On the Link of Some Semi-bent Functions with Kloosterman Sums

Sihem Mesnager[1] and Gérard Cohen[2]

[1] Department of Mathematics, University of Paris VIII and University of Paris XIII, CNRS UMR 7539 LAGA (Laboratoire Analyse, Géometrie et Applications), France
mesnager@math.jussieu.fr
[2] Ecole Nationale Supérieure des Télécommunications -Telecom-Paristech, UMR 5141, CNRS, France
cohen@telecom-paristech.fr

Abstract. We extensively investigate the link between the semi-bentness property of some Boolean functions in polynomial forms and Kloosterman sums.

Keywords: Boolean function, Semi-bent function, Walsh-Hadamard transformation, Kloosterman sums.

1 Introduction

Let n be a positive integer. A Boolean function f on $\mathbb{F}_{2^n}$ is an $\mathbb{F}_2$-valued function over the Galois field $\mathbb{F}_{2^n}$ of order 2^n. Boolean functions play an important role in coding theory (and in particular the class of Reed-Muller codes [20], [9]) on one hand and symmetric cryptography (block ciphers and stream ciphers) [2] on the other hand. Various criteria related to cryptographically desirable Boolean functions have been proposed, such as balancedness, high nonlinearity, correlation immunity, satisfiability of the propagation criterion etc.

The notion of *semi-bent function* has been introduced by Chee, Lee and Kim at Asiacrypt' 94 [7]. In fact, these functions had been previously investigated under the name of three-valued almost optimal Boolean functions in [1]. Moreover, they are particular cases of the so-called plateaued functions [30,29]. Semi-bent functions are widely studied in cryptography because, besides having low Hadamard transform which provides protection against fast correlation attacks [22] and linear cryptanalysis [21], they possess desirable properties such as low autocorrelation, propagation criteria, resiliency and high algebraic degree. Semi-bent functions have been paid a lot of attention in code division multiple access (CDMA) communication systems for sequence design [12], [26], [13], [14], [15], [16], [17] etc. In fact, highly nonlinear functions correspond to sequences that have low cross-correlation with the m-sequences (maximum-length linear feedback shift -register sequences) represented by an absolute trace function $Tr_1^m(x)$. Semi-bent functions exist for even or odd number of variables. When n is even, the semi-bent functions are those Boolean functions whose Hadamard transform

Y.M. Chee et al. (Eds.): IWCC 2011, LNCS 6639, pp. 263–272, 2011.

takes values 0 and $\pm 2^{\frac{n+2}{2}}$. They are balanced (up to the addition of a linear function) and have maximal non-linearity for balanced plateaued functions. When n is odd, the lower bound for the maximum size of the Hadamard transform is not known in general. However, this lower bound has been shown to be $2^{\frac{n+1}{2}}$ when the function is quadratic [20] or when $n = 3, 5, 7$ [25]. Also, it has been shown in [27], [28] that the lower bound for the maximum size of the Hadamard transform does not exceed $\frac{27}{32} \times 2^{\frac{n+1}{2}}$ when $n \geq 15$ is odd. Functions which achieve this lower bound with equality are the semi-bent functions, whose Hadamard transform only takes on the three values 0, $\pm 2^{\frac{n+1}{2}}$ [8].

In this paper, some Boolean functions in polynomial forms with even number of variables are considred. Some papers have been devoted to the construction of semi-bent functions whose expression is a power polynomial $Tr_1^n(x^d)$ for a suitably chosen d and particular values of n (n even). A recent work in this topic is due to Charpin et al. [6] for the construction of quadratic semi-bent functions. A very recent work is [3], in which semi-bent functions in even dimension are characterized and many infinite classes with maximum algebraic degree have been derived from a subclass of bent functions (more precisely, Dillon Partial Spreads $\mathcal{PS}_{ap}$-like). Recall that bent functions are those Boolean functions whose Hadamard transform takes values $\pm 2^{\frac{n}{2}}$. Our main intention in this paper is to investigate the link between Kloosterman sums and the semi-bentness property of functions defined on $\mathbb{F}_{2^n}$ ($n = 2m$) whose polynomial forms are given by (*):

$$Tr_1^n\left(ax^{r(2^m-1)}\right) + Tr_1^2\left(bx^{\frac{2^n-1}{3}}\right) + Tr_1^m\left(c'x^{2^m+1}\right) + Tr_1^n\left(dx^{(2^m-1)s+1}\right)$$

where r is a positive integer such that $gcd(r, 2^m + 1) = 1$, $s \in \left\{0, \frac{1}{4}, \frac{1}{6}, 3\right\}$ ($\frac{1}{4}$ and $\frac{1}{6}$ are understood modulo $2^m + 1$), $a \in \mathbb{F}_{2^m}^\star$, $b \in \mathbb{F}_4$, $c' \in \mathbb{F}_{2^m}$ and $d \in \mathbb{F}_2$. The paper is organized as follows. In section 2, we fix our main notation and recall the necessary background. Next, in section 3, we give some technical results. Finally, in section 4, we characterize some infinite classes of semi-bent parameterized Boolean functions of the form (*) in terms of the evaluation of the classical Kloosterman sum on the single parameter a.

2 Notation and Preliminaries

For any set E, we will denote $E \setminus \{0\}$ by $E^\star$.

• *Boolean functions in polynomial forms*
For any positive integer k, and for any 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: $\forall x \in \mathbb{F}_{2^k}$, $Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}}$. In particular, the *absolute trace* over $\mathbb{F}_2$ is the function $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. Recall that, for every integer r dividing k, the trace function Tr_r^k satisfies the transitivity property, that is, $Tr_1^k = Tr_1^r \circ Tr_r^k$.

Every non-zero Boolean function f defined over $\mathbb{F}_{2^n}$ has a (unique) trace expansion of the form:

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1})$$

called its polynomial form, where Γ_n is the set of integers obtained by choosing one element in each cyclotomic coset of 2 modulo $2^n - 1$, $o(j)$ is the size of the cyclotomic coset of 2 modulo $2^n - 1$ containing j, $a_j \in \mathbb{F}_{2^{o(j)}}$ and, $\epsilon = wt(f)$ 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 equal to the maximum 2-weight of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$.

• *Walsh transform and semi-bent functions*
Let f be a Boolean function on $\mathbb{F}_{2^n}$. Its *"sign" function* is the integer-valued function $\chi(f) := (-1)^f$. The *W*alsh 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:

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

Semi-bent functions [7], [8] can be defined as follows:

Definition 1. *For even n, a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be semi-bent if $\widehat{\chi_f}(\omega) \in \{0, \pm 2^{\frac{n+2}{2}}\}$, for all $\omega \in \mathbb{F}_{2^n}$. For odd n, a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be semi-bent if $\widehat{\chi_f}(\omega) \in \{0, \pm 2^{\frac{n+1}{2}}\}$, for all $\omega \in \mathbb{F}_{2^n}$.*

It is well known (see for instance [2]) that the algebraic degree of a semi-bent Boolean function defined on $\mathbb{F}_{2^n}$ is at most $\frac{n}{2}$.

• *Niho power functions*
Let $n = 2m$ be an even integer. Recall that a positive integer d (always understood modulo $2^n - 1$) is said to be a *Niho exponent*, and x^d is a *Niho power function*, if the restriction of x^d to $\mathbb{F}_{2^m}$ is linear or in other words $d \equiv 2^j \pmod{2^m - 1}$ for some $j < n$. As we consider $Tr_1^n(x^d)$, without loss of generality, we can assume that d is in the normalized form, with $j = 0$, and then we have a unique representation $d = (2^m - 1)s + 1$ with $2 \leq s \leq 2^m$. Four examples of infinite classes of Niho bent functions are known up to linear equivalence. The simplest one is the quadratic function $x \mapsto Tr_1^m\left(cx^{2^m+1}\right)$; $c \in \mathbb{F}_{2^m}^\star$. Three infinite classes of Niho bent functions in univariate form have been given in [11]:

1. $x \mapsto Tr_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)3+1}\right)$, $a_1 \in \mathbb{F}_{2^n}^\star$, $a_2 \in \mathbb{F}_{2^n}^\star$; (if $m \equiv 2 \pmod 4$ then a_2 must be a fifth power of an element in $\mathbb{F}_{2^n}$; otherwise a_2 can be any nonzero element of $\mathbb{F}_{2^n}$).
2. $x \mapsto Tr_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)\frac{1}{4}+1}\right)$, $a_1 \in \mathbb{F}_{2^n}^\star$, $a_2 \in \mathbb{F}_{2^n}^\star$, m odd;
3. $x \mapsto Tr_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)\frac{1}{6}+1}\right)$, $a_1 \in \mathbb{F}_{2^n}^\star$, $a_2 \in \mathbb{F}_{2^n}^\star$ m even.

• *Kloosterman sums*
We need to introduce a classical binary exponential sum on $\mathbb{F}_{2^m}$ (where m is an arbitrary positive integer):

Definition 2. *The classical binary Kloosterman sums on $\mathbb{F}_{2^m}$ are:*

$$K_m(a) := \sum_{x \in \mathbb{F}_{2^m}} \chi\big(Tr_1^m(ax + \frac{1}{x})\big), \quad a \in \mathbb{F}_{2^m}$$

The Kloosterman sums are generally defined on the multiplicative group $\mathbb{F}_{2^m}^\star$ of $\mathbb{F}_{2^m}$. In this paper we extend to 0 assuming that $\chi(Tr_1^m(\frac{1}{x})) = 1$ for $x = 0$ (in fact, $Tr_1^m(\frac{1}{x}) = Tr_1^m(x^{2^{m-1}-1})$).

The following Proposition is directly obtained from the result of Lachaud and Wolfmann in [18] which is suitable for any m (even or odd).

Proposition 3. *[18] Let m be a positive integer. The set $\{K_m(a), a \in \mathbb{F}_{2^m}\}$ is the set of all the integers multiple of 4 in the range $[-2^{(m+2)/2}+1, 2^{(m+2)/2}+1]$.*

• *Some additional background*
Let $n = 2m$ be an even integer. Let x be an element of $\mathbb{F}_{2^n}$. The conjugate of x over a subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$ will be denoted by $\bar{x} = x^{2^m}$ and the relative norm with respect to the quadratic field extension $\mathbb{F}_{2^n}/\mathbb{F}_{2^m}$ by $norm(x) = x\bar{x}$. Also, we denote by U the set $\{u \in \mathbb{F}_{2^n} \mid norm(u) = 1\}$, which is the group of $(2^m + 1)$-st roots of unity. Note that since the multiplicative group of the field $\mathbb{F}_{2^n}$ is cyclic and 2^m+1 divides 2^n-1, the order of U is 2^m+1. Finally, note that the unit 1 is the single element in $\mathbb{F}_{2^m}$ of norm one and every non-zero element x of $\mathbb{F}_{2^n}$ has a unique decomposition as: $x = yu$ with $y \in \mathbb{F}_{2^m}^\star$ and $u \in U$.

3 Some Technical Results

We state a well-known result (different proofs can be found in [18], [10], [19],[5]).

Proposition 4. *Let $n = 2m$, r a positive integer such that $\gcd(r, 2^m + 1) = 1$ and $a \in \mathbb{F}_{2^m}$. Let U be the group of $(2^m + 1)$-st roots of unity. Then,*

$$\sum_{u \in U} \chi\left(Tr_1^n(au^r)\right) = 1 - K_m(a)$$

The following result can be derived from [24], which extends Proposition 4.

Proposition 5. *Let $n = 2m$ with m odd and r a positive integer such that $\gcd(r, 2^m + 1) = 1$. Let U be the group of $(2^m + 1)$-st roots of unity. Let $b \in \mathbb{F}_4^\star$, $a \in \mathbb{F}_{2^m}$ and ζ be a generator of the cyclic group U. Then,*

$$\sum_{u \in U} \chi\left(Tr_1^n(au^r) + Tr_1^2(bu^{\frac{2^m+1}{3}})\right) = \begin{cases} \frac{K_m(a)-1+4C_m(a,a)}{3} & \text{if } b = 1 \\ \frac{K_m(a)-1-2C_m(a,a)}{3} & \text{if } b \neq 1 \end{cases}$$

Thanks to Proposition 5 one can prove the following result.

Corollary 6. *Let $n = 2m$ with $m > 3$ odd and r be a positive integer such that $\gcd(r, 2^m + 1) = 1$. Let U be the group of $(2^m + 1)$-st roots of unity. Let $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_4$. Then*

$$\sum_{u \in U} \chi\left(Tr_1^n(au^r) + Tr_1^2(bu^{\frac{2^m+1}{3}})\right) = 1 \tag{1}$$

if and only if

- *$b = 0$ and $K_m(a) = 0$,*
- *or, $b \neq 0$ and $K_m(a) = 4$.*

4 Some Semi-bent Functions in Univariate Forms

In this section, we investigate under which conditions on its coefficients a Boolean function whose univariate form is given by (2) ($\frac{1}{2}$ is understood modulo $2^m + 1$) is semi-bent.

$$\begin{aligned} &Tr_1^n\left(ax^{r(2^m-1)}\right) + Tr_1^2\left(bx^{\frac{2^n-1}{3}}\right) + Tr_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) \\ &\quad + Tr_1^n(dx^{(2^m-1)s+1}) \end{aligned} \tag{2}$$

where r is a positive integer such that $gcd(r, 2^m + 1) = 1$, $s \in \left\{0, \frac{1}{4}, \frac{1}{6}, 3\right\}$ ($\frac{1}{4}$ and $\frac{1}{6}$ are understood modulo $2^m + 1$), $a \in \mathbb{F}_{2^m}^\star$, $b \in \mathbb{F}_4$, $c \in \mathbb{F}_{2^n}$ and $d \in \mathbb{F}_2$. Firstly, we introduce the following decomposition $\mathbb{F}_{2^n}^\star = \bigcup_{u \in U} u\mathbb{F}_{2^m}^\star$. Let $g_{a,b,c,d}^{(r,s)}$ be of any Boolean function of the form (2); note that the restriction of $g_{a,b,c,d}^{(r,s)}$ to any coset $u\mathbb{F}_{2^m}^\star$ ($u \in U$), is affine. More precisely,

- If $b \neq 0$, we consider the functions $g_{a,b,c,d}^{(r,s)}$ of the form (2) only when m is odd. We then have, thanks to the transitivity of the trace function:

$$\forall y \in \mathbb{F}_{2^m}^\star, g_{a,b,c,d}^{(r,s)}(uy) = Tr_1^m(\alpha_u y) + \beta_u \tag{3}$$

  with

$$\begin{aligned} \alpha_u &= Tr_m^n\left(du^{(2^m-1)s+1} + cu^{(2^m-1)\frac{1}{2}+1}\right) = Tr_m^n\left(du^{(2^m-1)s+1} + c\right), \\ \beta_u &= Tr_1^n\left(au^{r(2^m-1)}\right) + Tr_1^2\left(bu^{\frac{2^n-1}{3}}\right). \end{aligned}$$

- Otherwise (that is, $b = 0$), we consider the functions $g_{a,0,c,d}^{(r,s)}$ of the form (2) (without condition on the parity of m). Then, we have thanks to the transitivity of the trace function:

$$\forall y \in \mathbb{F}_{2^m}^\star, g_{a,0,c,d}^{(r,s)}(uy) = Tr_1^m(\alpha_u y) + \beta_u \tag{4}$$

with

$$\alpha_u = Tr_m^n\left(du^{(2^m-1)s+1} + c\right),$$
$$\beta_u = Tr_1^n\left(au^{r(2^m-1)}\right).$$

Therefore, the Walsh transform of a generic function of the form (2) can be computed as follows.

Lemma 7. *Let U be the group of (2^m+1)-st roots of unity. The Walsh transform of a generic element of the form (2) is (taking the same notation as in (3) or (4)) :*

$$\forall \omega \in \mathbb{F}_{2^n},\ \widehat{\chi_{g^{(r,s)}_{a,b,c,d}}}(\omega) = 1 - \sum_{u\in U}\chi(\beta_u) + 2^m \sum_{u\in U}\delta_0(\alpha_u + Tr_m^n(\omega u))\chi(\beta_u) \quad (5)$$

where δ_0 is the indicator of the singleton $\{0\}$, that is, $\delta_0(z) = 1$ if $z = 0$ and 0 otherwise.

Proof. Suppose m odd and $b \neq 0$. Let $\omega \in \mathbb{F}_{2^n}$. The Walsh transform of $g^{(r,s)}_{a,b,c,d}$ is defined as

$$\widehat{\chi_{g^{(r,s)}_{a,b,c,d}}}(\omega) = \sum_{x\in\mathbb{F}_{2^n}} \chi(g^{(r,s)}_{a,b,c,d}(x) + Tr_1^n(wx)).$$

Any element $x \in \mathbb{F}_{2^n}^\star$ having a unique polar decomposition $x = uy$ with $u \in U$ and $y \in \mathbb{F}_{2^m}^\star$, we have:

$$\begin{aligned}\widehat{\chi_{g^{(r,s)}_{a,b,c,d}}}(\omega) &= 1 + \sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^\star} \chi(g^{(r,s)}_{a,b,c,d}(uy) + Tr_1^n(wuy))\\ &= 1 + \sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^\star} \chi\left(Tr_1^m\left((\alpha_u + Tr_m^n(wu))y\right) + \beta_u\right)\\ &= 1 - \sum_{u\in U}\chi(\beta_u) + 2^m\sum_{u\in U}\delta_0(\alpha_u + Tr_m^n(\omega u))\chi(\beta_u)\end{aligned}$$

because $\sum_{y\in\mathbb{F}_{2^m}}\chi(Tr_1^m(\lambda y)) = 0$ if $\lambda \neq 0$ and 2^m if $\lambda = 0$. Likewise, one can establish (5) by similar calculations when $b = 0$ (for m even or odd).

We are now going to investigate several subfamilies of (2). We begin with a preliminary technical statement.

Lemma 8. *Let $w \in \mathbb{F}_{2^n}^\star$ and $c \in \mathbb{F}_{2^n}^\star \setminus \mathbb{F}_{2^m}$. The number of $u \in U$ such that $Tr_m^n(wu + c) = 0$ equals 0 or 2.*

Proof. One has

$$\begin{aligned}Tr_m^n(wu + c) = 0 &\iff wu + w^{2^m}u^{2^m} + Tr_m^n(c) = 0\\ &\iff u^2 + w^{-1}Tr_m^n(c)u + w^{2^m-1} = 0.\end{aligned}$$

Now recall that the quadratic equation $X^2 + aX + b = 0$, $a \neq 0$, admits 0 or 2 solutions.

Next we recall a result shown in [11].

Lemma 9. *For every $w \in \mathbb{F}_{2^n}$, the three following equations admits 0 or 2 solutions in U.*

$$Tr_m^n(wu + u^{\frac{1}{2}}) = 1 \tag{6}$$

$$Tr_m^n(wu + u^5) = 1 \tag{7}$$

$$Tr_m^n(wu^3 + u^2) + 1 = 0 \tag{8}$$

Now, one can prove the following results.

Theorem 10. *Let $n = 2m$. Let r be a positive integer such that $gcd(r, 2^m+1) = 1$. Let $a \in \mathbb{F}_{2^m}^\star$ and $c \in \mathbb{F}_{2^n}^\star \setminus \mathbb{F}_{2^m}$. Then, $g_{a,0,c,0}^{(r,0)}$ is semi-bent if and only if $K_m(a) = 0$.*

Proof. Using the notation of (4), one has

$$\alpha_u = Tr_m^n(c), \quad \beta_u = Tr_1^n(au^{r(2^m-1)})$$

The equation $Tr_m^n(wu + c) = 0$ admits 0 or 2 solutions for every $w \in \mathbb{F}_{2^n}^\star$ by Lemma 8. Therefore $\sum_{u\in U} \delta_0(\alpha_u + Tr_m^n(wu))\chi(\beta_u) \in \{0, \pm 2\}$ for every $w \in \mathbb{F}_{2^n}^\star$. In the case where $w = 0$, since $\alpha_u = Tr_m^n(c) \neq 0$ because $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, $\sum_{u\in U} \delta_0(\alpha_u) = 0$. Basicly, for every $w \in \mathbb{F}_{2^n}$, $\widehat{\chi_{g_{a,0,c,0}^{(r,0)}}}(w) = 1 - \sum_{u\in U} \chi(Tr_1^n(au^{r(2^m-1)}))$ mod 2^{m+1}. Recall that the function $g_{a,0,c,0}^{(r,0)}$ is semi-bent if and only if $\widehat{\chi_{g_{a,0,c,0}^{(r,0)}}}(w) \in \{0, \pm 2^{m+1}\}$ for every $w \in \mathbb{F}_{2^n}$. Now, since

$$-2^{m+1} < -2^m - 1 \leq \sum_{u\in U} \chi(Tr_1^n(au^{r(2^m-1)})) \leq 2^m + 1 < 2^{m+1}$$

then, $g_{a,0,c,0}^{(r,0)}$ is semi-bent if and only if

$$\sum_{u\in U} \chi(Tr_1^n(au^{r(2^m-1)})) = 1.$$

Using the fact that $u \mapsto u^{2^m-1}$ is a permutation of U since $\gcd(2^m-1, 2^m+1) = 1$, we then conclude thanks to Proposition 4.

Remark 11. *The Niho part of a function $g_{a,0,c,0}^{(r,0)}$ in univariate form is $Tr_1^n(cx^{(2^m-1)\frac{1}{2}} + 1)$. Note that*

$$Tr_1^n(cx^{(2^m-1)\frac{1}{2}+1}) = Tr_1^m(Tr_m^n(c^2)x^{2^m+1}).$$

Moreover, recall that $o(j)$ denotes the size of the cyclotomic coset of 2 modulo $2^n - 1$ containing j. We have, $o((2^m-1)\frac{1}{2} + 1) = m$, $o((2^m-1)3 + 1) = n$, $o((2^m-1)\frac{1}{4} + 1) = n$ and $o((2^m-1)\frac{1}{6} + 1) = n$. So in the sequel, it suffices to use the previous identity to get the polynomial form of the presented functions.

Theorem 12. *Let $n = 2m$ with $m > 3$ odd. Let r be a positive integer such that $gcd(r, 2^m + 1) = 1$. Let $a \in \mathbb{F}_{2^m}^\star$, $b \in \mathbb{F}_4^\star$ and $c \in \mathbb{F}_{2^n}^\star \setminus \mathbb{F}_{2^m}$. Then, the function $g_{a,b,c,0}^{(r,0)}$ is semi-bent if and only if $K_m(a) = 4$.*

Proof. Using the notation of (3), we are in the case where

$$\alpha_u = Tr_m^n(c), \quad \beta_u = Tr_1^n(au^{r(2^m-1)}) + Tr_1^2(bu^{\frac{2^n-1}{3}}).$$

Using the same arguments as in the beginning of the proof of Theorem 10, we get that $g_{a,b,c,0}^{(r,0)}$ is semi-bent if and only

$$\sum_{u \in U} \chi(Tr_1^n(au^{r(2^m-1)}) + Tr_1^2(bu^{\frac{2^n-1}{3}})) = 1.$$

We finally conclude thanks to Corollary 6.

Theorem 13. *Let $n = 2m$ with m odd. Let r be a positive integer such that $gcd(r, 2^m + 1) = 1$. Let $a \in \mathbb{F}_{2^m}^\star$ and $c \in \mathbb{F}_{2^n}^\star$ such that $Tr_m^n(c) = 1$. Then, $g_{a,0,c,1}^{(r,\frac{1}{4})}$ is semi-bent if and only if, $K_m(a) = 0$.*

Proof. Using the notation of (4), note that we are here in the case where

$$\alpha_u = Tr_n^m(c) + Tr_m^n(u^{(2^m-1)\frac{1}{4}+1}) = 1 + Tr_m^n(u^{\frac{1}{2}})$$
$$\beta_u = Tr_1^n(au^{r(2^m-1)}).$$

Thanks to Lemma 9 (using equation (6)) and noting that $1 + Tr_m^n(u^{\frac{1}{2}})$ has 2 solutions in U, one can repeat the arguments of proof of Theorem 10 and then conclude by Proposition 4.

Thanks to Corollary 6 and Lemma 9 (using equation (6)) one can prove the following result.

Theorem 14. *Let $n = 2m$ with $m > 3$ odd. Let r be a positive integer such that $gcd(r, 2^m + 1) = 1$. Let $a \in \mathbb{F}_{2^m}^\star$, $b \in \mathbb{F}_4^\star$ and $c \in \mathbb{F}_{2^n}^\star$ such that $Tr_m^n(c) = 1$. Then, $g_{a,b,c,1}^{(r,\frac{1}{4})}$ is semi-bent if and only if, $K_m(a) = 4$.*

Thanks to Lemma 9 (using equation (7)) and Proposition 4, one can prove the following result.

Theorem 15. *Let $n = 2m$. Let r be a positive integer such that $gcd(r, 2^m + 1) = 1$. Let $a \in \mathbb{F}_{2^m}^\star$ and $c \in \mathbb{F}_{2^n}^\star$ such that $Tr_m^n(c) = 1$. Then, the function $g_{a,0,c,1}^{(r,3)}$ is semi-bent if and only if, $K_m(a) = 0$.*

Thanks to Lemma 9 (using equation (7)) and Corollary 6, one can prove the following result.

Theorem 16. *Let $n = 2m$ with $m > 3$ odd. Let r be a positive integer such that $gcd(r, 2^m + 1) = 1$. Let $a \in \mathbb{F}_{2^m}^\star$, $b \in \mathbb{F}_4^\star$ and $c \in \mathbb{F}_{2^n}^\star$ such that $Tr_m^n(c) = 1$. Then, the function $g_{a,b,c,1}^{(r,3)}$ is semi-bent if and only if, $K_m(a) = 4$.*

Thanks to Lemma 9 (using equation (8)) and Proposition 4, one can prove the following result.

Theorem 17. *Let $n = 2m$ with m even. Let r be a positive integer such that $gcd(r, 2^m + 1) = 1$. Let $a \in \mathbb{F}_{2^m}^\star$ and $c \in \mathbb{F}_{2^n}^\star$ such that $Tr_m^n(c) = 1$. Then, the function $g_{a,0,c,1}^{(r,\frac{1}{6})}$ is semi-bent if and only if, $K_m(a) = 0$.*

Remark 18. *Note that all the functions presented in the previous theorems are of maximal algebraic degree for a semi-bent function, namely m.*

Remark 19. *Note that the characterizations of semi-bent functions given in this paper can also be derived from Theorem 1 in [3] and using the results on bent functions in [24], [23] and [11].*

5 Conclusion

In this paper some functions in polynomial form in even dimension are considered. We derive explicit criteria involving Kloosterman sums for determining whether a function sum of some trace functions, is semi-bent or not. Kloosterman sums are used as a very convenient tool to study the semi-bentness property of those functions.

References

1. Charpin, P., Canteaut, A., Carlet, C., Fontaine, C.: On cryptographic properties of the cosets of R(1,m). IEEE Transactions on Information Theory 47, 1494–1513 (2001)
2. Carlet, C.: Boolean Functions for Cryptography and Error Correcting Codes. In: Crama, Y., Hammer, P.L. (eds.) Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. University Press, Cambridge (2010)
3. Carlet, C., Mesnager, S.: A note on Semi-bent Boolean functions. Cryptology ePrint Archive, Report no 486, `http://eprint.iacr.org/2010/486`
4. Carlitz, L.: Explicit evualation of certain exponential sums. Math. Scand. 44, 5–16 (1979)
5. Charpin, P., Helleseth, T., Zinoviev, V.: The divisibility modulo 24 of Kloosterman sums of $GF(2^m)$, m odd. Journal of Combinatorial Theory, Series A 114, 322–338 (2007)
6. Charpin, P., Pasalic, E., Tavernier, C.: On bent and semi-bent quadratic Boolean functions. IEEE Transactions on Information Theory 51(12), 4286–4298 (2005)
7. Chee, S., Lee, S., Kim, K.: Semi-bent Functions. In: Safavi-Naini, R., Pieprzyk, J.P. (eds.) ASIACRYPT 1994. LNCS, vol. 917, pp. 107–118. Springer, Heidelberg (1995)
8. Cheon, J.H., Chee, S.: Elliptic curves and resilient functions. In: Won, D. (ed.) ICISC 2000. LNCS, vol. 2015, pp. 386–397. Springer, Heidelberg (2001)
9. Cohen, G., Honkala, I., Litsyn, S., Lobstein, A.: Covering codes. North-Holland, Amsterdam (1997)
10. Dillon, J.F., Dobbertin, H.: New cyclic difference sets with Singer parameters. Finite Fields and Their Applications 10(3), 342–389 (2004)

11. Dobbertin, H., Leander, G., Canteaut, A., Carlet, C., Felke, P., Gaborit, P.: Construction of bent functions via Niho Power Functions. Journal of Combinatorial therory, Serie A 113, 779–798 (2006)
12. Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Transactions on Information Theory, 14 (1), 154–156 (1968)
13. Helleseth, T.: Some results about the cross-correlation function between two maximal linear sequences. Discr. Math. 16, 209–232 (1976)
14. Helleseth, T.: Correlation of m-sequences and related topics. In: Ding, C., Helleseth, T., Niederreiter, H. (eds.) Proc. SETA 1998. Discrete Mathematics and Theoretical Computer Science, pp. 49–66. Springer, London (1999)
15. Helleseth, T., Kumar, P.V.: Sequences with low correlation. In: Pless, V.S., Huffman, W.C., Brualdi, R.A. (eds.) Handbook of Coding Theory, Part 3: Applications, ch. 21, pp. 1765–1853. Elsevier, Amsterdam (1998)
16. Khoo, K., Gong, G., Stinson, D.R.: A new family of Gold-like sequences. IEEE Trans. Inform. Theory, 181 (2002)
17. Khoo, K., Gong, G., Stinson, D.R.: A new characterization of semibent and bent functions on finite fields. Des. Codes. Cryptogr., 38(2), 279–295 (2006)
18. Lachaud, G., Wolfmann, J.: The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Transactions on Information Theory 36(3), 686–692 (1990)
19. Leander, G.: Monomial Bent Functions. IEEE Transactions on Information Theory 2(52), 738–743 (2006)
20. MacWilliams, F.J., Sloane, N.J.: The theory of error-correcting codes. North-Holland, Amsterdam (1977)
21. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
22. Meier, W., Staffelbach, O.: Fast correlation attacks on stream ciphers. In: Günther, C.G. (ed.) EUROCRYPT 1988. LNCS, vol. 330, pp. 301–314. Springer, Heidelberg (1988)
23. Mesnager, S.: Recent Results on Bent and Hyper-bent Functions and Their Link With Some Exponential Sums. In: Proceedings of IEEE Information Theory Workshop, ITW 2010, Dublin (2010)
24. Mesnager, S.: A new class of Bent Boolean functions in polynomial forms. In: Proceedings of International Workshop on Coding and Cryptography, WCC 2009, pp. 5–18 (2009)
25. Mykkeltveit, J.: The covering radius of the (128, 8) reed-muller code is 56. IEEE Transactions on Information Theory 26, 359–362 (1980)
26. Niho, Y.: Multi-valued cross-correlation functions between two maximal linear recursive sequences. Ph.D. dissertation, Univ. Sothern Calif., Los Angeles (1972)
27. Patterson, N.J., Wiedemann, D.H.: The covering radius of the (215, 16) Reed-Muller code is at least 16276. IEEE Transactions on Information Theory 29, 354–356 (1983)
28. Patterson, N.J., Wiedemann, D.H.: Wiedemann. Correction to the covering radius of the (215,16) Reed-Muller code is at least 16276. IEEE Transactions on Information Theory 36, 443 (1990)
29. Zheng, Y., Zhang, X.-M.: Plateaued functions. In: Varadharajan, V., Mu, Y. (eds.) ICICS 1999. LNCS, vol. 1726, pp. 284–300. Springer, Heidelberg (1999)
30. Zheng, Y., Zhang, X.M.: Relationships between bent functions and complementary plateaued functions. In: Song, J.S. (ed.) ICISC 1999. LNCS, vol. 1787, pp. 60–75. Springer, Heidelberg (2000)