On constructions of semi-bent functions from bent functions

Gérard Cohen and Sihem Mesnager

In honour of our friend Ilya Dumer for his sixtieth birthday

Abstract. Plateaued functions are significant in cryptography as they possess various desirable cryptographic properties. Two important classes of plateaued functions are those of bent functions and semi-bent functions, due to their combinatorial and algebraic properties. Constructions of bent functions have been extensively investigated. However only few constructions of semi-bent functions have been proposed in the literature. In general, finding new constructions of bent and semi-bent functions is not a simple task. The paper is devoted to the construction of semi-bent functions with even number of variables. We show that bent functions give rise to primary and secondary-like constructions of semi-bent functions.

1. Introduction

A Boolean function over the Galois field $\mathbb{F}_{2^n}$ is said r-plateaued if the values of its Walsh transform belong to the set $\{0, \pm 2^{\frac{n+r}{2}}\}$. Plateaued functions [**30, 29**] are significant in cryptography as they possess desirable various cryptographic characteristics such as high nonlinearity, resiliency, propagation criteria, low additive autocorrelation and high algebraic degree. Two important classes of plateaued functions are those of bent functions and of semi-bent functions, due to their algebraic and combinatorial properties.

Bent functions introduced in 1974 [**9**] ,[**27**] are extremal objects in combinatorics and Boolean function theory. Bent functions exist only with even number of variables. They 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 (RM) codes. Indeed, bent functions realize the maximal possible distance from first-order RM codes; RM codes are quite popular, particularly in view of their recursive structure, exploited for their decoding in a few influencial papers by Ilya Dumer (see [**10**],[**1**] for recent advances). By achieving optimum nonlinearity, bent functions permit to resist linear attacks in the best

Key words and phrases. Boolean functions, Walsh transform, Bent functions, Semi-bent functions.

possible way. Bent functions also satisfy the propagation criterion with respect to the non-zero vector. But, being neither balanced nor correlation immune, they are improper for direct cryptographic use. Thanks to the well known Parseval identity, the maximum nonlinearity they attain implies that the Hadamard Walsh transform of an n-variable (n even) bent function takes only the two values $\pm 2^{n/2}$. A good survey of bent functions can be found in the book chapter of Carlet [**4**].

Semi-bent functions have been introduced by Chee, Lee and Kim [**8**] and previously investigated under the name of three-valued almost optimal Boolean functions [**2**]. Semi-bent functions exist in even or odd dimension. In both cases, they are defined in terms of Walsh Hadamard transform. In even dimension, an n-variable Boolean function is said to semi -bent if its Hadamard Walsh transform takes three values 0 and $\pm 2^{\frac{n+2}{2}}$. Very recently, the development of the theory of semi-bent functions has increased. 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 a low Hadamard transform (which provides protection against fast correlation attacks [**19**] and linear cryptanalysis [**18**]), have low autocorrelation, satisfy the propagation criteria and high algebraic degree. Secondly, beside their practical use in cryptography, they are also widely used in code division multiple access (CDMA) communication systems for sequence design [**11**], [**26**], [**12**], [**13**], [**14**], [**15**], [**16**].

A lot of research has been devoted to designing constructions of bent functions. The reader can see [**4**] for general constructions of bent functions and the paper [**20**] for a complete state of the art on bent functions over the Galois field $\mathbb{F}_{2^n}$. However, only few constructions have been proposed for semi-bent functions. In even dimension, there exist some constructions of quadratic semi-bent functions ([**7**] and in [**28**]) and infinite classes of semi-bent functions with maximal algebraic degree obtained very recently in [**6**]. The reader can also see the reference [**21**] for recent results dealing with the constructions of semi-bent functions via Dillon and Niho exponents under some conditions (on the coefficients of the Boolean functions defined on $\mathbb{F}_{2^n}$) directly related to the Kloosterman sums; in particular, it was shown in [**24**] and [**21**] that the zeros and the value four of binary Kloosterman sums give rise to semi-bent functions in even dimension with maximum degree, as well as to constructions of semi-bent functions of multiples traces terms under some conditions (on the coefficients of the Boolean functions defined on $\mathbb{F}_{2^n}$) involving the Dickson polynomials. Very recently, it was shown in [**6**] and [**23**] that the oval polymomials from finite projective geometry give rise to several constructions of semi-bent functions. In these references, several constructions of semi-bent functions in bivariate representation obtained from bent functions have been provided.

In this paper, we focus on the constructions of semi-bent functions. The idea is to exploit the known constructions of bent functions to design new semi-bent functions and therefore extend the list of the known primary constructions of semi-bent functions in even dimension. We organize this paper as follows. Section 2 is an introductory part providing some preliminaries including definitions and

background related to Boolean functions. Section 3 is devoted to the constructions of semi-bent functions from bent functions. Firstly, we revisited a part of a joint work of the second author with Carlet [**6**] by studying more in details (and providing a direct proof) of those constructions on the Galois field $\mathbb{F}_{2^n}$ (n even) by considering $\frac{n}{2}$-spreads of $\mathbb{F}_{2^n}$. Secondly, we treat the case of a kind of recursive construction of semi-bent functions (we shall call it a "secondary-like construction"). We prove that an indirect sum involving both bent and semi-bent functions leads to semi-bent functions. Finally, we construct semi-bent functions on $\mathbb{F}_{2^{n+2}}$ coming from bent functions on $\mathbb{F}_{2^n}$.

2. Notation and preliminaries

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

• *Boolean functions and polynomial forms*:
Let n be a positive integer. A Boolean function f in n variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. In cryptography, the most usual representation of these functions is the *algebraic Normal Form* (ANF) :

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

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.
Another possible representation of Boolean functions uses the identification between the vector-space $\mathbb{F}_2^n$ and the finite field $\mathbb{F}_{2^n}$. It represents 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 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 of the form called its *polynomial form*. First, 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 $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. We make use of the following known property of the trace function $Tr_1^n(x) = Tr_1^n(x^2)$ and for every integer r dividing k, the transitivity property of Tr_r^k, that is, $Tr_1^k = Tr_1^r \circ Tr_r^k$.
Now, the polynomial form of a Boolean function defined on $\mathbb{F}_{2^n}$ f is given by :

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

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,
- $a_j \in \mathbb{F}_{2^{o(j)}}$,
- $\epsilon = wt(f)$ modulo 2 where $wt(f)$, is the *Hamming weight* of the image vector of f, that is, the cardinality of its support $supp(f) := \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.

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 an affine function is a Boolean function whose algebraic degree is at most 1.

• *Walsh-Hadamard transform*

Let $\chi : \mathbb{F}_2 \mapsto \mathbb{Z}$ denote the nontrivial additive character of $\mathbb{F}_2$. The *"sign" function* of a Boolean function f is the integer-valued function $\chi_f = (-1)^f$.

Let f be a Boolean function defined on $\mathbb{F}_2^n$. Then the *Walsh Hadamard transform* of f is the discrete Fourier transform of χ_f, whose value at $\omega \in \mathbb{F}_2^n$ is defined as follows:

$$\forall \omega \in \mathbb{F}_2^n, \quad \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\omega \cdot x}$$

where "$\cdot$" is the scalar product in $\mathbb{F}_2^n$ defined as $x \cdot y = \sum_{i=1}^n x_i y_i$.

The notion of Walsh transform refers to a scalar product (note that in the definition of the Walsh transform, we can take any inner product; the cryptographic properties are not related to a particular choice, therefore the issue of the choice of the isomorphism does not arise). 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 : $x \cdot y = \sum_{i=1}^n x_i y_i = Tr_1^n(xy)$ for $x, y \in \mathbb{F}_{2^n}$. Thus 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 χ_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

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

and also the inverse Fourier formula

$$\sum_{\omega \in \mathbb{F}_{2^n}} \widehat{\chi_f}(\omega) = 2^n (-1)^{f(0)}.$$

Thanks to Parseval's relation and the inverse Fourier formula, one can prove the following well-known statement.

LEMMA 2.1. *Let f be a function on $\mathbb{F}_{2^n}$ such that for all $\omega \in \mathbb{F}_{2^n}$, $\widehat{\chi_f}(\omega) \geq 0$, then f is linear.*

• *Bent functions and semi-bent functions*:

Bent functions can be defined in terms of the Walsh transform as follows.

DEFINITION 2.2. A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be bent if $\widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}$, for all $\omega \in \mathbb{F}_{2^n}$.

Using Parseval's identity, one can prove (see for instance [**22**]) the following useful criterion of bentness in terms of congruence.

LEMMA 2.3. *Let g be a function on $\mathbb{F}_{2^n}$ with $n = 2m$. Then g is bent if and only if* $\forall \omega \in \mathbb{F}_{2^n}, \widehat{\chi_g}(\omega) \equiv 2^m \pmod{2^m + 1}$.

Semi-bent functions on $\mathbb{F}_{2^n}$ exist for can n even or n odd. But we are interested in this paper only in semi-bent functions when n even. Such functions are defined as follows.

DEFINITION 2.4. A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be semi-bent if $\widehat{\chi_f}(\omega) \in \{0, \pm 2^{\frac{n+2}{2}}\}$, for all $\omega \in \mathbb{F}_{2^n}$.

It is well known (see for instance [**4**]) that the algebraic degree of a bent and a semi-bent (with n even) Boolean function defined on $\mathbb{F}_{2^n}$ is at most $\frac{n}{2}$. Consequently, the Hamming weight of all these functions is even. Therefore, the polynomial form of these functions is

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) \tag{2.1}$$

where Γ_n, $o(j)$ are defined as above and $a_j \in \mathbb{F}_{2^{o(j)}}$.

From now, $n = 2m$ is an (even) integer.

3. Constructions of semi-bent functions from bent functions

In the sequel, we present several constructions of semi-bent functions involving bent functions.

3.1. Constructions of semi-bent functions on the Galois field $\mathbb{F}_{2^n}$ by considering m-spreads.

First recall that every non-zero element x of $\mathbb{F}_{2^n}$ has a unique decomposition (called the *polar decomposition*) as: $x = yu$ with $y \in \mathbb{F}_{2^m}^\star$ and $u \in U$ where U is the set defined by $\{u \in \mathbb{F}_{2^n} \mid norm(u) = 1\} = \{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$. In the sequel, U will always denote the cyclic group of $(2^m + 1)$-st roots of unity.

An m-spread of $\mathbb{F}_{2^n}$ can be defined as follow.

DEFINITION 3.1. An m-spread of $\mathbb{F}_{2^n}$ is a set of pairwise supplementary m-dimensional subspaces of $\mathbb{F}_{2^n}$ whose union equals $\mathbb{F}_{2^n}$.

In a joint work of the author with Carlet [**6**], semi-bent functions on $\mathbb{F}_{2^n}$ such that their restrictions to the elements of an m-spread have degree at most 1 have been investigated. As far as we know, the only m-spread in the literature is the set $\{u\mathbb{F}_{2^m}, u \in U\}$ where $U := \{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$ (viewed in $\mathbb{F}_{2^n}$) and its image by the linear automorphisms. Note that such an m-spread viewed in bivariate representation (that is, viewed in $\mathbb{F}_{2^n} \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$) corresponds to the sets $\{E_a, E_\infty\}$ where $E_a := \{(x, ax)\,;\, x \in \mathbb{F}_{2^m}\}$ and $E_\infty := \{(0, y)\,;\, y \in \mathbb{F}_{2^m}\}$.

First let $\mathcal{C}_n$ be 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 $f(0) = 0$. And let $\mathcal{L}_n$ be 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 $f(0) = 0$. Note that $f \in \mathcal{C}_n$ means that there exists a Boolean function

$b : U \to \mathbb{F}_2$ such that $f(uy) = b(u), \forall u \in U, \forall y \in \mathbb{F}_{2^m}^\star$ with $f(0) = 0$. While $f \in \mathcal{L}_n$ means that there exist a mapping $a : U \to \mathbb{F}_{2^m}$ and a Boolean function $b : U \to \mathbb{F}_2$ such that $f(uy) = Tr_1^m(a(u)y), \forall u \in U, \forall y \in \mathbb{F}_{2^m}^\star$.

In univariate form, functions of $\mathcal{C}_n$ are the so-called Dillon-like functions built with *Dillon-like exponents*. The name of Dillon-like exponent has been introduced in [**20**]. Such exponents are of the form $s(2^m - 1)$. In [**22**], the second author has proved the following statement.

PROPOSITION 3.2. *([**22**]) Let $n = 2m$. Let f be a Boolean function defined on $\mathbb{F}_{2^n}$ such that $f(0) = 0$. The three assertions are equivalent:*

1. $f(x) = \sum_i Tr_1^{o(d_i)}(a_i x^{d_i})$ *with* $\forall i, d_i \equiv 0 \pmod{2^m - 1}$;
2. $\forall u \in U$, *the restriction of* f *to* $u\mathbb{F}_{2^m}^\star$ *is constant (that is,* $f(uy) = f(u), \forall y \in \mathbb{F}_{2^m}^\star$*);*
3. $\forall \omega \in \mathbb{F}_{2^n}$ *the restriction of* f *to* $\omega\mathbb{F}_{2^m}^\star$ *is constant (that is,* $f(\omega y) = f(\omega), \forall y \in \mathbb{F}_{2^m}^\star$*).*

The following statement has been proved in a joint work of the second author with Carlet [**5**].

PROPOSITION 3.3. *([**5**]) Let f be a Boolean function over $\mathbb{F}_{2^n}$ and $f(t) = \sum_{d=0}^{2^n-1} a_d t^d$ its univariate representation. Then the restrictions of f to the vectorspaces $\omega\mathbb{F}_{2^m}$, $\omega \in \mathbb{F}_{2^n}^\star$, are all linear if and only if the only exponents d such that $a_d \neq 0$ are congruent to powers of 2 modulo $2^m - 1$, more precisely, $d \equiv 2^j \pmod{2^m - 1}$ for some j, $0 \leq j \leq m - 1$.*

The exponents d in the previous proposition are currently called the *Niho exponents* since they were first studied by Niho in his thesis [**26**]. Moreover, it is well known that a Niho exponent d (always understood modulo $2^n - 1$) can be written in normalized form as $d = (2^m - 1)s + 1$ with $0 < s < 2^m - 1$ (note that $d \equiv -2s + 1$ modulo $2^m + 1$). In univariate form, functions of $\mathcal{L}_n$ are called Niho functions since they are constructed via Niho exponents. Now, let us introduce the following notation.

NOTATION 3.4. Denote by $\mathcal{D}_n$ the bent functions in $\mathcal{C}_n$ and by $\mathcal{N}_n$ the bent functions in $\mathcal{L}_n$.

According to the discussion above, we have

$$\mathcal{D}_n = \{f \mid f(x) = \sum_i Tr_1^{o(d_i)}(a_i x^{d_i}) \text{ with } \forall i, d_i \equiv 0 \pmod{2^m - 1}, f \text{ bent with } f(0) = 0\}$$

and

$$\mathcal{N}_n = \{f \mid f(x) = \sum_i Tr_1^{o(d_i)}(a_i x^{d_i}) \text{ with } \forall i, d_i = (2^m - 1)s_i + 1, 2 \leq s_i \leq 2^m, f \text{ bent with} f(0) = 0\}.$$

A list of the known functions in $\mathcal{D}_n$ can be found in [**25**] with additional functions in [**17**]. A list of the known functions in $\mathcal{N}_n$ can be found for instance in [**20**].

In the following, semi-bent functions on $\mathbb{F}_{2^n}$ such that their restrictions to the elements of the m-spread $u\mathbb{F}_{2^m}$ are affine, are revisited. We introduce the following notation.

NOTATION 3.5.

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

Note that $f \in \mathcal{A}_n$ means that there exists a mapping $a : U \to \mathbb{F}_{2^m}$ and a Boolean function $b : U \to \mathbb{F}_2$ such that $f(uy) = Tr_1^m(a(u)y) + b(u)$, $\forall u \in U, \forall y \in \mathbb{F}_{2^m}^\star$.

We denote by $f_{a,b}$ (where $a : U \to \mathbb{F}_{2^m}$ and $b : U \to \mathbb{F}_2$) a function in $\mathcal{A}_n$. Therefore, we have the following natural decomposition:

$$f_{a,b} = f_{a,0} + f_{0,b}$$

where $f_{a,0}$ is a Boolean function defined on $\mathbb{F}_{2^n}$ such that its restrictions to $u\mathbb{F}_{2^m}^\star$ $(u \in U)$ are linear and $f_{0,b}$ is a Boolean function on $\mathbb{F}_{2^n}$ such that its restrictions to $u\mathbb{F}_{2^m}^\star$ $(u \in U)$ are constant.

REMARK 3.6. $f_{a,b} \in \mathcal{A}_n$ if and only if $1 + f_{a,b} \in \mathcal{A}_n$. Indeed, if $f_{a,b} \in \mathcal{A}_n$ then, $\forall u \in U,\ \forall y \in \mathbb{F}_{2^m}^\star$, we have

$$1 + f_{a,b}(uy) = Tr_1^m(a(u)y) + b'(u)$$

with $b'(u) := b(u) + 1$, which means that $1 + f_{a,b} \in \mathcal{A}_n$. The converse is trivial, and we have $1 + f_{a,b} = f_{a,b+1}$.

NOTATION 3.7. For $\epsilon \in \{0, 1\}$, set

$$\mathcal{A}_n^\epsilon := \{f \in \mathcal{A}_n \mid f_{a,b}(0) = \epsilon\}.$$

We have

$$\mathcal{A}_n^\epsilon = \mathcal{A}_n^0 \cup \mathcal{A}_n^1 = \mathcal{A}_n^0 \cup (1 + \mathcal{A}_n^0)$$

where $1 + \mathcal{A}_n^0$ is the complement of functions in $\mathcal{A}_n^0$. In the following, we are interested in identifying the functions in $\mathcal{A}_n$ which are semi-bent. Since semi-bentness is affine invariant, it suffices to study the semi-bent functions in $\mathcal{A}_n^0$.

The Walsh transform of a function in $\mathcal{A}_n^0$ can be expressed as follows.

PROPOSITION 3.8. *Let $f_{a,b}$ be a function in $\mathcal{A}_n^0$. Then the Walsh transform of $f_{a,b}$ equals $\widehat{\chi_{f_{a,b}}}(\omega) = 1 - \sum_{u\in U}(-1)^{b(u)} + 2^m \sum_{u\in U | a(u)+Tr_m^n(\omega u)=0}(-1)^{b(u)}, \forall \omega \in \mathbb{F}_{2^n}$.*

PROOF. Let $f_{a,b} \in \mathcal{A}_n^0$. For all $\omega \in \mathbb{F}_{2^n}$, we have (using the polar decomposition and the properties of trace functions)

$$\begin{aligned}
\widehat{\chi_{f_{a,b}}}(\omega) &= 1 + \sum_{x\in\mathbb{F}_{2^n}^\star} (-1)^{f_{a,b}(x)+Tr_1^n(\omega x)} \\
&= 1 + \sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^\star} (-1)^{f_{a,b}(uy)+Tr_1^n(\omega uy)} \\
&= 1 + \sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^\star} (-1)^{Tr_1^m(a(u)y)+b(u)+Tr_1^m(Tr_m^n(\omega u)y)} \\
&= 1 + \sum_{u\in U}\Big(\sum_{y\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(a(u)y)+b(u)+Tr_1^m(Tr_m^n(\omega u)y)} - (-1)^{b(u)}\Big) \\
&= 1 - \sum_{u\in U}(-1)^{b(u)} + \sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(a(u)y)+b(u)+Tr_1^m(Tr_m^n(\omega u)y)} \\
&= 1 - \sum_{u\in U}(-1)^{b(u)} + \sum_{u\in U}(-1)^{b(u)}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m((a(u)+Tr_m^n(\omega u))y)}.
\end{aligned} \tag{3.1}$$

But $\sum_{y\in\mathbb{F}_{2^m}}\chi(Tr_1^m\Big((a(u)+Tr_m^n(\omega u))y\Big)$

$$=\begin{cases}2^m & \text{if } a(u)+Tr_m^n(\omega u)=0\\ 0 & \text{otherwise}\end{cases}$$

that is, $\sum_{y\in\mathbb{F}_{2^m}}(-1)^{Tr_1^m\Big((a(u)+Tr_m^n(\omega u))y\Big)}=2^m\delta_0(a(u)+Tr_m^n(\omega u))$, where δ_0 is such that $\delta(x)=1$ if $x=0$ and, 0 otherwise.

$$\widehat{\chi_{f_{a,b}}}(\omega)=1-\sum_{u\in U}(-1)^{b(u)}+\sum_{u\in U}(-1)^{b(u)}2^m\delta_0(a(u)+Tr_m^n(\omega u)) \tag{3.2}$$
$$=1-\sum_{u\in U}(-1)^{b(u)}+2^m\sum_{u\in U|a(u)+Tr_m^n(\omega u)=0}(-1)^{b(u)}.$$

□

Next we provide an alternative direct proof of the following theorem (Corollary 5, [**6**]) which identifies in particular all the semi-bent functions in $\mathcal{A}_n$. The reader can notice that the theorem has been obtained in [**6**] by applying Theorem 1 in [**6**]. Moreover, the statement concerns only the functions whose restrictions to the m-spreads are affine but not constant and not linear (in fact, it is proved in [**5**] that there exist no semi-bent functions whose restrictions to the m-spreads are linear).

THEOREM 3.9. *Let $n=2m$ with $m>2$. A semi-bent function in $\mathcal{A}_n$ can be written as the sum of a (bent) function in $\mathcal{D}_n$ and a (bent) function in $\mathcal{N}_n$, where $\mathcal{A}_n$, $\mathcal{D}_n$ and $\mathcal{N}_n$ are defined as in Notation 3.5 and Notation 3.4.*

PROOF. According to the discussion above, it suffices to treat the case of semi-bent functions in $\mathcal{A}_n^0$. So, let $f_{a,b}\in\mathcal{A}_n^0$.
According to Proposition 3.8,

$$\widehat{\chi_{f_{a,b}}}(\omega)=1-\sum_{u\in U}(-1)^{b(u)}+2^m\sum_{u\in E_\omega}(-1)^{b(u)},\forall\omega\in\mathbb{F}_{2^n}$$

where $E_\omega:=\{u\in U\mid a(u)+Tr_m^n(\omega u)=0\}$.
Now, $f_{a,b}$ is semi-bent if and only if $\widehat{\chi_{f_{a,b}}}(\omega)\in\{0,\pm 2^{m+1}\},\forall\omega\in\mathbb{F}_{2^n}$, which implies that $\widehat{\chi_{f_{a,b}}}(\omega)\equiv 0 \pmod{2^m},\forall\omega\in\mathbb{F}_{2^n}$, that is, $\sum_{u\in U}(-1)^{b(u)}\equiv 1 \pmod{2^m}$. Therefore, $\sum_{u\in U}(-1)^{b(u)}\in\{1,1+2^m,1-2^m\}$ (since the multiplicative group U is of order 2^m+1). Three cases have to be considered.
Recall the following decomposition: $f_{a,b}=f_{a,0}+f_{0,b}$, where $f_{a,0}$ (resp. $f_{0,b}$) is such that its restrictions to each multiplicative coset $u\mathbb{F}_{2^m}^\star$ $(u\in U)$ is constant (resp. linear).
• Case 1: $\sum_{u\in U}(-1)^{b(u)}=1$.
The function $f_{0,b}$ is such that its restrictions to the multiplicative cosets $u\mathbb{F}_{2^n}^\star$ are constant for every $u\in U$. Hence, for every $\omega\in\mathbb{F}_{2^n}$ the restriction of $f_{0,b}$ to $\omega\mathbb{F}_{2^m}^\star$ is constant (that is, $f_{0,b}(\omega y)=f_{0,b}(\omega),\forall y\in\mathbb{F}_{2^m}^\star$). Indeed, if $\omega\in\mathbb{F}_{2^n}^\star$, then using the polar decomposition, we have: $\omega=uz$ with $u\in U$ and $z\in\mathbb{F}_{2^m}^\star$. Hence, $\forall y\in\mathbb{F}_{2^m}^\star$, $f_{0,b}(\omega y)=f_{0,b}(uzy)=f_{0,b}(u)=f_{0,b}(uz)=f_{0,b}(\omega)$.
Consider the polynomial form of $f_{0,b}$: $f_{0,b}(x)=\sum_{i=1}^{2^n-2}Tr_1^{o(i)}(a_ix^i)+a_{2^n-1}x^{2^n-1}$ (since $f_{0,b}(0)=0$). Then (since $y\in\mathbb{F}_{2^m}^\star\subset\mathbb{F}_{2^n}^\star$ and $y^i=1$ for $i\equiv 0 \pmod{2^m-1}$),

we have: $\forall \omega \in \mathbb{F}_{2^n}$, $\forall y \in \mathbb{F}_{2^m}^\star$,

$$
\begin{aligned}
f_{0,b}(\omega y) &= \sum_{i=1}^{2^n-2} Tr_1^{o(i)}(a_i \omega^i y^i) + a_{2^n-1}\omega^{2^n-1} \\
&= \sum_{i=1 | i \equiv 0 \pmod{2^m-1}}^{2^n-2} Tr_1^{o(i)}(a_i \omega^i) + a_{2^n-1}\omega^{2^n-1} \\
&+ \sum_{i=1 | i \not\equiv 0 \pmod{2^m-1}}^{2^n-2} Tr_1^{o(i)}(a_i \omega^i y^i) + a_{2^n-1}\omega^{2^n-1}.
\end{aligned} \tag{3.3}
$$

Now, note that for $y = 1$, we have

$$
\begin{aligned}
f_{0,b}(\omega) &= \sum_{i=1 | i \equiv 0 \pmod{2^m-1}}^{2^n-2} Tr_1^{o(i)}(a_i \omega^i + a_{2^n-1}\omega^{2^n-1}) \\
&+ \sum_{i=1 | i \not\equiv 0 \pmod{2^m-1}}^{2^n-2} Tr_1^{o(i)}(a_i \omega^i) + a_{2^n-1}\omega^{2^n-1}.
\end{aligned}
$$

But we have $f_{0,b}(\omega y) + f_{0,b}(\omega) = 0$, $\forall \omega \in \mathbb{F}_{2^n}, \forall y \in \mathbb{F}_{2^m}^\star$. Therefore, $\forall \omega \in \mathbb{F}_{2^n}, \forall y \in \mathbb{F}_{2^m}^\star$, $\sum_{i=1 | i \not\equiv 0 \pmod{2^m-1}}^{2^n-2} Tr_1^{o(i)}(a_i(y^i+1)\omega^i) = 0$ Now, using the unicity of the polar decomposition, we obtain $\forall i \in [1, 2^n-2], i \not\equiv 0 \pmod{2^m-1}, a_i(y^i+1) = 0$. In particular, if y equals a primitive element β of $\mathbb{F}_{2^m}$ then $y^i = \beta^i \neq 1$. Hence, $\forall i \in [1, 2^n-2], i \not\equiv 0 \pmod{2^m-1}, a_i = 0$, which proves that the polynomial form of $f_{0,b}$ is: $f_{0,b}(x) = \sum_i Tr_1^{o(d_i)}(a_i x^{d_i})$ with $\forall i, d_i \equiv 0 \pmod{2^m-1}$. At this stage, let us prove that the condition $\sum_{u \in U}(-1)^{b(u)} = 1$ is equivalent to the fact that $f_{0,b}$ is bent. To this end, let us compute the Walsh transform of $f_{0,b}$ for $\omega \in \mathbb{F}_{2^n}$.

$$
\begin{aligned}
\widehat{\chi_{f_{0,b}}}(\omega) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\sum_i Tr_1^{o(d_i)}(a_i x^{d_i}) + Tr_1^n(\omega x)} \\
&= 1 + \sum_{x \in \mathbb{F}_{2^n}^\star} (-1)^{\sum_i Tr_1^{o(d_i)}(a_i x^{d_i}) + Tr_1^n(\omega x)} \\
&= 1 + \sum_{u \in U} \sum_{y \in \mathbb{F}_{2^m}^\star} (-1)^{\sum_i Tr_1^{o(d_i)}(a_i y^{d_i} u^{d_i}) + Tr_1^n(\omega y u)} \\
&= 1 + \sum_{u \in U} \sum_{y \in \mathbb{F}_{2^m}^\star} (-1)^{\sum_i Tr_1^{o(d_i)}(a_i u^{d_i}) + Tr_1^n(\omega y u)} \\
&= 1 + \sum_{u \in U} (-1)^{\sum_i Tr_1^{o(d_i)}(a_i u^{d_i})} \sum_{y \in \mathbb{F}_{2^m}^\star} (-1)^{Tr_1^n(\omega y u)} \\
&= 1 + \sum_{u \in U} (-1)^{\sum_i Tr_1^{o(d_i)}(a_i u^{d_i})} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^n(\omega y u)} \\
&- \sum_{u \in U} (-1)^{\sum_i Tr_1^{o(d_i)}(a_i u^{d_i})}.
\end{aligned} \tag{3.4}
$$

Firstly, if $\omega = 0$ then, $\widehat{\chi_f}(0) = 1 + 2^m \sum_{u \in U}(-1)^{\sum_i Tr_1^{o(d_i)}(a_i u^{d_i})} - \sum_{u \in U}(-1)^{\sum_i Tr_1^{o(d_i)}(a_i u^{d_i})}$. Hence, the condition $\sum_{u \in U}(-1)^{b(u)} = 1$ is equivalent to $\widehat{\chi_f}(0) = 2^m$ that is, $f_{0,b}$

bent. Otherwise, if $\omega \neq 0$ then, $\sum_{y\in\mathbb{F}_{2^m}} \chi(Tr_1^n(\omega yu)) = \sum_{y\in\mathbb{F}_{2^m}} \chi(Tr_1^m(Tr_m^n(\omega u)y))$

$$= \begin{cases} 2^m & \text{if } Tr_m^n(\omega u) = 0, \text{ that is, if } u^{2^m-1} = \omega^{1-2^m} \\ 0 & \text{otherwise.} \end{cases}$$

Since $x \mapsto x^{2^m-1}$ is a permutation of U then, $\sum_{y\in\mathbb{F}_{2^m}} \chi(Tr_1^n(\omega yu))$

$$= \begin{cases} 2^m & \text{if } u = \omega^{-1} \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, $\widehat{\chi_f}(\omega) = 1 - \sum_{u\in U}(-1)^{\sum_i Tr_1^{o(d_i)}(a_i u^{d_i})} + 2^m(-1)^{f(\omega^{-1})}$. Hence, $f_{0,b}$ is bent if and only if $\sum_{u\in U}(-1)^{\sum_i Tr_1^{o(d_i)}(a_i u^{d_i})} = 1$ that is, $\sum_{u\in U}(-1)^{b(u)} = 1$. Therefore, we have proved that the condition on $b(u)$ implies that $f_{0,b}$ is bent. Moreover, for every $\omega \in \mathbb{F}_{2^n}$, $\widehat{\chi_{f_{a,b}}}(\omega) = 2^m \sum_{u\in E_\omega}(-1)^{b(u)} \in \{0, \pm 2^{m+1}\}$. Hence, $\sum_{u\in E_\omega}(-1)^{b(u)} \equiv 0 \pmod 2$. But $\sum_{u\in E_\omega}(-1)^{b(u)} \equiv \sum_{u\in E_\omega} 1 \pmod 2$. Thus, $\#E_\omega \equiv 0 \pmod 2$ that is, $\#E_\omega$ is even for every $\omega \in \mathbb{F}_{2^n}$. Set $\#E_\omega = 2\kappa(\omega)$ with $\kappa(w) \in \mathbb{Z}$. Now, we have $f_{a,0}(uy) = Tr_1^m(a(u)y)$. Hence, $\widehat{\chi_{f_{a,0}}}(\omega) = 1 - \sum_{u\in U}(-1)^0 + 2^m \sum_{u\in E_\omega}(-1)^0$, that is, $\widehat{\chi_{f_{a,0}}}(\omega) = 1 - \#U + 2^m \#E_\omega = 2^m(\#E_\omega - 1)$. Therefore, $\widehat{\chi_{f_{a,0}}}(\omega) = 2^m(2\kappa(\omega) - 1) \equiv -2^m \pmod{2^{m+1}} \equiv 2^m \pmod{2^{m+1}}$. Thus, according to Lemma 2.3, $f_{a,0}$ is bent and then, $f_{a,0}$ belongs to $\mathcal{L}_n$.

• Case 2: $\sum_{u\in U}(-1)^{b(u)} = 1 + 2^m$.

Since $\#U = 2^m + 1$, the mapping $u \mapsto b(u)$ vanishes on U. Thus $f_{a,b} = f_{a,0}$. Now, recall that we have $\widehat{\chi_{f_{a,0}}} = 2^m(\#E_\omega - 1), \forall \omega \in \mathbb{F}_{2^n}$. Since $f_{a,b}$ is semi-bent then, $2^m(\#E_\omega - 1) \in \{0, \pm 2^{m+1}\}$, that is, $\#E_\omega \in \{1, 3\}$. Hence, $\widehat{\chi_{f_{a,0}}} \geq 0$ which implies, according to Lemma 2.1, that $f_{a,0}$ is linear and its Walsh spectrum equals $\{0, 2^n\}$. This contradicts the semi-bentness of $f_{a,0} = f_{a,b}$. The Case 2 is thus excluded.

• Case 3: $\sum_{u\in U}(-1)^{b(u)} = 1 - 2^m$.

One can prove that there exists a unique $u_o \in U$ such that $b(u_0) = 0$ and $b(u) = 1$ for every $u \in U\backslash\{u_0\}$. Indeed, for $\epsilon \in \{0, 1\}$ denote by B_ϵ the set $\{u \in U \mid b(u) = \epsilon\}$. We have $\sum_{u\in U}(-1)^{b(u)} = \sum_{u\in B_0}(-1)^{b(u)} + \sum_{u\in B_1}(-1)^{b(u)} = 1 - 2^m = \#B_0 - \#B_1$. Hence, $\#B_0 = 1$ and $\#B_1 = 2^m$ (since $\#B_0 + \#B_1 = \#U = 2^m + 1$).

The function $u \in U \mapsto b(u)$ thus equals $\mathbf{1}_U + \mathbf{1}_{u_0\mathbb{F}_{2^m}}$ and $f_{a,b} = f_{a,0} + \mathbf{1}_U + \mathbf{1}_{u_0\mathbb{F}_{2^m}}$. Now, we have $\widehat{\chi_{f_{a,b}}}(\omega) = 2^m + 2^m \sum_{u\in E_\omega}(-1)^{b(u)}, \forall \omega \in \mathbb{F}_{2^n}$ (where E_ω is defined as above). Since $f_{a,b}$ is semi-bent, one has necessarily $2^m(1 + \sum_{u\in E_\omega}(-1)^{b(u)}) \in \{0, \pm 2^{m+1}\}$, that is $1 + \sum_{u\in E_\omega}(-1)^{b(u)} \in \{0, \pm 2\}$. But $(-1)^{b(u)} \equiv 1 \pmod 2$. Hence $\#E_\omega$ is odd (in particular, $\#E_\omega \geq 1$). But $f_{a,0}(uy) = Tr_1^m(a(u)y)$, hence $\widehat{\chi_{f_{a,0}}}(\omega) = 1 - \sum_{u\in U}(-1)^0 + 2^m \sum_{u\in E_\omega}(-1)^0 = 2^m(\#E_\omega - 1) \geq 0$. According to Lemma 2.1, we deduce that the function $f_{a,0}$ is linear. Thus, $f_{a,b} = f_{a,0} + \mathbf{1}_U + \mathbf{1}_{u_0\mathbb{F}_{2^m}}$ with $f_{a,b}$ semi-bent and $f_{a,0} + \mathbf{1}_U$ is an affine function. Therefore the function $g := \mathbf{1}_{u_0\mathbb{F}_{2^m}}$ is semi-bent. Thus its Hamming weight $wt(g) \in \{2^{n-1} - 2^m, 2^{n-1} + 2^m, 2^{n-1}\}$ (since $\widehat{\chi_g}(0) = 2^n - 2wt(g) \in \{0, 2^{m+1}, -2^{m+1}\}$). But (using the definition of g) we have $wt(g) = 2^m$. We conclude that for $m > 2$ the function g can not be semi-bent. The proof follows. □

3.2. A construction of semi-bent functions via the indirect sum.

In 2004, Carlet [**3**] has introduced a secondary construction of bent functions that he called *indirect sum*. This construction generalizes the well-known direct sum given by Dillon and Rothaus [**9, 27**] and is defined as follows.

DEFINITION 3.10. 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 (that is, h is the concatenation of the four functions f_1, $f_1 \oplus 1$, f_2 and $f_2 \oplus 1$, in an order controled by $g_1(y)$ and $g_2(y)$):

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

This construction was used in [**3**] to construct bent functions from bent functions in lower dimension. In the following, we show that the indirect sum could be used to construct semi-bent functions from both bent and semi-bent functions in lower dimension. More precisely, we prove the following result which can be viewed as a secondary-like construction [1].

THEOREM 3.11. *Let $n = r + s$ with r and s two even intergers. Let h be defined as in Definition 3.10. Suppose 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 :

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

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

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

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. □

[1] As opposed to "secondary constructions " which means constructions of new functions from ones having the same properties.

REMARK 3.12. 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 3.11, that is, suppose that f_1 and f_2 are bent and that g_1 and g_2 are semi-bent.

3.3. A 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.

PROPOSITION 3.13. *Let n be an even positive integer. Let f be a Boolean function over $\mathbb{F}_{2^n}$. For $\delta \in \mathbb{F}_4$, we define a Boolean function f_δ over $\mathbb{F}_{2^{n+2}} \simeq \mathbb{F}_{2^n} \times \mathbb{F}_4$ 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 $\mathbb{F}_{2^{n+2}}$.

PROOF. Let us compute the Walsh transform at every $\omega := (\omega', \omega_1) \in \mathbb{F}_{2^n} \times \mathbb{F}_4$.

$$\begin{aligned} \widehat{\chi_{f_\delta}}(\omega) &= \sum_{y \in \mathbb{F}_{2^n}} \sum_{z \in \mathbb{F}_{2^2}} (-1)^{f_\delta(y,z) + Tr_1^n(\omega' y) + Tr_1^2(\omega_1 z)} \\ &= \sum_{y \in \mathbb{F}_{2^n}} (-1)^{f(y) + Tr_1^n(\omega' y)} \sum_{z \in \mathbb{F}_{2^2}} (-1)^{Tr_1^2(z(\omega_1 + \delta)} \\ &= \widehat{\chi_f}(\omega') \sum_{z \in \mathbb{F}_{2^2}} (-1)^{Tr_1^2(z(\omega_1 + \delta)}. \end{aligned} \tag{3.5}$$

Now, since f is bent then $\widehat{\chi_f}(\omega') = \pm 2^{\frac{n}{2}}$. On the other hand,

$$\sum_{z \in \mathbb{F}_{2^2}} (-1)^{Tr_1^2(z(\omega_1 + \delta)} = \begin{cases} 4 & \text{if } \omega_1 = \delta \\ 0 & \text{otherwise.} \end{cases}$$

Hence, $\widehat{\chi_{f_\delta}}(\omega) \in \{0, 2^{\frac{n+2}{2}+1}, -2^{\frac{n+2}{2}+1}\}$ proving that f_δ is semi-bent on $\mathbb{F}_{2^n} \times \mathbb{F}_4$. □

4. Conclusion

A lot of research has been devoted to designing constructions of bent functions. This paper investigates constructions of semi-bent functions. To this end, bent functions are exploited to produce new semi-bent functions and thereby extend the list of known primary constructions of semi-bent functions in even dimension.

References

1. M. Burnashev and I. Dumer, *Error-exponents for recursive Decoding of Reed-Muller codes on a binary-symmetric channel*, IEEE Trans. Inform Theory vol 52, No 11, 2006, pp. 4880–4892.
2. A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine., *On cryptographic properties of the cosets of R(1,m)*, IEEE Transactions on Information Theory, vol. 47, 2001, pp. 1494–1513.
3. C. Carlet, *On the secondary constructions of resilient and bent functions*, Proceedings of the Workshop on Coding, Cryptography and Combinatorics 2003, published by Birkhäuser Verlag, 2004, pp. 3–28.
4. ———, *Boolean Functions for Cryptography and Error Correcting Codes*, Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering" published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.), 2010, pp. 257–397.

5. C. Carlet and S. Mesnager, *On Dillon's class H of bent functions, Niho bent functions and O-polynomials*, Journal of Combinatorial Theory, Series A, Vol 118, no. 8, 2011, pp. 2392–2410.
6. ———, *On Semi-bent Boolean Functions*, IEEE Transactions on Information Theory-IT, Vol 58 No 5, 2012, pp. 3287–3292.
7. P. Charpin, E. Pasalic, and C. Tavernier., *On bent and semi-bent quadratic Boolean functions*, IEEE Transactions on Information Theory, vol. 51, no. 12, 2005, pp. 4286–4298.
8. S. Chee, S. Lee, and K. Kim, *Semi-bent Functions*, Advances in Cryptology-ASIACRYPT94. Proc. 4th Int. Conf. on the Theory and Applications of Cryptology, Wollongong, Australia. Pieprzyk, J. and Safavi-Naini, R., Eds., Lect. Notes Comp. Sci, vol 917, 1994, pp. 107–118.
9. J. Dillon, *Elementary Hadamard difference sets*, PhD dissertation, University of Maryland.
10. I. Dumer, *Recursive Decoding and its performance for low-rate Reed-Muller codes*, IEEE Trans. Inform Theory vol 50, No 5, 2004, pp. 811–823.
11. R. Gold, *Maximal recursive sequences with 3-valued recursive crosscorrelation functions*, IEEE Trans. Inform. Theory 14 (1), 1968, pp. 154–156.
12. T. Helleseth, *Some results about the cross-correlation function between two maximal linear sequences*, Discr. Math, vol. 16, 1976, pp. 209–232.
13. ———, *Correlation of m-sequences and related topics*, Proc. SETA98, Discrete Mathematics and Theoretical Computer Science, C. Ding, T. Helleseth, and H. Niederreiter, Eds. London, U.K.: Springer, 1999, pp. 49–66.
14. T. Helleseth and P. V. Kumar, *Sequences with low correlation*, Handbook of Coding Theory, Part 3: Applications, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, chapter. 21, 1998, pp. 1765–1853.
15. K. Khoo, G. Gong, and D. R. Stinson, *A new family of Gold-like sequences*, IEEE Trans. Inform. Theory Lausanne, Switzerland, 2002, p. 181.
16. ———, *A new characterization of semibent and bent functions on finite fields*, Des. Codes. Cryptogr. vol. 38, no. 2, 2006, pp. 279–295.
17. N. Li, T. Helleseth, X. Tang, and A. Kholosha, *Several new classes of bent functions from Dillon exponents*, IEEE Transactions on Information Theory Vol 59(3), 2013, pp. 1818–1831.
18. M. Matsui, *Linear cryptanalysis method for DES cipher.*, Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science 765, 1994, pp. 386–397.
19. W. Meier and O. Staffelbach, *Fast correlation attacks on stream ciphers.*, Advances in Cryptology, EUROCRYPT'88, Lecture Notes in Computer Science 330, 1988, pp. 301–314.
20. S. Mesnager, *Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials*, IEEE Transactions on Information Theory **57** (2011), no. 9, 5996–6009.
21. ———, *Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials.*, IEEE Transactions on Information Theory-IT, Vol 57, No 11, 2011, pp. 7443–7458.
22. ———, *Bent functions from Spreads. Preprint.*, 2013.
23. ———, *Semi-bent functions from oval polynomials*, Proceedings of Fourteenth International Conference on Cryptography and Coding, Oxford, United Kingdom, IMACC 2013, LNCS 8308, Springer, Heidelberg, 2013, pp. 1–15.
24. S. Mesnager and G. Cohen, *On the link of some semi-bent functions with Kloosterman sums*, IWCC (Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, eds.), Lecture Notes in Computer Science, vol. 6639, Springer, 2011, pp. 263–272.
25. S. Mesnager and J.P. Flori, *Hyper-bent functions via Dillon-like exponents.*, IEEE Transactions on Information Theory. Vol 59 (5), 2013, pp. 3215– 3232.
26. Y. Niho, *Multi-valued cross-correlation functions between two maximal linear recursive sequences*, Ph.D. dissertation, Univ. Sothern Calif., Los Angeles, 1972.
27. O.S. Rothaus, *On "bent" functions*, J. Combin.Theory Ser A 20, 1976, pp. 300–305.
28. G. Sun and C.Wu, *Construction of Semi-Bent Boolean Functions in Even Number of Variables*, Chinese Journal of Electronics, vol 18, No 2, 2009.
29. Y. Zheng and X. M. Zhang, *Plateaued functions*, Advances in Cryptology-ICICS 1999, vol 1726 Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1999, pp. 284–300.
30. ———, *Relationships between bent functions and complementary plateaued functions*, Lecture Notes in Computer Science, vol 1787, 1999, pp. 60–75.

Ecole Nationale Supérieure des Télécommunications -Telecom-Paristech, UMR 5141, CNRS, France.
E-mail address: cohen@telecom-paristech.fr

Department of Mathematics, University of Paris VIII and University of Paris XIII. CNRS UMR 7539 LAGA (Laboratoire Analyse, Géometrie et Applications), Sorbonne Paris Cité, 2 rue de la liberté, F-93526 Saint-Denis Cedex, France.
E-mail address: smesnager@univ-paris8.fr