More $\mathcal{PS}$ and $\mathcal{H}$-like bent functions

Claude Carlet*

Abstract

Two constructions/classes of bent functions are derived from the notion of spread. The first class, $\mathcal{PS}$, gives a useful framework for designing bent functions which are constant (except maybe at 0) on the elements of a (partial) spread. Dillon has deduced the explicit class $\mathcal{PS}_{ap}$ of bent functions obtained from the spread of all multiplicative cosets of $\mathbb{F}_{2^m}^*$ (added with 0) in $\mathbb{F}_{2^{2m}}^*$ (that we shall call the Dillon spread). The second class, H, later slightly modified into a class called $\mathcal{H}$ so as to relate it to the so-called Niho bent functions, is up to addition of affine functions the set of bent functions whose restrictions to the spaces of the Dillon spread are linear. It has been observed that the functions in $\mathcal{H}$ are related to o-polynomials, and this has led to several explicit classes of bent functions. In this paper we first apply the $\mathcal{PS}$ construction to a larger class of spreads, well-known in the finite geometry domain and that we shall call André's spreads, and we describe explicitly the $\mathcal{PS}$ corresponding bent functions and their duals. We also characterize those bent functions whose restrictions to the spaces of an André spread are linear. This leads to a notion extending that of o-polynomial. Finally, we obtain similar characterizations for the $\mathcal{H}$-like functions derived from the spreads used by Wu to deduce $\mathcal{PS}$ bent functions from the Dempwolff-Müller pre-quasifield, the Knuth pre-semifield and the Kantor pre-semifield. In each case, this also leads to a new notion on polynomials.

1 Introduction

Bent functions [4, 9] are the indicators of difference sets in elementary Abelian 2-groups. They play roles in cryptography, coding theory, designs and sequences. Bent functions are those functions f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ whose derivatives $f(x) + f(x + a)$, $a \neq 0$, are balanced. Equivalently, their Hamming distance to the set of affine functions (i.e. their *nonlinearity*) takes the maximal possible value $2^{n-1} - 2^{n/2-1}$, and equivalently again, their Walsh transform $W_f(a) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}$ (where "$\cdot$" denotes an inner product in $\mathbb{F}_2^n$), takes values $\pm 2^m$ only (this characterization is independent of the choice of the inner product in $\mathbb{F}_2^n$). They exist for every n even. We shall denote $n = 2m$ in the

*C. Carlet is with the LAGA, Universities of Paris 8 and Paris 13; CNRS, UMR 7539; Address: University of Paris 8, Department of Mathematics, 2 rue de la liberté, 93526 Saint-Denis cedex 02, France. Email: claude.carlet@univ-paris8.fr.

sequel.
If f is bent, then the *dual function* $\widetilde{f}$ of f, defined on $\mathbb{F}_2^n$ by:

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

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)

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

(whose global degree $\max\{|I|,\, a_I \neq 0\}$, called the algebraic degree of f, is then at most m, as proved in [9]), but are often better viewed either in univariate or in bivariate representations: 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, and f being Boolean, $f(x)$ can be written under the (non-unique) form $Tr_1^n(P(x))$ where $P(x)$ is a polynomial over $\mathbb{F}_{2^n}$. A unique form exists that we shall not use in this paper. We also 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 $\max_{(i,j) \mid a_{i,j} \neq 0}(w_2(i) + w_2(j))$. 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 $\mathbb{F}_{2^m}$, and tr_1^m is the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$.
The set of bent functions is invariant under composition on the right by any affine automorphism. 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*.

Determining all bent functions (or more practically, classifying them under the action of the general affine group) being out of reach, several constructions of explicit bent functions have been investigated, which lead to infinite classes. Class $\mathcal{H}$ (a slight modification of the original class H of Dillon) is the set of bent functions whose restrictions to the multiplicative cosets of $\mathbb{F}_{2^m}^\star$ (added with $\{0\}$) are linear. In univariate form, the functions of this class are often

called Niho bent. The general *Partial Spreads class* $\mathcal{PS}$ 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 $\mathcal{PS}^+$. J. Dillon exhibits in [4] a subclass of $\mathcal{PS}^-$, denoted by $\mathcal{PS}_{ap}$, whose elements can be defined explicitly. The elements of $\mathcal{PS}_{ap}$ are the functions of the form $f(x,y) = g\left(x\,y^{2^m-2}\right)$, where $x,y \in \mathbb{F}_{2^m}$, *i.e.* $f(x,y) = g\left(\frac{x}{y}\right)$ 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 [1].
Applying the $\mathcal{PS}$ construction to the larger class of spreads introduced by André gives $\mathcal{PS}_{ap}$-like bent functions in an explicit form. We give the expression of their duals as well. We then characterize those bent functions whose restrictions to the spaces of an André spread are linear. This leads to a notion on polynomials which includes the notion of o-polynomial as a particular case. Finally, we obtain similarly characterizations for the functions linear over each element of one of the three spreads related to the Dempwolff-Müller pre-quasifield, the Knuth pre-semifield and the Kantor pre-semifield. In each case, this also leads to a new notion on polynomials.

2 More spreads of $\mathbb{F}_{2^m}^2 \sim \mathbb{F}_{2^n}$: André's spreads

Partial spreads are sets of (at least) 2^{m-1} supplementary m-dimensional vector subspaces of $\mathbb{F}_{2^n}$. Two partial sets are well known in the Boolean functions community and have been used to build bent functions:

1. The Dillon spread, constituted of the 2^m+1 multiplicative cosets of $\mathbb{F}_{2^m}^*$ in $\mathbb{F}_{2^n}^*$ (to each of which is of course adjoined 0); these 2^m+1 pairwise supplementary vectorspaces completely cover $\mathbb{F}_{2^n}$; their set is then a *full spread*; the corresponding $\mathcal{PS}^-$ and $\mathcal{PS}^+$ functions obtained by choosing 2^{m-1} (resp. $2^{m-1}+1$) of these spaces constitute the so-called $\mathcal{PS}_{ap}$ class ("ap" for "affine plane"); all of them have algebraic degree m. The elements of this spread can be viewed in bivariate form. The spaces are then:
$$\{(0,y),\, y \in \mathbb{F}_{2^m}\} \text{ and } \{(x,xz), x \in \mathbb{F}_{2^m}\}, z \in \mathbb{F}_{2^m}.$$
2. For m even, a set of $2^{m-1}+1$ pairwise supplementary m-dimensional $\mathbb{F}_2$-vector subspaces introduced by Dillon [4] (and reported in [1]) whose corresponding $\mathcal{PS}^+$ function is quadratic (hence, up to EA-equivalence, every quadratic function belongs to $\mathcal{PS}^+$ for $n \equiv 0$ [mod 4]).

But other full spreads exist, introduced by J. André in the fifties and independently by Bruck later. Let k be any divisor of m. Let N_k^m be the norm map from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^k}$:

$$N_k^m(x) = x^{\frac{2^m-1}{2^k-1}}.$$

Let ϕ be any function from $\mathbb{F}_{2^k}$ to $\mathbb{Z}/(m/k)\mathbb{Z}$. Then, denoting $\phi \circ N_k^m$ by φ (it can be any function from $\mathbb{F}_{2^m}$ to $\mathbb{Z}/(m/k)\mathbb{Z}$ which is constant on any coset of the subgroup U of order $\frac{2^m-1}{2^k-1}$ of $\mathbb{F}_{2^m}^*$), the $\mathbb{F}_2$-vector spaces:

$$\{(0,y),\ y \in \mathbb{F}_{2^m}\}\ and\ \{(x, x^{2^{k\varphi(z)}} z), x \in \mathbb{F}_{2^m}\},\ \ where\ z \in \mathbb{F}_{2^m}$$

form together a spread of $\mathbb{F}_{2^m}^2$. Indeed, suppose that $x^{2^{k\varphi(y)}} y = x^{2^{k\varphi(z)}} z$ for some nonzero elements x, y, z of $\mathbb{F}_{2^m}$, then we have $N_k^m(x^{2^{k\varphi(y)}} y) = N_k^m(x^{2^{k\varphi(z)}} z)$, that is, $N_k^m(x^{2^{k\varphi(y)}}) N_k^m(y) = N_k^m(x^{2^{k\varphi(z)}}) N_k^m(z)$; equivalently, since $x \mapsto x^{2^{k\varphi(z)}}$ is in the Galois group of $\mathbb{F}_{2^m}^2$ over $\mathbb{F}_{2^k}$, $N_k^m(x) N_k^m(y) = N_k^m(x) N_k^m(z)$ and hence $N_k^m(y) = N_k^m(z)$ and $\varphi(y) = \varphi(z)$, which together with $x^{2^{k\varphi(y)}} y = x^{2^{k\varphi(z)}} z$ implies then $y = z$.

3 The $\mathcal{PS}$ bent functions associated to André's spreads and their duals

Let us give the explicit expression of these functions. A pair $(x, y) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}$ belongs to $\{(x, x^{2^{k\varphi(z)}} z), x \in \mathbb{F}_{2^m}\}$ if and only if

$$y = x^{2^{k\varphi(z)}} z = x^{2^{k\phi\left(\frac{N_k^m(y)}{N_k^m(x)}\right)}} z = x^{2^{k\varphi(y/x)}} z. \tag{2}$$

Then if g is any balanced Boolean function on $\mathbb{F}_{2^m}$ vanishing at 0, the function

$$f(x, y) = g\left(\frac{y}{x^{2^{k\varphi(y/x)}}}\right) \tag{3}$$

(with the usual convention $\frac{y}{0} = 0$) belongs to the $\mathcal{PS}$ class of bent functions and is potentially inequivalent to $\mathcal{PS}_{ap}$ functions. This gives new explicit bent functions in the class $\mathcal{PS}$.

If S is the support of g, then since $0 \notin S$, the support of f is equal to the union $\bigcup_{z \in S} \{(x, x^{2^{k\varphi(z)}} z), x \in \mathbb{F}_{2^m}\}$, less $\{0\}$. The support of the dual of f is the union of the orthogonals of these spaces, less $\{0\}$ as well. The orthogonal of $\{(x, x^{2^{k\varphi(z)}} z), x \in \mathbb{F}_{2^m}\}$ is $\{(x', y') \in \mathbb{F}_{2^m}^2\ ;\ \forall x \in \mathbb{F}_{2^m},\ tr_1^m(xx' + x^{2^{k\varphi(z)}} zy') = 0\} = \{(x', y') \in \mathbb{F}_{2^m}^2\ ;\ \forall x \in \mathbb{F}_{2^m},\ tr_1^m((x' + (zy')^{2^{m-k\varphi(z)}})x) = 0\} = \{(x', y') \in \mathbb{F}_{2^m}^2\ ;\ x' + (zy')^{2^{m-k\varphi(z)}} = 0\} = \{((zy')^{2^{m-k\varphi(z)}}, y');\ y' \in \mathbb{F}_{2^m}^2\}$; hence we have:

$$\widetilde{f}(x, y) = g\left(\frac{x^{2^{k\varphi(x/y)}}}{y}\right). \tag{4}$$

Of course, if g does not vanish at 0, the function defined by (3) is bent as well. We can see this by changing g into its complement $g + 1$ (which changes f and its dual into their complements as well).

Theorem 1 *Let m be any positive integer and k any divisor of m. Let φ be an integer-valued function over $\mathbb{F}_{2^m}$, constant on each multiplicative coset of the subgroup U of order $\frac{2^m-1}{2^k-1}$ of $\mathbb{F}_{2^m}^*$. Let g be any balanced Boolean function over $\mathbb{F}_{2^m}$ and let f be defined by (3) with the convention $\frac{1}{0}=0$. Then f is bent and it dual is given by (4).*

Note that the $\mathcal{PS}_{ap}$ class corresponds to the case where ϕ is the null function. Note that it also corresponds to the case $k=m$ since we have then $f(x,y)=g\left(\frac{y}{x}\right)$, because $x^{2^m}=x$. Note finally that if $k=1$ then $N_k^m(x)=1$ for every $x\neq 0$ and the groups of the spread are $\{(0,y),\, y\in\mathbb{F}_{2^m}\}$ and $\{(x,0), x\in\mathbb{F}_{2^m}\}$ and $\{(x,x^{2^j}z), x\in\mathbb{F}_{2^m}\}, z\in\mathbb{F}_{2^m}^*$ for some j and $f(x,y)=g\left(\frac{y}{x^{2^j}}\right)$; the functions are in the $\mathcal{PS}_{ap}$ class up to linear equivalence.

4 A generalization of class $\mathcal{H}$ of bent functions based on the new spreads

A Boolean function over $\mathbb{F}_{2^m}^2$ is linear over each element of the spread recalled at Section 2 if and only if there exists a mapping $G:\mathbb{F}_{2^m}\mapsto\mathbb{F}_{2^m}$ and $\mu\in\mathbb{F}_{2^m}$ such that, for every $y\in\mathbb{F}_{2^m}$, $f(0,y)=tr_1^m(\mu y)$ and, for every $x,z\in\mathbb{F}_{2^m}$:

$$f(x,x^{2^{k\varphi(z)}}z)=tr_1^m(G(z)x) \tag{5}$$

where tr_1^m is the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. Note that up to EA-equivalence we can assume that $\mu=0$ (indeed, we can add the linear n-variable function $(x,y)\mapsto tr_1^m(\mu y)$ to f; this changes μ into 0 and, according to (2), $G(z)$ into $G(z)+(\mu z)^{2^{m-k\varphi(z)}}$). Taking $\mu=0$ and using (2) again, Relation (5) is satisfied for every $z\in\mathbb{F}_{2^m}$ if and only if:

$$\forall x,y\in\mathbb{F}_{2^m},\; f(x,y)=tr_1^m\left(G\left(\frac{y}{x^{2^{k\varphi(y/x)}}}\right)x\right). \tag{6}$$

Denoting by δ_0 the Kronecker symbol, the value of the Walsh transform $W_f(a,b)=\sum_{x,y\in\mathbb{F}_{2^m}}(-1)^{f(x,y)+tr_1^m(ax+by)}$ equals then, for , for every $(a,b)\in\mathbb{F}_{2^m}^2$:

$$\begin{aligned}
&\sum_{(x,y)\in\mathbb{F}_{2^m}^2}(-1)^{tr_1^m\left(G\left(\frac{y}{x^{2^{k\varphi(y/x)}}}\right)x+ax+by\right)}=\\
&2^m\delta_0(b)+\sum_{x\in\mathbb{F}_{2^m}^*,z\in\mathbb{F}_{2^m}}(-1)^{tr_1^m\left(G(z)x+ax+bx^{2^{k\varphi(z)}}z\right)}=\\
&2^m(\delta_0(b)-1)+\sum_{z\in\mathbb{F}_{2^m}}\sum_{x\in\mathbb{F}_{2^m}}(-1)^{tr_1^m\left(\left(G(z)+a+(bz)^{2^{m-k\varphi(z)}}\right)x\right)}=\\
&2^m\left(\delta_0(b)-1+|\{z\in\mathbb{F}_{2^m};\; G(z)+a+(bz)^{2^{m-k\varphi(z)}}=0\}|\right).
\end{aligned}$$

Hence, f is bent if and only if, for every $a, b \in \mathbb{F}_{2^m}$, the size $|\{z \in \mathbb{F}_{2^m};\ G(z) + a + (bz)^{2^{m-k\varphi(z)}} = 0\}|$ equals 1 if $b = 0$ and equals 0 or 2 if $b \in \mathbb{F}_{2^m}^*$.

Definition 1 *Let m be any positive integer and k any divisor of m. Let φ be an integer-valued function over $\mathbb{F}_{2^m}$, constant on each multiplicative coset of the subgroup U of order $\frac{2^m-1}{2^k-1}$ of $\mathbb{F}_{2^m}^*$. A permutation polynomial $G(z)$ is a φ-polynomial if, for every $b \in \mathbb{F}_{2^m}^*$ and every $a \in \mathbb{F}_{2^m}$, their exist two values of z or none such that*

$$G(z) + (bz)^{2^{m-k\varphi(z)}} = a.$$

If φ is null, this notion corresponds to that of o-polynomial (see e.g. [2]); in other words, a 0-polynomial is an o-polynomial.

Theorem 2 *Let m be any positive integer and k any divisor of m. Let φ be an integer-valued function over $\mathbb{F}_{2^m}$, constant on each multiplicative coset of the subgroup U of order $\frac{2^m-1}{2^k-1}$ of $\mathbb{F}_{2^m}^*$. Let G be any mapping from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ and let f be defined by (6) with the convention $\frac{1}{0} = 0$. Then f is bent if and only if G is a φ-polynomial.*

Remark 1 *Under the hypotheses of Definition 1 and Theorem 2, the mapping $\psi : z \mapsto z^{2^{m-k\varphi(z)}}$ is bijective (and in general not linear). Indeed, each multiplicative coset of U is globally invariant under ψ since it is globally invariant under $z \mapsto z^{2^k}$, and the restriction of ψ to any such coset is clearly injective since φ is constant on it. Note that $\psi^{m/k}$ (that is, ψ composed m/k times with itself) is identity.*

By the bijective change of variable $z \mapsto \psi^{-1}(z) = z^{2^{k\varphi(z)}}$, the equation $G(z) + (bz)^{2^{m-k\varphi(z)}} = a$ is then equivalent to

$$H(z) + b^{2^{m-k\varphi(z)}} z = a, \tag{7}$$

where $H(z) = G(z^{2^{k\varphi(z)}}) = G \circ \psi^{-1}(z)$, is a permutation.

Remark 2 *By raising the equation $G(z)+(bz)^{2^{m-k\varphi(z)}} = a$ to the power $2^{m-k\varphi(z)}$, this equation is also equivalent to $H'(z)+bz = a^{2^{k\varphi(z)}}$, where $H'(z) = (G(z))^{2^{k\varphi(z)}}$, but H' is in general not equal to $\psi^{-1} \circ G$ (nor to $G \circ \psi^{-1}$) and the bijectivity of G does not imply the bijectivity of H'.*

4.1 Case where φ is constant

If $\varphi(z) = 0$ for every z, then the construction has been addressed in [2]. If $\varphi(z) = i \neq 0$ for every z, then the condition of Theorem 2 is equivalent to saying that $H(z) = (G(z))^{2^{ki}}$ is an o-polynomial (see the list in [2]). If the coefficients of H are all in $\mathbb{F}_2$ (this is the case of all polynomials in the list, except the two last ones, called Subiaco and Adelaide o-polynomials, see more in [5]), the function corresponding to $i = 0$ is $f(x, y) = tr_1^m\left(H\left(\frac{y}{x}\right) x\right)$ and the function (6) corresponding to $i \neq 0$ is $f(x,y) = tr_1^m\left(H\left(\frac{y^{2^{m-ki}}}{x}\right)x\right)$, which is linearly equivalent. Hence no new bent function (up to EA-equivalence) arises.

Open question: Do Subiaco and Adelaide o-polynomials give new bent functions up to EA-equivalence, when used as above with $i \neq 0$?

4.2 Case where φ is not constant

This case can potentially lead to new bent functions but is more complex. To see how complex it is, we can choose an example of permutation H and try to determine what are those functions φ, constant on each coset of U, for which Equation (7) has 0 or 2 solutions for every $b \neq 0$. Let us study the simplest possible function $H(z) = z^2$ (for which we know that $\varphi = 0$ works). For such choice of H, Equation (7) is equivalent to $\left(\frac{z}{b^{2^{m-k\varphi(z)}}}\right)^2 + \frac{z}{b^{2^{m-k\varphi(z)}}} = \frac{a}{b^{2^{m-k\varphi(z)}+1}}$. A necessary condition for such equality to hold is that $tr_1^m\left(\frac{a}{b^{2^{m-k\varphi(z)}+1}}\right) = 0$. Imposing such condition, choosing $u \in \mathbb{F}_{2^m}$ such that $tr_1^m(u) = 1$, and defining $c = \sum_{j=1}^{m-1}\left(\frac{a}{b^{2^{m-k\varphi(z)}+1}}\right)^{2^j}\left(\sum_{k=0}^{j-1} u^{2^k}\right)$, we have $c + c^2 = (c+1) + (c+1)^2 = u\, tr_1^m\left(\frac{a}{b^{2^{m-k\varphi(z)}+1}}\right) + \left(\frac{a}{b^{2^{m-k\varphi(z)}+1}}\right) tr_1^m(u) = \frac{a}{b^{2^{m-k\varphi(z)}+1}}$. The choice of u such that $tr_1^m(u) = 1$ being done, the equation $\left(\frac{z}{b^{2^{m-k\varphi(z)}}}\right)^2 + \frac{z}{b^{2^{m-k\varphi(z)}}} = \frac{a}{b^{2^{m-k\varphi(z)}+1}}$ is then equivalent to:

$$\begin{cases} z = b^{2^{m-k\varphi(z)}}\left(\sum_{j=1}^{m-1}\left(\frac{a}{b^{2^{m-k\varphi(z)}+1}}\right)^{2^j}\left(\sum_{k=0}^{j-1} u^{2^k}\right) + \epsilon\right),\ \epsilon \in \mathbb{F}_2 \\ tr_1^m\left(\frac{a}{b^{2^{m-k\varphi(z)}+1}}\right) = 0 \end{cases} . \tag{8}$$

We would need then to see what are the functions φ constant on each coset of U such that, for every $b \neq 0$, there are 0 or 2 values satisfying (8).

Remark 3 *By the bijective change of variable $z \mapsto \frac{z^{2^{k\varphi(z)}}}{b}$, the equation $G(z) + (bz)^{2^{m-k\varphi(z)}} = a$ is equivalent to*

$$G\left(\frac{z^{2^{k\varphi(z)}}}{b}\right) + z = a.$$

Hence if G is a power function, this equation is equivalent to $\frac{G(z^{2^{k\varphi(z)}})}{G(b)} + z = a$ and we deduce that G is then a φ-polynomial if and only if $G(z^{2^{k\varphi(z)}}) = G \circ \psi^{-1}(z)$ is an o-polynomial.
Denoting the o-polynomial $G \circ \psi^{-1}(z)$ by $P(z)$, the corresponding bent function given by (6) is then $f(x,y) = tr_1^m\left(\frac{G(y)}{G(x^{2^{k\varphi(y/x)}})}x\right) = tr_1^m\left(\frac{P\left(y^{2^{m-k\varphi(y/x)}}\right)}{P(x)}x\right)$.

Since five among the nine known classes of o-polynomials are power functions, it is interesting to see whether G and P can both be power functions without that φ be constant. Note that m is then odd since all examples of power o-polynomials are with m odd. Let us suppose that $G(z) = z^d$ and $P(z) = z^e$, where d and e are both co-prime with $2^m - 1$. Suppose that $\frac{m}{k}$ is co-prime with $2^k - 1$, then every element $z \in \mathbb{F}_{2^m}^*$ is the product of an element t of $\mathbb{F}_{2^k}^*$ and of an element u of norm 1 (since the norm of any element z of $\mathbb{F}_{2^k}^*$ equals $z^{\frac{m}{k}}$ and can then take any value in $\mathbb{F}_{2^k}^*$), that is, an element of U. The condition that $G(z^{2^{k\varphi(z)}}) = P(z)$ for all $z = tu$ in $\mathbb{F}_{2^m}^*$ ($t \in \mathbb{F}_{2^k}^*$, $u \in U$) is equivalent to $tu^{2^{k\varphi(t)}} = (tu)^{\frac{e}{d}}$ and then to $\begin{cases} \frac{e}{d} \equiv 1 \ [mod\ 2^k - 1] \\ \frac{e}{d} \equiv 2^{k\varphi(t)} \ [mod\ \frac{2^m-1}{2^k-1}] \end{cases}$. Unfortunately, this implies that φ is constant since $\varphi(t) \leq \frac{m}{k} - 1$ and $\frac{2^m-1}{2^k-1} = \sum_{i=0}^{m/k-1} 2^{ki}$.

4.2.1 The case $k = m/2$ (m even)

In this case, $\varphi(z) = \phi(z^{2^{m/2}+1})$, where ϕ is a Boolean function on $\mathbb{F}_{2^{m/2}}$ and $z^{2^{m-k\varphi(z)}} = \begin{cases} z \text{ if } \phi(z^{2^{m/2}+1}) = 0 \\ z^{2^{m/2}} \text{ if } \phi(z^{2^{m/2}+1}) = 1 \end{cases}$.

4.2.2 The case $k = m/3$ (m divisible by 3)

In this case, $\varphi(z) = \phi(z^{2^{2m/3}+2^{m/3}+1})$, where ϕ is a Boolean function on $\mathbb{F}_{2^{m/2}}$ and $z^{2^{m-k\varphi(z)}} = \begin{cases} z \text{ if } \phi(z^{2^{2m/3}+2^{m/3}+1}) = 0 \\ z^{2^{2m/3}} \text{ if } \phi(z^{2^{2m/3}+2^{m/3}+1}) = 1 \\ z^{2^{m/3}} \text{ if } \phi(z^{2^{2m/3}+2^{m/3}+1}) = 2 \end{cases}$.

4.2.3 The case $k = 2$ (m even)

In this case, $\varphi(z) = \phi(z^{\frac{2^m-1}{3}})$, where ϕ is a function from $\mathbb{F}_4$ to $\mathbb{Z}/(m/2)\mathbb{Z}$ and $z^{2^{m-k\varphi(z)}}$ equals $z^{4^{m/2-\phi(z)}}$.

5 Further generalizations of class $\mathcal{H}$ based on pre-quasifields

Recently, Wu [10] studied three other full spreads, related algebraic structures weaker than fields. Pre-quasifields are Abelian finite groups having a second law $*$ which is left-distributive with respect to the first law and is such that the right and left multiplications by a nonzero element are bijective, and that the left-multiplication by 0 is absorbent. As shown by Kantor in [7], every such pre-quasifield leads to the spread of the $\mathbb{F}_2$-vector spaces $\{(0, y), y \in \mathbb{F}_{2^m}\}$ and $\{(x, z \star x), x \in \mathbb{F}_{2^m}\}$, $z \in \mathbb{F}_{2^m}$ and allows defining $\mathcal{PS}$ bent functions. Wu determined explicitely the $\mathcal{PS}$ functions deduced from the Dempwolff-Müller pre-quasifield, the Knuth pre-semifield (a pre-quasifield which remains one when

$a*b$ is replaced by $b*a$) and the Kantor pre-semifield. In all three cases, m is odd. Note that in the case of a non-commutative pre-semifield, we have potentially the second spread of the $\mathbb{F}_2$-vector spaces $\{(0,y),\, y\in\mathbb{F}_{2^m}\}$ and $\{(x, x\star z), x\in\mathbb{F}_{2^m}\}$, $z\in\mathbb{F}_{2^m}$. We characterize now the $\mathcal{H}$-like functions associated to these spreads.

5.1 $\mathcal{H}$-like bent functions from the Dempwolff-Müller prequasifield

Assume k and m are odd integers with $(k,m)=1$. Let $e=2^{m-1}-2^{k-1}-1$, $L(x)=\sum_{i=0}^{k-1}x^{2^i}$, and define $x\star y = x^e L(xy)$. Then $(\mathbb{F}_{2^m},+,\star)$ is a prequasifield [3], leading to the spread of the $\mathbb{F}_2$-vector spaces $\{(0,y),\, y\in\mathbb{F}_{2^m}\}$ and $\{(x, z\star x), x\in\mathbb{F}_{2^m}\} = \{(x, z^e L(xz)), x\in\mathbb{F}_{2^m}\}$, $z\in\mathbb{F}_{2^m}$.
A Boolean function over $\mathbb{F}_{2^m}^2$ is linear over each element of this spread if and only if there exists a mapping $G:\mathbb{F}_{2^m}\mapsto\mathbb{F}_{2^m}$ and $\mu\in\mathbb{F}_{2^m}$ such that, for every $y\in\mathbb{F}_{2^m}$, $f(0,y)=tr_1^m(\mu y)$ and, for every $x,z\in\mathbb{F}_{2^m}$:

$$f(x, z^e L(xz)) = tr_1^m(G(z)x). \tag{9}$$

Up to EA-equivalence we can assume that $\mu=0$, since we can add the linear n-variable function $(x,y)\mapsto tr_1^m(\mu y)$ to f; this changes μ into 0 and $G(z)$ into $G(z)+\lambda$ where λ is such that $tr_1^m(\mu y)=tr_1^m(\lambda x)$ when $(x,y)\in\{(x, z^e L(xz)), x\in\mathbb{F}_{2^m}\}$, that is, $\lambda=\sum_{i=0}^{k-1}(\mu z^e)^{2^{-i}}z$.
Taking $\mu=0$, Relation (9) is satisfied for every $z\in\mathbb{F}_{2^m}$ if and only if:

$$\forall x,y\in\mathbb{F}_{2^m},\ f(x,y)=tr_1^m\left(G\left(\frac{1}{xD_d\left(\frac{y^2}{x^{2^k+1}}\right)}\right)x\right), \tag{10}$$

where D_d is the Dickson polynomial of index the inverse d of 2^k-1 modulo 2^n-1. Indeed, taking the same notation as Wu [10], the relation $y=z\star x = z^e L(xz) = F(z,x)$ is equivalent to $z=F_x^{-1}(y)$ and the inverse of F_x has been determined in [10].
The Walsh transform $W_f(a,b)=\sum_{x,y\in\mathbb{F}_{2^m}}(-1)^{f(x,y)+tr_1^m(ax+by)}$ equals then:

$$2^m\delta_0(b)+\sum_{x\in\mathbb{F}_{2^m}^*, z\in\mathbb{F}_{2^m}}(-1)^{tr_1^m(G(z)x+ax+bz^eL(xz))} =$$

$$2^m\delta_0(b)+\sum_{x\in\mathbb{F}_{2^m}^*, z\in\mathbb{F}_{2^m}}(-1)^{tr_1^m\left(G(z)x+ax+\sum_{i=0}^{k-1}(bz^e)^{2^{-i}}zx\right)} =$$

$$2^m(\delta_0(b)-1+|\{z\in\mathbb{F}_{2^m};\, G(z)+a+\sum_{i=0}^{k-1}(bz^e)^{2^{-i}}z=0\}|).$$

Hence:

Theorem 3 *A Boolean function f defined by (10) is bent if and only if G is a permutation and the equation $G(z)+\sum_{i=0}^{k-1}(bz^e)^{2^{-i}}z=a$ has 0 or 2 solutions for every $b\neq 0$ and every a.*

5.2 $\mathcal{H}$-like bent functions from the Knuth pre-semifield

Assume m is an odd integer and $\beta \in \mathbb{F}_{2^m}^*$. Then $x \star y = xy + x^2 tr_1^m(\beta y) + y^2 tr_1^m(\beta x)$ defines a pre-semifield [8], leading to the spread of the $\mathbb{F}_2$-vector spaces $\{(0,y),\, y \in \mathbb{F}_{2^m}\}$ and $\{(x, z\star x), x \in \mathbb{F}_{2^m}\} = \{(x, zx + x^2 tr_1^m(\beta z) + z^2 tr_1^m(\beta x)), x \in \mathbb{F}_{2^m}\}$, $z \in \mathbb{F}_{2^m}$.

A Boolean function over $\mathbb{F}_{2^m}^2$ is linear over each element of this spread if and only if there exists a mapping $G : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ and $\mu \in \mathbb{F}_{2^m}$ such that, for every $y \in \mathbb{F}_{2^m}$, $f(0,y) = tr_1^m(\mu y)$ and, for every $x, z \in \mathbb{F}_{2^m}$:

$$f(x, zx + x^2 tr_1^m(\beta z) + z^2 tr_1^m(\beta x)) = tr_1^m(G(z)x). \qquad (11)$$

Up to EA-equivalence we can assume that $\mu = 0$, since we can add the linear n-variable function $(x,y) \mapsto tr_1^m(\mu y)$ to f; this changes μ into 0 and $G(z)$ into $G(z) + \lambda$ where λ is such that $tr_1^m(\mu y) = tr_1^m(\lambda x)$ when $(x,y) \in \{(x, zx + x^2 tr_1^m(\beta z) + z^2 tr_1^m(\beta x)), x \in \mathbb{F}_{2^m}\}$, that is, $\lambda = \mu z + tr_1^m(\beta z)\mu^{2^{m-1}} + \beta tr_1^m(\mu z^2)$. Taking $\mu = 0$, Relation (11) is satisfied for every $z \in \mathbb{F}_{2^m}$ if and only if, for all $x, y \in \mathbb{F}_{2^m}$, $f(x,y)$ equals:

$$tr_1^m\left(G\left((1 + tr_1^m(\beta x))\frac{y}{x} + x tr_1^m\left(\beta \frac{y}{x}\right) + x tr_1^m(\beta x) C_{\frac{1}{\beta x}}\left(\frac{y}{x^2}\right)\right) x\right), \qquad (12)$$

where $C_a(x) = \sum_{i=0}^{m-1} c_i x^{2^i}$, where $c_0 = \frac{1}{a^{2^i}} + \frac{1}{a^{3\cdot 2^i}} + \cdots + \frac{1}{a^{(m-3)\cdot 2^i}}$ and if i is odd, then $c_i = 1 + \frac{1}{a^{2^i}} + \frac{1}{a^{3\cdot 2^i}} + \cdots + \frac{1}{a^{(i-2)\cdot 2^i}} + \frac{1}{a^{(i+1)\cdot 2^i}} + \cdots + \frac{1}{a^{(m-1)\cdot 2^i}}$ and if i is even, then $c_i = 1 + \frac{1}{a^{2\cdot 2^i}} + \frac{1}{a^{4\cdot 2^i}} + \cdots + \frac{1}{a^{(i-2)\cdot 2^i}} + \frac{1}{a^{(i+1)\cdot 2^i}} + \cdots + \frac{1}{a^{(m-2)\cdot 2^i}}$. Indeed, as above, the relation $y = z \star x = zx + x^2 tr_1^m(\beta z) + z^2 tr_1^m(\beta x) = F(z,x)$ is equivalent to $z = F_x^{-1}(y)$ and the inverse of F_x has been determined in [10]. The Walsh transform $W_f(a,b) = \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{f(x,y) + tr_1^m(ax+by)}$ equals then:

$$2^m \delta_0(b) + \sum_{x \in \mathbb{F}_{2^m}^*, z \in \mathbb{F}_{2^m}} (-1)^{tr_1^m\left(G(z)x + ax + b(zx + x^2 tr_1^m(\beta z) + z^2 tr_1^m(\beta x))\right)} =$$

$$2^m(\delta_0(b) - 1 + |\{z \in \mathbb{F}_{2^m};\, G(z) + a + bz + b^{2^{m-1}} tr_1^m(\beta z) + \beta tr_1^m(bz^2)\}|).$$

Hence:

Theorem 4 *A Boolean function f defined by (12) is bent if and only if G is a permutation and the equation $G(z) + bz + b^{2^{m-1}} tr_1^m(\beta z) + \beta tr_1^m(b^{2^{m-1}} z) = a$ has 0 or 2 solutions for every $b \neq 0$ and every a.*

5.3 $\mathcal{H}$-like bent functions from the Kantor pre-semifield

Assume m is an odd integer. Then $x \star y = x^2 y + tr_1^m(xy) + x tr_1^m(y)$ defines a pre-semifield [6], leading to the spread of the $\mathbb{F}_2$-vector spaces $\{(0,y),\, y \in \mathbb{F}_{2^m}\}$ and $\{(x, z\star x), x \in \mathbb{F}_{2^m}\} = \{(x, z^2 x + tr_1^m(zx) + z tr_1^m(x)), x \in \mathbb{F}_{2^m}\}$ (respectively, $\{(x, x\star z), x \in \mathbb{F}_{2^m}\} = \{(x, x^2 z + tr_1^m(xz) + x tr_1^m(z)), x \in \mathbb{F}_{2^m}\}$), where $z \in \mathbb{F}_{2^m}$.

A Boolean function over $\mathbb{F}_{2^m}^2$ is linear over each element of this spread if and only if there exists a mapping $G : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ and $\mu \in \mathbb{F}_{2^m}$ such that, for every $y \in \mathbb{F}_{2^m}$, $f(0,y) = tr_1^m(\mu y)$ and, for every $x, z \in \mathbb{F}_{2^m}$:

$$f(x, z^2x + tr_1^m(zx) + ztr_1^m(x)) = tr_1^m(G(z)x). \tag{13}$$

Respectively:

$$f(x, x^2z + tr_1^m(xz) + xtr_1^m(z)) = tr_1^m(G(z)x). \tag{14}$$

Up to EA-equivalence we can assume that $\mu = 0$, since we can add the linear n-variable function $(x,y) \mapsto tr_1^m(\mu y)$ to f; this changes μ into 0 and $G(z)$ into $G(z) + \lambda$ where λ is such that $tr_1^m(\mu y) = tr_1^m(\lambda x)$ when $(x,y) \in \{(x, z^2x + tr_1^m(zx) + ztr_1^m(x)), x \in \mathbb{F}_{2^m}\}$ (respectively $\{(x, x^2z + tr_1^m(xz) + xtr_1^m(z)), x \in \mathbb{F}_{2^m}\}$), that is, $\lambda = \mu z^2 + ztr_1^m(\mu) + tr_1^m(\mu z)$ (respectively, $(\mu z)^{2^{m-1}} + ztr_1^m(\mu) + \mu tr_1^m(z)$). Taking $\mu = 0$, Relation (13) is satisfied for every $z \in \mathbb{F}_{2^m}$ if and only if, for all $x, y \in \mathbb{F}_{2^m}$, $f(x,y)$ equals:

$$tr_1^m\left(G\left(\left[(xy)^{2^{m-1}} + \sum_{i=0}^{\frac{m-1}{2}} (xy)^{2^{2i}-1} + \sum_{i=0}^{\frac{m-3}{2}} x^{2^{2i}} tr_1^m(xy)\right] \frac{tr_1^m(x)}{x} \right.\right.$$
$$\left.\left. + x^{2^{m-1}-1}y^{2^{m-1}} + x^{2^{m-1}-1}tr_1^m(xy)\right) x\right). \tag{15}$$

Indeed, as above, the relation $y = z \star x = z^2x + tr_1^m(zx) + ztr_1^m(x) = F(z,x)$ is equivalent to $z = F_x^{-1}(y)$ and the inverse of F_x has been determined in [10]. Relation (14) is satisfied for every $z \in \mathbb{F}_{2^m}$ if and only if, for all $x, y \in \mathbb{F}_{2^m}$, $f(x,y)$ equals:

$$tr_1^m\left(G\left(\frac{y}{x^2} + tr_1^m\left(\frac{1}{x}\right)\left(\frac{tr_1^m\left(\frac{y}{x^2}\right)}{x^2} + \frac{tr_1^m\left(\frac{y}{x}\right)}{x}\right) + \left(tr_1^m\left(\frac{1}{x}\right) + 1\right)\right.\right.$$
$$\left.\left.\left(\frac{tr_1^m\left(\frac{y}{x^2}\right) + tr_1^m\left(\frac{y}{x}\right)}{x^2} + \frac{tr_1^m\left(\frac{y}{x^2}\right)}{x}\right)\right) x\right). \tag{16}$$

Indeed, the relation $y = x^2z + tr_1^m(xz) + xtr_1^m(z)$ implies for $x \neq 0$ that $\begin{cases} z = \frac{y}{x^2} + \frac{tr_1^m(xz)}{x^2} + \frac{tr_1^m(z)}{x} \\ tr_1^m(xz) = tr_1^m\left(\frac{y}{x}\right) + tr_1^m(xz)tr_1^m\left(\frac{1}{x}\right) + tr_1^m(z) \\ tr_1^m(z) = tr_1^m\left(\frac{y}{x^2}\right) + \left(tr_1^m(xz) + tr_1^m(z)\right) tr_1^m\left(\frac{1}{x}\right) \end{cases}$ and is then equivalent to $z = \frac{y}{x^2} + tr_1^m\left(\frac{1}{x}\right)\left(\frac{tr_1^m\left(\frac{y}{x^2}\right)}{x^2} + \frac{tr_1^m\left(\frac{y}{x}\right)}{x}\right) + \left(tr_1^m\left(\frac{1}{x}\right) + 1\right)\left(\frac{tr_1^m\left(\frac{y}{x^2}\right) + tr_1^m\left(\frac{y}{x}\right)}{x^2} + \frac{tr_1^m\left(\frac{y}{x^2}\right)}{x}\right)$.

In the case of (13), the Walsh transform $W_f(a,b) = \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{f(x,y) + tr_1^m(ax+by)}$ equals then:

$$2^m\delta_0(b) + \sum_{x \in \mathbb{F}_{2^m}^*, z \in \mathbb{F}_{2^m}} (-1)^{tr_1^m\left(G(z)x + ax + bz^2x + btr_1^m(zx) + bztr_1^m(x)\right)} =$$
$$2^m(\delta_0(b) - 1 + |\{z \in \mathbb{F}_{2^m};\, G(z) + a + bz^2 + ztr_1^m(b) + tr_1^m(bz) = 0\}|.$$

Hence:

Theorem 5 *A Boolean function f defined by (15) is bent if and only if G is a permutation and the equation $G(z) + bz^2 + ztr_1^m(b) + tr_1^m(bz) = a$ has 0 or 2 solutions for every $b \neq 0$ and every a.*

In the case of (14), the Walsh transform $W_f(a,b) = \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{f(x,y)+tr_1^m(ax+by)}$ equals then:

$$2^m \delta_0(b) + \sum_{x \in \mathbb{F}_{2^m}^*, z \in \mathbb{F}_{2^m}} (-1)^{tr_1^m\left(G(z)x+ax+bx^2z+btr_1^m(xz)+bxtr_1^m(z)\right)} =$$

$$2^m(\delta_0(b) - 1 + |\{z \in \mathbb{F}_{2^m};\, G(z) + a + (bz)^{2^{m-1}} + ztr_1^m(b) + btr_1^m(z)\}|).$$

Hence:

Theorem 6 *A Boolean function f defined by (16) is bent if and only if G is a permutation and the equation $G(z) + (bz)^{2^{m-1}} + ztr_1^m(b) + btr_1^m(z) = a$ has 0 or 2 solutions for every $b \neq 0$ and every a.*

6 Conclusion

We have specified the $\mathcal{PS}$ bent functions related to the André spreads and their duals. Maybe these functions were part of the folklore in a part of the community of difference sets, but as far as we know, they were never given in a paper, all the more in explicit form, neither their duals. We have introduced 4 classes of $\mathcal{H}$-like bent functions related to this same André spreads and to the spreads derived from the Dempwolff-Müller pre-quasifield, the Knuth pre-semifield and the Kantor pre-semifield. Each of these 4 classes leads to a notion similar to that of o-polynomial but significantly different. The notion of o-polynomial is very simple in its definition but very difficult to be handled; it has given huge work to mathematicians, who came up with 9 classes only, in a period of 40 years. These four similar notions are slightly more complex and it seems that it is not possible to relate them to that of o-polynomial in a way allowing deriving such polynomials from known o-polynomials. The work to obtain examples of such polynomials seems difficult; we propose this as future work.

Acknowledgement We are indebted to William Kantor who informed us of the existence of the André spreads.

References

[1] 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, pp. 257-397, 2010. Preliminary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html

[2] C. Carlet and S. Mesnager. On Dillon's class H of bent functions, Niho bent functions and o-polynomials. Journal of Combinatorial Theory-JCT-serie A 118, pages 2392-2410, 2011.

[3] U. Dempwolff and P. Müller. Permutation polynomials and translation planes of even order. *Adv. Geom.*, vol. 13, pp. 293-313, 2013.

[4] Dillon J.: Elementary Hadamard difference sets. PhD dissertation. Univ. of Maryland, 1974.

[5] T.Helleseth, A. Kholosha and S. Mesnager. Niho Bent Functions and Subiaco Hyperovals. *Proceedings of the 10-th International Conference on Finite Fields and Their Applications (Fq'10), Contemporary Math., AMS*, Vol 579, pp. 91-101, 2012.

[6] W. Kantor. Spreads, translation planes and Kerdock sets. II. SIAM J. Alg. Discr. Methods, vol. 3, pp. 308-318, 1982.

[7] W. Kantor. Bent functions generalizing Dillon's partial spread functions. arXiv:1211.2600

[8] D. Knuth, ÒA class of projective planes,Ó Trans. Amer. Math. Soc., vol. 115, pp. 541-549, 1965.

[9] Rothaus O. S.: On bent functions, J. Combin. Theory, Ser. A **20**, 300–305 (1976).

[10] B. Wu. $\mathcal{PS}$ bent functions constructed from finite pre-quasifield spreads. http://arxiv.org/abs/1308.3355