Hyper-bent functions and cyclic codes

Claude Carleta, Philippe Gaboritb

a INRIA, Domaine de Voluceau, Rocquencourt, BP 105 - 78153, Le Chesnay, Cedex, France
b LACO, Université de Limoges, 123, av. A. Thomas, 87060 Limoges, France

Received 20 November 2003
Available online 1 June 2005

Abstract

Bent functions are those Boolean functions whose Hamming distance to the Reed–Muller code of order 1 equal $2^{n-1} - 2^{n/2-1}$ (where the number $n$ of variables is even). These combinatorial objects, with fascinating properties, are rare. Few constructions are known, and it is difficult to know whether the bent functions they produce are peculiar or not, since no way of generating at random bent functions on 8 variables or more is known.

The class of bent functions contains a subclass of functions whose properties are still stronger and whose elements are still rarer. Youssef and Gong have proved the existence of such hyper-bent functions, for every even $n$. We prove that the hyper-bent functions they exhibit are exactly those elements of the well-known $\mathcal{PS}_n$ class, introduced by Dillon, up to the linear transformations $x \mapsto x^\delta$, $\delta \in F_{2^n}^\times$. Hyper-bent functions seem still more difficult to generate at random than bent functions; however, by showing that they all can be obtained from some codewords of an extended cyclic code $H_n$ with small dimension, we can enumerate them for up to 10 variables. We study the non-zeroes of $H_n$ and we deduce that the algebraic degree of hyper-bent functions is $n/2$. We also prove that the functions of class $\mathcal{PS}_n$ are some codewords of weight $2^{n-1} - 2^{n/2-1}$ of a subcode of $H_n$ and we deduce that for some $n$, depending on the factorization of $2^n - 1$, the only hyper-bent functions on $n$ variables are the elements of the class $\mathcal{PS}_n$, obtained from $\mathcal{PS}_n$ by composing the functions by the transformations $x \mapsto x^\delta$, $\delta \neq 0$, and by adding constant functions. We prove that non-$\mathcal{PS}_n$ hyper-bent functions exist for $n = 4$, but it is not clear whether they exist for greater $n$. We also construct potentially new bent functions for $n = 12$.

© 2005 Elsevier Inc. All rights reserved.

Keywords: Bent function; Difference set; Error correcting code

E-mail addresses: claude.carlet@inria.fr (C. Carlet), gaborit@unilim.fr (P. Gaborit).

1 Member of the University of Paris 8 (MAATICA H)

0097-3165/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
1. Introduction

A Boolean function \( f \) on \( n \) variables is an \( F_2 \)-valued function on the space \( F_2^n \) of \( n \)-tuples over \( F_2 \). The addition in \( F_2 \) and the addition of Boolean functions will be denoted by \( \oplus \). The addition in \( F_2^n \) and in finite fields will be denoted by \( + \), since there will be no ambiguity.

We call support of \( f \) the set \( \{ x \in F_2^n / f(x) = 1 \} \) and we denote it by \( \text{Supp}(f) \). Its size is by definition the weight of \( f \) and is denoted by \( w_H(f) \). A Boolean function \( f \) is balanced if \( w_H(f) = 2^{n-1} \).

Every Boolean function \( f \) on \( F_2^n \) admits a unique representation as a polynomial over \( F_2 \) on \( n \) binary variables of the form

\[
\sum_{I \subseteq \{1, \ldots, n\}} a_I \prod_{i \in I} x_i.
\]

This representation is called the algebraic normal form (ANF) of \( f \). We will call (algebraic) degree of \( f \) and denote by \( \deg f \) the degree of its ANF, and we denote by \( R(d, n) \) the set of all those Boolean functions on \( F_2^n \) whose degrees are upper bounded by \( d \) (the so-called Reed–Muller code \(^2\) of order \( d \) on \( F_2^n \)). The elements of \( R(1, n) \) are called affine functions. The ANFs of affine functions have the form \( a \cdot x + b \) where \( a, b \in F_2^n \) and where \( a \cdot x = \bigoplus_{i=1}^n a_i x_i \) is the usual inner product. As usual, we can endow the vectorspace \( F_2^n \) with the structure of the field \( F_{2^n} \) : we choose a basis \( (x_1, \ldots, x_n) \) of this field, viewed as an \( n \)-dimensional vectorspace over \( F_2 \) and we identify every element of this field with the \( n \)-tuple of its coordinates. Then the affine functions have the form \( \text{Tr}(ax + b) \) where \( a, b \in F_{2^n} \) and where \( \text{Tr} \) is the trace function from \( F_{2^n} \) to \( F_2 \), or equivalently \( \text{Tr}(ax) \oplus \epsilon \) where \( a \in F_{2^n} \) and \( \epsilon \in F_2 \).

To every Boolean function \( f \), we classically associate the “sign” function \( f_\epsilon \) of \( f \) defined as \( f_\epsilon(x) = (-1)^{f(x)} \). The discrete Fourier transform \( \hat{f}_\epsilon \) of \( f_\epsilon \) will be called the Walsh transform of \( f \). By definition, \( \hat{f}_\epsilon(b) \) equals \( \sum_{x \in F_2^n} (-1)^{f(x) \oplus \epsilon \cdot b} \). The Walsh transform satisfies Parseval’s relation:

\[
\sum_{b \in F_2^n} \hat{f}_\epsilon^2(b) = 2^{2n}
\]

and the inverse Fourier formula,

\[
\hat{f}_\epsilon = 2^nf_\epsilon
\]

(which is more generally valid for every real-valued function).

The Hamming distance between two Boolean functions \( f_1 \) and \( f_2 \) on \( F_2^n \) equals by definition the weight of \( f_1 \oplus f_2 \). We call nonlinearity of \( f \) and we denote by \( \mathcal{NL}(f) \) the minimum distance between \( f \) and all affine functions. This notion is closely related to the linear attack by Matsui \([22]\) and the Boolean functions used in the S-boxes of block ciphers must have high nonlinearities. The Boolean functions used in the pseudo-random generators of stream ciphers, also, have preferably high nonlinearities, as shown in \([3]\).

\(^2\) \( R(d, n) \) is identified with a set of binary vectors of length \( 2^n \) via the truth tables of the functions.
For every Boolean function \( f \), the nonlinearity \( \mathcal{NL}(f) \) and the Walsh transform \( \widehat{f}(b) \) satisfy the relation:

\[
\mathcal{NL}(f) = 2^n - 1 - \frac{1}{2} \max_{b \in \mathbb{F}_2^n} |\widehat{f}(b)|.
\]

(4)

Because of Parseval’s relation (2), \( \mathcal{NL}(f) \) is upper bounded by \( 2^n - 2^{n/2} - 1 \). This bound is tight for every \( n \) even. The functions achieving it are called \textit{bent}; their distances to all affine functions equal \( 2^n - 2^{n/2} - 1 \).

The nonlinearity is an \textit{affine invariant}: if two functions \( f \) and \( g \) are \textit{linearly equivalent} (that is, if there exists a linear isomorphism \( L \) such that \( g = f \circ L \)) or if they are \textit{affinely equivalent} (there exists an affine isomorphism \( L \) such that \( g = f \circ L \)), then they have same nonlinearity. The notion of bent function is therefore also affinely invariant (that is, invariant under the action of the general affine group).

Bent functions have very nice combinatorial properties (see Section 2). Their degrees are upper bounded by \( n/2 \) (this bound is called \textit{Rothaus’ bound}) as shown in [26]. The determination of all bent functions, or more precisely the classification of these functions under the action of the general affine group has been achieved for \( n \leq 6 \) in [26], but it is unknown for \( n \geq 8 \) (it has been done for \( n = 8 \) in [16], only for functions of degrees at most 3). Some constructions of bent functions exist, cf. [4,5,7,9,11–13,15,17,18,23], but we cannot know whether the bent functions they produce are peculiar or not. Indeed, if we try to generate at random bent functions on \( n = 8 \) variables, or more, by extracting Boolean functions of degrees at most \( n/2 \) and rejecting those which are not bent, we get no bent function, because they are too rare. There exists a nice method [10] for obtaining bent functions by choosing a Boolean function of degree at most \( n/2 \) and then changing this function bit by bit in such a way that a bent function is eventually obtained. But this generation of bent functions seems to be far from being random.

The class of bent functions contains the subclass of \textit{hyper-bent} functions: those Boolean functions over \( \mathbb{F}_{2^n} \) with minimum distance \( 2^n - 2^{n/2} - 1 \) to the set of all functions of the form \( \text{Tr}(ax^i + b) \), where \( i \) is coprime with \( 2^n - 1 \). We know that the subclass of hyper-bent functions is non-empty because Youssef and Gong have proved in [27] the existence, for every even \( n \), of such functions. We shall show at Section 2.3 that the hyper-bent functions they exhibit are those elements of the well-known \( \mathcal{PS}_{\text{ap}} \) class (see Section 2), up to the linear transformation \( x \mapsto \delta x, \delta \neq 0 \), and we shall give an alternative proof of the hyper-bentness of \( \mathcal{PS}_{\text{ap}} \) functions.

Obviously, if there does not exist a way of generating at random bent functions, one can wonder how there could exist one for hyper-bent functions. We shall show in Section 3 that all hyper-bent functions belong to an extended cyclic code of small dimension. It is an easy task to choose at random the elements of such a code, and the proportion of hyper-bent functions in this code is sufficient for getting many of them. We deduce the complete determination of hyper-bent functions on 6, 8 and 10 variables and a method for generating pseudo-randomly hyper-bent functions on 12 variables. We prove that the algebraic degree of hyper-bent functions is \( n/2 \). We also prove that for some \( n \), depending on the factorization of \( 2^n - 1 \), the only hyper-bent functions with \( n \) variables are those elements of the class \( \mathcal{PS}_{\text{ap}}^\# \), obtained from \( \mathcal{PS}_{\text{ap}} \) by composing the functions by the transformations...
x ↦ δx, δ ≠ 0, and by adding constant functions. We prove that non PS hyper-bent functions exist for n = 4 but it is not sure that others exist for greater n.

2. Background on bent functions

A Boolean function f on $F_2^n$ is bent if and only if its Walsh transform satisfies $\hat{f}(b) = \pm 2^{n/2}$, for every $b \in F_2^n$. The notion of bent function does not change if we replace the dot product “·” by any other inner product on $F_2^n$ (since any inner product has the form $\langle x, s \rangle = x \cdot L(s)$, where L is an auto-adjoint linear isomorphism, i.e. an isomorphism whose associated matrix is symmetric). In particular, if $F_2^n$ is identified with the Galois field $F_2^n$ as recalled above, we can take for inner product $\langle x, s \rangle = Tr(xs)$.

We have seen above that the notion of bent function is affinely invariant. More precisely, it is possible to show that the automorphism group of the class of bent functions (i.e. the set of permutations on $F_2^n$ which lets this class invariant) equals the general affine group. Clearly, if $f$ is bent and $\ell$ is affine, then $f \oplus \ell$ is bent. A class of bent functions is called complete if it is globally invariant under the action of the general affine group and the addition of affine functions.

Denoting by $D_a f$ the derivative of $f$, that is, the Boolean function $f(x) \oplus f(x + a)$, the function $f$ is bent if and only if: $\forall a \in F_2^n$, $w_H(D_a f) = 2^n - 1$. Equivalently, $f$ is bent if and only if the $2^n \times 2^n$ matrix $H = \left((-1)^{f(x+y)}\right)_{x,y \in F_2^n}$ is a Hadamard matrix (i.e. satisfies $H \times H^t = 2^n I_d$), that is, if and only if the support of $f$ is a difference set.

If $f$ is bent, then the dual $\tilde{f}$ of $f$, defined on $F_2^n$ by $\hat{\tilde{f}}(u) = 2^{n/2}(-1)^{\hat{f}(u)}$ is also bent and its own dual is $f$ itself, because of Relation (3).

All the quadratic bent functions are known: any such function

$$f(x) = \bigoplus_{1 \leq i < j \leq n} a_{i,j} x_i x_j \oplus h(x) \quad (h \text{ affine}, a_{i,j} \in F_2)$$

is bent if and only if one of the following equivalent properties is satisfied:

1. its Hamming weight is equal to $2^{n-1} \pm 2^{n-1}$;
2. its associated symplectic form: $\varphi_f : (x, y) \mapsto f(0) \oplus f(x) \oplus f(y) \oplus f(x + y)$ is non-degenerate (i.e. has kernel $\{0\}$);
3. the skew-symmetric matrix $M = (m_{i,j})_{i,j \in \{1, \ldots, n\}}$ over $F_2$, defined by: $m_{i,j} = a_{i,j}$ if $i < j$, $m_{i,j} = 0$ if $i = j$, and $m_{i,j} = a_{j,i}$ if $i > j$, is regular (i.e. has determinant 1); indeed, $M$ is the matrix of the bilinear form $\varphi_f$;

3 Thus, bent functions are also related to designs, since any difference set can be used to construct a symmetric design, cf. [1, pp. 274–278]. The notion of difference set is anterior to that of bent function, but it had not been much studied for elementary 2-groups before the introduction of bent functions.
4. \( f(x) \) is equivalent, up to an affine nonsingular transformation, to: \( x_1 x_2 \oplus x_3 x_4 \oplus \cdots \oplus x_{n-1} x_n \oplus \varepsilon (\varepsilon \in F_2) \).

The following property was first proved in [26]:

**Proposition 1.** Let \( n \) be any even integer greater than or equal to 4. The degree of any bent function on \( F_2^n \) is at most \( \frac{n}{2} \).

2.1. Constructions

Bent functions are not classified, but we can try to know as many bent functions as possible. So, constructions have been designed. The two main ones are the following:

1. The **Maiorana–McFarland’s class** \( \mathcal{M} \) (cf. [12, 23]) is the set of all the Boolean functions on \( F_2^n = \{(x, y), x, y \in F_2^n\} \), of the form

\[
    f(x, y) = x \cdot \pi(y) \oplus g(y),
\]

where \( \pi \) is any permutation \(^4\) on \( F_2^n \) and \( g \) any Boolean function on \( F_2^n \) (“\( \cdot \)” denotes here the inner product in \( F_2^n \)). Any such function is bent and the dual function \( \tilde{f}(x, y) \) equals: \( y \cdot \pi^{-1}(x) \oplus g(\pi^{-1}(x)) \), where \( \pi^{-1} \) is the inverse permutation of \( \pi \). The completed class of \( \mathcal{M} \) contains all the quadratic bent functions.

2. The **Partial Spreads class** \( \mathcal{PS} \), introduced in [12] by Dillon, is the set of all the sums (modulo 2) of the indicators of \( 2^n/2 - 1 \) or \( 2^n/2 + 1 \) “disjoint” \( \frac{n}{2} \)-dimensional subspaces of \( F_2^n \) (“disjoint” meaning that any two of these spaces intersect in 0 only, and therefore that their sum is direct and equal to \( F_2^n \)). Dillon exhibits in [12] a subclass of \( \mathcal{PS} \), denoted by \( \mathcal{PS}_{ap} \), whose elements are defined in an explicit form: \( F_2^n \) is identified with the Galois field \( F_{2^n} \) (an inner product in this field being defined as \( x \cdot y = tr(xy) \), where \( tr \) is the trace function from \( F_{2^n} \) to \( F_2 \); we know that the notion of bent function is independent of the choice of the inner product); the space \( F_2^n \approx F_{2^n/2} \times F_{2^n/2} \), viewed as a 2-dimensional \( F_{2^n/2} \)-vectorspace, is equal to the “disjoint” union of its \( 2^n/2 + 1 \) lines through the origin; these lines are \( \frac{n}{2} \)-dimensional \( F_2 \)-subspaces of \( F_2^n \). Choosing any \( 2^n/2 - 1 \) of the lines, different from those of equations \( x = 0 \) and \( y = 0 \), leads, by definition, to an element of \( \mathcal{PS}_{ap} \), that is, to a function of the form \( f(x, y) = g\left(\frac{x}{y}\right)\), i.e. \( g\left(\frac{x}{y}\right) \) with \( \frac{x}{y} = 0 \) if \( y = 0 \), where \( g \) is a balanced Boolean function on \( F_{2^n/2} \) which vanishes at 0 (note that the balancedness of \( g \) is a necessary and sufficient condition for \( f \) being bent). The complements of these functions are the functions \( g(\frac{x}{y}) \) where \( g \) is balanced and does not vanish at 0. In both cases, the dual of \( g(\frac{x}{y}) \) is \( g(\frac{y}{x}) \).

Secondary constructions (of new bent functions from known ones) also exist, but we shall not use them in this paper.

---

\(^4\) The bijectivity of \( \pi \) is a necessary and sufficient condition.
2.2. On the number of bent functions

The class of bent functions produced by the Maiorana–McFarland’s construction is by far the widest class, compared to the classes obtained from the other usual constructions. The number of bent functions of the form (5) equals \( (2^n/2) \times 2^{2^n} \), and is asymptotically equivalent to \( \left( \frac{2^n}{e} \right)^{2^n} \sqrt{2\pi 2^n} \) (according to Stirling’s formula) while \(\mathcal{PS}\text{ap}\) contains \( \left( \frac{2^n}{2^n-1} \right) \approx \frac{2^n + \frac{1}{2}}{\sqrt{\pi 2^n}} \) functions. However, the number of (bent) Maiorana–McFarland’s functions seems negligible with respect to the total number of bent functions. The number of (bent) functions which are affinely equivalent to Maiorana–McFarland’s functions is unknown; it is at most equal to the number of Maiorana–McFarland’s functions times the number of affine automorphisms, that equals \(2^n(2^n-1)(2^n-2)\cdots(2^n-2^n-1)\). It seems also negligible with respect to the total number of bent functions. The number of bent functions on a given number of variables is not known. Rothaus’ inequality implies that the number of bent functions is at most \(2^{1+n+\cdots+(n/2)} = 2^{2n-1} + \frac{1}{2}(n/2)\) (let us call the naive bound this upper bound). We know that for \(n = 6\), the number of bent functions is approximately equal to \(2^{32}\) (cf. [25]), which is much less than \(2^{25} + \frac{1}{2} (6) = 2^{42}\). An upper bound improving upon the naive bound has been found recently [8]. It is exponentially better than the naive bound since it divides it by approximately \(2^{2^n-\frac{n}{2}-1}\). But this bound seems to be far from the exact number of bent functions.

2.3. Hyper-bent functions

In [27], A. Youssef and G. Gong study the Boolean functions \(f\) on the field \(F_{2^n}\) (\(n\) even) whose Hamming distance to all functions \(Tr(ax^i) \oplus \varepsilon (a \in F_{2^n}, \varepsilon \in F_2, i\text{ coprime with } 2^n - 1)\) equals \(2^{n-1} \pm 2^{\frac{n}{2}} - 1\). These functions are bent, since every affine function has the form \(Tr(ax) \oplus \varepsilon\). They are called hyper-bent functions.\(^5\) Equivalently, \(f\) is hyper-bent if and only if \(\sum_{x \in F_{2^n}} (-1)^{f(x)@Tr(ax^i)} \) equals \(\pm 2^{\frac{n}{2}}\) for every \(a \in F_{2^n}\) and every \(i\), coprime with \(2^n - 1\). Since we have \(\sum_{x \in F_{2^n}} (-1)^{f(x)@Tr(ax^i)} = \sum_{x \in F_{2^n}} (-1)^{f(x^i)@Tr(ax)}\), where \(j\) is the inverse of \(i\) modulo \(2^n - 1\), we deduce:

**Proposition 2.** Let \(n\) be any even integer. A Boolean function \(f\) on \(F_{2^n}\) is hyper-bent if and only if the function \(f(x^i)\) is bent for every \(i\), coprime with \(2^n - 1\).

The condition of Proposition 2 is so strong that it seems impossible to satisfy. Astonishingly enough, Youssef and Gong show that hyper-bent functions exist. They partially state

\(^5\) The term of hyper-bent was also used in [6] to describe another notion; we use it here only for the notion introduced by Youssef and Gong.
this main result of [27] in terms of sequences. We prefer stating it below, using only the terminology of Boolean functions. The following proposition is an easy translation of their result:

**Proposition 3 (Youssef and Gong [27]).** Let \( n \) be any even integer and \( \alpha \) a primitive element of \( \mathbb{F}_{2^n} \). Let \( f \) be a Boolean function on \( \mathbb{F}_{2^n} \) such that \( f(0) = 0 \) and \( f(x^{2^{n/2}+1}x) = f(x) \) for every \( x \in \mathbb{F}_{2^n} \). Then \( f \) is hyper-bent if and only if the weight of the vector \( (f(1), f(\alpha), f(\alpha^2), \ldots, f(x^{2^{n/2}})) \) equals \( 2^{n/2-1} \).

We show now that these functions are well-known.

**Proposition 4.** The functions \( f \) of Proposition 3, such that \( f(1) = 0 \) are the elements of class \( \mathcal{P}\mathcal{S}_{\text{ap}} \). Those such that \( f(1) = 1 \) are the functions of the form \( f(x) = f'(\delta x) \) where \( \delta \in \mathbb{F}_{2^n}^* \), \( f' \in \mathcal{P}\mathcal{S}_{\text{ap}} \) and \( f'(\delta) = 1 \).

**Proof.** Let us denote \( x^{2^{n/2}+1} \) by \( \beta \). We have \( f(\beta x) = f(x) \) for every \( x \in \mathbb{F}_{2^n} \), and therefore \( f(\beta^j x) = f(x) \) for every \( x \in \mathbb{F}_{2^n} \) and every integer \( j \). It is well-known that the set \( \{0, \beta, \ldots, \beta^{2^{n/2}-1}\} \) equals the finite field \( \mathbb{F}_{2^{2^{n/2}}} \). So the condition on \( f \) can be written: \( f(yx) = f(x), \forall y \in \mathbb{F}_{2^{2^{n/2}}} \). Such a function is completely characterized by its values on any set of representatives of the elements of \( \mathbb{F}_{2^n}^*/\mathbb{F}_{2^{2^{n/2}}}^* \)—for instance \( \{1, \alpha, \ldots, x^{2^{n/2}}\} \). Let \( \omega \) be an element of \( \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^{2^{n/2}}} \) such that \( f(\omega) = f(1) \) (such an element must exist, since \( f \) has weight \( 2^{n-1} - 2^{n/2-1} \)). The pair \( (1, \omega) \) is a basis of the \( \mathbb{F}_{2^{2^{n/2}}-}\)vectorspace \( \mathbb{F}_{2^n} \). Hence, we have \( \mathbb{F}_{2^n} = \mathbb{F}_{2^{2^{n/2}}} + \omega \mathbb{F}_{2^{2^{n/2}}} \). For every \( y, y' \in \mathbb{F}_{2^{2^{n/2}}} \), we have then \( f(y' + \omega y) = f \left( \frac{y'}{y} + \omega \right) \), if \( y \neq 0 \), and \( f(y' + \omega y') = f(1) = f(\omega) \), if \( y = 0 \) and \( y' \neq 0 \). Thus, denoting by \( g \) the function defined on \( \mathbb{F}_{2^{2^{n/2}}} \) by \( g(z) = f(z + \omega) \), we have \( f(y' + \omega y) = g \left( \frac{y'}{y} \right) \) for every \( (y, y') \neq (0, 0) \), with \( \frac{y'}{y} = 0 \) if \( y = 0 \). If \( f(1) = 0 \), then we have \( f(y' + \omega y) = g \left( \frac{y'}{y} \right) \) for every \( y, y' \) and \( f \) belongs then to \( \mathcal{P}\mathcal{S}_{\text{ap}} \). If \( f(1) = 1 \), then, choosing \( \delta \in \mathbb{F}_{2^n}^* \) such that \( f(\frac{1}{\delta}) = 0 \), we can apply the proof above to the function \( f'(x) = f \left( \frac{x}{\delta} \right) \). \( \square \)

We denote by \( \mathcal{P}\mathcal{S}^\#_{\text{ap}} \), the class of hyper-bent functions described in Propositions 3 and 4, extended by the addition of the two constant functions.

**Remarks.**

1. The functions of the class \( \mathcal{P}\mathcal{S}^\#_{\text{ap}} \) are the functions of weight \( 2^{n-1} \pm 2^{n/2-1} \) such that \( f(x^{2^{n/2}+1}x) = f(x) \).

2. From [27] the number of \( \mathcal{P}\mathcal{S}^\#_{\text{ap}} \) functions with \( n \) variables is \( 2 \left( \frac{2^{n/2}+1}{2^{2^{n/2}}-1} \right) \).

Note that the definition of \( \mathcal{P}\mathcal{S}_{\text{ap}} \) depends on the identification chosen between the vectorspaces \( \mathbb{F}_{2^{2^{n/2}}} \) and \( \mathbb{F}_{2^n} \). Note also that, thanks to Proposition 4, there is no need to prove that these functions have degree \( n/2 \), since Dillon proved it in [12], whereas Youssef and
Thus, if $z$ had to prove it. Let us give here a different proof of their hyper-bentness:

An alternative proof that the functions of class $\mathcal{PS}_{ap}$ are hyper-bent: Let $\omega$ be any element in $F_{2^n} \setminus F_{2^{n/2}}$. As above, we have $F_{2^n} = F_{2^{n/2}} + \omega F_{2^{n/2}}$. Moreover, every element $y$ of $F_{2^{n/2}}$ satisfies $y^2 = y$ and therefore, we have $Tr(y) = 0$. Consider the inner product in $F_{2^n}$ defined by: $y \cdot y' = Tr(y y')$; the subspace $F_{2^{n/2}}$ is its own orthogonal; hence, the sum $\sum_{y \in F_{2^{n/2}}} (-1)^{Tr(\lambda y)}$ is null if $\lambda \notin F_{2^{n/2}}$ and equals $2^{n/2}$ if $\lambda \in F_{2^{n/2}}$.

Consider any element of the class $\mathcal{PS}_{ap}$, i.e. choose a balanced Boolean function $g$ on $F_{2^n}$, vanishing at 0, and define $f(y' + \omega y) = g\left(\frac{y'}{y}\right)$, with $\frac{y'}{y} = 0$ if $y = 0$. For every $a \in F_{2^n}$, we have

$$\sum_{x \in F_{2^n}} (-1)^{f(x) + Tr(a \cdot x')} = \sum_{y, y' \in F_{2^{n/2}}} (-1)^{g\left(\frac{y'}{y}\right) + Tr(a (y' + \omega y))}.$$

Denoting $\frac{y'}{y}$ by $z$, we see that the sum $\sum_{y \in F_{2^{n/2}}, y' \in F_{2^{n/2}}} (-1)^{g\left(\frac{y'}{y}\right) + Tr(a (y' + \omega y))}$ equals

$$\sum_{z \in F_{2^{n/2}}, y \in F_{2^{n/2}}} (-1)^{g(z) + Tr(a (z + \omega) y)}.$$ The sum $\sum_{y' \in F_{2^{n/2}}} (-1)^{g(0) + Tr(a y^i)}$ equals $(-1)^{g(0)} 2^{n/2}$ if $a \in F_{2^{n/2}}$ and is null otherwise.

Thus, $\sum_{x \in F_{2^n}} (-1)^{f(x) + Tr(a \cdot x')} = \sum_{z \in F_{2^{n/2}}} (-1)^g(z) \sum_{y \in F_{2^{n/2}}} (-1)^{Tr(a(z + \omega) y) y^i} = \sum_{z \in F_{2^{n/2}}} (-1)^g(z) + (-1)^g(0) 2^{n/2} 1_{F_{2^{n/2}}}(a)$.

The sum $\sum_{z \in F_{2^{n/2}}} (-1)^g(z)$ is null since $g$ is balanced.

The sum $\sum_{z \in F_{2^{n/2}}} (-1)^g(z) \sum_{y \in F_{2^{n/2}}} (-1)^{Tr(a(z + \omega) y) y^i}$ equals $\pm 2^{n/2}$ if $a \notin F_{2^{n/2}}$, since we prove in the next Lemma that there exists exactly one $z \in F_{2^{n/2}}$ such that $a(z + \omega) y^i \in F_{2^{n/2}}$; and this sum is null if $a \in F_{2^{n/2}}$ (this can be checked, if $a = 0$ thanks to the balancedness of $g$, and if $a \neq 0$ because $y^i$ ranges over $F_{2^{n/2}}$ and $a(z + \omega) y^i \notin F_{2^{n/2}}$). This completes the proof. □

**Lemma 1.** Let $n$ be any positive integer. Let $a$ and $\omega$ be two elements of the set $F_{2^n} \setminus F_{2^{n/2}}$ and let $i$ be coprime with $2^n - 1$. There exists a unique element $z \in F_{2^{n/2}}$ such that $a(z + \omega) y^i \in F_{2^{n/2}}$.

**Proof.** Let $j$ be the inverse of $i$ modulo $2^n - 1$. We have $a(z + \omega) y^i \in F_{2^{n/2}}$ if and only if $z \in \omega + a^{-j} \times F_{2^{n/2}}$. The sets $\omega + a^{-j} \times F_{2^{n/2}}$ and $F_{2^{n/2}}$ are two flats whose directions $a^{-j} \times F_{2^{n/2}}$ and $F_{2^{n/2}}$ are subspaces whose sum is direct and equals $F_{2^{n}}$. Hence, they have a unique vector in their intersection. □

**Remarks.** (1) The automorphism group of the class of hyper-bent functions is different from that of the class of bent functions (which equals the general affine group). Indeed, it is a simple matter to show, for instance, that it does not contain the mapping $x \mapsto x + 1$. And
it obviously contains all the mappings \( x \mapsto ax^j \) \((a \in F_{2^n}; i \text{ coprime with } 2^n - 1)\), whereas these mappings do not belong to the automorphism group of the class of bent functions, except if \( i \) is a power of 2. We conjecture that the automorphism group of the class of hyper-bent functions equals the set of all the mappings \( x \mapsto ax^j \) \((a \in F_{2^n}; i \text{ coprime with } 2^n - 1)\).

(2) The expression of the elements of class \( \mathcal{P} \mathcal{S}_{ap}^\# \) in terms of Proposition 3 shows that the automorphism group of \( \mathcal{P} \mathcal{S}_{ap}^\# \) equals this same group. Note that the dual of any function in \( \mathcal{P} \mathcal{S}_{ap}^\# \) belongs to \( \mathcal{P} \mathcal{S}_{ap}^\# \), and is therefore hyper-bent.

3. Cyclic codes and their relationship with hyper-bent and bent functions

3.1. Background on cyclic codes

In all this subsection, we refer to [21,24]. Let \( N = 2^n - 1 \) for \( n \) a positive integer and let \( a \) be a primitive element of \( F_{2^n} \). Let \( C \) be a binary cyclic code of length \( N \) with generator polynomial \( g(X) \) in \( F_2[X]/(X^N + 1) \). The polynomial \( g(X) \) is the product of some minimal polynomials \( M_i(X) \), \( i \in I \), for \( M_i(X) = \prod_{j \in C_i} (X - \alpha^j) \), where \( C_i \) is the 2-cyclotomic coset of \( i \) modulo \( 2^n - 1 \). The roots of \( g(X) \) are the elements \( \alpha^j \), where \( j \) belongs to the defining set \( T = \sqcup_{i \in I} C_i \). These elements \( \alpha^j \) are called the zeroes of the cyclic code. The elements \( \alpha^j \) where \( j \in \{0, \ldots, 2^n - 2\} \) and \( j \not\in \sqcup_{i \in I} C_i \) are called the non-zeroes of the cyclic code. The dimension of \( C \) equals the number of non-zeroes of the code. Every element \((f_0, f_1, \ldots, f_{N-1})\), identified with the polynomial \( f(X) = f_0 \oplus f_1 X \oplus \cdots \oplus f_{N-1} X^{N-1} \), belongs to \( C \) if and only if \( f(X) \) vanishes at every zero \( \alpha^j \) of the code, that is, if and only if \( f_0 + f_1 \alpha^j + \cdots + f_{N-1} \alpha^{(N-1)j} = 0 \) for every such \( j \). Note that, \( N \) being equal to \( 2^n - 1 \), the vector \((f_0, f_1, \ldots, f_{N-1})\) can be identified with the restriction of a Boolean function \( f \) to the set \( F_{2^n} \), defined by \( f(\alpha^j) = f_i \), for every integer \( i = 0, \ldots, 2^n - 2 \).

A cyclic code \( C \) of length \( N \) being given, the extended code of \( C \) is the set of vectors \((f_{-\infty}, f_0, \ldots, f_{N-1})\), where \( f_{-\infty} = f_0 \oplus \cdots \oplus f_{N-1} \). It is a linear code of length \( N + 1 \) and of the same dimension as \( C \). The vector \((f_{-\infty}, f_0, f_1, \ldots, f_{N-1})\) can be identified with a Boolean function \( f \) on \( F_{2^n} \) whose algebraic degree is smaller than \( n \).

The Reed–Muller code \( R(d, n) \) is an extended cyclic code for every \( d < n \) (see [21,24]): the zeroes of the corresponding cyclic code \((R^*(d, n), \text{the punctured Reed–Muller code of order } d)\) are the elements \( \alpha^j \) such that \( 1 \leq j \leq 2^n - 2 \) and such that the number of 1’s in the binary expansion of \( j \) (its 2-weight) is at most equal to \( n - d - 1 \). For \( d = n - 2 \), this gives the extended Hamming code. The non-zeroes of \( R^*(1, n) \) are the elements \( \alpha^j \) for \( i \) in \( \{0\} \cup C_{-1} \).

Cyclic codes can also be considered in terms of the trace function. Any codeword of a cyclic code with non-zeroes \( \alpha^j \) for \( i \in C_{u_1} \cup \cdots \cup C_{u_l} \), can be represented as \( \sum_{i=1}^l Tr(a_i x^{-u_i}) \), \( a_i \in F_{2^n} \). A more compact representation uses the trace functions from \( F_{2^{2n}} \) to \( F_2 \), where \( n_i \) is the size of \( C_{u_i} \) (see [21, p. 579]) but we shall not need it here.

We now cite a simple result on the divisibility of certain cyclic codes. This result can be considered in terms of degenerate cyclic codes ([21, p. 223]) and also in terms of results of divisibility in [2].
Proposition 5. Let $C$ be a cyclic code of odd length $N$ over $F_2$ with defining set $T$. Assume that some positive integer $d$ divides $N$ as well as all the elements of $\{1, \ldots, N-1\} \setminus T$. Then $d$ divides the weight of any codeword of $C$. More precisely, $C$ is the repetition of $d$ times a shorter code.

3.2. Extended cyclic codes and hyper-bent functions

Since, according to Rothaus’ bound, the algebraic degree of any bent function is upper bounded by $n/2$, every bent function belongs to the Reed–Muller code of order $n/2$. As we said above, it is a simple matter to generate at random the elements of this extended code, but, unfortunately, the proportion of bent functions among the elements of this extended cyclic code is too small to find bent functions by generating random codewords.

In the case of hyper-bent functions, there exists a code with relatively small dimension which contains all hyper-bent functions:

Proposition 6. All hyper-bent functions on $n$ variables belong to the extended cyclic code $H_n$ whose zeroes are all the elements of the form $x^j$, where $i$ is coprime with $2^n - 1$ and $1 \leq j \leq 2^n - 2$ has 2-weight at most $n/2 - 1$.

Proof. According to Proposition 2, every hyper-bent function belongs to the intersection of all the images of the Reed–Muller code of order $n/2$ by the mappings $f \mapsto f(x^i)$, where $i$ is coprime with $2^n - 1$. The proposition follows. □

For $i$ an integer, let us denote by $w_2(i)$ the 2-weight of $u = i \mod (2^n - 1)$ with $0 \leq u \leq 2^n - 2$ (hence, $w_2(-i) = w_2(2^n - 1 - i)$).

We will need the following simple lemma on $w_2$:

Lemma 2. For any $1 \leq a \leq 2^n - 2$: $w_2(a) + w_2(-a) = n$.

Proof. If $a = \sum_{i=0}^{n-1} a_i 2^i$ with $a_i \in \{0, 1\}$, then $2^n - 1 - a = \sum_{i=0}^{n-1} (1 - a_i) 2^i$, and $w_2(a) + w_2(-a) = w_2(a) + w_2(2^n - 1 - a) = \sum_{i=0}^{n-1} a_i + \sum_{i=0}^{n-1} (1 - a_i) = n$. □

We can then characterize $H_n$ in terms of its non-zeroes:

Proposition 7. The non-zeroes of $H_n$ are the $x^j$’s such that $j$ is zero or $j$ satisfies that the 2-weight of $ij$ is equal to $n/2$ for any $i$ coprime with $2^n - 1$.

Proof. Proposition 6 implies that the non-zeroes of $H_n$ are the $x^j$’s such that $j$ is zero or $j$ satisfies that the 2-weight of $ij$ is greater or equal to $n/2$ for any $i$ coprime with $2^n - 1$. Now let $x^j$ be a non-zero of $H_n$. If $i$ is coprime with $2^n - 1$ then $-i$ is also coprime with $2^n - 1$, therefore since $w_2(ij) \geq n/2$ and $w_2(-ij) \geq n/2$, Lemma 2 assures $w_2(ij) = w_2(-ij) = n/2$. □

According to the property, recalled in Section 3, on the representation of the codewords of cyclic codes by means of the trace function, we deduce:
Theorem 1. Every hyper-bent function $f : F_{2^n} \rightarrow F_2$, can be represented as: $f(x) = \sum_{i=1}^n \text{Tr}(a_i x^i) \oplus e$, where $a_i \in F_{2^n}$, $e \in F_2$ and $w_2(t_i) = n/2$. Consequently, all hyper-bent functions have algebraic degree $n/2$.

Remark. We have recalled at Section 3.1 that Boolean functions admit a representation of the form $f(x) = \sum_{i=1}^n \text{Tr}(a_i x^i) \oplus e$, where $a_i \in F_{2^n}$, $e \in F_2$ and where the $t_i$'s are the representatives of 2-cyclotomic cosets modulo $2^n - 1$. Rothaus’ bound together with the fact that $f$ is hyper-bent if and only if $f(x^i)$ is bent for every $i$ coprime with $2^n - 1$ and Lemma 2 imply directly Theorem 1. So the coding theoretic viewpoint is not indispensable here. However, we shall see in the sequel that it brings more insight on the problem of knowing whether hyper-bent functions exist outside class $PS_{ap}$.

Since $H_n$ contains $PS_{ap}$, we know it is not reduced to the set of constant functions. We identify a subset of non-zeroes of $H_n$ in the following proposition.

Definition 1. Let $i$ be an element of the ring of integers modulo $2^n - 1$. One says that $i$ is symmetric if $i$ and $-i$ belong to the same 2-cyclotomic coset modulo $2^n - 1$. We define $B_n$ the code with non-zeroes $\alpha i$ for $i$ symmetric.

Note that $i$ is symmetric if and only if there exists an integer $j$ such that $2^n - 1$ divides $i(2^j + 1)$. Clearly, the set of symmetric elements is an ideal of the ring of integers modulo $2^n - 1$.

Proposition 8. Every $\alpha i$ for $i$ a symmetric element is a non-zero of $H_n$, and $B_n$ is a subcode of $H_n$.

Proof. Let $j$ be symmetric. First remark that the 2-weight is constant in any 2-cyclotomic coset. From Lemma 2, we have that if $j \neq 0$, $w_2(j) + w_2(-j) = n$ and then $w_2(j) = w_2(-j) = n/2$. Since the set of symmetric elements is an ideal of the ring of integers modulo $2^n - 1$, we deduce that for any $i$, $w_2(ij) = n/2$, hence $\alpha j$ is a non-zero of $H_n$, according to Proposition 7. □

In the next proposition we give a description of the symmetric elements and we deduce the dimension of $B_n$. We first recall two classical lemmas of number theory:

Lemma 3. Let $n$ be (uniquely) written in the form $n = 2^r p$ with $p$ odd. Then $2^n - 1 = (2^p - 1) \prod_{k=1}^r (2^{n/2^k} + 1)$ where all the factors of the product are pairwise coprime.

Proof. The fact that $2^n - 1 = (2^p - 1) \prod_{k=1}^r (2^{n/2^k} + 1)$ is obvious. Two factors $2^{n/2^k} + 1$ and $2^{n/2^l} + 1$ ($k > l$) are coprime since $2^{n/2^k} + 1$ is a divisor of $2^{n/2^l} - 1$ and since $2^{n/2^l} - 1$ and $2^{n/2^l} + 1$ are coprime. And $2^p - 1$ is coprime with any factor $2^{n/2^k} + 1$ since it is coprime with $2^p + 1$ and since if $k < r$ then it divides $2^{n/2^k} - 1$. □

For any integer $n$, written uniquely as $n = 2^r p$, with $p$ odd, let us define $v_2(n) = r$. 

Lemma 4. Let $n$ and $j$ be two integers with $n$ even, the following holds:
if $v_2(j) \geq v_2(n)$ then $gcd(2^j + 1, 2^n - 1) = 1$,
if $v_2(j) \leq v_2(n) - 1$ then $gcd(2^j + 1, 2^n - 1) = 2^{gcd(j, \frac{n}{2})} + 1$.

Proof. This simple result can be obtained by first decomposing $2^n - 1$ as in Lemma 3
and then by using classical methods of number theory which can for instance be found in
([20, Exercise 125]).

We now give the dimension of $B_n$, we also give a proof although this result may be
already known:

Proposition 9. Let us write $n = 2^r p$ for $p$ odd and $r \geq 1$. The symmetric elements of $(2^n - 1)$
are the multiples of $(2^n - 1)$ divided by one of its factors $2^{n/2^k} + 1$. The dimension of $B_n$ is
$1 + \sum_{k=1}^{r} 2^{n/2^k}$.

Proof. We know that $i$ (considered as an element of the ring of integers modulo $2^n - 1$)
is symmetric if and only if there exists an integer $j$ such that $2^n - 1$ divides $i(2^j + 1)$. Hence,
every multiple of $2^n - 1$ divided by one of its factors $2^{n/2^k} + 1$ is symmetric. Being pairwise
disjoint by Lemma 3, for $i$ ranging over $\{1, \ldots, r\}$, the number of such nonzero multiples
equals $1 + \sum_{k=1}^{r} 2^{n/2^k}$.

Let us prove that these elements are the only symmetric elements. Let $i$ be symmetric
then there exists an integer $j$ and an integer $t$ such that $i(2^j + 1) = t(2^n - 1)$. From
Lemma 4, one gets either $gcd(2^j + 1, 2^n - 1) = 1$, in which case $i \equiv 0 \pmod{2^n - 1}$,
or $gcd(2^j + 1, 2^n - 1) = 2^{gcd(j, \frac{n}{2})} + 1$. In the latter case one obtains
$i = t' \cdot \frac{2^{n-1}}{2^{gcd(j, \frac{n}{2})} + 1}$
where $t' = \frac{t(2^{gcd(j, \frac{n}{2})} + 1)}{2^j + 1}$ is an integer. Now necessarily in this case $v_2(j) \leq v_2(n) - 1$ and
gcd($j, \frac{n}{2}$) = $2v_2(j)q$ for $q$ odd and $q$ divides $p$. Since any integer of the form $x + 1$ divides
$x^s + 1$ for $s$ odd we deduce that there exists $1 \leq k \leq r$ such that $(2^{gcd(j, \frac{n}{2})} + 1)$ divides
$(2^{n/2^k} + 1)$ and the result follows.

We look now at the relationship between $B_n$ and $\mathcal{PS}_{ap}^d$. We begin with a direct conse-
cquence of Proposition 9.

Lemma 5. For any positive even $n$ and any non-negative $a \leq 2^{n/2}$, the integer $a(2^{n/2} - 1)$
(considered as an element of the ring of integers modulo $2^n - 1$) is symmetric.

Thus, $B_n$ contains as a subcode the extended cyclic code $A_n$ whose non-zeroes are the
powers of $\alpha$ whose exponents are all the multiples of $2^{n/2} - 1$. This code has a tight
relationship with class $\mathcal{PS}_{ap}^d$:

Theorem 2. The functions of class $\mathcal{PS}_{ap}^d$ are those codewords of weights $2^{n-1} \pm 2^{n/2-1}$
of the extended cyclic code $A_n$ of length $2^n$, whose non-zeroes are $\alpha^{a(2^{n/2} - 1)}$ for $0 \leq a \leq 2^{n/2}$.
Equivalently, the $\mathcal{PS}_{ap}^d$ functions are the functions of weight $2^{n-1} \pm 2^{n/2-1}$ which can be
written as $\sum_{i=1}^{\ell} Tr(a_i x^{j_i})$ for $a_i \in F_{2^n}$ and $j_i$ a multiple of $2^{n/2} - 1$ with $j_i \leq 2^n - 1$. 
Proof. Let \( f \) be a \( \mathcal{PS}^\# \) function, then by definition, if one changes \( x \) into \( x^{2^n/2+1}x \) in the sum \( \sum_{x \in F_{2^n}} x^i f(x) \), we obtain \( x^{(2^n/2+1)} \sum_{x \in F_{2^n}} x^i f(x) \), since \( f(x^{2^n/2+1}) = f(x) \). Hence, we have
\[
(1 + x^{(2^n/2+1)}) \sum_{x \in F_{2^n}} x^i f(x) = 0.
\]
Therefore, if \( i(2^n/2 + 1) \) is not a multiple of \( 2^n - 1 \), i.e. if \( i \) is not a multiple of \( 2^n/2 - 1 \), then \( \sum_{x \in F_{2^n}} x^i f(x) = 0 \), and \( x^i \) is a zero of the polynomial \( \sum_{j=0}^{2^n-2} f(a^j)x^j \) representing the Boolean function \( f \). In other words, all the functions of \( \mathcal{PS}^\# \) are contained in the code \( A_n \).

Conversely, let \( f \) be an element of weight \( 2^{n-1} \pm 2^{n/2-1} \) in \( A_n \), represented by the polynomial \( f(X) = f_0 + f_1 X + \cdots + f_{2^n-2} X^{2^n-2} \). The generator polynomial of the cyclic code \( A_n \) is \( g(X) = X^{2^n-1} - 1 = \sum_{i=0}^{2^n/2-2} X^{(2^n/2+1)i} \), since this polynomial admits as root any \( x^i \) such that \( i \) is not a multiple of \( 2^n/2 - 1 \), and since its degree \( (2^n/2 + 1)(2^n/2 - 2) \) equals the number of these roots. Then we have \( X^{2^n/2+1}g(X) = g(X) \), and this implies \( f_{i+2^n/2+1} = f_i \) for every \( i = 0, 1, \ldots, 2^n - 2 \), that is, viewing now \( f \) as a Boolean function, \( f(x^{2^n/2+1}) = f(x) \) for every \( x \in F_{2^n}^* \). If \( f(0) = 0 \), then the restriction of \( f \) to \( F_{2^n}^* \) has the same weight as \( f \). Hence, according to Proposition 5 applied with \( d = 2^{n/2} - 1 \), \( f \) has then weight \( 2^{n-1} - 2^{n/2-1} \) and the vector \( \left( f(1), f(x), f(x^2), \ldots, f(x^{2^n/2}) \right) \) has therefore weight \( 2^{n/2-1} \). Thus, \( f \) belongs to the class described in Proposition 3. If \( f(0) = 1 \), then applying this property to the function \( f \oplus 1 \) completes the proof. \( \square \)

Remarks

(1) According to Proposition 9 when \( n \equiv 2 \) (mod 4), \( A_n = B_n \) since they have the same non-zeroes,
(2) When \( n \equiv 0 \) (mod 4), \( A_n \) is strictly included in \( B_n \) (and therefore in \( H_n \)). Indeed:

(i) for any \( 1 \leq a \leq 2^{n/4} \), \( x^{(2^n/2+1)(2^n/4)} \) is a non-zero of \( B_n \),
(ii) for any \( 1 \leq a \leq 3 \), \( x^{d(2^n-1)/3} \) is a non-zero of \( B_n \).

Meanwhile there exist values of \( n \) such that \( H_n = A_n \):

Theorem 3. Let \( n \geq 6 \) and \( n \equiv 2 \) (mod 4), if there is no divisor \( d \) of \( 2^n - 1 \) such that \( w_2(d) = n/2 \), except the multiples of \( 2^{n/2} - 1 \), then \( H_n = A_n \).

Proof. Assume that all the divisors of \( 2^n - 1 \) have 2-weight different from \( n/2 \), except the multiples of \( 2^{n/2} - 1 \). Let \( \alpha^a \) be a non-zero of \( H_n \), with \( a \) not a multiple of \( 2^{n/2} - 1 \) and let \( d = gcd(a, 2^n - 1) \) then \( a = bd \) with \( gcd(b, 2^n - 1) = 1 \). In which case, \( b \) is invertible modulo \( 2^n - 1 \). From the definition of hyper-bent functions, \( w_2(b^{-1}a) \) must equal \( n/2 \); thus \( w_2(d) = n/2 \) which is impossible. \( \square \)

Corollary 1. Let \( n \geq 6 \) and \( n \equiv 2 \) (mod 4), if \( n \) is such that \( 2^{n/2} - 1 \) and \( 2^{n/2+1}/3 \) are prime numbers, then \( H_n = A_n \).

Proof. In that case, the only possible divisors of \( 2^n - 1 \) which are not multiples of \( 2^{n/2} - 1 \) are 3, \( 2^{n/2+1}/3 \) and \( 2^{n/2} + 1 \). We notice that \( 2^{n/2+1}/3 = 1 + \sum_{i=1}^{n/2} 2^{2i-1} \), and then none of these three possible divisors has 2-weight \( n/2 \). \( \square \)
Table 1
Codes $H_n$ for $4 \leq n \leq 12$

<table>
<thead>
<tr>
<th>$n$</th>
<th>Dim</th>
<th>Non-zeroes cosets of $H_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>7</td>
<td>0, 3, 5</td>
</tr>
<tr>
<td>6</td>
<td>9</td>
<td>0, 7, 21</td>
</tr>
<tr>
<td>8</td>
<td>23</td>
<td>0, 15, 45, 51, 85</td>
</tr>
<tr>
<td>10</td>
<td>33</td>
<td>0, 31, 93, 155, 341</td>
</tr>
<tr>
<td>12</td>
<td>73</td>
<td>0, 63, 189, 315, 441, 455, 693, 819, 1365</td>
</tr>
</tbody>
</table>

Table 2
Number of hyper-bent functions

| $n$ | Hyper-bent | $|\mathcal{PS}^\#_{ap}|$ | Number of words of weight $2^{n-1} \mp 2^{n/2}$ of $H_n$ |
|-----|------------|--------------------------|--------------------------------------------------|
| 4   | 56         | 20                       | 56                                               |
| 6   | 252        | 252                      | 252                                              |
| 8   | 48 620     | 48 620                   | 785 188                                          |
| 10  | 2 333 606 220 | 2 333 606 220       | 2 333 606 220                                   |
| 12  | ?          | $2 \left( \frac{65}{32} \right)$ | $\leq 2^{73}$                                   |

Example. For instance the previous corollary can be applied for $n = 6, 10$ and 14 and Theorem 3 for $n = 18$.

3.3. Numerical results on hyper-bent functions for $4 \leq n \leq 12$

The code $H_n$ has relatively small dimension. We sum up in Table 1 the dimension of $H_n$ and we indicate representatives of the 2-cyclotomic cosets $C_j$ corresponding to the non-zeroes of the code $H_n$.

Potential hyper-bent functions in the code $H_n$ correspond to codewords of weights $2^{n-1} \mp 2^{n/2-1}$ and $2^{n-1} + 2^{n/2-1}$; the number of these codewords is given in Table 2, together with the number of hyper-bent functions, for $4 \leq n \leq 12$, when it is known.

Note that in the same way that one can check the bentness of a codeword $f$ of length $2^n$ by computing the weight distribution of $f + R(1, n)$, one can check the hyper-bentness of a codeword $f$ by computing the weight distributions of the sums of $f$ and of the extended cyclic codes with non-zeroes $\alpha^j$, $j \in \{0\} \cup C_i$; for $i$ coprime with $2^n - 1$. Indeed, the non-zeroes of $RM(1, n)$ are $\alpha^j$, $j \in \{0\} \cup C_{-1}$ and $i$ is coprime with $2^n - 1$ if and only if $-i$ is coprime with $2^n - 1$.

Since we know that all the elements of class $\mathcal{PS}^\#_{ap}$ are hyper-bent, it is natural to specify the relationship between $\mathcal{PS}^\#$ and the set of hyper-bent functions. We saw that for $n = 6, 10$ and 14, $H_n = A_n$ and the only hyper-bent functions are then the elements of $\mathcal{PS}^\#_{ap}$. We completed Table 2 by computing, for $n = 4$ and 8, the number of all possible hyper-bent functions of $H_n$. We sum up in the following what we know on hyper-bent functions for $4 \leq n \leq 12$. 
• \( n = 4 \): 26 of the 56 hyper-bent functions have a dual function which is also hyper-bent, among which 20 are in class \( \mathcal{PS}^\#_{ap} \). We observed that the 20 functions which are in class \( \mathcal{PS}^\#_{ap} \) correspond to the words of weights 6 and 10 of the extended cyclic codes with non-zeroes \( x^j, \ j \in \{0, C_3\} \).

• \( n = 6 \): in that case, there are 252 hyper-bent functions which are all in class \( \mathcal{PS}^\#_{ap} \).

• \( n = 8 \): there are 48 620 hyper-bent functions which are all in class \( \mathcal{PS}^\#_{ap} \).

• \( n = 10 \): there are 2 333 606 220 hyper-bent functions which are all in class \( \mathcal{PS}^\#_{ap} \).

• \( n = 12 \): in that case, we only know that the number of hyper-bent functions is upper bounded by the number of codewords of \( H_{12} \); all random choices of hyper-bent functions we tried led to \( \mathcal{PS}^\#_{ap} \) functions.

Note that for \( n \leq 14 \) all the non-zeroes are completely described by the multiples of \( 2^{n/2} - 1 \) and the classes of Proposition 9.

Also hyper-bent functions which are not in \( \mathcal{PS}^\#_{ap} \) are only known for \( n = 4 \) at present.

**Proposition 10.** The only \( n \leq 100 \) and \( n \equiv 2 \pmod{4} \), for which there may exist hyper-bent functions, not belonging to \( \mathcal{PS}^\#_{ap} \), are \{22, 30, 46, 66, 70, 78, 86, 90\}.

**Proof.** This result is a direct application of Theorem 3. \( \square \)

**Remark.** Concerning the inclusion between \( B_n \) and \( H_n \), one may ask whether \( B_n = H_n \) in general? In fact computations show that this is true up to \( n = 20 \) but that for \( n = 22 \), \( B_n \) is strictly included in \( H_n \).

Eventually our results on hyper-bent functions raise the following natural question: Is it possible to find hyper-bent functions which are not in \( \mathcal{PS}^\#_{ap} \) (and therefore not in \( A_n \)) for \( n \geq 6 \)?

### 3.4. Extended cyclic codes and bent functions

Now we want to construct bent functions using cyclic codes. We saw that the non-zeroes which are composed with multiples of \( 2^{n/2} - 1 \), lead to \( \mathcal{PS}^\#_{ap} \) functions. Another family of cyclic codes which lead to bent functions is the class of quadratic bent functions which correspond to the codewords of appropriate weights of \( RM(2, n) \). One may also cite the bent functions obtained through the Kasami exponent [14].

After non-exhaustive searches, we found potentially new bent functions. We constructed bent functions from cyclic codes for \( n = 6 \) (in this case all bent functions are classified but we can however observe constructions whose generalization may lead to new classes) and \( n = 12 \). We could relate these functions to infinite classes of bent functions. This will be the subject of a forthcoming paper, with more co-authors.

• \( n = 6 \): the code with non-zeroes \( x^j, \ j \in \{0, C_7, C_{21}, C_{27}\} \) has 392 words of weights 28 and 36 which correspond all to bent functions (to be compared with the 252 hyper-bent functions).
\( n = 12 \): the code with non-zeroes \( x^j \), \( j \in \{0, C_{1503}\} \) has 3640 words of weight 2016 and 2080 which contain 910 bent functions. All these bent functions are of degree 3.

Acknowledgments

We thank Gregor Leander for useful discussions. We also thank the anonymous referee who pointed out the existence and the dimension of the code \( B_n \).

References