. 1993. *Dickson Polynomials*. Longman Scientic & Technical, Harlow, Essex, UK.

Ronjom, S., and Helleseth, T. 2007. A new attack on the filter generator. *IEEE Transactions on Information theory* 53(5):1752–1758.

Rothaus, O. 1976. On "bent" functions. *J. Combin.Theory Ser* 20:300–305.

Segre, B. 1962. Ovali e curve σ nei piani di galois di caratteristica due. *Atti dell' Accad. Naz. Lincei Rend* 32(8):785–790.

Cherowitzo, W.E., O'Keefe, C.M. and Penttila, T. 2003. A unified construction of finite geometries associated with q-clans in characteristic two. *Advances in Geometry* 3:1–21.