On Semi-bent Functions and Related Plateaued Functions Over the Galois Field $\mathbb{F}_{2^n}$

Sihem Mesnager

Abstract Plateaued functions were introduced in 1999 by Zheng and Zhang as good candidates for designing cryptographic functions since they possess desirable various cryptographic characteristics. They are defined in terms of the Walsh–Hadamard spectrum. Plateaued functions bring together various nonlinear characteristics and include two important classes of Boolean functions defined in even dimension: the well-known bent functions and the semi-bent functions. Bent functions (including their constructions) have been extensively investigated for more than 35 years. Very recently, the study of semi-bent functions has attracted the attention of several researchers. Much progress in the design of such functions has been made. The chapter is devoted to certain plateaued functions. The focus is particularly on semi-bent functions defined over the Galois field $\mathbb{F}_{2^n}$ (n even). We review what is known in this framework and investigate constructions.

1 Introduction

The so-called plateaued functions in n variables (or r-plateaued functions) were introduced in 1999 by Zheng and Zhang in [54] for $0 < r < n$. They were first studied by these authors in [55, 56] and further by Carlet and Prouff in [7] as good candidates for designing cryptographic functions. The Walsh–Hadamard spectrum is a very important tool to define and design plateaued functions. An n-variable Boolean function is said to be r-plateaued if the values of its Walsh transform belong to the set $\{0, \pm 2^{\frac{n+r}{2}}\}$ for some fixed r, $0 \leq r \leq n$. Consequently, plateaued functions have low Hadamard transform, which provides protection against fast correlation attacks [33] and linear cryptanalysis [31]. It has been shown in [54] that plateaued functions are significant in cryptography as they possess desirable

S. Mesnager (✉)
Department of Mathematics, University of Paris VIII, LAGA (Laboratoire Analyse, Géometrie et Applications), UMR 7539, CNRS, Paris, France

University of Paris XIII, Sorbonne Paris Cité, 2 rue de la liberté, 93526 Saint-Denis Cedex, France
e-mail: smesnager@univ-paris8.fr

Ç.K. Koç (ed.), *Open Problems in Mathematics and Computational Science*,
DOI 10.1007/978-3-319-10683-0_11

various cryptographic characteristics such as high nonlinearity, resiliency, low additive autocorrelation, and high algebraic degree and satisfy propagation criteria. Plateaued functions bring together various nonlinear characteristics. They include three significant classes of Boolean functions: the well-known bent functions, the near-bent functions and the semi-bent functions. More precisely, the bent functions are exactly 0-plateaued functions, the near-bent (also called semi-bent in odd dimension) are 1-plateaued functions, and the semi-bent functions are 2-plateaued functions. 0-plateaued functions and 2-plateaued functions on $\mathbb{F}_{2^n}$ exist when n is even, while the 1-plateaued functions on $\mathbb{F}_{2^n}$ exist when n is odd.

For $r \in \{0, 1, 2\}$, r-plateaued functions have been actively studied and have attractive much attention due to their cryptographic, algebraic, and combinatorial properties.

In the mathematical field of combinatorics, bent functions (or 0-plateaued functions) are a special type of Boolean functions. Introduced and named in 1974 by Rothaus [46] in research not published until 1976, firstly studied by Dillon [14], bent functions are so called because they are as different as possible from all linear and affine functions (more precisely, they are at maximum Hamming distance from the set of all affine functions). They are extremal objects in combinatorics and Boolean function theory and have been studied for about 35 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 sequence theory, as difference sets, and especially in coding theory, as elements of Reed-Muller codes. Bent functions exist only with even number of inputs n and have 2-valued spectrum $\pm 2^{\frac{n}{2}}$. The definition of bent function has been extended in several ways, leading to different classes of generalized bent functions that share many of the useful properties of the original. A lot of research has been devoted to designing constructions of bent functions. The reader can refer to the book's chapter of Carlet [4] for general constructions of bent functions and to the following references [37, 41, 44] for a complete state of the art on bent functions defined over the Galois field $\mathbb{F}_{2^n}$, including the main constructions obtained until 2012.

Another special family of plateaued functions defined in even dimension is the set of semi-bent functions. The notion of *semi-bent function* has been introduced in 1994 by Chee et al. [11]. Nevertheless, these functions had been previously investigated in [2] under the name of three-valued almost optimal Boolean functions. Very recently, the development of the theory of semi-bent functions has increased. For very recent results on the treatment of semi-bent functions, we refer to [6,38–40,43]. The motivation for their study is firstly related to their use in cryptography (we recall that in the design of cryptographic functions, various characteristics need be considered simultaneously). Indeed, unlike bent functions, semi-bent functions can also be balanced and resilient. They also possess various desirable characteristics such as low autocorrelation, and a maximal nonlinearity among balanced plateaued functions, satisfy the propagation criteria, and have high algebraic degree. Secondly, besides their practical use in cryptography, they are also widely used in code division multiple access (CDMA) communication systems for sequence design

(see, e.g., [17, 19–21, 23, 24, 45]). In this context, families of maximum-length sequences (maximum-length linear feedback shift-register sequences) having three-valued cross-correlation are used. Such sequences have received a lot of attention since the late 1960s and can be generated by a semi-bent function [10]. Up to 2011, the main constructions of semi-bent functions in even dimension are either quadratic functions [48] or derived from power polynomials $Tr_1^n(x^d)$ for a suitably chosen d (see [10]). Since then, several constructions of semi-bent functions have been proposed in the literature. The principal engine of this progress is the result of several important observations in connection with the construction of bent functions [5, 36, 42]. We shall describe this more precisely in Sect. 4.2.

The chapter is devoted to certain plateaued functions. Special attention is directed to semi-bent functions. We review what is known in this context and investigate new constructions. The chapter is organized as follows. In Sect. 2, we fix our main notation and recall the necessary background. Section 3 is devoted to r-plateaued functions. We recall some basic concepts concerning these functions. In Sects. 3.1–3.3, we treat special classes of r-plateaued functions and present an overview related to the notion of bent, near-bent, and semi-bent functions, respectively. Next, in Sect. 4, we focus on the class of semi-bent functions. We survey the constructions discovered recently. We first point out the relationship between the semi-bentness property of some type of functions and some exponential sums (involving Dickson polynomials). Secondly, we emphasize the link between semi-bent functions and some bent functions. Finally, we study the new connections between semi-bent functions and oval polynomials from projective finite geometry and investigate several constructions. Open problems related to semi-bent functions are given in Sect. 4.

2 Background

For any set E, $E^\star = E \setminus \{0\}$ and $\#E$ will denote the cardinality of E. For any positive integer k, $\mathbb{F}_{2^k}$ denotes the finite field of order 2^k.

Let n be a positive integer. A Boolean function f is a map from the vector space $\mathbb{F}_2^n$ of all binary vectors of length n to the finite field with two elements $\mathbb{F}_2$, i.e., $f : \mathbb{F}_2^n \to \mathbb{F}_2$. The *Hamming weight of a Boolean function* f on $\mathbb{F}_2^n$, denoted by $wt(f)$, is the size of the support of the function,i.e., the set $\{x \in \mathbb{F}_2^n / \ f(x) \neq 0\}$. The *Hamming distance* $d_H(f, g)$ between two functions f and g is the size of the set $\{x \in \mathbb{F}_2^n / \ f(x) \neq g(x)\}$. Thus it equals $w_H(f \oplus g)$.

In cryptography, the most usual representation of these functions is the *algebraic normal form* (ANF) :

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right)$$

where the a_I's are in $\mathbb{F}_2$. The terms $\prod_{i\in I} x_i$ are called monomials. The *algebraic degree* of a Boolean function f equals the global degree of its (unique) ANF, that is, the maximum degree of those monomials whose coefficients are nonzero.

There exist several kinds of possible trace (univariate) representations of Boolean functions (see, e.g., [4, p. 266]) which are not necessary unique and use the identification between the vector space $\mathbb{F}_2^n$ and the field $\mathbb{F}_{2^n}$. A possible representation of Boolean functions using such an identification is to consider any Boolean function as a polynomial in one variable $x \in \mathbb{F}_{2^n}$ of the form $f(x) = \sum_{j=0}^{2^n-1} a_j x^j$ where the a_j's are elements of the field. This representation exists for every function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$, and such a function f is Boolean if and only if a_0 and a_{2^n-1} belong to $\mathbb{F}_2$ and $a_{2j} = a_j^2$ for every $j \neq 0, 2^n - 1$, where $2j$ is taken modulo $2^n - 1$. This allows representing $f(x)$ in a (unique) trace expansion. Recall that for any positive integer k, and r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$, denoted by Tr_r^k, is the mapping defined as

$$Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}}.$$

In particular, we denote the *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ by $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

A unique representation of a Boolean function over $\mathbb{F}_{2^n}$ by means of trace functions is of the form

$$f(x) = \sum_{j\in\Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1}) \tag{1}$$

called its *polynomial form*, where:

- Γ_n is the set of integers obtained by choosing one element in each cyclotomic class of 2 modulo $2^n - 1$ (the most usual choice for j is the smallest element in its cyclotomic class, called the coset leader of the class).
- $o(j)$ is the size of the cyclotomic coset of 2 modulo $2^n - 1$ containing j (recall that, the cyclotomic class of 2 modulo $2^n - 1$ denoted by $C(j)$ is defined as $C(j) := \{j, j2, j2^2, j2^3, \ldots, j2^{o(j)-1}\}$ where $o(j)$ is the smallest positive integer such that $j2^{o(j)} \equiv j \pmod{2^n - 1}$).
- $a_j \in \mathbb{F}_{2^{o(j)}}$.
- $\epsilon = wt(f)$ modulo 2 where $wt(f)$ is the *Hamming weight* of the image vector of f, that is, the cardinality of its support $\mathrm{supp}(f) := \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.

Note that the expression of f given by (1) 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 algebraic degree of f is then equal to the maximum 2-weight of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$. Recall that the 2-weight $w_2(j)$ of an integer j equals by definition the number of 1's in its binary expansion. In particular, affine functions are those of algebraic degree at most 1.

Quadratic functions are those of algebraic degree 2. They can be represented as follows: when n is even,

$$f(x) = \sum_{i=1}^{\frac{n}{2}-1} Tr_1^n(a_i x^{2^i+1}) + Tr_1^{\frac{n}{2}}(a_{\frac{n}{2}} x^{1+2^{\frac{n}{2}}})$$

where $a_i \in \mathbb{F}_{2^n}, \forall i, 0 \leq i \leq n/2$ and $a_{\frac{n}{2}} \in \mathbb{F}_{2^{n/2}}$.

When n is odd,

$$f(x) = \sum_{i=1}^{\frac{n-1}{2}} Tr_1^n(a_i x^{2^i+1}), a_i \in \mathbb{F}_{2^n}.$$

The rank of a quadratic function f is defined as follows:

$$\text{rank}(f) = n - \dim_{\mathbb{F}_2} \text{rad}(B_f)$$

where $\text{rad}(B_f) := \{x \in \mathbb{F}_{2^n} \mid B_f(x, y) = 0, \forall y \in \mathbb{F}_{2^n}\}$ with B_f the bilinear form defined as

$$B_f(x, y) := f(x + y) + f(x) + f(y).$$

Set $k_f := \dim_{\mathbb{F}_2} \text{rad}(B_f)$. Then 2 divides $(n - k_f)$. Any quadratic Boolean function on $\mathbb{F}_{2^n}$ has a rank $2t$ with $0 \leq t \leq \lfloor \frac{n}{2} \rfloor$ [29] and can be obtained as follows: set $\tilde{B}_f(x, y) := f(0) + f(x) + f(y) + f(x + y)$. Then the rank of f equals $2t$ if and only if the equation $\tilde{B}_f(x, y) = 0$ for any $y \in \mathbb{F}_{2^n}$ in x has exactly 2^{n-2t} solutions. The set $E_f := \{x \in \mathbb{F}_{2^n}, \mid \forall y \in \mathbb{F}_{2^n}, \tilde{B}_f(x, y) = 0\}$ is called the linear kernel of f.

Note that a significant result dealing with quadratic Boolean functions of rank $2t$ has been obtained by Helleseth and Kumar [21] (see Theorem 1).

The *bivariate representation* of Boolean functions is defined only when $n = 2m$ is even 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

$$\max_{(i,j) \mid a_{i,j} \neq 0} (w_2(i) + w_2(j)),$$

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 in two variables over $\mathbb{F}_{2^m}$.

Now, let f be a Boolean function over $\mathbb{F}_{2^n}$ and $a \in \mathbb{F}_{2^n}$. The derivative of f with respect to a is defined as

$$D_{af}(x) = f(x) + f(x + a), \forall x \in \mathbb{F}_{2^n}.$$

For $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, the second-order derivative of f with respect to (a, b) is defined as

$$D_b D_{af}(x) = f(x) + f(x + b) + f(x + a) + f(x + a + b), \forall x \in \mathbb{F}_{2^n}.$$

The notion of Walsh transform refers to a scalar product. When $\mathbb{F}_2^n$ is identified with the field $\mathbb{F}_{2^n}$ by an isomorphism between these two n-dimensional vector spaces over $\mathbb{F}_2$, it is convenient to choose the isomorphism such that the canonical scalar product "$\cdot$" in $\mathbb{F}_2^n$ coincides with the canonical scalar product in $\mathbb{F}_{2^n}$, which is the trace of the product : $x \cdot y = Tr_1^n(xy)$ for $x, y \in \mathbb{F}_{2^n}$.

If f is a Boolean function defined on $\mathbb{F}_{2^n}$, then the Walsh–Hadamard transform of f is the discrete Fourier transform of the sign function $\chi_f := (-1)^f$ of f, whose value at $\omega \in \mathbb{F}_{2^n}$ is defined as follows:

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\omega x)}.$$

The Walsh transform satisfies the well-known Parseval's relation

$$\sum_{\omega \in \mathbb{F}_{2^n}} \widehat{\chi_f}^2(\omega) = 2^{2n}.$$

Note that not all values of the Walsh–Hadamard transform can have the same sign, except when the function is affine. This comes from the fact that we then have $\left(\sum_{\omega \in \mathbb{F}_{2^n}} \widehat{\chi_f}(\omega)\right)^2 = \sum_{\omega \in \mathbb{F}_{2^n}} \widehat{\chi_f}^2(\omega)$ which implies that all these values are null except one (see, for instance, [42]).

The Walsh–Hadamard transform is an important tool for research in cryptography. It plays an important role to characterize many cryptographic criteria for Boolean functions but also to define some significant cryptographic Boolean functions used in various type of symmetric cryptosystems.

Finally, the rank of quadratic Boolean functions is connected with the distribution of its Walsh–Hadamard transform values. The following result concerning the distribution of the Walsh transform of quadratic Boolean functions is due to Helleseth and Kumar.

Table 1 Walsh spectrum of quadratic function with rank $2t$

Value of $\widehat{\chi_f}(\omega)$, $\omega \in \mathbb{F}_{2^n}$	Number of occurrences
0	2^{n-2t}
2^{n-t}	$2^{2t-1}+2^{t-1}$
-2^{n-t}	$2^{2t-1}-2^{t-1}$

Theorem 1 ([21]) *Let f be a quadratic Boolean function on $\mathbb{F}_{2^n}$ with rank $2t$, $0 \le t \le \lfloor \frac{n}{2} \rfloor$. Then the distribution of its Walsh transform is given in Table 1.*

3 Plateaued Functions

Plateaued Boolean functions can be defined as follows.

Definition 1 A Boolean function f defined over $\mathbb{F}_{2^n}$ is said to be r-plateaued if the values of its Walsh transform $\widehat{\chi_f}$ are in $\{0, \pm 2^{\frac{n+r}{2}}\}$, for some fixed r, $r = 0, 1, \ldots, n$.

The r-plateaued functions exist only when $n-r$ is even; equivalently, if n and r have the same parity (which implies that 2 divides $n+r$). The value $\lambda := 2^{\frac{n+r}{2}}$ is usually called *the amplitude*.

Remark 1 Note that if f is an r-plateaued function on $\mathbb{F}_{2^n}$, then its Walsh transform $\widehat{\chi_f}$ can be expressed by $\widehat{\chi_f} = ((-1)^g + (-1)^h)2^{\frac{n+r-2}{2}}$ for some Boolean g and h defined over $\mathbb{F}_{2^n}$.

Plateaued functions can be characterized by their second-order derivatives. More precisely:

Proposition 1 ([7]) *A Boolean function f on $\mathbb{F}_{2^n}$ is plateaued if and only if there exists λ (necessarily the amplitude of f) such that for every $x \in \mathbb{F}_{2^n}$*

$$\sum_{a,b \in \mathbb{F}_{2^n}} (-1)^{D_a D_b f(x)} = \lambda^2$$

where $D_a D_b f$ is the second-order derivative of f with respect to $(a,b) \in \mathbb{F}_{2^n}^2$.

A direct consequence of the previous proposition is that all the quadratic functions are plateaued. Several properties of plateaued functions have been studied. Concerning the degree of r-plateaued functions, it has been shown in [56] that for a given fixed n and r with $r > 0$, the maximum possible degree of r-plateaued on $\mathbb{F}_{2^n}$ is $\frac{n-r+2}{2}$ (while the maximum possible degree of 0-plateaued on $\mathbb{F}_{2^n}$ is $\frac{n}{2}$) and that this upper bound is sharp. Other properties of plateaued functions can be found in [2].

The existence of r-plateaued functions on $\mathbb{F}_{2^n}$ ($0 < r < n$) has been shown in [56]. However, there exist some results concerning the nonexistence of certain

types of plateaued functions. More precisely, Xia et al. have proved in [52] that there are no homogeneous[1] 0-plateaued of degree $\frac{n}{2}$ when $n \geq 4$. This result on the nonexistence of homogeneous 0-plateaued functions has been extended on one hand by Meng et al. [34] for functions of degree $\frac{n}{2}-k$ $(0 \leq k \leq \frac{n}{2})$ and on the other hand by Hyun et al. [22] for 0-plateaued functions f (not necessarily homogeneous) of minimum degree (i.e., the lowest degree among the degrees of nonconstant terms in f $\frac{n}{2}-k$ $(0 \leq k \leq \frac{n}{2})$. Moreover, very recently, it has been proved in [22] the nonexistence of r-plateaued functions on $\mathbb{F}_{2^n}$ $(0 < r < n)$ with certain degree for a given $n \geq N$ and r (where N is some integer depending on r). More precisely:

Proposition 2 ([22]) *For any nonnegative integer k, there exists an integer N such that for an integer $n \geq N$, there is no r-plateaued function $(0 < r < n)$ over $\mathbb{F}_{2^n}$ of minimum degree $\frac{n-r+2}{2}-k$, where N is the smallest integer satisfying $\binom{\frac{N+r}{2}+k}{r+k} < 2^{\frac{N+r-2}{2}}-1$.*

As a consequence, it has been shown in [22] that there is no homogeneous 1-plateaued function over $\mathbb{F}_{2^n}$ of degree $\frac{n+1}{2}$ when $n \geq 7$, and there is no homogeneous 2-plateaued function over $\mathbb{F}_{2^n}$ of degree $\frac{n}{2}$ when $n \geq 6$.

3.1 Plateaued Functions: The Special Class of 0-Plateaued Functions (Bent Functions)

Bent functions introduced in 1974 [14,46] are extremal objects in combinatorics and Boolean function theory. They are maximally nonlinear Boolean functions. Recall that the *nonlinearity* of a Boolean function f, denoted by $\mathrm{nl}(f)$, is defined as the minimum Hamming distance between f and all affine functions (i.e., of degree at most 1). It can be expressed by means of the Walsh transform as follows:

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{b \in \mathbb{F}_{2^n}} \left|\widehat{\chi_f}(b)\right|.$$

Because of the well-known Parseval's relation $\sum_{b \in \mathbb{F}_{2^n}} \widehat{\chi_f}(b)^2 = 2^{2n}$, $\mathrm{nl}(f)$ is upper bounded by $2^{n-1} - 2^{n/2-1}$. This bound is tight for n even.

Definition 2 Let n be an even integer. A Boolean function on $\mathbb{F}_{2^n}$ is said to be bent if the upper bound $2^{n-1} - 2^{n/2-1}$ on its nonlinearity $\mathrm{nl}(f)$ is achieved with equality.

Bent functions on $\mathbb{F}_{2^n}$ exist then only when n is even. We have the following main characterization of the bentness for Boolean functions in terms of the Walsh transform:

[1] A Boolean function f is said to be homogeneous of degree r if $f(x) = \sum_{i=0}^{2^n-1} a_i x^i$ where $a_i = 0$ for $wt(i) \neq r$, where $wt(i)$ is the Hamming weight of i.

Table 2 Walsh spectrum of bent functions (0-plateaued) f with $f(0) = 0$

Value of $\widehat{\chi_f}(\omega)$, $\omega \in \mathbb{F}_{2^n}$	Number of occurrences
$2^{\frac{n}{2}}$	$2^{n-1} + 2^{\frac{n-2}{2}}$
$-2^{\frac{n}{2}}$	$2^{n-1} - 2^{\frac{n-2}{2}}$

Proposition 3 *Let n be an even integer. A Boolean function f is then bent if and only if its Walsh transform satisfies $\widehat{\chi_f}(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_{2^n}$.*

Hence, the Walsh transform provides a basic characterization of bentness. However, for a given Boolean function f, the Walsh transform can definitely not be used in practice to test in an efficient way the bentness of f, especially if all its values are computed naively one at a time as exponential sums. Thanks to Parseval's identity, one can determine the number of occurrences of each value of the Walsh transform of a bent function (see Table 2).

Bent functions are not classified. A complete classification of these functions is elusive and looks hopeless. So it is important to design constructions in order to find as many of bent functions as possible. A good reference for general properties and general constructions of bent functions is the book's chapter of Carlet [4]. We refer to [37] and [41] for a survey and a general overview of the constructions discovered recently including the relationship between the bentness property of some type of bent functions and some exponential sums, namely, Kloosterman sums (involving Dickson polynomials). Finally, note that a nice construction of bent functions have been derived from plateaued functions in [8].

3.2 *Plateaued Functions: The Special Class of* 1*-Plateaued Functions (Near-Bent Functions)*

Near-bent functions (or 1-plateaued functions) on $\mathbb{F}_{2^n}$ exist only when n is odd. They are defined as follows.

Definition 3 Let n be an odd integer. A Boolean function on $\mathbb{F}_{2^n}$ is said to be near-bent if its Walsh transform satisfies $\widehat{\chi_f}(a) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ for all $a \in \mathbb{F}_{2^n}$.

Note that a function from $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is said to be almost bent if it has Walsh-Fourier spectrum $\{0, \pm 2^{\frac{n+1}{2}}\}$, that is, the same as a near-bent function. The difference between an almost bent function and a near-bent function is that almost bent functions map $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, whereas near-bent functions map $\mathbb{F}_{2^n} \to \mathbb{F}_2$. In this context, $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost bent if and only if each of the Boolean functions $x \mapsto Tr_1^n(vf(x))$ is near-bent, for all $v \in \mathbb{F}_{2^n}^\star$.

Thanks to Parseval's identity, one can determine the number of occurrences of each value of the Walsh transform of a near-bent function (see Table 3).

Table 3 Walsh spectrum of near-bent functions (1-plateaued) f with $f(0) = 0$

Value of $\widehat{\chi_f}(\omega)$, $\omega \in \mathbb{F}_{2^n}$	Number of occurrences
0	2^{n-1}
$2^{\frac{n+1}{2}}$	$2^{n-2} + 2^{\frac{n-3}{2}}$
$-2^{\frac{n+1}{2}}$	$2^{n-1} - 2^{\frac{n-3}{2}}$

Again from Parseval's identity, it is straightforward to see that the support of the Walsh transform $\widehat{\chi_f}$ of a near-bent function f on $\mathbb{F}_{2^n}$ is of cardinality 2^{n-1} (i.e., $\#\mathrm{supp}(\widehat{\chi_f}) = 2^{n-1}$).

In the particular case of quadratic functions, there exists a criterion on the near-bentness involving the dimension of the linear kernel (see, e.g., [10]). More precisely, it is well known (see Sect. 8.5.2 in [4]) that a quadratic Boolean function f over $\mathbb{F}_{2^n}$ has for Walsh support the set of elements $\alpha \in \mathbb{F}_{2^n}$ such that $Tr_1^n(\alpha x) + f(x)$ is constant on E_f, where $E_f := \{x \in \mathbb{F}_{2^n}, \mid \forall y \in \mathbb{F}_{2^n}, f(x+y) + f(x) + f(y) + f(0) = 0\}$ is the linear kernel of f. It has been proved that f is near-bent over $\mathbb{F}_{2^n}$, if and only if E_f has dimension 1 (i.e., has size 2). Note that from Theorem 1, it is easy to see that quadratic Boolean function f is near-bent if and only if the rank of f is $n-1$, that is, $k_f = 1$.

Several constructions of quadratic near-bent functions have been obtained in the literature. We give a list of the known families of quadratic near-bent functions on $\mathbb{F}_{2^n}$, n odd:

- $f(x) = Tr_1^n(x^{2^i+1})$, $gcd(i,n) = 1$ [17].
- $f(x) = \sum_{i=1}^{\frac{n-1}{2}} Tr_1^n(x^{1+2^i})$ [1].
- $f(x) = \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} c_i Tr_1^n(x^{1+2^i})$, $c_i \in \mathbb{F}_2$ [10].
- $f(x) = Tr_1^n(x^{2^i+1} + x^{2^j+1} + x^{2^t+1})$, $1 \le i < j \le t \le \frac{n-1}{2}$, $i + j = t$,$gcd(n,i) = gcd(n,j) = gcd(n,i+j) = 1$ [10].
- $f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr_1^n(x^{1+2^i})$, $c_i \in \mathbb{F}_2$, $gcd(x^n+1, c(x)) = x+1$ where $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$ [24].
- $f(x) = Tr_1^n(x^{2^i+1}) + Tr_1^n(x^{2^i+1})$, $gcd(n, i+j) = gcd(n, i-j)$ [24].
- $f(x) = \sum_{i=0}^{r} Tr_1^n(x^{1+2^{k+id}})$, $gcd(2k+rd, n) = 1$ [24].
- $f(x) = \sum_{i=1}^{\frac{q-1}{2}} Tr_1^n(x^{1+2^{pi}}) + Tr_1^n(x^{1+2^q})$, $n = pq$, $3 \not| p$, p odd, q odd, $gcd(p,q) = 1$ [16].

Because bent functions exist in even dimensions and near-bent functions exist in odd dimensions, the possibility exists of moving up and down between bent and near-bent functions. The four possibilities are discussed in [26]; see also some results in [2]. In [27], Leander and McGuire have considered the problem on going up from a near-bent function to a bent function and proposed constructions. In particular, it has been shown that two n-variable functions g and h (n odd) are near-bent with complementary Walsh supports (i.e., $\mathrm{supp}(\widehat{\chi_g}) \cap \mathrm{supp}(\widehat{\chi_h}) = \emptyset$) if and only if the $(n+1)$-variable function $x \mapsto f(x, x_{n+1}) = g(x) + x_{n+1}h(x)$; $x \in \mathbb{F}_2^n$, $x_{n+1} \in \mathbb{F}_2$ is bent. The restrictions to a $(2n)$-bent function to any hyperplan

and to the complement of this hyperplan (view as $(2n-1)$-Booleans functions) are near-bent. The problem of the construction of $(2n)$-bent functions from two $(2n-1)$-near-bent functions has also been considered by Wolfmann with a different point of view in [49]. Some progress on this question has been made very recently in [51] and [50]. In particular, Wolfmann [50] has introduced a way to construct new bent functions starting from a near-bent functions having a specific derivative or from a bent function such that the sum of the two components is a Boolean function of degree 1. Some open problems have been presented by Wolfmann [50] in the continuation of his interesting approach.

In 2005, Charpin et al. [10] have proved that some classes of near-bent functions can been derived via the composition with nonpermutation linear polynomials. In fact, the composition of any linear permutation polynomial P with a quadratic near-bent function gives rise again to a near-bent function $x \mapsto f(P(x))$. However, it is not necessary for P to be a permutation polynomial in order for $f \circ P$ to be near-bent. In fact, one may choose a linear mapping P from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ which is still near-bent. Charpin et al. [10] have exhibited some nonpermutation linear polynomials that preserve the near-bentness property when composed with a quadratic near-bent function. For more details on the treatment of near-bent functions, we send the reader to [10].

Finally, very few secondary constructions of near-bent functions (i.e., constructions of new near-bent functions from two or several already known ones) have been proposed in the literature. The following statement shows that secondary constructions of near-bent functions can be derived under a condition involving the derivative functions.

Theorem 2 *Let n be an odd integer. Let f and g be two near-bent functions over $\mathbb{F}_{2^n}$. Assume that there exists an element a of $\mathbb{F}_{2^n}$ such that $D_{af} = D_a g$. Then the function $h = f + D_{af}(f+g)$ is a near-bent function on $\mathbb{F}_{2^n}$.*

Proof Let us compute the Walsh transform of h for every $\omega \in \mathbb{F}_{2^n}$. We have

$$\widehat{\chi_h}(\omega) = \sum_{x\in\mathbb{F}_{2^n}} \chi(h(x) + Tr_1^n(\omega x)) = \sum_{x\in\mathbb{F}_{2^n}} \chi(f(x) + D_{af}(x)(f+g)(x) + Tr_1^n(\omega x)).$$

Now, one can split the sum depending whether D_{af} is equal to 1 or not (recall that $D_{af}(x) = f(x) + f(x+a)$):

$$\begin{aligned}\widehat{\chi_h}(\omega) &= \sum_{x\in\mathbb{F}_{2^n}\,|\,D_{af}=0} \chi(f(x) + Tr_1^n(\omega x)) + \sum_{x\in\mathbb{F}_{2^n}\,|\,D_{af}=1} \chi(g(x) + Tr_1^n(\omega x)) \\ &= \frac{1}{2}\Big(\sum_{x\in\mathbb{F}_{2^n}} \chi(f(x) + Tr_1^n(\omega x)) + \sum_{x\in\mathbb{F}_{2^n}} \chi(f(x+a) + Tr_1^n(\omega x))\Big) \\ &\quad + \frac{1}{2}\Big(\sum_{x\in\mathbb{F}_{2^n}} \chi(g(x) + Tr_1^n(\omega x)) - \sum_{x\in\mathbb{F}_{2^n}} \chi(g(x+a) + Tr_1^n(\omega x))\Big).\end{aligned}$$

Hence,

$$\begin{aligned}\widehat{\chi_h}(\omega) &= \frac{1}{2}\Big(\sum_{x\in\mathbb{F}_{2^n}} \chi(f(x)+Tr_1^n(\omega x)) + \sum_{x\in\mathbb{F}_{2^n}} \chi(f(x)+Tr_1^n(\omega(x+a)))\Big)\\ &\quad+\frac{1}{2}\Big(\sum_{x\in\mathbb{F}_{2^n}} \chi(g(x)+Tr_1^n(\omega x)) - \sum_{x\in\mathbb{F}_{2^n}} \chi(g(x)+Tr_1^n(\omega(x+a)))\Big)\\ &= \frac{1}{2}\Big(\widehat{\chi_f}(\omega)(1+\chi(Tr_1^n(\omega a)))\Big) + \frac{1}{2}\Big(\widehat{\chi_g}(\omega)(1-\chi(Tr_1^n(\omega a)))\Big).\end{aligned}$$

Now, f and g being near bent, therefore if $Tr_1^n(\omega a) = 0$, then $\widehat{\chi_h}(\omega) = \widehat{\chi_f}(\omega) \in \{0, \pm 2^{\frac{n+1}{2}}\}$. And if $Tr_1^n(\omega a) = 1$, then $\widehat{\chi_h}(\omega) = \widehat{\chi_g}(\omega) \in \{0, \pm 2^{\frac{n+1}{2}}\}$, which completes the proof. □

3.3 *Plateaued Functions: The Special Class of 2-Plateaued Functions (Semi-Bent Functions)*

Semi-bent functions (or 2-plateaued functions) on $\mathbb{F}_{2^n}$ exist only when n is even. So, in this section n denotes an even integer, and we set $m = \frac{n}{2}$. Semi-bent functions are defined as follows.

Definition 4 Let n be an even integer. A Boolean function on $\mathbb{F}_{2^n}$ is said to be semi-bent if its Walsh transform satisfies $\widehat{\chi_f}(a) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ for all $a \in \mathbb{F}_{2^n}$.

Thanks to Parseval's identity, one can determine the number of occurrences of each value of the Walsh transform of a semi-bent function (see Table 4).

Using the relationship between the nonlinearity and the Walsh spectrum, it is immediate to see that the nonlinearity of a semi-bent function on $\mathbb{F}_{2^n}$ equals $2^{n-1} - 2^{\frac{n}{2}}$. In addition, the possible values of the Hamming weight of a semi-bent function are 2^{n-1}, $2^{n-1} - 2^m$ and $2^{n-1} + 2^m$.

Many recent progresses have been made on the treatment of semi-bent functions. In the next section, we focus on the constructions of such functions.

Table 4 Walsh spectrum of semi-bent functions (2-plateaued) f with $f(0) = 0$

Value of $\widehat{\chi_f}(\omega)$, $\omega \in \mathbb{F}_{2^n}$	Number of occurrences
0	$2^{n-1} + 2^{n-2}$
$2^{\frac{n+2}{2}}$	$2^{n-3} + 2^{\frac{n-4}{2}}$
$-2^{\frac{n+2}{2}}$	$2^{n-3} - 2^{\frac{n-4}{2}}$

4 Semi-Bent Functions (in Even Dimension): Constructions and Characterizations

In the following, we present a general overview of the main known constructions of semi-bent functions and investigate new constructions.

4.1 On Constructions of Quadratic Semi-Bent Functions

The first papers dealing with constructions of semi-bent functions have been dedicated to quadratic functions. In this particular case of functions, there exists a criterion on the semi-bentness involving the dimension of the linear kernel defined above (see, e.g., [10]). More precisely, it has been proved that f is semi-bent over $\mathbb{F}_{2^n}$, if and only if its linear kernel E_f (defined previously) has dimension 2. Note that from Theorem 1, it is easy to see that quadratic Boolean function is semi-bent if and only if the rank of f is $n-2$, that is, $k_f = 2$.

Several constructions of quadratic semi-bent functions have been obtained in the literature. We give a list of the known quadratic semi-bent functions on $\mathbb{F}_{2^n}$, $n = 2m$:

- $f(x) = \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} c_i Tr_1^n(x^{1+2^i})$, $c_i \in \mathbb{F}_2$, $gcd(\sum_{i=1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i}), x^n + 1) = x^2 + 1$ [10].
- $f(x) = Tr_1^n(\alpha x^{2^i+1})$, $\alpha \in \mathbb{F}_{2^n}^\star$, i even, m odd [48].
- $f(x) = Tr_1^n(\alpha x^{2^i+1})$, m even, i odd, $\alpha \in \{x^3, x \in \mathbb{F}_{2^n}^\star\}$ where $\alpha \in \mathbb{F}_{2^n}^\star$ [48].
- $f(x) = Tr_1^n(\alpha x^{2^i+1})$, m odd, i odd, $gcd(m,i) = 1$, $\alpha \in \{x^3, x \in \mathbb{F}_{2^n}^\star\}$ where $\alpha \in \mathbb{F}_{2^n}^\star$ [48].
- $f(x) = Tr_1^n(x^{2^i+1} + x^{2^j+1})$, m odd, $1 \leq i < j < m$, $gcd(n, i+j) = gcd(n, j-i) = 1)$, $gcd(n, i+j) = gcd(n, j-i) = 2$ [48].
- $f(x) = \sum_{i=1}^{\frac{m-1}{2}} Tr_1^n(\beta x^{1+4^i})$, m odd, $\beta \in \mathbb{F}_4^\star$ [16].
- $f(x) = \sum_{i=1}^{\frac{m-1}{2}} c_i Tr_1^n(\beta x^{1+4^i})$, $c_i \in \mathbb{F}_2$, $\beta \in \mathbb{F}_4^\star$, m odd, $gcd(\sum_{i=1}^{\frac{m-1}{2}} c_i(x^i + x^{m-i}), x^m + 1) = x + 1$ [16].
- $f(x) = \sum_{i=1}^{k} Tr_1^n(\beta x^{1+4^{di}})$ $\beta \in \mathbb{F}_4^\star$, m odd, $d \geq 1$, $1 \leq k \leq \frac{m-1}{2}$, $gcd(k+1, m) = gcd(k, m) = gcd(d, m) = 1$ [16].
- $f(x) = Tr_1^n(\beta x^{1+4^i} + \beta x^{1+4^j})$ $\beta \in \mathbb{F}_4^\star$, m odd, $1 \leq i < j \leq \lfloor \frac{n}{4} \rfloor$, $gcd(i+j, m) = gcd(j-i, m) = 1$ [16].
- $f(x) = Tr_1^n(\beta x^{1+4^i} + x^{1+4^j} + x^{1+4^t})$, $\beta \in \mathbb{F}_4^\star$, m odd, $1 \leq i < j < t \leq \lfloor \frac{n}{4} \rfloor$, $i + j = t$, $gcd(i, m) = gcd(j, m) = gcd(j, t) = 1$ [16].
- $f(x) = Tr_1^n(\beta x^{1+4^i} + \beta x^{1+4^j} + \beta x^{1+4^t})$, $\beta \in \mathbb{F}_4^\star$, $1 \leq i < j < t \leq \lfloor \frac{n}{4} \rfloor$, $i + j = 2t$, $j - i = 3^h p$, $3 \not| p$, $n = 3^k q$, $3 \not| q$, $gcd(2t, m) = 1$, $h \geq k$ [16].
- $f(x) = Tr_1^n(\beta x^{1+4^i} + \beta x^{1+4^j} + \beta x^{1+4^t})$, $\beta \in \mathbb{F}_4^\star$, m odd, $1 \leq i, j, t \leq \lfloor \frac{n}{4} \rfloor$, $j - i = 2t$, $t \neq i$, $j + i = 3^u p$, $3 \not| p$, $n = 3^v q$, $3 \not| q$, $gcd(2t, m) = 1$, $u \geq v$ [16].

- $f(x) = Tr_1^n(\beta x^{1+4^i} + \beta x^{1+4^j} + \beta x^{1+4^t}), \beta \in \mathbb{F}_4^\star, 1 \leq i, j, t \leq \lfloor \frac{n}{4} \rfloor, j - i = 2t, t \neq i, j + i = 3^u p, 3 \not| p, n = 3^v q, 3 \not| q, gcd(2t, m) = 1, u \geq v$ [16].
- $f(x) = Tr_1^n(\beta x^{1+4^i} + \beta x^{1+4^j} + \beta x^{1+4^t} + \beta x^{1+4^s}), \beta \in \mathbb{F}_4^\star, 1 \leq i, j, t, s \leq \lfloor \frac{n}{4} \rfloor, i < j, t < s, i + j = t + s = r, t \neq i, gcd(r, m) = gcd(m, s - i) = gcd(m, s - j) = 1$ [16].

4.2 On Constructions of Semi-Bent Functions From Bent Functions

In the following subsections, we are dealing with the construction of semi-bent functions from bent functions. We shall present several such kinds of constructions. A natural problem arises is:

Problem 1 Find new primary constructions of bent functions from semi-bent functions.

4.2.1 Primary Constructions in Univariate Representation from Niho and Dillon Bent Functions

In 2011, many concrete constructions of semi-bent functions of maximum algebraic degree have been discovered. Indeed, in [38], the semi-bentness of several infinite families functions in polynomial form constructed via Dillon and Niho exponents has been studied in detail. From this study, explicit criteria in terms of Kloosterman sums for deciding whether a function expressed as a sum of trace functions is semi-bent or not have been derived. Kloosterman sums have been used as a very suitable tool to study the semi-bentness property of several functions in univariate representation. In particular, we have showed in [38] that the values 0 and 4 of Kloosterman sums defined on $\mathbb{F}_{2^m}$ give rise to semi-bent functions on $\mathbb{F}_{2^n}$. Below is the list of the known semi-bent functions constructed via the zero of Kloosterman sums:

- $f(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^n(cx^{(2^m-1)\frac{1}{2}+1}), K_m(a) = 0$ [38].
- $f(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^n(cx^{(2^m-1)\frac{1}{2}+1}) + Tr_1^n(x^{(2^m-1)\frac{1}{4}+1}), Tr_m^n(c) = 1, m$ odd, $K_m(a) = 0$ [38].
- $f(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^n(cx^{(2^m-1)\frac{1}{2}+1}) + Tr_1^n(x^{(2^m-1)3+1}), K_m(a) = 0$ $Tr_m^n(c) = 1$ [38].
- $f(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^n(cx^{(2^m-1)\frac{1}{2}+1}) + Tr_1^n(x^{(2^m-1)\frac{1}{6}+1}); Tr_m^n(c) = 1,$ $K_m(a) = 0, m$ even [38].
- $f(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^n(\alpha x^{2^m+1}) + Tr_1^n(\sum_{i=1}^{2^{v-1}-1} x^{(2^m-1)\frac{i}{2^v}+1}); \gcd(v, m) = 1, \alpha \in \mathbb{F}_{2^n}, Tr_m^n(\alpha) = 1, K_m(a) = 0$ [38].

Below is the list of the known semi-bent functions constructed via the value four of Kloosterman sums:

- $f(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}}) + Tr_1^n(cx^{(2^m-1)\frac{1}{2}+1})$; m odd, $K_m(a) = 4$ [38].
- $f(x) = Tr_1^n(ax^{3(2^m-1)}) + Tr_1^n(cx^{(2^m-1)\frac{1}{2}+1}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$; m odd and $m \not\equiv 3 \pmod 6$ $K_m(a) = 4$ [38].
- $f(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}}) + Tr_1^n(cx^{(2^m-1)\frac{1}{2}+1}) + Tr_1^n(x^{(2^m-1)\frac{1}{4}+1})$, m odd, $K_m(a) = 4$ [38].
- $f(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}}) + Tr_1^n(cx^{(2^m-1)\frac{1}{2}+1}) + Tr_1^n(x^{3(2^m-1)+1})$; $Tr_m^n(c) = 1$, m odd, $K_m(a) = 4$ [38].
- $f(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^n(\alpha x^{2^m+1}) + Tr_1^n(\sum_{i=1}^{2^{\nu}-1} x^{(2^m-1)\frac{i}{2^{\nu}}+1}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$; $\gcd(\nu, m) = 1$, $\alpha \in \mathbb{F}_{2^n}$, $Tr_m^n(\alpha) = 1$, m odd, $K_m(a) = 4$ ([38]).

All the families of semi-bent functions presented above are of maximum algebraic degree m and then are suitable for use in symmetric cryptosystems.

The previous constructions can be generalized leading to general constructions of semi-bent functions via Dillon-like exponents and Niho exponents. First, recall that *Dillon-like exponents* are of the form $s(2^m - 1)$.

A positive integer s (always understood modulo $2^n - 1$) is said to be a *Niho exponent* and x^s a Niho power function, if the restriction of x^s to $\mathbb{F}_{2^m}$ is linear. One can show that the restriction of the power function $x \mapsto x^s$ to $\mathbb{F}_{2^m}$ is linear then $s = 2^j$ for some $j < n$. As we consider $Tr_1^n(x^d)$, without loss of generality, we can assume that s is in the normalized (unique) representation $s = (2^m - 1)d + 1$ with $1 \leq d \leq 2^m$.

The following statement is due to Carlet and the author [6]. An alternative direct proof has been proposed in [12].

Theorem 3 ([6, 12]) *Denote by Ω_n the set of Boolean functions f defined on $\mathbb{F}_{2^n}$ by $f(x) = \sum_{i \in \Gamma_{n,m}} Tr_1^{o(i)}(a_i x^i)$ where $\Gamma_{n,m}$ is the set of cyclotomic cosets $[i]$ such that $i \equiv 0 \pmod{2^m - 1}$. Denote by Δ_n the set of Boolean functions f defined on $\mathbb{F}_{2^n}$ by $f(x) = \sum_{i \in \Lambda'_{n,m}} Tr_1^{o(i)}(a_i x^i)$ where $\Lambda'_{n,m}$ is the set of cyclotomic cosets $[i]$ such that $i \equiv 2^j \pmod{2^m - 1}$ for some j ($j < n$). Set*

$$\mathscr{D}_n := \{f \in \Omega_n \text{ such that } f \text{ is bent with } f(0) = 0\}$$

and set

$$\mathscr{N}_n := \{f \in \Delta_n \text{ such that } f \text{ is bent with } f(0) = 0\}.$$

Let $g \in \mathscr{D}_n$ and $h \in \mathscr{N}_n$. Then $g + h$ is semi-bent on $\mathbb{F}_{2^n}$.

Let us specify some infinite families of semi-bent functions in univariate form. Firstly, we give a list of infinite families containing bent functions defined on $\mathbb{F}_{2^n}$

belonging to the class $\mathscr{PS}_{\text{ap}}$; here, $K_m(a) := \sum_{x\in\mathbb{F}_{2^m}} \chi\left(Tr_1^m(ax+\frac{1}{x})\right)$ denotes the binary Kloosterman sums on $\mathbb{F}_{2^m}$ and $C_m(a,a) := \sum_{x\in\mathbb{F}_{2^m}} \chi\left(Tr_1^m(ax^3+ax)\right)$ denotes the cubic sums on $\mathbb{F}_{2^m}$:

- $g_1(x) = Tr_1^n(ax^{r(2^m-1)})$; $\gcd(r, 2^m+1) = 1$, $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 0$ [9].
- $g_2(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$; $\gcd(r, 2^m+1) = 1$, $m > 3$ odd, $b \in \mathbb{F}_4^\star$, $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 4$ [36].
- $g_3(x) = Tr_1^n(a\zeta^i x^{3(2^m-1)}) + Tr_1^2(\beta^j x^{\frac{2^n-1}{3}})$; m odd and $m \not\equiv 3 \pmod 6$, β is a primitive element of $\mathbb{F}_4$, ζ is a generator of the cyclic group U of (2^m+1)-th of unity, $(i,j) \in \{0,1,2\}^2$, $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 4$ and $Tr_1^m(a^{1/3}) = 0$ [35].
- $g_4(x) = Tr_1^n(a\zeta^i x^{3(2^m-1)}) + Tr_1^2(\beta^j x^{\frac{2^n-1}{3}})$; m odd and $m \not\equiv 3 \pmod 6$, β is a primitive element of $\mathbb{F}_4$, ζ is a generator of the cyclic group U of (2^m+1)-th of unity, $i \in \{1,2\}$, $j \in \{0,1,2\}$, $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) + C_m(a,a) = 4$ and $Tr_1^m(a^{1/3}) = 1$ [35].
- $g_5(x) = \sum_{i=1}^{2^{m-1}-1} Tr_1^n\left(\beta x^{i(2^m-1)}\right)$; $\beta \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2$ [18].
- $g_6(x) = \sum_{i=1}^{2^{m-2}-1} Tr_1^n\left(\beta x^{i(2^m-1)}\right)$; m odd and $\beta^{(2^m-4)^{-1}} \in \{x \in \mathbb{F}_{2^m}^\star; Tr_1^m(x) = 0\}$ [18].

Secondly, we give a list of known Niho bent functions in $\mathscr{N}_n$:

- $h_1(x) = Tr_1^m\left(a_1 x^{2^m+1}\right)$; $a_1 \in \mathbb{F}_{2^m}^\star$.
- $h_2(x) = Tr_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)3+1}\right)$.
  $a_1 \in \mathbb{F}_{2^n}^\star$, $a_2^{2^m+1} = a_1 + a_1^{2^m} = \beta^5$ for some $\beta \in \mathbb{F}_{2^n}^\star$ [15];
- $h_3(x) = Tr_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)\frac{1}{4}+1}\right)$.
  $a_1 \in \mathbb{F}_{2^n}^\star a_2^{2^m+1} = a_1 + a_1^{2^m}$, m odd [15].
- $h_4(x) = Tr_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)\frac{1}{6}+1}\right)$; $a_1 \in \mathbb{F}_{2^n}^\star$ $a_2^{2^m+1} = a_1 + a_1^{2^m}$, m even [15].
- $h_5(x) = Tr_1^n\left(\alpha x^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} x^{s_i}\right)$, $r > 1$ such that $gcd(r,m) = 1$, $\alpha \in \mathbb{F}_{2^n}$ such that $\alpha + \alpha^{2^m} = 1$, $s_i = (2^m-1)\frac{i}{2^r} \pmod{2^m+1} + 1$, $i \in \{1,\ldots,2^{r-1}-1\}$ [25].

By Theorem 3, we recover the families in univariate form containing semi-bent functions derived previously by the author in [38].

A complete list of the known functions in $\mathscr{D}_n$ can be found in [44] with additional functions in [28] Now, note that $\mathscr{D}_n$ coincides with the set of Boolean functions $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ such that the restriction to $u\mathbb{F}_{2^m}^\star$ is constant for every $u \in U$ with $f(0) = 0$ while $\mathscr{L}_n$ coincides with the set of Boolean functions on $\mathbb{F}_{2^n}$ such that the restriction to $u\mathbb{F}_{2^m}^\star$ is linear for every $u \in U$ with $f(0) = 0$.

A stronger version of the previous statement has been proved in [6].

Theorem 4 ([6]) *Let $n = 2m$ with $m > 2$. Keeping the same notation as in Theorem 3. Set*

$$\mathscr{A}_n := \{f : \mathbb{F}_{2^n} \to \mathbb{F}_2 \text{ s.t the restriction to } u\mathbb{F}_{2^m}^\star \text{ is affine for every } u \in U\}.$$

Then a function f in $\mathscr{A}_n$ is semi-bent if and only if f can be written as the sum of a function in $\mathscr{D}_n$ and a function in $\mathscr{L}_n$.

Example 1 Identify the semi-bent Boolean function f over $\mathbb{F}_{64}$ of the form $f(x) = Tr_1^6(ax^{36}) + Tr_1^6(bx^{32}) + Tr_1^6(cx^{56})$. Set $f = g + h$ where $g : x \in \mathbb{F}_{64} \mapsto Tr_1^6(cx^{56})$ and $h : x \in \mathbb{F}_{64} \mapsto Tr_1^6(ax^{36}) + Tr_1^6(bx^{32})$. We have $36 \equiv 1 \pmod 7$, $36 \equiv 2^2 \pmod 7$ and $56 \equiv 0 \pmod 7$. So 36 and 32 are Niho exponents, while 56 is a Dillon exponent. According to the above result, f is semi-bent if and only if its Niho part (that is, the function h) is bent and its Dillon part (i.e., the function g) is bent. On one hand, the bentness of h depends only on the bentness of $x \mapsto Tr_1^6(ax^{36})$ (since $x \mapsto Tr_1^6(bx^{32})$ is linear). But $36 = 7 \times \frac{1}{2} + 1$ where $\frac{1}{2}$ is understood modulo 9. Thus, the function $x \mapsto Tr_1^6(ax^{36})$ is bent if and only if $Tr_3^6(a) = a + a^8 \neq 0$. Hence, h is bent if and only if $a + a^8 \neq 0$ ($a \in \mathbb{F}_{64}$). On the other hand, $g(x)$ is of the form $Tr_1^n(cx^{2^m-1})$ with $m = \frac{n}{2} = 3$ (the size of the cyclotomic class of 56 modulo $2^6 - 1 = 63$ is 6). Therefore, g is bent, if and only if $K_m(c^{2^m+1}) = K_3(c^9) = 0$ where K_m denotes the Kloosterman sums over $\mathbb{F}_{2^m}$. Let α be a primitive element of $\mathbb{F}_8$ such that $\alpha^3 + \alpha^2 + 1 = 0$. Then, it is easy to check that g is bent, if and only if $c^9 \in \{\alpha, \alpha^2, \alpha^4\}$, that is, $c^9 = \alpha^{2^j}$ for some j (since the Kloosterman sums is invariant under the Frobenius mapping). Finally, one can conclude that f is semi-bent on $\mathbb{F}_{64}$, if and only if $a + a^8 \neq 0$ and $c^9 = \alpha^{2^j}$ for some j where $\alpha \in \mathbb{F}_8$ such that $\alpha^3 + \alpha^2 + 1 = 0$.

Recall [14] that a *spread* is a collection $\{E_i,\ i = 1, \ldots, 2^m + 1\}$ of vector spaces of dimension $m = n/2$ such that $E_i \cap E_j = \{0\}$ for every i and j and $\bigcup_{i=1}^{2^m+1} E_i = \mathbb{F}_{2^n}$. The classical example of spread is $\{u\mathbb{F}_{2^m}\ ;\ u \in U\}$ where U is the multiplicative group $\{u \in \mathbb{F}_{2^n}; u^{2^m+1} = 1\}$. Theorem 4 can be stated in more general setting as follows.

Theorem 5 ([6]) *Let $m \geq 2$ and $n = 2m$. Let $\{E_i,\ i = 1, \ldots, 2^m + 1\}$ be a spread in $\mathbb{F}_{2^n}$ and h a Boolean function whose restriction to every E_i is linear (possibly null). Let S be any subset of $\{1, \ldots, 2^m + 1\}$ and $g = \sum_{i \in S} 1_{E_i} \pmod 2$ where 1_{E_i} is the indicator of E_i. Then $g + h$ is semi-bent if and only if g and h are bent.*

Given a spread $(E_i)_{i=1,\ldots,2^m+1}$, the previous theorem provides a characterization of the semi-bentness for a function whose restriction to every E_i^* is affine (i.e., equal to the sum of a function whose restriction to every E_i is linear and of a function whose restriction to every E_i^* is constant).

Remark 2 One can modify the hypothesis of Theorem 5 by assuming that we have only a partial spread. There exists an example due for m even to Dillon [14] of a partial spread in $\mathbb{F}_{2^n} \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ which is not included in a spread: $E_\infty = \{0\} \times \{0\} \times \mathbb{F}_{2^{m-1}} \times \mathbb{F}_2$ and $E_a = \{(x, \epsilon, a^2x + aTr_1^{m-1}(ax) + a\epsilon, Tr_1^{m-1}(ax)); (x, \epsilon) \in \mathbb{F}_{2^{m-1}} \times \mathbb{F}_2\}$ for $a \in \mathbb{F}_{2^{m-1}}$ (the corresponding function g is quadratic bent). By modifying the hypothesis, we need then to add a condition on the E_i's, and we have only a sufficient condition for $g + h$ being semi-bent:

Let g be a bent function in the $\mathscr{PS}$ class, equal to the sum modulo 2 of the indicators of $l := 2^{m-1}$ or $2^{m-1} + 1$ pairwise "disjoint" vector spaces E_i having

dimension m, and h a bent function which is linear on each E_i. Assume additionally that for every $c \in \mathbb{F}_{2^n}$ there exist at most 2 indices i such that $\forall e \in E_i$, $h(e) = Tr_1^n(ce)$. Then $g + h$ is semi-bent.

Problem 2 Find semi-bent functions obtained by applying the result of Remark 2.

Problem 3 Show that some semi-bent functions obtained above in [6] are not extendable to $(n + 2)$-variable bent functions (or deduce new bent functions from them).

4.2.2 Primary Constructions in Bivariate Representation from the Class $\mathscr{H}$ of Bent Functions

Semi-bent functions in bivariate representation have been derived from the class $\mathscr{H}$ of bent functions introduced by Carlet and the author in [5] and from the partial spread class $\mathscr{PS}_{\text{ap}}$ of bent functions introduced by Dillon [14]. Recall that functions of the class $\mathscr{PS}_{\text{ap}}$ are a subclass of the partial spread class $\mathscr{PS}$ defined as the set of all the sums (modulo 2) of the indicators of 2^{m-1} or $2^{m-1} + 1$ pairwise supplementary m-dimensional subspaces of $\mathbb{F}_{2^n}$. The elements of $\mathscr{PS}_{\text{ap}}$ can be defined in an explicit form as follows.

Definition 5 Let $n = 2m$ and let $\mathbb{F}_{2^n}$ be identified, as a vector space, with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. The partial spread class $\mathscr{PS}_{\text{ap}}$ consists of all the functions f defined as follows: let g be a balanced Boolean function over $\mathbb{F}_{2^m}$ (i.e., $wt(g) = 2^{m-1}$) such that $g(0) = 0$ (but, in fact, this last condition is not necessary for f to be bent). Then f is defined from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_2$ as $f(x, y) = g(\frac{x}{y})$ (i.e., $g(xy^{2^m-2})$) with $\frac{x}{y} = 0$ if $y = 0$.

The functions from class $\mathscr{PS}_{\text{ap}}$ are those whose supports can be uniquely written as $\bigcup_{u \in S} u\mathbb{F}_{2^m}^\star$ where U is the set $\{u \in \mathbb{F}_{2^n}; u^{2^m+1} = 1\}$ and S is a subset of U of size 2^{m-1}. We shall also include in $\mathscr{PS}_{\text{ap}}$ the complements of these functions.

Now, functions of the class $\mathscr{H}$ are defined in bivariate form as follows.

Definition 6 ([5]) Functions h of the class $\mathscr{H}$ defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ are of the form

$$h(x, y) = \begin{cases} Tr_1^m\left(x\psi\left(\frac{y}{x}\right)\right) \text{ if } x \neq 0 \\ Tr_1^m(\mu y) \text{ if } x = 0 \end{cases} \tag{2}$$

where $\psi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ and $\mu \in \mathbb{F}_{2^m}$ and satisfying the following condition:

$$\forall \beta \in \mathbb{F}_{2^m}^\star, \text{the function } z \mapsto G(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m}, \tag{3}$$

where G is defined as: $G(z) := \psi(z) + \mu z$.

The current list of examples of functions h from the class $\mathscr{H}$ is the following:

- $h(x, y) = Tr_1^m(x^{-5}y^6)$, m odd.
- $h(x, y) = Tr_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}})$, m odd.

- $h(x,y) = Tr_1^m(x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$, $m = 2k-1$.
- $h(x,y) = Tr_1^m(x^{-3\cdot(2^{k-1}-1)}y^{3\cdot 2^{k-1}-2})$, $m = 2k-1$.
- $h(x,y) = Tr_1^m(x^{1-2^k-2^{2k}}y^{2^k+2^{2k}})$, $m = 4k-1$.
- $h(x,y) = Tr_1^m(x^{2^{3k-1}-2^{2k}+2^k}y^{1-2^{3k-1}+2^{2k}-2^k})$, $m = 4k-1$.
- $h(x,y) = Tr_1^m(x^{1-2^{2k+1}-2^{3k+1}}y^{2^{2k+1}+2^{3k+1}})$, $m = 4k+1$.
- $h(x,y) = Tr_1^m(x^{2^{3k+1}-2^{2k+1}+2^k}y^{1-2^{3k+1}+2^{2k+1}-2^k})$, $m = 4k+1$.
- $h(x,y) = Tr_1^m(x^{1-2^k}y^{2^k} + x^{-(2^k+1)}y^{2^k+2} + x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$, $m = 2k-1$.
- $h(x,y) = Tr_1^m(y(y^{2^k+1}x^{-(2^k+1)} + y^3x^{-3} + yx^{-1})^{2^{k-1}-1})$, $m = 2k-1$;
- $h(x,y) = Tr_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}} + x^{\frac{1}{2}}y^{\frac{1}{2}} + x^{\frac{1}{6}}y^{\frac{5}{6}})$, m odd.
- $h(x,y) = Tr_1^m(x[D_{\frac{1}{5}}(\frac{y}{x})]^6)$, m odd, where $D_{\frac{1}{5}}$ is the Dickson polynomial of index $\frac{1}{5}$.

The following result provides constructions of semi-bent functions from the classes $\mathscr{H}$ and $\mathscr{PS}_{\text{ap}}$.

Theorem 6 ([6]) *The sum of a function defined on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ from the class $\mathscr{PS}_{\text{ap}}$ and a function defined on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ from the class $\mathscr{H}$ is semi-bent on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$.*

4.2.3 A Construction from Bent Functions via the Indirect Sum

In [3], Carlet has introduced a secondary construction (which means a construction of new functions from ones having the same properties) of bent functions. Later, such a construction was called as the "*indirect sum*" because it generalizes the well-known direct sum introduced by Dillon and Rothaus [14, 46]. The indirect sum is defined as follows.

Definition 7 ([3]) Let $n = r + s$ where r and s are positive integers. Let f_1, f_2 be Boolean functions defined on $\mathbb{F}_{2^r}$ and g_2, g_2 be two Boolean functions defined on $\mathbb{F}_{2^s}$. Define h as follows (i.e., h is the concatenation of the four functions f_1, $f_1\oplus 1$, f_2, and $f_2\oplus 1$, in an order controlled by $g_1(y)$ and $g_2(y)$):

$$\forall(x,y)\in\mathbb{F}_{2^r}\times\mathbb{F}_{2^s},\quad h(x,y) = f_1(x)+g_1(y)+(f_1(x)+f_2(x))(g_1(y)+g_2(y)).$$

Using the indirect sum, we derive a general constructions of semi-bent functions from both bent and semi-bent functions.

Theorem 7 *Let $n = r+s$ with r and s two even integers. Let h be as in Definition 7. Assume that f_1 and f_2 are semi-bent on $\mathbb{F}_{2^r}$ and that g_1 and g_2 are bent on $\mathbb{F}_{2^s}$. Then h is semi-bent on $\mathbb{F}_{2^n}$.*

Proof Set $r = 2\rho$ and $s = 2\sigma$. Let's compute the Walsh transform of h for every $(a, b) \in \mathbb{F}_{2^r} \times \mathbb{F}_{2^s}$. We have

$$\widehat{\chi_h}(a,b) = \sum_{x\in\mathbb{F}_{2^r}} \sum_{y\in\mathbb{F}_{2^s}} \chi(f_1(x) + g_1(y) + (f_1(x) + f_2(x))(g_1(y) + g_2(y)) + Tr_1^r(ax) + Tr_1^s(by)).$$

Now, one can split the sum depending whether $g_1(y) + g_2(y)$ is equal to 1 or not :

$$\widehat{\chi_h}(a,b) = \sum_{x\in\mathbb{F}_{2^r}} \sum_{y\in\mathbb{F}_{2^s} | g_1(y)+g_2(y)=1} \chi(f_2(x) + g_1(y) + Tr_1^r(ax) + Tr_1^s(by)) + \sum_{y\in\mathbb{F}_{2^s} | g_1(y)+g_2(y)=0} \chi(f_1(x) + g_1(y) + Tr_1^r(ax) + Tr_1^s(by)).$$

Now, note that the indicator of the set $\{y \in \mathbb{F}_{2^s} \mid g_1(y) + g_2(y) = 1\}$ can be written as $\frac{1-\chi(g_1(y)+g_2(y))}{2}$. Similarly, one can write the indicator of the set $\{y \in \mathbb{F}_{2^s} \mid g_1(y) + g_2(y) = 0\}$ as $\frac{1+\chi(g_1(y)+g_2(y))}{2}$. Hence,

$$\widehat{\chi_h}(a,b) = \widehat{\chi_{f_1}}(a)\left(\frac{\widehat{\chi_{g_1}}(b) + \widehat{\chi_{g_2}}(b)}{2}\right) + \widehat{\chi_{f_2}}(a)\left(\frac{\widehat{\chi_{g_1}}(b) - \widehat{\chi_{g_2}}(b)}{2}\right).$$

Now, if g_1 and g_2 are bent, then

$$\left(\frac{\widehat{\chi_{g_1}}(b) - \widehat{\chi_{g_2}}(b)}{2}\right)\left(\frac{\widehat{\chi_{g_1}}(b) + \widehat{\chi_{g_2}}(b)}{2}\right) = \frac{1}{4}\left(\left(\widehat{\chi_{g_1}}(b)\right)^2 - \left(\widehat{\chi_{g_2}}(b)\right)^2\right) = 0.$$

and thus only the two following situations can occur

$$\frac{\widehat{\chi_{g_1}}(b) - \widehat{\chi_{g_2}}(b)}{2} = 0 \text{ and } \frac{\widehat{\chi_{g_1}}(b) + \widehat{\chi_{g_2}}(b)}{2} = \pm 2^\sigma$$

or

$$\frac{\widehat{\chi_{g_1}}(b) - \widehat{\chi_{g_2}}(b)}{2} = \pm 2^\sigma \text{ and } \frac{\widehat{\chi_{g_1}}(b) + \widehat{\chi_{g_2}}(b)}{2} = 0.$$

Now f_1 and f_2 being semi-bent : $\widehat{\chi_{f_1}}(a) \in \{0, \pm 2^{\rho+1}\}$ and $\widehat{\chi_{f_2}}(a) \in \{0, \pm 2^{\rho+1}\}$. Therefore $\widehat{\chi_h}(a,b) \in \{0, \pm 2^{\rho+\sigma+1}\}$ proving that h is semi-bent. □

Remark 3 Obviously, the roles of f_1 and f_2 can be exchanged with those of g_1 and g_2. This means that one can exchange the property of bentness and semi-bentness in Theorem 7.

4.2.4 A Simple Construction of Semi-Bent Functions from Bent Functions by Field Extension

Another kind of construction of semi-bent functions from bent functions is given by the simple following statement. When we identify $\mathbb{F}_{2^n}$ with the vector space $\mathbb{F}_2^n$, it corresponds to a simple construction of an $(n+2)$-variable semi-bent function from an n-variable bent function.

Proposition 4 ([12]) *Let n be an even positive integer. Let f be a Boolean function over $\mathbb{F}_{2^{n+2}} \simeq \mathbb{F}_{2^n} \times \mathbb{F}_4$. For $\delta \in \mathbb{F}_4$, we define a Boolean function f_δ over $\mathbb{F}_{2^n} \times \mathbb{F}_4$ by*

$$f_\delta(y, z) = f(y) + Tr_1^2(\delta z), \forall\, y \in \mathbb{F}_{2^n}, z \in \mathbb{F}_4.$$

If f is bent over $\mathbb{F}_{2^n}$ then f_δ is semi-bent over $\mathbb{F}_{2^{n+2}}$.

4.2.5 Construction of Semi-Bent Functions from Bent Functions by Considering the Derivative Functions

Recall that the derivative of a Boolean function f on $\mathbb{F}_{2^n}$ with respect $a \in \mathbb{F}_{2^n}$ is defined by $D_{af}(x) = f(x) + f(x+a)$. The following construction of semi-bent functions from bent functions under a strong condition on the derivatives functions has been shown in [48].

Theorem 8 ([48]) *Let n be an even positive integer. Let f and g be two bent functions over $\mathbb{F}_{2^n}$. Assume that there exists $a \in \mathbb{F}_{2^n}$ such that $D_{af}(x) = D_a g(x) + 1$ for all $x \in \mathbb{F}_{2^n}$. Then the function $h = f + g + D_{af} + D_a(fg)$ is semi-bent over $\mathbb{F}_{2^n}$.*

A possible construction of semi-bent functions by applying Theorem 8 is provided by the following statement.

Proposition 5 *Let f be a bent function defined over $\mathbb{F}_{2^n}$ (with n even). Define a Boolean function g by $g(x) = f(x+a) + Tr_1^n(bx), \forall x \in \mathbb{F}_{2^n}$ where a and b are elements of $\mathbb{F}_{2^n}$ such that $Tr_1^n(ab) = 1$. Then the function $h = f + g + D_{af} + D_a(fg)$ is semi-bent over $\mathbb{F}_{2^n}$.*

Proof The bentness is invariant under the addition of linear functions. Thus g is also bent. Moreover, one has $D_a g(x) = g(x) + g(x+a) = f(x+a) + Tr_1^n(bx) + f(x) + Tr_1^n(bx) + Tr_1^n(ab) = D_{af}(x) + Tr_1^n(ab) = D_{af}(x) + 1$. The proposition follows from Theorem 8. □

Notice that quadratics semi-bent functions can be easily derived from Proposition 5.

Problem 4 Find other examples of constructions of non-quadratic semi-bent functions h starting from two bent functions f and g satisfying $D_{af}(x) = D_{ag}(x) + 1$ for some $a \in \mathbb{F}_{2^n}$.

4.3 A General Construction of Semi-Bent Functions Based on Maiorana–McFarland's Construction

Recall that the Maiorana–McFarland's constructions are the best known primary constructions of bent functions [14,32]. The *Maiorana–McFarland class* is the set of all the Boolean functions on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ of the form $f(x, y) = x \cdot \pi(y) + g(y)$; $x, y \in \mathbb{F}_{2^m}$ 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). By computing the Walsh transform, it is easy to see that if π is a 2-to-1 mapping from $\mathbb{F}_{2^m}$ to on $\mathbb{F}_{2^m}$, then f is semi-bent on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Consequently, the reader notices that using the Maiorana–McFarland method, any permutation leads to the construction of bent functions and any mapping 2-to-1 leads to the construction of semi-bent functions.

The following statement provides an example of construction of semi-bent functions via the Maiorana–McFarland method.

Proposition 6 *Let r be a positive integer. Set $m = 2r - 1$. Let g be any Boolean function over $\mathbb{F}_{2^m}$. Define over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ a Boolean function by $f(x, y) = Tr_1^m(xy^{2^r+2} + xy) + g(y)$, $\forall (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Then f is semi-bent.*

Proof We have to prove that f is semi-bent, that is, its Walsh transform takes only the values 0, 2^{m+1} and -2^{m+1}. Compute the Walsh transform of f. For every $(a, b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, we have:

$$\begin{aligned}
\widehat{\chi_f}(a,b) &= \sum_{x\in\mathbb{F}_{2^m}} \sum_{y\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(xy^{2^r+2}+xy)+g(y)+Tr_1^m(ax)+Tr_1^m(by)} \\
&= \sum_{y\in\mathbb{F}_{2^m}} (-1)^{g(y)+Tr_1^m(by)} \sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(xy^{2^r+2}+xy))+Tr_1^m(ax)} \\
&= \sum_{y\in\mathbb{F}_{2^m}} (-1)^{g(y)+Tr_1^m(by)} \sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m((y^{2^r+2}+y)x)} \\
&= 2^m \sum_{y\in\mathbb{F}_{2^m} | y^{2^r+2}+y=a} (-1)^{g(y)+Tr_1^m(by)}.
\end{aligned}$$

Now, according to Cusick and Dobbertin [13], the equation $y^{2^r+2} + y = a$ has 0 or 2 solutions in $\mathbb{F}_{2^m}$. The mapping $y \in \mathbb{F}_{2^m} \mapsto y^{2^r+2} + y + a$ is 2-to-1 for every $a \in \mathbb{F}_{2^m}$. Therefore,

$$\widehat{\chi_f}(a,b) \in \{0, \pm 2^{m+1}\}$$

which completes the proof. □

4.4 A Construction from APN Functions

Let us recall the definition of *almost perfect nonlinear* (APN) functions.

Definition 8 Let F be a mapping from $\mathbb{F}_{2^m}$ to itself (m a positive integer). The function f is said to be APN if, $max_{a\in\mathbb{F}^\star_{2^m}} max_{b\in\mathbb{F}_{2^m}} \#\{x \in \mathbb{F}_{2^m} \mid F(x+a)+F(x) = b\} = 2$.

APN functions are important research objects in cryptography and coding theory. Given an APN function, one can derive a construction of semi-bent function in the sprit of Maiorana–McFarland's method.

Proposition 7 *Let m be a positive integer. Let $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be an APN function, g a Boolean function over $\mathbb{F}_{2^m}$ and $\alpha \in \mathbb{F}^\star_{2^m}$. Denote by $D_\alpha F$ the derivative function of F with respect to α defined by $D_\alpha F(x) = F(x+\alpha) + F(x), \forall x \in \mathbb{F}_{2^m}$. Define over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ a Boolean function by $f(x, y) = Tr_1^m(xD_\alpha F(y)) + g(y), \forall (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Then f is semi-bent.*

Proof Let us compute the Walsh transform of f. For every $(a, b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, we have

$$\begin{aligned}\widehat{\chi_f}(a,b) &= \sum_{x\in\mathbb{F}_{2^m}}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(xD_\alpha F(y))+g(y)+Tr_1^m(ax)+Tr_1^m(by)} \\ &= \sum_{y\in\mathbb{F}_{2^m}} (-1)^{g(y)+Tr_1^m(by)} \sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(x(D_\alpha F(y)+a))} \\ &= 2^m \sum_{y\in\mathbb{F}_{2^m} | D_\alpha F(y)=a} (-1)^{g(y)+Tr_1^m(by)}.\end{aligned}$$

Now, since F is APN, the mapping $y \in \mathbb{F}_{2^m} \mapsto D_\alpha F(y)$ is 2-to-1 for every $\alpha \in \mathbb{F}^\star_{2^m}$. Hence, $\widehat{\chi_f}(a, b) \in \{0, \pm 2^{m+1}\}$ which completes the proof. □

4.5 Several Constructions from Hyperovals and Oval Polynomials

Let $PG_2(2^n)$ be the two-dimensional projective space over $\mathbb{F}_{2^n}$. The one-dimensional subspaces of $\mathbb{F}^3_{2^n}$ are then the points, and the two-dimensional subspaces of $\mathbb{F}^3_{2^n}$ are called the lines. A hyperoval in $PG_2(2^n)$ can be defined as follows.

Definition 9 (Hyperoval) A hyperoval in $PG_2(2^n)$ is a set of $2^n + 2$ points; no three of them are collinear (i.e., lie in a line[2]).

[2]We say a point $p = (x_0, \ldots, x_n)$ is on a line $L[y_0, \ldots, y_n]$ if and only if $x_0y_0 + x_1y_1 + \cdots x_ny_n = 0$.

A particular type of polynomials on $\mathbb{F}_{2^n}$ give rise to hyperovals in $PG_2(2^n)$. More precisely:

Definition 10 *An oval polynomial* on $\mathbb{F}_{2^n}$ is a polynomial G on $\mathbb{F}_{2^n}$ such that the set of points $\{(1, t, G(t)), t \in \mathbb{F}_2^n\} \cup \{(0, 0, 1), (0, 1, 0)\}$ (denoted by $D(G)$) forms a hyperoval of $PG_2(2^n)$ (for short, *an o-polynomial*).

There is a close connection between the hyperovals and the o-polynomials since a hyperoval of $PG_2(2^n)$ can be represented by $D(G)$ where G is an o-polynomial on $\mathbb{F}_{2^n}$. In fact, there exists a necessary and sufficient condition for a mapping over $\mathbb{F}_{2^n}$ to give a hyperoval of $PG_2(2^n)$. This leads to a reformulation of the definition of an o-polynomial given as follows.

Definition 11 A permutation polynomial G over $\mathbb{F}_{2^n}$ is an o-polynomial if, for every $\gamma \in \mathbb{F}_{2^n}$, the function

$$z \in \mathbb{F}_{2^n} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} & \text{if } z \neq 0 \\ 0 & \text{if } z = 0 \end{cases}$$

is a permutation of $\mathbb{F}_{2^n}$.

Note that if G is an *o*-polynomial over $\mathbb{F}_{2^n}$ then, $z \in \mathbb{F}_{2^n} \mapsto G(z) + \alpha z$ is 2-to-1 for every $\alpha \in \mathbb{F}_{2^n}^\star$.

The current list, up to equivalence, of the known o-polynomials on $\mathbb{F}_{2^m}$ is given in [5].

A simple construction of semi-bent functions from hyperovals of $PG_2(2^m)$ with $m > 2$ is given by the following statement.

Theorem 9 *Let k be a positive integer such that $2 \leq k \leq 2^m - 2$. Let $D(k) := \{(1, t, t^k), t \in \mathbb{F}_{2^m}\} \cup \{(0, 0, 1), (0, 1, 0)\}$ ($m > 2$) be a hyperoval of $PG_2(2^m)$ and g be a Boolean function on $\mathbb{F}_{2^m}$. Then the function f defined over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by $f(x, y) = Tr_1^m(xy^k + xy) + g(y)$ is semi-bent.*

Proof We have to prove that f is semi-bent, that is, its Walsh transform takes only the values 0, 2^{m+1} and -2^{m+1}. Compute the Walsh transform of f. For every $(a, b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, we have:

$$\begin{aligned}
\widehat{\chi_f}(a, b) &= \sum_{x \in \mathbb{F}_{2^m}} \sum_{y \in \mathbb{F}_{2^m}} \chi\Big(Tr_1^m(xy^k + xy) + g(y) + Tr_1^m(ax) + Tr_1^m(by)\Big) \\
&= \sum_{y \in \mathbb{F}_{2^m}} \chi\Big(g(y) + Tr_1^m(by)\Big) \sum_{x \in \mathbb{F}_{2^m}} \chi\Big(Tr_1^m(xy^k + xy) + Tr_1^m(ax)\Big) \\
&= \sum_{y \in \mathbb{F}_{2^m}} \chi\Big(g(y) + Tr_1^m(by)\Big) \sum_{x \in \mathbb{F}_{2^m}} \chi\Big(Tr_1^m((y^k + y + a)x)\Big) \\
&= 2^m \sum_{y \in \mathbb{F}_{2^m} | y^k + y = a} \chi\Big(g(y) + Tr_1^m(by)\Big).
\end{aligned}$$

Now, since $D(k)$ is a hyperoval of $PG_2(2^m)$ then according to Maschietti [30], the equation $y^k + y + a = 0$ has either zero or two distinct solutions in $\mathbb{F}_{2^m}$ for every $a \in \mathbb{F}_{2^m}$ $(m > 2)$. Therefore, $\widehat{\chi_f}(a, b) \in \{0, \pm 2^{m+1}\}$ which completes the proof. □

An application of Theorem 9 is given by the next proposition.

Proposition 8 *Let m be a positive odd integer with $m > 2$. Let g be a Boolean function on $\mathbb{F}_{2^m}$. Then the function f defined over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by $f(x, y) = Tr_1^m(xy^6 + xy) + g(y)$ is semi-bent.*

Proof According to Theorem 9, f is semi-bent if $D(6) := \{(1, t, t^6), t \in \mathbb{F}_{2^m}\} \cup \{(0, 0, 1), (0, 1, 0)\}$ $(m > 2)$ is a hyperoval of $PG_2(2^m)$. According to Segre and Bartocci [47], for m odd with $m > 3$, $D(6)$ is a hyperoval of $PG_2(2^m)$. It remains to check the case $m = 3$. According to Maschietti [30], it suffices to prove that the equation $y^6 + y = a$ has either zero solution or two distinct solutions in $\mathbb{F}_{2^m}$, for every $a \in \mathbb{F}_{2^m}$. The result is trivial for $a = 0$. Now, let $a \in \mathbb{F}_{2^m}^\star$. Using the fact that $y^7 = 1$ for $y \neq 0$, it is easy to see that the number of solutions of the equation $y^6 + y = a$ in $\mathbb{F}_{2^m}$ is equal to the number of solutions of $y^2 + ay + 1 = 0$ in $\mathbb{F}_{2^m}^\star$, which equals 2 (since if $y^2 + ay + 1 = 0$ has two identical solutions implies that $a = 0$, which contradicts the hypothesis). □

In the following, we show how one can construct several infinite classes of semi-bent functions from o-polynomials. The first result in this direction was given in [6] which is closely related to the construction of semi-bent functions in bivariate representation from the class $\mathscr{H}$ of bent functions and the class of partial spreads $\mathscr{PS}_{\text{ap}}$ given by Theorem 6.

Theorem 10 ([6]) *Let G be an o-polynomial on $\mathbb{F}_{2^m}$, and g be Boolean function on $\mathbb{F}_{2^m}$ such that $g(0) = 0$ and $wt(g) = 2^{m-1}$ (i.e., g is balanced on $\mathbb{F}_{2^m}$). Let $\mu \in \mathbb{F}_{2^m}$. Define over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ the Boolean function f by*

$$f(x, y) = Tr_1^m(\mu y + xG(yx^{2^m-2})) + g(yx^{2^m-2}), \quad (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}.$$

Then f is semi-bent.

Very recently, several more constructions of semi-bent functions have been derived from o-polynomials [40]. An important point is that the notion of oval polynomial over $\mathbb{F}_{2^m}$ appears to be suitable to build 2-to-1 mappings on $\mathbb{F}_{2^m}$. Such a property has been used to built infinite classes of semi-bent functions.

Theorem 11 ([40]) *Let α be a primitive element of $\mathbb{F}_{2^m}$ and j a positive integer in the range $[0, 2^m - 2]$. Let G be an o-polynomial on $\mathbb{F}_{2^m}$ and g a Boolean function on $\mathbb{F}_{2^m}$. Define over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ a Boolean function f by*

$$f(x, y) = Tr_1^m(xG(y) + \alpha^j xy) + g(y), \quad (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}.$$

Then f is semi-bent.

Problem 5 Find other permutations G than oval polynomials having the property that $y \mapsto G(y) + \alpha^j y$ is 2-to-1 (which is the key in the proof of Theorem 11).

In the following, we emphasize the following observation.

Proposition 9 ([40]) *Any semi-bent function of Theorem 11 is the sum of two bent functions in the class of Maiorana–McFarland.*

Remark 4 Note that if we take at random two bent functions, even in the class of Maiorana–McFarland, their sum would not be probably semi-bent in most cases (the reader should notice that semi-bent functions of Theorem 10 can also be decomposed in the sum of two bent functions).

Problem 6 Find new constructions of semi-bent functions using permutations other than oval polynomials.

Another construction of semi-bent function in bivariate representation has been derived by the author in [40].

Theorem 12 ([40]) *Let m be a positive integer. Assume $m = 2m_1 + 1$ odd. Let G be an o-polynomial on $\mathbb{F}_{2^m}$ and g be a Boolean function on $\mathbb{F}_{2^m}$. Define a Boolean function f in bivariate representation as*

$$\begin{aligned} f(x,y) = Tr_1^m\left(xG^{2^{m_1}+1+1}(y) + xyG^{2^{m_1}+1}(y) + xG^3(y) + xyG^2(y)\right) \\ + Tr_1^m\left((xy^{2^{m_1}+1} + xy^2 + x)G(y) + xy^{2^{m_1}+1+1} + xy + xy^3\right) \\ + g(y), (x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}. \end{aligned}$$

Then f is semi-bent on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

Now, Theorems 11 and 12 can be generalized since other semi-bent functions of a more general form can be obtained from o-polynomials.

Theorem 13 ([40]) *Let π_1 and π_2 be two permutations of $\mathbb{F}_{2^m}$ whose composition $\pi_1 \circ \pi_2^{-1}$ is an o-polynomial on $\mathbb{F}_{2^m}$. Let g be a Boolean function over $\mathbb{F}_{2^m}$. Let f be the Boolean function defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by*

$$(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}, \quad f(x,y) = Tr_1^m(x(\pi_1(y) + \pi_2(y))) + g(y).$$

Then f is semi-bent.

A first consequence of the previous theorem is the following statement which provides another primary construction of semi-bent functions.

Theorem 14 ([40]) *Let m be an odd positive integer. Define the Boolean function f on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ as*

$$(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}, \quad f(x,y) = Tr_1^m\left(y^6x + y^5x + y^3x + yx\right) + g(y)$$

where g is any Boolean function over $\mathbb{F}_{2^m}$. Then f is semi-bent.

A generalization of Theorem 12 is given by the following statement.

Theorem 15 ([40]) *Let π be a permutation of $\mathbb{F}_{2^m}$. Let α be a primitive element of $\mathbb{F}_{2^m}$ and j a nonnegative integer. Let G be an o-polynomial and g a Boolean function over $\mathbb{F}_{2^m}$. Define*

$$\forall (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}, \quad f(x, y) = Tr_1^m(\pi(G(y) + \alpha^{jy})x) + g(y).$$

Then f is semi-bent.

Let $L(x) = \sum_{s=0}^{m-1} \alpha_s x^{2^s}$ and $l(x) = \sum_{s=0}^{m-1} \alpha_s x^s$ be two polynomial over $\mathbb{F}_{2^m}$. $L(x)$ and $l(x)$ are the 2-associate of each other. More specifically, $l(x)$ is the conventional 2-associate of $L(x)$ and $L(x)$ is the linearized 2-associate of $l(x)$. It is well known that L is a linear permutation polynomial, if and only if, the determinant of the matrix $(\alpha_{i-j}^{2^i})_{0 \le i,j \le m-1}$ is not zero.

A possible construction of semi-bent functions involving linearized polynomials and oval polynomials is given by the following statement.

Proposition 10 *Let $L(x)$ and $l(x)$ two polynomials on $\mathbb{F}_{2^m}$ defined as above. Assume that $l(x)$ is co-prime with $x^m - 1$. Let $a \in \mathbb{F}_{2^m}$ such that $Tr_1^m(a) = 0$ and δ be a non zero elements of $\mathbb{F}_{2^m}$. Let G be an o-polynomial on $\mathbb{F}_{2^m}$ and g any Boolean function on $\mathbb{F}_{2^m}$. Then the function f defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ as*

$$f(x, y) = Tr_1^m\Big(axTr_1^m(G(y) + \delta y) + xL(G(y) + \delta y)\Big) + g(y)$$

is semi-bent.

Proof The proposition follows from Theorem 15 and Corollary 3.6 in [53]. □

In [5], we have introduced the notion of *o-equivalence* between two oval polynomials.

Definition 12 ([5]) Two functions G and G' are o-equivalent if one can be obtained from the other by a sequence of the following list of transformations:

1. $G \mapsto G'$ where $G' : z \in \mathbb{F}_{2^m} \mapsto G'(z) := G(\lambda z + \mu)$ with $\lambda \in \mathbb{F}_{2^m}^{\star}$ and $\mu \in \mathbb{F}_{2^m}$,
2. $G \mapsto G'$ where $G' : z \in \mathbb{F}_{2^m} \mapsto G'(z) := \lambda G(z) + \mu$ with $\lambda \in \mathbb{F}_{2^m}^{\star}$ and $\mu \in \mathbb{F}_{2^m}$,
3. $G \mapsto G'$ where $G' : z \in \mathbb{F}_{2^m} \mapsto G'(z) := zG(z^{2^m-2})$ (with $G(0) = 0$),
4. $G \mapsto G'$ where $G' : z \in \mathbb{F}_{2^m} \mapsto G'(z) := G(z^{2^j})^{2^{m-j}}$ where $j \in \mathbb{N}$,
5. $G \mapsto G'$ where $G' : z \in \mathbb{F}_{2^m} \mapsto G'(z) := G^{-1}(z)$.

Recall the notion of extended affine equivalence between two Boolean functions.

Definition 13 Two Boolean functions f and f' defined on $\mathbb{F}_{2^n}$ are called extended affine equivalent (EA-equivalent) if $f' = f \circ \phi + \ell$ where the mapping ϕ is an affine automorphism on $\mathbb{F}_{2^n}$ and ℓ is an affine Boolean function (affine functions are those whose algebraic degree is at most 1).

A discussion about the *EA-equivalence* between two semi-bent Boolean functions constructed from o-equivalent ovals polynomials can be found in [40].

4.6 Secondary Constructions of Semi-Bent Functions

In general, "secondary constructions" means constructions of new functions from ones having the same properties. Only few secondary constructions of semi-bent functions have been considered in the literature. An example of a secondary construction of semi-bent functions based on a strong condition on the derivative functions has been given in [48].

Theorem 16 ([48]) *Let f and g be two semi-bent functions over $\mathbb{F}_{2^n}$ (with n even). Assume that there exists an element a in $\mathbb{F}_{2^n}$ such that $D_{af} = D_a g$. Then the function $h = f + D_{af}(f + g)$ is semi-bent on $\mathbb{F}_{2^n}$.*

The reader notices that Theorem 7 shows that the indirect sum could be used to construct semi-bent functions from both bent and semi-bent functions. The construction derived from Theorem 7 can be therefore viewed as a secondary-like construction of semi-bent functions.

Problem 7 Find new secondary constructions of semi-bent functions, that is, constructions of new semi-bent functions from two or several already known ones.

Conclusion
The research activity on bent functions has lasted over 35 years and remains intensive. However, very recently, many advances have been made subsequently on super classes of bent functions (plateaued functions, etc.) and related classes of bent functions (semi-bent functions, etc.). In particular many new connections in the framework of semi-bent functions with other domains of mathematics and computer science (Dickson polynomial, Kloosterman sums, spreads, oval polynomial, finite geometry, coding, cryptography, sequences, etc.) have been exhibited. The research in this framework is relatively new (comparatively to the context of bent functions) and is becoming very active. Despite recent progress, much remains to do. In particular, although many concrete constructions of semi-bent functions have been discovered, the general structure of semi-bent functions is still unclear.

Acknowledgements The author wishes to thank Claude Carlet for his careful reading and interesting comments.

References

1. S. Boztas, P.V. Kumar, Binary sequences with Gold-like correlation but larger linear span. IEEE Trans. Inf. Theory **40**(2), 532–537 (1994)
2. A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, On cryptographic properties of the cosets of R(1,m). IEEE Trans. Inf. Theory **47**, 1494–1513 (2001)
3. C. Carlet, On the secondary constructions of resilient and bent functions, in *Proceedings of the Workshop on Coding, Cryptography and Combinatorics 2003* (Birkhäuser, Basel, 2004), pp. 3–28
4. C. Carlet, Boolean functions for cryptography and error correcting codes, in Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, ed. by Y. Crama, P.L. Hammer (Cambridge University Press, Cambridge, 2010), pp. 257–397
5. C. Carlet, S. Mesnager, On Dillon's class H of bent functions, niho bent functions and O-polynomials. J. Comb. Theory Ser. A **118**(8), 2392–2410 (2011)
6. C. Carlet, S. Mesnager, On Semi-bent Boolean Functions. IEEE Trans. Inf. Theory **58**(5), 3287–3292 (2012)
7. C. Carlet, E. Prouff, On plateaued functions and their constructions, in *Proceedings of Fast Software Encryption (FSE)*. Lecture Notes in Computer Science, vol. 2887 (2003), pp. 54–73
8. A. Cesmelioglu, W. Meidl, A construction of bent functions from plateaued functions. Des. Codes Cryptogr. **66**(1–3), 231–242 (2013)
9. P. Charpin, G. Gong, Hyperbent functions, Kloosterman sums and Dickson polynomials. IEEE Trans. Inform. Theory **54**(9), 4230–4238 (2008)
10. P. Charpin, E. Pasalic, C. Tavernier, On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inf. Theory **51**(12), 4286–4298 (2005)
11. S. Chee, S. Lee, K. Kim, Semi-bent functions, in *Advances in Cryptology-ASIACRYPT94. Proceedings of 4th International Conference on the Theory and Applications of Cryptology*, Wollongong, ed. by J. Pieprzyk, R. Safavi-Naini. Lecture Notes in Computer Science, vol. 917 (1994), pp. 107–118
12. G. Cohen, S. Mesnager, On constructions of semi-bent functions from bent functions. Journal Contemporary Mathematics 625, Discrete Geometry and Algebraic Combinatorics, Americain Mathematical Society, 141–154 (2014)
13. T.W. Cusick, H. Dobbertin, Some new three-valued crosscorrelation functions for binary m-sequences. IEEE Trans. Inf. Theory **42**(4), 1238–1240 (1996)
14. J. Dillon, Elementary Hadamard difference sets, Ph.D. dissertation, University of Maryland, 1974
15. H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, P. Gaborit, Construction of bent functions via Niho Power Functions. J. Comb. Theory Ser. A **113**, 779–798 (2006)
16. D. Dong, L. Qu, S. Fu, C. Li, New constructions of semi-bent functions in polynomial forms. Math. Comput. Model. **57**, 1139–1147 (2013)
17. R. Gold, Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory **14** (1), 154–156 (1968)
18. F. Gologlu, Almost bent and almost perfect nonlinear functions, exponential sums, geometries and sequences, Ph.D. dissertation, University of Magdeburg, 2009
19. T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences. Discrete. Math. **16**, 209–232 (1976)
20. T. Helleseth, Correlation of m-sequences and related topics, in *Proceedings of SETAO98, Discrete Mathematics and Theoretical Computer Science*, ed. by C. Ding, T. Helleseth, H. Niederreiter (Springer, London, 1999), pp. 49–66
21. T. Helleseth, P.V. Kumar, Sequences with low correlation, in *Handbook of Coding Theory, Part 3: Applications*, chap. 21, ed. by V.S. Pless, W.C. Huffman, R.A. Brualdi (Elsevier, Amsterdam, 1998), pp. 1765–1853

22. J.Y. Hyun, H. Lee, Y. Lee, Nonexistence of certain types of plateaued functions. Discrete Appl. Math. **161**(16–17), 2745–2748 (2013)
23. K. Khoo, G. Gong, D.R. Stinson, A new family of Gold-like sequences, in *Proceedings IEEE International Symposium on Information Theory*, Lausanne (2002)
24. K. Khoo, G. Gong, D.R. Stinson, A new characterization of semi-bent and bent functions on finite fields. J. Design Codes Cryptogr. **38**(2), 279–295 (2006)
25. G. Leander, A. Kholosha, Bent functions with 2^r Niho exponents. IEEE Trans. Inf. Theory **52**(12), 5529–5532 (2006)
26. G. Leander, G. McGuire, Spectra of functions, subspaces of matrices, and going up versus going down, in *International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC)*. Lecture Notes in Computer Science, vol. 4851 (Springer, Berlin, 2007), pp. 51–66
27. G. Leander, G. McGuire, Construction of bent functions from near-bent functions. J. Comb. Theory Ser. A **116**, 960–970 (2009)
28. N. Li, T. Helleseth, X. Tang, A. Kholosha, Several new classes of bent functions from Dillon exponents. IEEE Trans. Inf. Theory **59**(3), 1818–1831 (2013)
29. F.J. MacWilliams, N.J. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977)
30. A. Maschietti, Difference sets and hyperovals. J. Design Codes Cryptogr. **14**(1), 89–98 (1998)
31. M. Matsui, Linear cryptanalysis method for DES cipher, in *Proceedings of EUROCRYPT'93*. Lecture Notes in Computer Science, vol. 765 (1994), pp. 386–397
32. R.L. McFarland, A family of noncyclic difference sets. J. Comb. Theory Ser. A **15**, 1–10 (1973)
33. W. Meier, O. Staffelbach, Fast correlation attacks on stream ciphers, in *Advances in Cryptology, EUROCRYPT'88*. Lecture Notes in Computer Science, vol. 330 (1988), 301–314
34. Q. Meng, H. Zhang, M. Yang, J. Cui, On the degree of homogeneous bent functions. Discrete Appl. Math. **155**(5), 665–669 (2007)
35. S. Mesnager, A new family of hyper-bent boolean functions in polynomial form, in *Proceedings of Twelfth International Conference on Cryptography and Coding, IMACC 2009*. Lecture Notes in Computer Science, vol. 5921 (Springer, Heidelberg, 2009), pp. 402–417
36. S. Mesnager, A new class of bent and hyper-bent Boolean functions in polynomial forms. J. Design Codes Cryptogr. **59**(1–3), 265–279 (2011)
37. S. Mesnager, Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. IEEE Trans. Inf. Theory **57**(9), 5996–6009 (2011)
38. S. Mesnager, Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. IEEE Trans. Inf. Theory **57**(11), 7443–7458 (2011)
39. S. Mesnager, Semi-bent functions with multiple trace terms and hyperelliptic curves, in *Proceeding of International Conference on Cryptology and Information Security in Latin America (IACR), Latincrypt 2012*. Lecture Notes in Computer Science, vol. 7533 (Springer, Berlin, 2012), pp. 18–36
40. S. Mesnager, Semi-bent functions from oval polynomials, in *Proceedings of Fourteenth International Conference on Cryptography and Coding*, Oxford, IMACC 2013. Lecture Notes in Computer Science, vol. 8308 (Springer, Heidelberg, 2013), pp. 1–15
41. S. Mesnager, Contributions on boolean functions for symmetric cryptography and error correcting codes, Habilitation to Direct Research in Mathematics (HdR thesis), December 2012
42. S. Mesnager, Bent functions from Spreads. Journal of the American Mathematical Society (AMS), Contemporary Mathematics 632. to appear.
43. S. Mesnager, G. Cohen, On the link of some semi-bent functions with Kloosterman sums, in *Proceedings of International Workshop on Coding and Cryptology, IWCC 2011*. Lecture Notes in Computer Science, vol. 6639 (Springer, Berlin, 2011), pp. 263–272
44. S. Mesnager, J.P. Flori, Hyper-bent functions via Dillon-like exponents. IEEE Trans. Inf. Theory **59**(5), 3215– 3232 (2013)

45. Y. Niho, Multi-valued cross-correlation functions between two maximal linear recursive sequences, Ph.D. dissertation, University of Sothern California, Los Angeles, 1972
46. O.S. Rothaus, On "bent" functions. J. Comb. Theory Ser. A **20**, 300–305 (1976)
47. B. Segre, U. Bartocci, Ovali ed altre curve nei piani di Galois di caratteristica due. Acta Arith. **18**(1), 423–449 (1971)
48. G. Sun, C. Wu, Construction of semi-bent Boolean functions in even number of variables. Chin. J. Electron. **18**(2), 231–237 (2009)
49. J. Wolfmann, Cyclic code aspects of bent functions, in *Finite Fields Theory and Applications, Contemporary Mathematics Series of the AMS*, vol. 518 (American Mathematical Society, Providence, 2010), pp. 363–384
50. J. Wolfmann, Special bent and near-bent functions. Adv. Math. Commun. **8**(1), 21–33 (2014)
51. J. Wolfmann, Bent and near-bent functions (2013). arxiv.org/abs/1308.6373
52. T. Xia, J. Seberry, J. Pieprzyk, C. Charnes, Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$. Discrete Appl. Math. **142**(1–3), 127–132 (2004)
53. P. Yuan, C. Ding, Permutation polynomials over finite fields from a powerful lemma. Finite Fields Appl. **17**, 560–574 (2011)
54. Y. Zheng, X.M. Zhang, Plateaued functions, in *Advances in Cryptology ICICS 1999*. Lecture Notes in Computer Science, vol. 1726 (Springer, Berlin, 1999), 284–300
55. Y. Zheng, X.M. Zhang, Relationships between bent functions and complementary plateaued functions. Lecture Notes in Computer Science, vol. 1787 (1999), pp. 60–75
56. Y. Zheng, X.M. Zhang, On plateaued functions. IEEE Trans. Inform. Theory **47**(3), 1215–1223 (2001)