Available online at www.sciencedirect.com
ScienceDirect
Finite Fields and Their Applications 14 (2008) 221–241
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

A new class of monomial bent functions

Anne Canteaut [a], Pascale Charpin [a,*], Gohar M. Kyureghyan [b]

[a] *INRIA projet CODES, B.P. 105, 78153 Le Chesnay Cedex, France*
[b] *Department of Mathematics, Otto-von-Guericke University of Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany*

Received 19 June 2006; revised 1 February 2007

Available online 12 March 2007

Communicated by Harald Niederreiter

Abstract

We study the Boolean functions $f_\lambda : \mathbf{F}_{2^n} \to \mathbf{F}_2$, $n = 6r$, of the form $f(x) = \mathrm{Tr}(\lambda x^d)$ with $d = 2^{2r} + 2^r + 1$ and $\lambda \in \mathbf{F}_{2^n}$. Our main result is the characterization of those λ for which f_λ are bent. We show also that the set of these cubic bent functions contains a subset, which with the constantly zero function forms a vector space of dimension $2r$ over $\mathbf{F}_2$. Further we determine the Walsh spectra of some related quadratic functions, the derivatives of the functions f_λ.

Keywords: Boolean function; Bent function; Monomial function; Cubic function; Quadratic function; Derivatives of Boolean functions; Permutation polynomials

1. Introduction

A number of recent papers are devoted to the description of new classes of bent functions. One of the main purpose is to determine bent functions which do not belong to a previously known class. For instance, in [4] are constructed non-normal bent functions and in [8] bent functions are obtained by concatenating quadratic functions. Another goal is to find new expressions of bent functions over finite fields. It is essentially the expressions by means of trace-functions which are considered in [13,17,18]. More generally, any polynomial $P(x)$ in $\mathbf{F}_{2^n}[x]$ can be viewed as a function with n inputs and n outputs. The properties of P are then studied by means of

* Corresponding author.
E-mail addresses: anne.canteaut@inria.fr (A. Canteaut), pascale.charpin@inria.fr (P. Charpin), gohar.kyureghyan@mathematik.uni-magdeburg.de (G.M. Kyureghyan).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2007.02.004

their 2^n component functions, the Boolean functions $x \mapsto \mathrm{Tr}(\lambda P(x))$ where Tr is the trace function from $\mathbf{F}_{2^n}$ to $\mathbf{F}_2$. Determining the weights of these functions is of great interest in coding theory and cryptography (see [1,13] and [7], for instance).

Our paper is a contribution to the study of the so-called *monomial* bent functions. The monomial Boolean functions $\mathbf{F}_{2^n}$ are those that can be expressed as $x \mapsto \mathrm{Tr}(\lambda x^d)$ for some $\lambda \in \mathbf{F}_{2^n}$ and an integer d. The characterization of the exponents d and the corresponding λ defining a bent monomial function on $\mathbf{F}_{2^n}$ is a difficult open problem. In this paper we study the monomial Boolean functions on fields $\mathbf{F}_{2^n}$ with $n = 6r$ $(r > 1)$ given by

$$f_\lambda(x) = \mathrm{Tr}\big(\lambda x^d\big), \quad d = 2^{2r} + 2^r + 1,\ \lambda \in \mathbf{F}_{2^n}^*. \tag{1}$$

We first prove that the weight of f_λ takes only three values when λ runs through $\mathbf{F}_{2^n}^*$, one of them corresponding to the bent case (Theorem 1). We later describe the set of those λ such that f_λ is bent and we prove that these functions are Maiorana–McFarland bent functions. Moreover, we show that a part of these functions form a subspace of dimension $2r$ of Boolean bent functions on $\mathbf{F}_{2^n}$. All these $2^{2r} - 1$ bent functions are cubic (Theorem 3).

The functions f_λ which are not bent appear as a concatenation of quadratic functions on $\mathbf{F}_{2^{3r}}$ (Theorem 2). We derive a divisibility property of their Walsh spectra (Corollary 1). In Section 3.4 we state some open problems on the Walsh spectra of these functions.

Many properties of a Boolean function are connected with the properties of its *derivatives*. For example, the derivatives of a Boolean function are used to obtain lower bounds on the *nonlinearity profile* [5]. The derivatives are also involved in the computations of several criteria about the optimality of a Boolean function for the cryptographic applications (see [6] and, for instance, [3]). In Section 4, we study the derivatives of a bent and non-bent function f_λ. We show that the Walsh transform of such a derivative takes either the values $\{0, \pm 2^{5r}\}$ or the values $\{0, \pm 2^{4r}\}$ (Theorem 4).

2. Preliminaries

In the whole paper, α is a primitive element of $\mathbf{F}_{2^n}$. A Boolean function on $\mathbf{F}_{2^n}$ is a function of the form $x \mapsto \mathrm{Tr}(P(x))$, where P is any polynomial in $\mathbf{F}_{2^n}[x]$ and Tr is the trace function from $\mathbf{F}_{2^n}$ to $\mathbf{F}_2$. Such a function is said to be *monomial* when P has only one term.

For any k dividing n and $n = uk$, we denote the trace function from $\mathbf{F}_{2^n}$ onto $\mathbf{F}_{2^k}$ as follows:

$$T_k^n(b) = b + b^{2^k} + \cdots + b^{2^{k(u-1)}}, \quad b \in \mathbf{F}_{2^n}.$$

Notation Tr is used for $k = 1$.

2.1. Boolean functions

Let f be any Boolean function on $\mathbf{F}_{2^n}$. The Hamming *weight* of f, denoted by $wt(f)$, is the number of $x \in \mathbf{F}_{2^n}$ such that $f(x) = 1$. We denote by $\mathcal{F}(f)$ the following value related to the Walsh transform of f:

$$\mathcal{F}(f) = \sum_{x \in \mathbf{F}_{2^n}} (-1)^{f(x)} = 2^n - 2wt(f). \tag{2}$$

The function f is said to be *balanced* if and only if $\mathcal{F}(f) = 0$ or, equivalently, $wt(f) = 2^{n-1}$. The linear Boolean functions on $\mathbf{F}_{2^n}$ are the functions

$$\varphi_a : x \mapsto \mathrm{Tr}(ax), \quad a \in \mathbf{F}_{2^n}.$$

The affine Boolean functions on $\mathbf{F}_{2^n}$ are $\varphi_a + c$ where $c \in \mathbf{F}_2$. The *Walsh transform* of f is the mapping

$$u \in \mathbf{F}_{2^n} \mapsto \mathcal{F}(f + \varphi_u).$$

The *Walsh spectrum* of f is the multiset

$$\left\{ \mathcal{F}(f + \varphi_u) \;\middle|\; u \in \mathbf{F}_{2^n} \right\}.$$

Definition 1. For even n, a Boolean function f on $\mathbf{F}_{2^n}$ is *bent* if and only if its Walsh transform takes the values $\pm 2^{n/2}$ only.

More precisely, the Walsh spectrum of a bent function f is:

$\mathcal{F}(f + \varphi_u)$	Number of $u \in \mathbf{F}_{2^n}$
$2^{n/2}$	$2^{n-1} + (-1)^{f(0)} 2^{n/2-1}$
$-2^{n/2}$	$2^{n-1} - (-1)^{f(0)} 2^{n/2-1}$

The *derivative* of f with respect to $b \in \mathbf{F}_{2^n}$, denoted by $D_b f$, is the Boolean function

$$D_b f : x \mapsto f(x) + f(x + b).$$

The bent functions are exactly the ones which have all their derivatives $D_b f$, $b \neq 0$, balanced. Observe that if f is a bent function and $L : \mathbf{F}_{2^n} \to \mathbf{F}_{2^n}$ is a affine permutation then $f \circ L$ is also bent. Also $f + l$ is bent for any affine function $l : \mathbf{F}_{2^n} \to \mathbf{F}_2$. The bent functions, which can be obtained from f with such transformations, are called affinely equivalent to f.

2.2. Quadratic Boolean functions

Let q be a power of 2 and V be an n-dimensional vector space over $\mathbf{F}_q$. A map $Q : V \to \mathbf{F}_q$ is called a *quadratic form* on V if

(a) $Q(c\mathbf{x}) = c^2 Q(\mathbf{x})$ for any $c \in \mathbf{F}_q$ and $\mathbf{x} \in V$,
(b) $B(\mathbf{x}, \mathbf{y}) := Q(\mathbf{x} + \mathbf{y}) + Q(\mathbf{x}) + Q(\mathbf{y})$ is bilinear on V.

The *kernel* K of a quadratic form Q is the subspace of V defined by

$$K = \left\{ \mathbf{x} \in V : \; B(\mathbf{x}, \mathbf{y}) = 0 \text{ for any } \mathbf{y} \in V \right\}.$$

Given a basis $\{\gamma_1, \ldots, \gamma_n\}$ of V, let $\mathbf{x} = \sum_{i=1}^{n} x_i \gamma_i := (x_1, \ldots, x_n)$, where $x_i \in \mathbf{F}_q$. Then using (a) and (b) we get

$$Q(\mathbf{x}) = Q\left(\sum_{i=1}^{n} x_i \gamma_i\right) = \sum_{i=1}^{n} Q(\gamma_i) x_i^2 + \sum_{i<j} B(\gamma_i, \gamma_j) x_i x_j.$$

Hence, the quadratic form Q can be expressed in the following form:

$$Q(\mathbf{x}) = \sum_{i \leqslant j} c_{ij} x_i x_j = \mathbf{x}\, \mathcal{C} \mathbf{x}^t, \tag{3}$$

where $\mathcal{C}$ is the upper triangular matrix with

$$c_{ij} = \begin{cases} Q(\gamma_i) & \text{if } i = j, \\ B(\gamma_i, \gamma_j) & \text{if } i < j. \end{cases}$$

Furthermore, (b) and (3) imply that $B(\mathbf{x}, \mathbf{y}) = \mathbf{x}\mathcal{B}\mathbf{y}^t$, where $\mathcal{B}$ is the symmetric matrix $\mathcal{C} + \mathcal{C}^t$. The matrix $\mathcal{B}$ is alternating as well, i.e., $\mathbf{x}\mathcal{B}\mathbf{x}^t = 0$. Indeed, $\mathbf{x}\mathcal{B}\mathbf{x}^t = B(\mathbf{x}, \mathbf{x}) = 0$. Note that the dimension $\mathbf{k}$ of the kernel K is equal to the corank of the matrix $\mathcal{B}$

$$\mathbf{k} = n - \operatorname{rank}(\mathcal{B}).$$

It is well known that the rank of an alternating matrix over any field is even [11, pp. 241, 242]. We collect the above information in the following proposition.

Proposition 1. *Let V be a vector space over a field $\mathbf{F}_q$ of characteristic 2 and $Q : V \to \mathbf{F}_q$ be a quadratic form. Then the dimension of V and the dimension of the kernel of Q have the same parity.*

In this paper we are interested in the case where V is an extension field $\mathbf{F}_{q^n}$ of $\mathbf{F}_q$. By counting it is easy to show that for any quadratic form $Q : \mathbf{F}_{q^n} \to \mathbf{F}_q$ there are unique $\delta_i \in \mathbf{F}_{q^n}$, $0 \leqslant i \leqslant \lfloor n/2 \rfloor$, such that

$$Q(x) = T_q^{q^n}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} \delta_i x^{q^i+1}\right),$$

except when n is even, in which case $\delta_{\lfloor n/2 \rfloor}$ is only unique modulo $\mathbf{F}_{q^{\lfloor n/2 \rfloor}}$ [14]. If $f : \mathbf{F}_{2^n} \to \mathbf{F}_2$ is a Boolean quadratic form, then its Walsh spectrum depends only on the dimension $\mathbf{k}$ of the kernel of f. More precisely, the Walsh spectrum of f is:

$\mathcal{F}(f + \varphi_u)$	Number of u
0	$2^n - 2^{n-\mathbf{k}}$
$2^{(n+\mathbf{k})/2}$	$2^{n-\mathbf{k}-1} + (-1)^{f(0)} 2^{(n-\mathbf{k}-2)/2}$
$-2^{(n+\mathbf{k})/2}$	$2^{n-\mathbf{k}-1} - (-1)^{f(0)} 2^{(n-\mathbf{k}-2)/2}$

(4)

Note that f is bent if and only if $\mathbf{k} = 0$. Assume that f is a monomial function of the form $x \mapsto \mathrm{Tr}(ax^{2^i+1})$, for some i, $1 \leqslant i \leqslant \lfloor n/2 \rfloor$. Set $S_i = \{y^{2^i+1} \mid y \in \mathbf{F}_{2^n}^*\}$. Then the dimension of the kernel of f is known to be

$$\mathbf{k} = \begin{cases} \gcd(n,i) & \text{if } \gcd(n,i) = \gcd(n,2i), \\ \gcd(n,2i) & \text{if } 2\gcd(n,i) = \gcd(n,2i) \text{ and } a \in S_i, \\ 0 & \text{if } 2\gcd(n,i) = \gcd(n,2i) \text{ and } a \notin S_i. \end{cases} \tag{5}$$

These last properties are explained in [20, Chapter 15] (see Figs. 15.2 and 15.5) and [21]; see also [2, Proposition 4]. For more information on the Walsh transform of the monomial quadratic forms see [13, Appendix]. The next lemma can be directly obtained from the definitions.

Lemma 1. *Let f be any quadratic Boolean function. The kernel K of f is the subspace of those b such that the derivative $D_b f$ is constant.*

2.3. The Maiorana–McFarland bent functions

The Maiorana–McFarland class of bent functions was introduced in [22] and extensively studied by Dillon [12, pp. 90–95]. It is usually called the *class* $\mathcal{M}$ of bent functions. A bent function from $\mathcal{M}$ can be viewed as a concatenation of certain affine Boolean functions.

In the next lemma we define the subclass of $\mathcal{M}$ that we will consider later. The concatenation is made relatively to the cosets of $\mathbf{F}_{2^t}$, a structure which is particularly adapted to the monomial bent functions. The proof of this lemma is in fact a general proof for the class $\mathcal{M}$. We give a sketch of proof to define this subclass clearly.

Lemma 2. *Let $n = 2t$ and $V = \mathbf{F}_{2^t}$. Denote by W a subspace of the representatives of the cosets of V, that is $\mathbf{F}_{2^n} = \bigcup_{a \in W}(a + V)$. Let us consider a function f on $\mathbf{F}_{2^n}$ defined by*

$$f : (y, a) \in V \times W \mapsto T_1^t\big(y\pi(a) + h(a)\big), \tag{6}$$

where π is a bijection from W to V and h is any function from W to V. Then, f is a bent function which belongs to the class $\mathcal{M}$.

Sketch of proof. Fixing a in (6), we get a function on $\mathbf{F}_{2^t}$, say f_a, which is affine relatively to y. Since π is a permutation, only one f_a is constant and all the others are balanced. Thus

$$\mathcal{F}(f) = \sum_{a \in W} \sum_{y \in V} (-1)^{f(y,a)} = 2^t (-1)^{T_1^t(h(a_0))},$$

where $\pi(a_0) = 0$. Note that the functions $y \mapsto T_1^t(y\pi(a))$ form the set of all linear functions on $\mathbf{F}_{2^t}$. Consider any linear function ℓ on $\mathbf{F}_{2^n}$ and its restrictions ℓ_a on the cosets of V. If the kernel of ℓ contains V, then each ℓ_a is constant. Otherwise the ℓ_a are affine and there is one and only one a such that $f_a + \ell_a$ is constant. Thus, $\mathcal{F}(f + \ell)$ and $\mathcal{F}(f)$ have the same absolute value. □

Remark 1. Let f be a bent function given by (6) and g an affinely equivalent function given by

$$g(x) = f \circ L(x),$$

where L is an affine permutation. Then g is also in class $\mathcal{M}$. More precisely, it is a concatenation of affine functions on the subspace $L^{-1}(V)$. In particular, the composition $f \circ s_\gamma$ of the linear function

$$s_\gamma : x \mapsto \gamma x$$

and f is a concatenation of affine functions on $\gamma^{-1}V$.

To introduce our method we consider in the next example the functions studied by Leander in [17]. We express such a function in a form close to form (6), which implies that a large part of these functions can be viewed as a concatenation of (not necessarily different) affine functions on the subfield.

Example 1. Let $n = 4r$, $r > 1$. We consider the functions on $\mathbf{F}_{2^n}$ defined by

$$g_\lambda : x \mapsto \mathrm{Tr}\big(\lambda x^d\big), \quad d = \big(2^r+1\big)^2,\ \lambda \in \mathbf{F}_{2^{2r}}^*. \tag{7}$$

In [17] it is proved that these functions are bent if $\lambda \in \mathbf{F}_4 \setminus \{0,1\}$ and r is odd. We will show that g_λ, for any r and for any $\lambda \in \mathbf{F}_{2^{2r}}^*$, has a similar form to (6). The notation is the same as in the statement of Lemma 2: $V = \mathbf{F}_{2^{2r}}$ and W is a subspace of the representatives of the cosets of V in $\mathbf{F}_{2^n}$. Then, for any $y \in V$ and $a \in W$, we compute:

$$\begin{aligned} g_\lambda(y,a) &= \mathrm{Tr}\big(\lambda(y+a)^{2^{2r}+2^{r+1}+1}\big) \\ &= \mathrm{Tr}\big(\lambda y^d\big) + \mathrm{Tr}\big(\lambda\big(y^{1+2^{r+1}}a + y^{2^{r+1}+1}a^{2^{2r}} + y^2 a^{2^{r+1}}\big)\big) \\ &\quad + \mathrm{Tr}\big(y\big(\lambda\big(a^{2^{2r}+2^{r+1}} + a^{2^{r+1}+1}\big) + \lambda^{2^{r-1}} a^{2^{r-1}(2^{2r}+1)}\big)\big) \\ &\quad + \mathrm{Tr}\big(\lambda a^{2^{2r}+2^{r+1}+1}\big) = A + B + C + D. \end{aligned}$$

We have $A = 0$ since λ and y are in $\mathbf{F}_{2^{2r}}$. Moreover,

$$B = \mathrm{Tr}\big(\lambda y^{2^{r+1}+1}\big(a^{2^{2r}} + a\big) + \lambda y^2 a^{2^{r+1}}\big) = \mathrm{Tr}\big(\lambda y^2 a^{2^{r+1}}\big),$$

since $\lambda y^{2^{r+1}+1}(a^{2^{2r}} + a) \in \mathbf{F}_{2^{2r}}$. Thus we have that *any function g_λ, defined by* (7), *is a concatenation of 2^{2r} affine functions on $\mathbf{F}_{2^{2r}}$*. In order to specify the form of these functions, we compute the part which is linear relatively to y:

$$C = \mathrm{Tr}\big(y\lambda\big(a^{2^{2r}+2^{r+1}} + a^{2^{r+1}+1}\big)\big),$$

since $\lambda^{2^{r-1}} a^{2^{r-1}(2^{2r}+1)} \in \mathbf{F}_{2^{2r}}$. Finally

$$g_\lambda(y,a) = T_1^{2r}\big(y\pi(a) + \lambda T_{2r}^{4r}\big(a^d\big)\big),$$

where π is the mapping from W to V given by

$$\pi(a) = \lambda\big(a + a^{2^{2r}}\big)^{2^{r+1}+1} + \lambda^{2^{2r-1}}\big(a + a^{2^{2r}}\big)^{2^r}.$$

2.4. Definition of the functions f_λ

Let $n = 6r$, $r > 1$ and α be a primitive element of $\mathbf{F}_{2^n}$. Further let the functions f_λ be defined by (1). Recall that $d = 2^{2r} + 2^r + 1$ and it holds

$$2^n - 1 = \left(2^{3r} - 1\right)\left(2^{3r} + 1\right) = d\left(2^{2r} - 1\right)\left(2^{2r} - 2^r + 1\right).$$

If $\lambda = \gamma\theta^d$ for some $\gamma, \theta \in \mathbf{F}_{2^n}$, then $f_\lambda(x) = f_\gamma(\theta x)$, and we call f_γ a shift of f_λ. A shift of f_λ has the same Walsh spectrum as f_λ does. Next we want to show that to obtain an information about Walsh spectrum of f_λ it is enough to consider $\lambda \in \mathbf{F}_{2^{3r}}$. Indeed, take the partition of the multiplicative group of $\mathbf{F}_{2^n}^*$ into the cosets of the subgroup $\langle\alpha^d\rangle$ generated with α^d, i.e.

$$\mathbf{F}_{2^n}^* = \bigcup_{i=0}^{d-1} \alpha^i \langle\alpha^d\rangle,$$

where $\langle\alpha^d\rangle = \{\alpha^{d\ell} \mid 0 \leqslant \ell < \frac{2^n-1}{d}\}$. Note that if two elements λ and γ belong to the same coset of $\langle\alpha^d\rangle$, then the functions f_λ and f_γ are shifts of each other. Finally, we observe that every coset of $\langle\alpha^d\rangle$ contains an element from the subfield $\mathbf{F}_{2^{3r}}$. More precisely, for any j, $0 \leqslant j \leqslant d-1$, $\alpha^{j(2^{3r}+1)}$ belongs to one and only one $\alpha^i\langle\alpha^d\rangle$. Indeed, we have

$$2^{3r} + 1 = \left(2^{3r} - 1\right) + 2 \equiv d\left(2^r - 1\right) + 2 \equiv 2 \pmod{d}.$$

Then $i = 2j$ if $0 \leqslant j \leqslant (d-1)/2$ and $i = 2j - d$, otherwise.

Lemma 3. *The subset of* $\mathbf{F}_{2^{3r}}$

$$\left\{\alpha^{j(2^{3r}+1)} \;\middle|\; 0 \leqslant j \leqslant d-1\right\}$$

is a set of the representatives of the cosets $\{\alpha^i\langle\alpha^d\rangle \mid 0 \leqslant i \leqslant d-1\}$ *with*

$$j = \begin{cases} i/2 & \text{if } i \text{ is even,} \\ (d+i)/2 & \text{if } i \text{ is odd.} \end{cases}$$

According to the previous lemma, to study the spectra of all the functions f_λ defined by (1), it is sufficient to study the functions that we introduce below.

Definition 2. Let $n = 6r$ with $r > 1$. Let us define the Boolean functions on $\mathbf{F}_{2^n}$:

$$f_\lambda(x) = \mathrm{Tr}\left(\lambda x^d\right), \quad \text{where } \begin{cases} d = 2^{2r} + 2^r + 1, \\ \lambda = \alpha^{j(2^{3r}+1)}, \\ 0 \leqslant j \leqslant d-1. \end{cases} \tag{8}$$

Remark 2. When $r = 1$, then $n = 6$ and $d = 7$. In this case, the bent functions f_λ belong to the class of bent functions of the form: $x \mapsto \mathrm{Tr}(\nu x^{2^t-1})$ (functions on $\mathbf{F}_{2^n}$ with $n = 2t$). These were studied by Dillon, as examples of the so-called PS bent functions [12]. When $n = 6$ we have

$f_\lambda(x) = \mathrm{Tr}(\lambda x^7)$, with $\lambda \in \mathbf{F}_8$ and it is very easy to determine the bent functions. We know that f_λ is bent if and only if the function on $\mathbf{F}_8$

$$g_\lambda : x \mapsto T_1^3\left(x^3 + \lambda x\right)$$

is balanced (see [17, §II.B]). But it is well known that this cubic function is balanced if and only if $T_1^3(\lambda) = 0$. We will see later that, in fact, this result holds when $r > 1$.

3. On the spectrum of f_λ

In this section f_λ is defined by (8). We denote by $\mathcal{G}$ the subgroup of $\mathbf{F}_{2^n}^*$ of order $2^{3r}+1$. Since $\gcd(2^{3r}+1, 2^{3r}-1) = 1$, any $x \in \mathbf{F}_{2^n}^*$ has a unique representation:

$$x = yz, \quad y \in \mathbf{F}_{2^{3r}}^* \text{ and } z \in \mathcal{G}. \tag{9}$$

3.1. The weight of f_λ

Here we prove that $wt(f_\lambda)$ takes only three values (Theorem 1). Recall that $\mathcal{F}(f_\lambda) = 2^n - 2wt(f_\lambda)$.

Proposition 2. *Let us define*

$$L_\lambda = \left\{z \in \mathcal{G} \mid T_r^{6r}\left(\lambda z^d\right) \neq 0\right\}.$$

Then the weight of f_λ is $wt(f_\lambda) = 2^{r-1} d \, \#L_\lambda$.

Proof. Using (9), we will express $wt(f_\lambda)$ as an integer sum on the pairs (y, z). Note that $y^d \in \mathbf{F}_{2^r}$, for $y \in \mathbf{F}_{2^{3r}}$, since $2^{3r} - 1 = (2^r - 1)d$. So, it is clear that the application $y \mapsto y^d$ is d-to-1 from $\mathbf{F}_{2^{3r}}^*$ onto $\mathbf{F}_{2^r}^*$.

Now, we have:

$$\begin{aligned} wt(f_\lambda) &= \sum_{x \in \mathbf{F}_{2^n}} \mathrm{Tr}\left(\lambda x^d\right) = \sum_{z,y} \mathrm{Tr}\left(\lambda (zy)^d\right) \\ &= \sum_{z \in \mathcal{G}} \sum_{y \in \mathbf{F}_{2^{3r}}} T_1^r\left(y^d T_r^{6r}\left(\lambda z^d\right)\right) \\ &= \sum_{z \in \mathcal{G}} d \sum_{\rho \in \mathbf{F}_{2^r}} T_1^r\left(\rho T_r^{6r}\left(\lambda z^d\right)\right) \\ &= \#L_\lambda \times d \times 2^{r-1}, \end{aligned}$$

since $\rho \mapsto T_1^r(\rho A)$ is linear on $\mathbf{F}_{2^r}$, for any $A \neq 0$. □

Our next goal is to compute the cardinality of L_λ. Actually, we will compute the cardinality of N_λ, which is introduced in the next lemma. We denote by $\overline{L_\lambda}$ the set $\mathcal{G} \setminus L_\lambda$:

$$\overline{L_\lambda} = \left\{z \in \mathcal{G} \mid T_r^{6r}\left(\lambda z^d\right) = 0\right\}.$$

Lemma 4. *Given a* $\lambda \in \mathbf{F}_{2^{3r}}$*, set*

$$N_\lambda = \left\{ y \in \mathbf{F}_{2^{3r}}^* \;\middle|\; T_r^{3r}(\lambda y) = 0 \text{ and } T_1^{3r}\left(\frac{1}{y}\right) = 1 \right\}. \tag{10}$$

Then $\#\overline{L_\lambda} = 2 \cdot \#N_\lambda + 1$.

Proof. Note that $z^{2^{3r}} = z^{-1}$ for any $z \in \mathcal{G}$. We have $z \in \overline{L_\lambda}$ if and only if $T_r^{6r}(\lambda z^d) = 0$. Since $\overline{L_\lambda}$ is contained in $\mathcal{G}$ and $\gcd(d, 2^{3r}+1) = 1$, the number of such z is also obtained by taking as a condition $T_r^{6r}(\lambda z) = 0$. Thus we want to compute the number of z satisfying

$$T_r^{6r}(\lambda z) = T_r^{3r}\left(\lambda\left(z + z^{-1}\right)\right) = 0,$$

since $\lambda \in \mathbf{F}_{2^{3r}}$. It is clear that z satisfies the equality above if and only if z^{-1} satisfies it too. On the other hand, it is well known that

$$\left\{ z + z^{-1} \;\middle|\; z \in \mathcal{G} \setminus \{1\} \right\} = \left\{ u \in \mathbf{F}_{2^{3r}}^* \;\middle|\; T_1^{3r}\left(\frac{1}{u}\right) = 1 \right\}$$

(see [16] for instance). Thus, computing $\#\overline{L_\lambda}$ is equivalent to computing the number of $u \in \mathbf{F}_{2^{3r}}^*$ satisfying $T_1^{3r}(u^{-1}) = 1$ and $T_r^{3r}(\lambda u) = 0$, which is the cardinality of N_λ. Moreover, each such u corresponds to a unique pair (z, z^{-1}) and we add 1, for $z = 1$, to obtain the cardinality of $\overline{L_\lambda}$. □

Theorem 1. *Let the functions* f_λ *(and* λ *itself) be defined by* (8)*. Let* G_d *denote the subgroup of order* d *of* $\mathbf{F}_{2^{3r}}^*$*. Consider the solutions* $v \in G_d$ *of the equation*:

$$v^2 + v\frac{T_r^{3r}(\lambda)}{\lambda^{2^r}} + \frac{1}{\lambda^{2^r-1}} = 0. \tag{11}$$

Then $\mathcal{F}(f_\lambda) = 2^n - 2^r d\,\#L_\lambda$ *where* $\#L_\lambda$ *is computed as follows.*

(a) *If Eq.* (11) *has one and only one solution in* G_d *then* $\#L_\lambda = 2^{2r}(2^r - 1)$*; this holds if and only if* $T_r^{3r}(\lambda) = 0$.
(b) *If Eq.* (11) *has no solution in* G_d *then* $\#L_\lambda = 2^r(2^{2r} - 2^r - 1)$.
(c) *Otherwise, Eq.* (11) *has two solutions in* G_d *and* $\#L_\lambda = 2^r(2^{2r} - 2^r + 1)$.

Consequently, we obtain:

Case	$\mathcal{F}(f_\lambda)$
(a)	2^{3r}
(b)	$2^{4r} + 2^{3r+1} + 2^{2r}$
(c)	$-(2^{4r} + 2^{2r})$

Proof. Let β be a primitive element of the subfield $\mathbf{F}_{2^{3r}}$. According to Lemma 4, computing $\#L_\lambda$ is equivalent to computing $\#N_\lambda$. Since $2^{3r}-1=(2^r-1)d$ we can express any $y\in\mathbf{F}_{2^{3r}}^*$ as follows:

$$y=u\beta^i,\quad u=\beta^{kd},\ 0\leqslant k\leqslant 2^r-2 \text{ and } 0\leqslant i\leqslant d-1.$$

Note that u belongs to $\mathbf{F}_{2^r}^*$ while β^i for $i\neq 0$ does not. Thus $T_r^{3r}(\lambda y)=uT_r^{3r}(\lambda\beta^i)$, which implies that (10) can be rewritten

$$N_\lambda=\bigcup_{i=0}^{d-1}\left\{y\in\beta^i\mathbf{F}_{2^r}^* \;\middle|\; T_r^{3r}\left(\lambda\beta^i\right)=0 \text{ and } T_1^{3r}\left(\frac{1}{y}\right)=1\right\}.$$

Let $I=\{0\leqslant i\leqslant d-1 \mid T_r^{3r}(\lambda\beta^i)=0\}$. The linear function $g:y\mapsto T_r^{3r}(y)$ from $\mathbf{F}_{2^{3r}}$ to $\mathbf{F}_{2^r}$ is surjective. So its kernel has dimension $2r$. Moreover, $g(y)=0$ for $y\in\beta^i\mathbf{F}_{2^r}^*$ as soon as $g(\beta^i)=0$, and therefore

$$\#I=\frac{2^{2r}-1}{2^r-1}=2^r+1.$$

Hence, with $y=u\beta^i$,

$$\begin{aligned}\#N_\lambda&=\sum_{i\in I}\#\left\{y\in\beta^i\mathbf{F}_{2^r}^* \;\middle|\; T_1^{3r}\left(\frac{1}{y}\right)=1\right\}\\&=\sum_{i\in I}\#\left\{u\in\mathbf{F}_{2^r}^* \;\middle|\; T_1^r\left(\frac{1}{u}T_r^{3r}\left(\beta^{-i}\right)\right)=1\right\}\\&=2^{r-1}\times\#\left\{i\in I \;\middle|\; T_r^{3r}\left(\beta^{-i}\right)\neq 0\right\}\\&=2^{r-1}\left(2^r+1-\#\left\{i\in I \;\middle|\; T_r^{3r}\left(\beta^{-i}\right)=0\right\}\right).\end{aligned}\tag{12}$$

Hence in order to find $\#N_\lambda$, we have to compute the number of i such that $i\in I$ and $T_r^{3r}(\beta^{-i})=0$. Setting $w=\beta^i$, $0\leqslant i\leqslant d-1$, we have to solve the system:

$$\begin{cases}\lambda w+(\lambda w)^{2^r}+(\lambda w)^{2^{2r}}=0,\\ \dfrac{1}{w}+\dfrac{1}{w^{2^r}}+\dfrac{1}{w^{2^{2r}}}=0.\end{cases}\tag{13}$$

Note that $w=1$ (i.e., $i=0$) is not a solution of (13). So we have $w^{2^r-1}\neq 1$, which allows us to express $w^{2^{2r}}$ from the second equation:

$$w^{2^{2r}}=\frac{w^{2^r}}{w^{2^r-1}+1},$$

that we substitute in the first equation. We can multiply this first equation by $w^{2^r-1}+1$ and we get:

$$\lambda\left(w^{2^r}+w\right)+\lambda^{2^r}\left(w^{2^{r+1}-1}+w^{2^r}\right)+\lambda^{2^{2r}}w^{2^r}=0,$$

which gives, with $\delta = T_r^{3r}(\lambda)$,

$$\delta w^{2^r} + \lambda w + \lambda^{2^r} w^{2^{r+1}-1} = 0.$$

Dividing the previous equation by $\lambda^{2^r} w$, we finally get:

$$w^{2(2^r-1)} + w^{2^r-1}\frac{\delta}{\lambda^{2^r}} + \frac{1}{\lambda^{2^r-1}} = 0.$$

Setting $v = w^{2^r-1}$, we get Eq. (11). Note that, by definition, v describes the subgroup G_d of $\mathbf{F}_{2^{3r}}^*$ of order d. Also, observe that because of definition of w, the correspondence $w \mapsto v$ is a bijection.

Equation (11) is an equation of degree 2 which has either 0 or 1 or 2 solutions in $\mathbf{F}_{2^{3r}}^*$. If it has 2 solutions, v_1 and v_2, then $v_1 \in G_d$ implies $v_2 \in G_d$ since $v_1 v_2 = 1/\lambda^{2^r-1}$. So (11) has one and only one solution in G_d if and only if $\delta = 0$. Using (12) we get $\#N_\lambda = 2^{r-1}2^r$; moreover, by Lemma 4, we have

$$\#L_\lambda = 2^{3r} + 1 - 2^{2r} - 1 = 2^r\left(2^{2r} - 2^r\right).$$

In the same way, when (11) has no solution in G_d we get $\#N_\lambda = 2^{r-1}(2^r + 1)$ and then $\#L_\lambda = 2^r(2^{2r} - 2^r - 1)$. If (11) has 2 solutions in G_d then $\#N_\lambda = 2^{r-1}(2^r - 1)$ and $\#L_\lambda = 2^r(2^{2r} - 2^r + 1)$, completing the proof of the cases (a)–(c). Then we are able to compute $\mathcal{F}(f_\lambda)$, using Proposition 2 and $\mathcal{F}(f_\lambda) = 2^n - 2wt(f_\lambda)$. □

Remark 3. We call the case (a) the *bent case* since f_λ could be bent in this case only. Clearly there are λ such that $\delta = T_r^{3r}(\lambda) = 0$. Moreover, our numerical results show that there are λ such that case (b) (respectively case (c)) holds. Note that Eq. (11) has no solution in $\mathbf{F}_{2^{3r}}$ if and only if

$$T_1^{3r}\left(\frac{\lambda^{2^r+1}}{\delta^2}\right) = T_1^r\left(\frac{1}{\delta^2}T_r^{3r}\left(\lambda^{2^r+1}\right)\right) = 1.$$

3.2. Another expression of f_λ

In this subsection we want to express any function f_λ by means of its restrictions on the (additive) cosets of $\mathbf{F}_{2^{3r}}$. We proceed as in Section 2.3. Set $V = \mathbf{F}_{2^{3r}}$ and let W be a subspace of $\mathbf{F}_{2^n}$ which is a set of the representatives of the cosets of V. Thus, for any $x \in \mathbf{F}_{2^n}$ there is a unique pair $(y, a) \in V \times W$ such that $x = y + a$. Then, we define

$$f_\lambda(y, a) = f_\lambda(y + a) = \mathrm{Tr}\left(\lambda(y + a)^d\right). \tag{14}$$

Theorem 2. *Let $\delta = T_r^{3r}(\lambda)$. Define the function π from W to V:*

$$\pi(a) = \lambda^{2^{2r}}\left(a + a^{2^{3r}}\right)^{2^{2r}+2^r} + \delta T_{3r}^{6r}\left(a^{2^{2r}+2^r}\right). \tag{15}$$

Then, for any $(y, a) \in V \times W$:

$$f_\lambda(y, a) = T_1^{3r}\left(y^{2^r+1}\delta\left(a + a^{2^{3r}}\right)^{2^{2r}} + y\pi(a) + \lambda\left(a^d + a^{2^{3r}d}\right)\right). \tag{16}$$

Proof. We compute $f_\lambda(y,a)$, which is defined by (14):

$$\begin{aligned} f_\lambda(y,a) &= \mathrm{Tr}\big(\lambda(y+a)^d\big) \\ &= \mathrm{Tr}\big(\lambda y^d\big) + \mathrm{Tr}\big(\lambda\big(a^{2^{2r}} y^{2^r+1} + a^{2^r} y^{2^{2r}+1} + a y^{2^r(2^r+1)}\big)\big) \\ &\quad + \mathrm{Tr}\big(\lambda\big(y^{2^{2r}} a^{2^r+1} + y^{2^r} a^{2^{2r}+1} + y a^{2^r(2^r+1)} + a^d\big)\big) \\ &= A + B + C. \end{aligned}$$

First $A = \mathrm{Tr}(\lambda y^d) = 0$ since λ and y are in $\mathbf{F}_{2^{3r}}$. Now, using the properties of the trace function, we have

$$\begin{aligned} B &= \mathrm{Tr}\big(y^{2^r+1}\big(\lambda a^{2^{2r}} + \lambda^{2^r} a^{2^{2r}} + \lambda^{2^{2r}} a^{2^{2r}}\big)\big) \\ &= \mathrm{Tr}\big(y^{2^r+1} a^{2^{2r}}\big(\lambda + \lambda^{2^r} + \lambda^{2^{2r}}\big)\big) \\ &= T_1^{3r}\big(y^{2^r+1}\delta\big(a + a^{2^{3r}}\big)^{2^{2r}}\big). \end{aligned}$$

Finally the part which is affine relatively to y is:

$$\begin{aligned} C &= \mathrm{Tr}\big(y\big(\lambda a^{2^r(2^r+1)} + \lambda^{2^r} a^{2^r(2^r+1)} + \lambda^{2^{2r}} a^{2^{2r}(2^{2r}+1)}\big) + \lambda a^d\big) \\ &= T_1^{3r}\big(y T_{3r}^{6r}(D) + \lambda T_{3r}^{6r}\big(a^d\big)\big), \end{aligned}$$

where

$$\begin{aligned} T_{3r}^{6r}(D) &= \big(\lambda^{2^{2r}} + \delta\big) T_{3r}^{6r}\big(a^{2^{2r}+2^r}\big) + \lambda^{2^{2r}} T_{3r}^{6r}\big(a^{2^{4r}+2^{2r}}\big) \\ &= \lambda^{2^{2r}} T_{3r}^{6r}\big(a^{2^{2r}}\big(a + a^{2^{3r}}\big)^{2^r}\big) + \delta T_{3r}^{6r}\big(a^{2^{2r}+2^r}\big) \\ &= \lambda^{2^{2r}}\big(a + a^{2^{3r}}\big)^{2^{2r}+2^r} + \delta T_{3r}^{6r}\big(a^{2^{2r}+2^r}\big) \end{aligned}$$

which is exactly $\pi(a)$, completing the proof of (16). □

3.3. The bent functions

Now we use Lemma 2 to characterize those λ such that f_λ is bent. A part of these bent functions form a subspace of the Boolean functions of degree 3.

Theorem 3. *The function f_λ, defined by* (8)*, is bent if and only if $T_r^{3r}(\lambda) = 0$. There are $2^r + 1$ such bent functions. In general, if λ runs through $\mathbf{F}_{2^n}^*$, then there are*

$$\big(2^{2r} - 1\big)\big(2^{3r} + 1\big)$$

bent functions f_λ, defined in (1)*. All these bent functions belong to the class $\mathcal{M}$. Moreover, the set*

$$\mathcal{B} = \big\{ f_\lambda \;\big|\; \lambda \in \mathbf{F}_{2^{3r}},\ T_r^{3r}(\lambda) = 0 \big\},$$

where f_0 is the null function, is a subspace of the vector space of Boolean functions on $\mathbf{F}_{2^n}$ over $\mathbf{F}_2$. Its dimension is $2r$ and any function $f_\lambda \in \mathcal{B}^*$ is a cubic bent function.

Proof. First, if $\delta \neq 0$ then f_λ cannot be bent, since $\mathcal{F}(f_\lambda) \notin \{\pm 2^{3r}\}$. This was proved by Theorem 1. So, we consider the functions f_λ expressed by (16) with $\delta = 0$. Notation is as in Theorem 2. Then we get:

$$f_\lambda(y,a) = T_1^{3r}\big(y\pi(a) + \lambda\big(a^d + a^{2^{3r}d}\big)\big) \tag{17}$$

with $\pi(a) = \lambda^{2^{2r}}(a + a^{2^{3r}})^{2^{2r}+2^r}$. The linear function $a \mapsto a + a^{2^{3r}}$ is a bijection from W to V, since its kernel is $W \cap V = \{0\}$. We conclude that π is a bijection from W to V because $2^r + 1$ and $2^{3r} - 1$ are coprime. According to Lemma 2, the functions expressed by (17) are bent functions belonging to the class $\mathcal{M}$. Now, set

$$S = \big\{\lambda = \alpha^{\ell(2^{3r}+1)} \;\big|\; 0 \leqslant \ell \leqslant d-1,\ T_r^{3r}(\lambda) = 0\big\}.$$

Note that S is the set of those λ corresponding to bent functions defined by (8). The application $y \mapsto T_r^{3r}(y)$, from V to $\mathbf{F}_{2^r}$, has a kernel of dimension $2r$. Moreover, for any $\lambda \in S$ we have $T_r^{3r}(\lambda u) = 0$ for any $u \in \mathbf{F}_{2^r}^*$. Then $\#S = (2^{2r}-1)/(2^r-1) = 2^r + 1$, implying that there are $2^r + 1$ bent functions defined by (8), each of them having $(2^n - 1)/d$ shifts. Thus, we get

$$\big(2^r+1\big)\big(2^{3r}+1\big)\big(2^r-1\big) = \big(2^{2r}-1\big)\big(2^{3r}+1\big)$$

bent functions f_λ, when λ runs through $\mathbf{F}_{2^n}^*$ (see Section 2.4). Moreover, as it was explained in Remark 1 these shifts are also elements of the class $\mathcal{M}$.

Let $\lambda \in S$. Consider the shifts $f_{u\lambda}$ of f_λ such that $u\lambda \in \mathbf{F}_{2^{3r}}$. This holds for $u \in \mathbf{F}_{2^r}^*$ only, since we must have $u = v^d$ for some v in $\mathbf{F}_{2^{3r}}$. So we have $2^r - 1$ such shifts. Since $T_r^{3r}(u\lambda) = 0$, we have proved that $\mathcal{B}$ contains $2^{2r} - 1$ bent functions. $\mathcal{B}$ is a subspace because of the linearity of the trace function: if f_λ and f_μ are in $\mathcal{B}$ then $f_{\lambda+\mu} \in \mathcal{B}$. All functions f_λ are of degree 3, completing the proof. □

To illustrate the previous theorem, we compute the number of bent functions for $r = 2$.

Example 2. Let $r = 2$; so $n = 12$ and $d = 21$. At first let us look more closely on the numerical results given in Table 1. They show that f_{α^i} is bent for $i \in \{7, 9\}$, where α is a primitive element of $\mathbf{F}_{2^{12}}$. Then we get five cosets $\alpha^i\langle\alpha^{21}\rangle$ whose elements define bent functions. Indeed i is a representative of its 2-cyclotomic coset modulo 21: 7 is the representative of $\{7, 14\}$ and 9 is the representative of $\{9, 15, 18\}$. So, we get at all $975 = 5 \times 195$ bent functions.

Now, using Lemma 3 and the previous calculation, we get five bent functions f_λ with $\lambda \in \mathbf{F}_{2^6}$:

$$\lambda = \alpha^{65j}, \quad j \in J,\ J = \{7, 14, 9, 15, 18\}.$$

And, using Theorem 3, there are $975 = 15 \times 65$ many bent f_λ if $\lambda \in \mathbf{F}_{2^{12}}$. The subspace of bent functions of dimension 4 is obtained by taking all elements λ in $\alpha^{65j}\langle\alpha^{21}\rangle$, $j \in J$, which belong also to the subfield $\mathbf{F}_{2^6}$, that is

$$\lambda = \alpha^{65\ell}, \quad \ell = j + kd,\ j \in J \text{ and } 0 \leqslant k \leqslant 2.$$

Table 1
Walsh spectra of f_{α^i} over $\mathbf{F}_{2^{12}}$ where α is a root of the primitive polynomial $x^{12}+x^6+x^4+x+1$. It corresponds to the case $r=2$, $n=12$ and $d=21$. The spectra of the functions $x \mapsto \mathrm{Tr}(\alpha^i x^{21})$, where $i \in I$ with $I=\{0,1,3,5,7,9\}$, are presented. The set I is a set of representatives of the 2-cyclotomic cosets modulo 21. In this table, a spectrum is presented as a list: *value* [*number*] *value* [*number*] ... . The set of all bent functions is described in Example 2

i	Weight of f	Spectra
0	$2^{11}+136$	112 [546] 48 [1092] −16 [1365] −80 [1092] −272 [1]
1	$2^{11}+136$	112 [546] 48 [1092] −16 [1365] −80 [1092] −272 [1]
3	$2^{11}+136$	112 [546] 48 [1092] −16 [1365] −80 [1092] −272 [1]
5	$2^{11}-200$	400 [1] 144 [441] 80 [84] 16 [1764] −48 [1764] −240 [42]
7	$2^{11}-32$	64 [2080] −64 [2016]
9	$2^{11}-32$	64 [2080] −64 [2016]

We get 15 such bent functions.

3.4. Functions which are not bent

In this section, we consider the functions f_λ which are not bent. We obtain the *divisibility* of the Walsh transform of such f_λ from Theorems 1 and 2.

Corollary 1. *Assume that $T_r^{3r}(\lambda) \neq 0$, i.e. f_λ is not bent. Set $s=2r$. Then for all $b \in \mathbf{F}_{2^n}$*

$$\mathcal{F}(f_\lambda+\varphi_b) \equiv 0 \pmod{2^s}.$$

Moreover, this does not hold for $s > 2r$.

Proof. Notation is as in Theorem 2. When f_λ is not bent, we have seen that it can be expressed as a concatenation of quadratic functions of the form $T_1^{3r}(\nu y^{2^r+1}+cy+c')$. This property holds for $f_\lambda+\varphi_b$ for any b. Indeed

$$\begin{aligned}(f_\lambda+\varphi_b)(y+a) &= f_\lambda(y+a)+\mathrm{Tr}\big(b(y+a)\big)\\ &= T_1^{3r}\big(\nu y^{2^r+1}+y\big(c+T_{3r}^{6r}(b)\big)+c'+T_{3r}^{6r}(ba)\big)\end{aligned}$$

and we have

$$\mathcal{F}(f_\lambda+\varphi_b)=\sum_a\sum_y (-1)^{(f_\lambda+\varphi_b)(y,a)}.$$

Any quadratic function of the form $y \mapsto T_1^{3r}(\nu y^{2^r+1})$ on $\mathbf{F}_{2^{3r}}$ is such that the values of its Walsh transform are $\{0, \pm 2^{2r}\}$ when $\nu \neq 0$. This is because the dimension $\mathbf{k}$ of its kernel equals r (see Section 2.2). We can conclude that $\mathcal{F}(f_\lambda+\varphi_b)$ is divisible by 2^{2r}. By Theorem 1, we know that $\mathcal{F}(f_\lambda)$ is divisible by 2^{2r} and not divisible by 2^{2r+1}, completing the proof. □

Concerning the *non-bent spectra*, our numerical results lead to several conjectures that we list below. To illustrate our purpose, we present the case $r=2$ in Table 1.

Conjecture 1. *There are three different spectra only, one "bent" and two "non-bent," for the functions f_λ. These three spectra correspond to the three cases listed in Theorem* 1.

For any non-bent function f_λ, the value $\mathcal{F}(f_\lambda)$ appears only once and the value 0 *never appears.*

4. Some quadratic functions: the derivatives

The derivative of f_λ ($\lambda \in \mathbf{F}_{2^n}^*$) with respect to $a \in \mathbf{F}_{2^n}^*$ is the function

$$D_a f_\lambda(x) = \mathrm{Tr}\big(\lambda x^d\big) + \mathrm{Tr}\big(\lambda(x+a)^d\big).$$

Our purpose, in this section, is to study some properties of these specific quadratic functions. Firstly, we are interested in the Walsh spectra of these functions. To obtain the Walsh spectra of the functions $D_a f_\lambda$ it is enough to consider the spectra of the functions $D_1 f_\mu$ with $\mu = \lambda a^d$. Indeed,

$$\begin{aligned} D_a f_\lambda(x) &= \mathrm{Tr}\big(\lambda x^d\big) + \mathrm{Tr}\big(\lambda(x+a)^d\big) \\ &= \mathrm{Tr}\big(\lambda a^d \big(a^{-1}x\big)^d\big) + \mathrm{Tr}\big(\lambda a^d \big(a^{-1}x+1\big)^d\big) \\ &= D_1 f_{\lambda a^d}\big(a^{-1}x\big). \end{aligned}$$

The following proposition gives more information about $D_a f_\lambda$.

Proposition 3. *Let $a \in \mathbf{F}_{2^n}^*$ and $\mu = \lambda a^d$. Then $D_1 f_\mu$ is the function $g_{a,\lambda}$ given by*

$$g_{a,\lambda}(x) = \mathrm{Tr}\big(\mu x^{2^{2r}+1} + Ax^{2^r+1} + Bx + \mu\big), \tag{18}$$

with

$$A = \mu + \mu^{2^{5r}}, \qquad B = \mu + \mu^{2^{4r}} + \mu^{2^{5r}}.$$

Consequently,

$$D_a f_\lambda(x) = g_{a,\lambda}\big(a^{-1}x\big).$$

Proof. According to the previous remark, it is sufficient to compute $D_1 f_{\lambda a^d}$ (denoted by $g_{a,\lambda}$):

$$\begin{aligned} g_{a,\lambda}(x) &= \mathrm{Tr}\big(\mu\big[x^{2^{2r}+2^r} + x^{2^{2r}+1} + x^{2^r+1} + x^{2^{2r}} + x^{2^r} + x + 1\big]\big) \\ &= \mathrm{Tr}\big(\mu x^{2^{2r}+1} + \big(\mu + \mu^{2^{5r}}\big)x^{2^r+1} + \big(\mu + \mu^{2^{4r}} + \mu^{2^{5r}}\big)x + \mu\big). \end{aligned}$$

□

4.1. The kernels of derivatives

The Walsh spectrum of the function $g_{a,\lambda}$ is equal to the one of the following functions:

$$h_\mu(x) = \mathrm{Tr}\big(\mu x^{2^{2r}+1} + \big(\mu + \mu^{2^{5r}}\big)x^{2^r+1}\big), \quad \mu = \lambda a^d, \tag{19}$$

for any a and any λ in $\mathbf{F}_{2^n}^*$. Note that h_μ is a quadratic form from $\mathbf{F}_{2^n}$ into $\mathbf{F}_2$. Thus using the results of Section 2.2, the Walsh spectrum of h_μ is completely defined as soon as the dimension of its kernel is known. Our next goal is to describe this kernel.

Lemma 5. *Let $K(\mu)$ be the kernel of the quadratic form h_μ and $A = \mu + \mu^{2^{5r}}$. Then $K(\mu)$ is the subspace of the roots of $P \in \mathbf{F}_{2^n}[x]$ given by*

$$P(x) = \mu x^{2^{2r}} + Ax^{2^r} + (\mu x)^{2^{4r}} + (Ax)^{2^{5r}}.$$

Proof. We compute the derivatives of h_μ with respect to any $b \in \mathbf{F}_{2^n}^*$:

$$\begin{aligned} D_b h_\mu(x) &= \mathrm{Tr}\big(\mu\big(x^{2^{2r}}b + b^{2^{2r}}x\big) + A\big(x^{2^r}b + b^{2^r}x\big) + \mu b^{2^{2r}+1} + Ab^{2^r+1}\big) \\ &= \mathrm{Tr}\big(x\big(\mu b^{2^{2r}} + Ab^{2^r} + (\mu b)^{2^{4r}} + (Ab)^{2^{5r}}\big)\big) + h_\mu(b). \end{aligned}$$

According to Lemma 1, we get for any $\mu \in \mathbf{F}_{2^n}^*$

$$K(\mu) = \big\{b \in \mathbf{F}_{2^n} \;\big|\; \mu b^{2^{2r}} + Ab^{2^r} + (\mu b)^{2^{4r}} + (Ab)^{2^{5r}} = 0\big\}. \qquad \square$$

Recall that a polynomial of the form $\sum_{i=0}^{m-1} a_i x^{q^i}$ with coefficients in an extension field $\mathbf{F}_{q^m}$ of $\mathbf{F}_q$ is called *a q-polynomial over $\mathbf{F}_{q^m}$* [19, p.107]. If $\mathbf{F}_{q^m}$ is considered as a vector space over $\mathbf{F}_q$, then q-polynomials are the linear maps of this vector space. Hence we can speak from the kernel of a q-polynomial. Clearly, the kernel and the image set of a q-polynomial are subspaces of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$. In particular, these sets have cardinality q^k for some k. The polynomial $P(x)$ considered here is a 2^r-polynomial. As a consequence, the dimension of the kernel of $P(x)$ (i.e., the dimension of any $K(\mu)$) equals kr for some k. On the other hand, $K(\mu)$ has at most 2^{4r} elements because $P(x)$ can be written as $(P'(x))^{2^r}$ with $\deg P' = 2^{4r}$.

Consider now the quadratic form from $\mathbf{F}_{q^6}$ to $\mathbf{F}_q$ ($q = 2^r$):

$$H_\mu(x) = T_r^{6r}\big(\mu x^{2^{2r}+1} + Ax^{2^r+1}\big).$$

The set of roots of $P(x)$ is also the kernel $\mathcal{K}$ of H_μ. Indeed, $\mathcal{K}$ is the set of those b such that $B(x) = 0$ for all x with

$$B(x) = H_\mu(x) + H_\mu(b) + H_\mu(x+b)$$

(see Section 2.2). Since $D_b h_\mu(x) = T_1^r(B(x))$, we get

$$B(x) = T_r^{6r}\big(P(b)x\big)$$

(see the proof of Lemma 5). Thus, the kernel $\mathcal{K}$ of H_μ is equal to $K(\mu)$. By Proposition 1, the dimension of $\mathcal{K}$ over $\mathbf{F}_{2^r}$ must have the same parity as 6, so it is even. We conclude that the dimension of $\mathcal{K}$ over $\mathbf{F}_{2^r}$ is either 2 or 4, implying that the one of $K(\mu)$ over $\mathbf{F}_2$ is either $2r$ or $4r$.

Proposition 4. *The kernel $K(\mu)$ of the quadratic function h_μ, defined by* (19)*, has dimension either $2r$ or $4r$.*

4.2. The spectrum of h_μ

In this subsection we determine for which μ the dimension of $K(\mu)$ is $2r$ and for which it is $4r$, studying the kernel of $P(x)$. First we prove two lemmas. The first lemma can be easily generalized to any finite field.

Lemma 6. *Let $q = 2^r$, $n = rm$ and $U(x)$ be any q-polynomial over $\mathbf{F}_{2^n}$. Set* $\operatorname{Im} U = \{U(x) \mid x \in \mathbf{F}_{2^n}\}$,

$$V = \left\{x \in \mathbf{F}_{2^n} \;\middle|\; U(x) + U(x)^{2^r} = 0\right\} \quad \text{and} \quad W = \left\{x \in \mathbf{F}_{2^n} \;\middle|\; U(x) = 0\right\}.$$

Then, $\operatorname{Im} U \cap \mathbf{F}_{2^r}$ *equals either $\mathbf{F}_{2^r}$ or $\{0\}$. Furthermore,* $\dim V$ *is equal to*

$$\begin{cases} \dim W & \text{if } \operatorname{Im} U \cap \mathbf{F}_{2^r} = \{0\}, \\ \dim W + r & \text{if } \operatorname{Im} U \cap \mathbf{F}_{2^r} = \mathbf{F}_{2^r}. \end{cases}$$

Proof. Suppose that there exist $\xi \in F_{2^r}^*$ and $x_0 \in \mathbf{F}_{2^n}$ such that $U(x_0) = \xi$. Then for any $\delta \in \mathbf{F}_{2^r}$ it holds

$$U\left(\delta \xi^{-1} x_0\right) = \delta \xi^{-1} U(x_0) = \delta,$$

proving the first statement. Recall that $U(x) + U(x)^{2^r} = 0$ if and only if $U(x) \in \mathbf{F}_{2^r}$. To complete the proof note that every element in $\operatorname{Im} U$ has 2^u many preimages, where $u = \dim W$. □

We again consider $K(\mu)$ and $P(x)$, as defined by Lemma 5.

Lemma 7. *For any μ, we have $P(x) = L(x^{2^r} + x)$ with*

$$L(x) = \mu x^{2^r} + (\mu x)^{2^{4r}} + \mu^{2^{5r}} \left(x^{2^{5r}} + x\right). \tag{20}$$

In particular, $K(\mu)$ contains $\mathbf{F}_{2^r}$. Furthermore, denoting by I be the image set of the mapping $x \mapsto x^{2^r} + x$, $x \in \mathbf{F}_{2^n}$, we have

$$\dim K(\mu) = \dim\left\{x \in I \;\middle|\; L(x) = 0\right\} + r. \tag{21}$$

Proof. We have:

$$\begin{aligned} P(x) &= \mu x^{2^{2r}} + \left(\mu + \mu^{2^{5r}}\right)x^{2^r} + \mu^{2^{4r}} x^{2^{4r}} + \left(\mu^{2^{5r}} + \mu^{2^{4r}}\right)x^{2^{5r}} \\ &= \mu\left(x + x^{2^r}\right)^{2^r} + \mu^{2^{4r}}\left(x + x^{2^r}\right)^{2^{4r}} + \mu^{2^{5r}}\left(x + x^{2^{4r}}\right)^{2^r} \\ &= L\left(x + x^{2^r}\right) \end{aligned}$$

with

$$x + x^{2^{4r}} = \left(x + x^{2^r}\right)^{2^{4r}} + \left(x + x^{2^r}\right)^{2^{5r}}.$$

Since $K(\mu)$ is the kernel of P, equality (21) is directly obtained. We use that every element from I has 2^r preimages. □

Proposition 4 and Lemma 7 imply that $P(x)$ has always some roots which do not belong to $\mathbf{F}_{2^r}$. Actually, we have to find the nonzero X such that

$$L(X) = 0, \quad X = x^{2^r} + x,\ x \in \mathbf{F}_{2^n}, \tag{22}$$

where L is defined by (20). Note that $X = x^{2^r} + x$ if and only if $T_r^{6r}(X) = 0$.

Lemma 8. *Let* $\sigma = \mu^{2^r+2^{4r}} + \mu^{2^r+2^{3r}} + \mu^{2^{2r}+2^{4r}}$. *The polynomial* L *is given by* (20). *Then we have*:

(a) *Assume* $\sigma \neq 0$. *If* X *is a solution of* (22) *then* $X = \sigma\gamma$ *for some* $\gamma \in \mathbf{F}_{2^{2r}}$.
(b) *If* $\sigma = 0$, *then any* y, $y = L(x) + L(x)^{2^r}$ *for some* x, *satisfies*

$$\mu^{2^{3r}} y + \mu^{2^{4r}} y^{2^{2r}} = 0$$

and μ *is a* $(2^r + 1)$*th power.*

Proof. We compute $R(x) = L(x) + L(x)^{2^r}$:

$$\begin{aligned} R(x) &= \mu x^{2^r} + (\mu x)^{2^{4r}} + \mu^{2^{5r}}\left(x^{2^{5r}} + x\right) + \mu^{2^r} x^{2^{2r}} + (\mu x)^{2^{5r}} + \mu\left(x + x^{2^r}\right) \\ &= Ax + \mu^{2^r} x^{2^{2r}} + \mu^{2^{4r}} x^{2^{4r}}, \end{aligned}$$

with $A = (\mu + \mu^{2^{5r}})$. Now we compute

$$\begin{aligned} M(x) &= \mu^{2^{3r}} R(x) + \mu^{2^{4r}} R(x)^{2^{2r}} \\ &= \left(\mu^{2^{3r}} A + \mu^{2^{4r}+1}\right)x + \left(\mu^{2^{3r}+2^r} + A^{2^{2r}}\mu^{2^{4r}}\right)x^{2^{2r}} \\ &= \sigma^{2^{2r}} x + \sigma x^{2^{2r}}, \end{aligned}$$

noticing that $(\mu^{2^{3r}} A + \mu^{2^{4r}+1})^{2^{4r}} = \sigma$. We get $M(\sigma) = 0$.

If $\sigma \neq 0$ then the kernel of M is exactly $\sigma\mathbf{F}_{2^{2r}}$. Hence the kernel of R is a subspace of $\sigma\mathbf{F}_{2^{2r}}$. But σ is a root of R too:

$$\begin{aligned} R(\sigma) = {} & \mu^{1+2^r+2^{4r}} + \mu^{1+2^r+2^{3r}} + \mu^{1+2^{2r}+2^{4r}} \\ & + \mu^{2^r+2^{4r}+2^{5r}} + \mu^{2^r+2^{3r}+2^{5r}} + \mu^{2^{2r}+2^{4r}+2^{5r}} \\ & + \mu^{1+2^r+2^{3r}} + \mu^{2^r+2^{3r}+2^{5r}} + \mu^{1+2^r+2^{4r}} \\ & + \mu^{2^{2r}+2^{4r}+2^{5r}} + \mu^{2^r+2^{4r}+2^{5r}} + \mu^{1+2^{2r}+2^{4r}} \\ = {} & 0. \end{aligned}$$

Consequently the kernel of R coincides with $\sigma\mathbf{F}_{2^{2r}}$. Since the kernel of L is a subspace of the kernel of R, then any nonzero solution of (22) belongs to $\sigma\mathbf{F}^*_{2^{2r}}$, completing the proof of (a).

Now suppose that $\sigma = 0$, so that M is the null polynomial. Hence any $y = R(x)$ satisfies $\mu^{2^{3r}} y + \mu^{2^{4r}} y^{2^{2r}} = 0$, that is, for any such nonzero y,

$$y^{2^{2r}-1} = \left(\frac{1}{\mu^{2^r-1}}\right)^{2^{3r}}. \tag{23}$$

This is possible only if μ is a (2^r+1)th power in $\mathbf{F}_{2^n}$, completing the proof. □

Now, we are ready to find the Walsh spectrum of h_μ, i.e. to determine the dimension of $K(\mu)$ (see Lemma 5).

Theorem 4. *Let* $\sigma = \mu^{2^r+2^{4r}} + \mu^{2^r+2^{3r}} + \mu^{2^{2r}+2^{4r}}$. *Then*

$$\dim K(\mu) = \begin{cases} 2r & \text{if } \sigma \neq 0, \\ 4r & \text{if } \sigma = 0. \end{cases}$$

Consequently, the Walsh transform of h_μ *takes the values* $\{0, \pm 2^{5r}\}$ *if* $\sigma = 0$ *and* $\{0, \pm 2^{4r}\}$, *otherwise.*

Proof. Notation is as in Lemma 8 and in its proof. Consider again the polynomial R which has degree 2^{4r}.

When $\sigma \neq 0$, we have shown in the proof of Lemma 8 that the kernel of R has dimension $2r$. Thus the dimension of the kernel of L is at most $2r$. By Lemma 7 it holds $\dim K(\mu) \leqslant 3r$, and Proposition 4 implies $\dim K(\mu) = 2r$.

Assume that $\sigma = 0$. By Lemma 8, we know that the image of R is contained in the subspace

$$J = \{0\} \cup \left\{ y \in \mathbf{F}_{2^n},\ y^{2^{2r}-1} = \mu^{-2^{3r}(2^r-1)} \right\},$$

where $\mu = \beta^{2^r+1}$ for some β. Clearly, we have $J = c\mathbf{F}_{2^{2r}}$ with $c = \beta^{-2^{3r}}$. Thus the image set of R has dimension at most $2r$. Therefore, the dimension of the kernel of R is at least $4r$. Since R has degree 2^{4r}, this dimension is exactly $4r$. Now, the kernel of L, say K_1, is a subspace of the kernel of R. Since $R(x) = L(x) + L(x)^{2^{2r}}$ we get from Lemma 6

$$\dim K_1 \in \{3r, 4r\}.$$

But $\dim K(\mu) = \dim K_1 + r$ (see Lemma 7) which leads to $\dim K(\mu) = 4r$, completing the proof. □

Table 2
The exponents d, defining bent Boolean functions on $\mathbf{F}_{2^n}$, $n = 2t$, of the form $x \mapsto \mathrm{Tr}(\lambda x^d)$ for some $\lambda \in \mathbf{F}_{2^n}$. An exhaustive search shows that there are no other d for $n \leqslant 20$

Type	Exponent	Condition	References
$\mathcal{PS}_{ap}$	$a(2^t - 1)$	$\gcd(a, 2^t + 1) = 1$	[12,16]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	[13]
Maiorana–McFarland	$2^i + 1$	$n = \gcd(n, i)s$, s even	[15]
	$(2^r + 1)^2$	$n = 4r$	[9,17]
	$2^{2r} + 2^r + 1$	$n = 6r$	This paper

5. Conclusions

The complete classification of monomial bent functions is not achieved. We give in Table 2 the list of known such functions. There are no other for $n \leqslant 20$. Actually, little is known about this corpus, as recalled in [17]. They do not all lie in the known classes, especially in class $\mathcal{M}$. For instance, some bent functions characterized in [13], namely with *Kasami exponents*, are not normal [4], implying that they do not belong to any previously known class. On the other hand, the most recent results on monomial bent functions provide subclasses of $\mathcal{M}$.

During our work, we investigated general tools for the study of monomial bent functions. Although our proofs, in this paper, seem specific, we introduce several tools for the study of a larger class of Boolean functions, expressed by trace functions, especially those which are of degree 3. Notably, we showed by Example 1 that some functions studied in [17] can be viewed as a concatenation of affine functions. This result will be completed in a forthcoming paper, in a more general context (see [9,10]).

The study of functions f_λ which are not bent leads to several open problems (see Conjecture 1). For this reason, we studied the properties of derivatives of all f_λ. Our study of the functions $g_{a,\lambda}$ can also be placed into the context of the general study of quadratic functions, a topic which is currently discussed [8,23].

References

[1] T. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy, On almost perfect nonlinear functions, IEEE Trans. Inform. Theory 52 (9) (2006) 4160–4170.
[2] A. Canteaut, P. Charpin, Decomposing bent functions, IEEE Trans. Inform. Theory 49 (8) (2003) 2004–2019.
[3] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, On cryptographic properties of the cosets of $R(1, m)$, IEEE Trans. Inform. Theory 47 (4) (2001) 1494–1513.
[4] A. Canteaut, M. Daum, G. Leander, H. Dobbertin, Normal and non normal bent functions, Discr. Appl. Math. 154 (2) (2006) 202–218.
[5] C. Carlet, Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications, Cryptology ePrint Archive, Report 2006/457, http://eprint.iacr.org/, 2006.
[6] C. Carlet, Boolean functions for cryptography and error correcting codes, in: Y. Crama, P. Hammer (Eds.), Boolean Methods and Models, Cambridge Univ. Press, in press.
[7] C. Carlet, P. Gaborit, Hyper-bent functions and cyclic codes, J. Combin. Theory Ser. A 113 (3) (2006) 466–482.
[8] P. Charpin, C. Tavernier, E. Pasalic, On bent and semi-bent quadratic Boolean functions, IEEE Trans. Inform. Theory 51 (12) (2005) 4287–4298.
[9] P. Charpin, G. Kyureghyan, On cubic bent functions in the class M, in: Proceedings of Algebraic and Combinatorial Coding Theory, ACCT-10, Zvenigorod, Russia, September 2006.
[10] P. Charpin, G. Kyureghyan, Cubic monomial bent functions: A subclass of $\mathcal{M}$, submitted for publication.
[11] P.M. Cohn, Algebra, vol. I, Wiley, 1982.
[12] J. Dillon, Elementary Hadamard difference sets, PhD dissertation, University of Maryland, 1974.

[13] J. Dillon, H. Dobbertin, New cyclic difference sets with Singer parameters, Finite Fields Appl. 10 (2004) 342–389.
[14] R.W. Fitzgerald, Highly degenerate quadratic forms over finite fields of characteristic 2, Finite Fields Appl. 11 (2005) 165–181.
[15] R. Gold, Maximal recursive sequences with 3-valued recursive crosscorrelation functions, IEEE Trans. Inform. Theory 14 (1) (1968) 154–156.
[16] G. Lachaud, J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, IEEE Trans. Inform. Theory 36 (3) (1990) 686–692.
[17] N.G. Leander, Monomial bent functions, IEEE Trans. Inform. Theory 52 (2) (2006) 738–743.
[18] N.G. Leander, A. Kholosha, Bent functions with 2^r Niho exponents, IEEE Trans. Inform. Theory 52 (12) (2006) 5529–5532.
[19] R. Lidl, H. Niederreiter, Finite Fields, Cambridge Univ. Press, 1983.
[20] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error Correcting Codes, North-Holland, 1986.
[21] R.J. McEliece, Finite Fields for Computer Scientists and Engineers, Kluwer, 1987.
[22] R.L. McFarland, A family of noncyclic difference sets, J. Combin. Theory Ser. A 15 (1973) 1–10.
[23] N.Y. Yu, G. Gong, Constructions of quadratic bent functions in polynomial forms, IEEE Trans. Inform. Theory 52 (7) (2006) 3291–3299.