Hyperbent functions, Kloosterman sums and Dickson polynomials

Pascale Charpin* Guang Gong†

*INRIA, B.P. 105, 78153 Le Chesnay Cedex, France, Pascale.Charpin@inria.fr

†Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, N2L3G1, CANADA, ggong@calliope.uwaterloo.ca

Abstract

This paper is devoted to the classification of hyperbent functions, *i.e.,* bent functions which are bent up to a primitive root change. We first exhibit an infinite class of monomial functions which are not hyperbent. This result means that Kloosterman sums at point 1 on $\mathbf{F}_{2^m}$ cannot be zero, unless $m = 4$. For the functions with multiple trace terms, we express their spectrum by means of Dickson polynomials. We then introduce a new tool to describe these hyperbent functions, whose efficiency is proving by the characterization of a class of binomial bent functions.

Keywords. Boolean function, hyperbent function, bent function, Kloosterman sum, Dickson polynomial, permutation polynomial.

1 Introduction

Hyperbent functions were introduced by Youssef and Gong in [20]. A Boolean bent function f, on $\mathbf{F}_{2^n}$, is said to be hyperbent if it is such that $f(x^k)$ is bent for any k coprime with 2^n-1. Actually, the first definition of hyperbent functions was based on a property of the so-called *extended Hadamard transform* of f which was introduced by Golomb and Gong in [13] (see (2) below). In [13], the authors proposed that S-boxes should not be approximated by a bijective monomial, providing a new criterion for the S-box design.

Further, an extensive study of hyperbent functions was made by Carlet and Gaborit [3]. These authors showed that the hyperbent functions exhibited in [20] are those elements of the $\mathcal{PS}_{ap}$ class due to Dillon [9]. They also established that hyperbent functions can be seen as some codewords of a cyclic code fully characterized by its non zeroes. However, the classification of hyperbent functions is not achieved and many problems remain open.

In particular, it seems difficult to define precisely an infinite class of hyperbent functions, as indicated by the number of Open Problems which we propose in the present paper. This is the context of our paper, since we mainly introduce new tools for the description of hyperbent functions.

In this paper we consider functions on $\mathbf{F}_{2^n}$, with $n = 2m$, or on any subfield of $\mathbf{F}_{2^n}$. Section 2 is a preliminary section. We explain the main objects which are here involved, fix the notation and describe the context.

Section 3 is devoted to monomial hyperbent functions. These famous bent functions, discovered by Dillon [9](1974), are strongly related with Kloosterman sums. We give a completed version of a result of Leander [16], which specifies the spectrum of such a function f_λ by means of $K_m(\lambda)$, the Kloosterman sum on $\mathbf{F}_{2^m}$ at point λ (Theorem 5). After several general properties, we focus on the case $\lambda = 1$. We prove that $K_m(1) \neq 0$ unless $m = 4$. In other terms, we prove that f_1, defined on $\mathbf{F}_{2^n}$, is not bent unless $n = 8$ (Theorem 6). We then solve a problem which was proposed by Dillon to the second author several years ago.

In Section 4 we show that the spectrum of a large class of Boolean functions, possibly hyperbent, can be described by means of Dickson polynomials (Theorem 7 and its proof). We further apply this result to a class of binomial functions and to the monomials, providing surprising results. By Theorem 8, we characterize a class of binomial hyperbent functions. Proposition 4 appears as a generalization. Monomial functions, which are related with the zeros of some Kloosterman sums, are here described by means of Dickson permutation polynomials.

2 The Main Objects

In this paper we consider functions on $\mathbf{F}_{2^n}$, or on some subfield of $\mathbf{F}_{2^n}$. The absolute trace on $\mathbf{F}_{2^n}$ is denoted by Tr, but for any k and r, where r divides k, we denote by T_r^k the trace function from $\mathbf{F}_{2^k}$ to $\mathbf{F}_{2^r}$:

$$T_r^k(\beta) = \beta + \beta^{2^r} + \beta^{2^{2r}} + \cdots + \beta^{2^{k-r}}.$$

Any Boolean function f over $\mathbf{F}_{2^n}$ is a function from $\mathbf{F}_{2^n}$ to $\mathbf{F}_2$. The *weight* of f, denoted $wt(f)$, is the Hamming weight of the image vector of f, that is the number of x such that $f(x) = 1$. For any Boolean function f over $\mathbf{F}_{2^n}$ we state its Hadamard transform :

$$a \in \mathbf{F}_{2^n} \ \mapsto \ \mathcal{F}(a) = \sum_{x \in \mathbf{F}_{2^n}} (-1)^{f(x)+Tr(ax)} \tag{1}$$

and its *extended Hadamard transform*

$$\mathcal{F}(a,k) = \sum_{x \in \mathbf{F}_{2^n}} (-1)^{f(x)+Tr(ax^k)}, \ a \in \mathbf{F}_{2^n}, \ \gcd(k, 2^n - 1) = 1. \tag{2}$$

Recall that, for even n, f is *bent* if and only if $\mathcal{F}(a) = \pm 2^{\frac{n}{2}}$ for all a. Also, f is said to be *balanced* if and only if $\mathcal{F}(0) = 0$.

2.1 Hyperbent Functions

Youssef and Gong proposed in [20] to strength the bent concept by using the extended Hadamard transform and stated the following :

Definition 1 *Any Boolean function on* $\mathbf{F}_{2^n}$, $n = 2m$, *is said* hyperbent *if its extended Hadamard transform takes the values* $\pm 2^m$ *only.*

They later introduce a class of possible hyperbent functions. In this paper, we restrict ourselves to the class of possible hyperbent functions defined as follows.

Definition 2 *Let* R *be a set of representatives of the cyclotomic cosets modulo* 2^m+1 *for which each coset has the full size* $2m$. *Let us define the Boolean functions on* $\mathbf{F}_{2^n}$ *of the form:*

$$f(x) = \sum_{r \in E} Tr(\beta_r x^{(2^m-1)r}) \text{ where } E \subseteq R,\ \beta_r \in \mathbf{F}_{2^n}. \tag{3}$$

Carlet and Gaborit, in [3], showed that any hyperbent function of the form (3) belongs to the class $\mathcal{PS}_{ap}$, a subclass of the partial spread family $\mathcal{PS}^-$ introduced by Dillon [9, pp.95-100]. We first recall the definition of $\mathcal{PS}^-$.

Theorem 1 [9] *Let* f *be a Boolean function over* $\mathbf{F}_{2^n}$, $n = 2m$, *and set*

$$E_f = \{\ x \in \mathbf{F}_{2^n} \mid f(x) = 1\ \}.$$

Let us denote by $\{S_i,\ i = 1, 2 \ldots N\}$ *a set of subspaces of* $\mathbf{F}_{2^n}$ *of dimension* m *satisfying:*

$$i \neq j \quad \Rightarrow \quad S_i \cap S_j = \{0\}\ .$$

The function f *is bent, and said to be in* $\mathcal{PS}^-$, *when it satisfies*

$$E_f = \bigcup_{i=1}^{N} S_i^* \quad \text{with } N = 2^{m-1},$$

where $S_i^* = S_i \setminus \{0\}$.

According to the previous theorem, we give now a sligthly different version of [20, Theorem 1]. Although the result is known, we present a brief proof of the next theorem, giving some elements which we will be useful.

Theorem 2 *Let us denote by $\mathcal{G}$ the cyclic subgroup of $\mathbf{F}_{2^n}^*$ of order 2^m+1. Let γ be a generator of $\mathcal{G}$. Let f be any function of type (3). Then f is hyperbent if and only if*

$$\#\ \{\ i \mid f(\gamma^i)=1,\ 0 \le i \le 2^m\ \} = 2^{m-1},$$

where $\#E$ denotes the cardinality of any set E.

Proof. Any $x \in \mathbf{F}_{2^n}^*$ can be written $x=yz$ with $y \in \mathbf{F}_{2^m}$ and $z \in \mathcal{G}$; moreover $f(0)=0$. Then $f(x)$ depends on z only :

$$f(x)=f(yz)=\sum_{r\in E} Tr(\beta_r z^{(2^m-1)r}) = f(z). \tag{4}$$

Now let us define the subspaces

$$S_i = \gamma^i\ \mathbf{F}_{2^m},\ 0 \le i \le 2^m. \tag{5}$$

Then f is constant on each S_i^*, equal to $f(\gamma^i)$. We now apply Theorem 1, observing that

$$E_f = \bigcup_{i\in I} S_i^*,\ I=\{\ i \mid f(\gamma^i)=1\ \}.$$

Setting $N=\#I$, we deduce that f is bent if and only if $N=2^{m-1}$. In this case, f is hyperbent because for any k coprime with 2^m+1 the map $\gamma^i \mapsto \gamma^{ik}$ is a permutation on $\mathcal{G}$. $\diamond$

The main problem, which is the precise characterization of function of type (3) which are bent (and then hyperbent) remains open.

Open Problem 1 *Characterize a class of functions f of type (3) which are bent, by giving explicitely the coefficients β_r.*

2.2 Monomial hyperbent functions

For the monomials functions of type (3), it is well-known that they can be defined by means of the Kloosterman sums. In this subsection, we consider the monomial Boolean functions from $\mathbf{F}_{2^n}$ to $\mathbf{F}_2$:

$$f_\lambda(x) = Tr(\lambda x^{2^m-1})\ ,\quad \lambda \in \mathbf{F}_{2^m}. \tag{6}$$

Let us define the Kloosterman sums over $\mathbf{F}_{2^m}$:

$$K_m(\lambda) = \sum_{y \in \mathbf{F}_{2^m}} (-1)^{T_1^m(\frac{1}{x} + \lambda x)}, \tag{7}$$

where $T_1^m(a)$ is the absolute trace on $\mathbf{F}_{2^m}$. Then we have the following result which is due to Dillon [9, 10]:

Theorem 3 *The function f_λ, defined by (6) is bent if and only if the Kloosterman sum K_m satisfies $K_m(\lambda) = 0$.*

The set of the values of Kloosterman sums was described by Lachaud and Wolfmann in [15] for any m (even or odd).

Lemma 1 *The set $\{K_m(\lambda),\ \lambda \in \mathbf{F}_{2^m}\}$, is the set of all the integers $s \equiv 0$ (mod 4) in the range $[-2^{(m+2)/2} + 1,\ 2^{(m+2)/2} + 1]$.*

As a consequence, these authors have proved that there are some λ such that $K_m(\lambda) = 0$. But the number of such λ remains unknown, leading to:

Open Problem 2 *Describe, for some sequence of m, the set of those λ such that f_λ is bent or, equivalently, $K_m(\lambda) = 0$.*

The previous problem appeared as a very difficult problem. Through numerical results it is possible to introduce some conjecture concerning a partial problem. In Section 3.2 we present our main result in this context : we completely solve the case $\lambda = 1$. Also, Open Problem 2 can be restricted as follows.

Lemma 2 *If $T_1^m(\lambda) = 1$ then $K_m(\lambda) \neq 0$,* i.e., *the function f_λ, defined by (6) is not bent.*

Proof. It comes directly from a result due to Helleseth and Zinoviev [14]: For any $m \geq 3$

$$K_m(\lambda) \ \equiv \ \begin{cases} 4 \mod 8, & \text{if} \quad T_1^m(\lambda) = 1, \\ 0 \mod 8, & \text{if} \quad T_1^m(\lambda) = 0. \end{cases} \tag{8}$$

This implies that $K_m(\lambda) \neq 0$ when $T_1^m(\lambda) = 1$. ◇

Remark 1 We can take $\lambda \in \mathbf{F}_{2^m}$ without loss of generality, in the definition of any monomial function f_λ when we are looking at its spectrum. This is because $2^m - 1$ is coprime with $2^m + 1$. Any $\lambda \in \mathbf{F}_{2^n}$ can be written $\lambda = uv$ with $u \in \mathbf{F}_{2^m}$ and v in the subgroup of $\mathbf{F}_{2^n}$ of order $2^m + 1$. Then f_λ has the same spectrum as f_u.

2.3 Dickson Polynomials

The main reference on Dickson polynomials is the book of Dickson [8]. An excellent presentation of the work of Dickson can be found in [18]. In our approach, we follows several recent papers where the reader can find a basic overview [11, 12]. A Dickson polynomial is defined by

$$D_r(x) = \sum_{i=0}^{r/2} \frac{r}{r-i} \left(\begin{array}{c} r-i \\ i \end{array} \right) x^{r-2i}, \ r = 2, 3, \cdots . \tag{9}$$

The Dickson polynomials have extensively investigated in recent about one hundred years under different contexts. Here we introduce some useful properties, on the Dickson polynomials of $\mathbf{F}_2[x]$. Note that they are known in many different contexts.

Dickson polynomial $D_r \in \mathbf{F}_2[x]$ are recursively defined by

$$\begin{array}{l} D_0(x) = 0 \text{ and } D_1(x) = x; \\ D_{i+2}(x) = xD_{i+1}(x) + D_i(x). \end{array} \tag{10}$$

Using this definition it is easy to prove the next properties which we use in the sequel.

Proposition 1 *The polynomials defined by (10) satisfy (for $i, j > 0$) :*

- $\deg(D_i) = i$,
- $D_{2i}(x) = (D_i(x))^2$,
- $D_{ij}(x) = D_i(D_j(x))$,
- $D_i(x + x^{-1}) = x^i + x^{-i}$.

We also have the following fundamental result.

Theorem 4 *The Dickson polynomial $D_i \in \mathbf{F}_2[x]$ is a permutation on $\mathbf{F}_{2^m}$ if and only if* $\gcd(i, 2^{2m} - 1) = 1$.

In Section 4, we will show that the bentness of a function with multiple trace terms is related to the Dickson polynomials.

3 Hyperbent Functions and Zeroes of Kloosterman sums

In this section, we show that the monomial functions $x \mapsto Tr(x^{r(2^m-1)})$ over $\mathbf{F}_{2^n}$, $n = 2m$, are not bent unless $m = 4$. This necessitates several preliminaries. In the next subsection, we are going to show that it is sufficient to treat the case $r = 1$.

3.1 Monomial Functions

Recently, Leander [16] proposed another proof of Theorem 3, giving more informations on the spectrum of functions f_λ defined by (6). The next theorem (and its proof) is principally due to Leander. There is a small mistake in [16, Th. 3], since the formula (13) (below) is stated for all a while it is not suitable for $a = 0$. In our proof, we include the case $a = 0$; we also consider monomial functions of general form, $f_{\lambda,r}$ instead of f_λ. This completed version will be useful later.

Theorem 5 *For every integer r coprime to 2^m+1, define the Boolean functions on $\mathbf{F}_{2^n}$, $n = 2m$:*

$$f_{\lambda,r}(x) = Tr(\lambda x^{r(2^m-1)}) \ , \quad \lambda \in \mathbf{F}_{2^m}^*. \tag{11}$$

Recall that K_m is the Kloosterman sum on $\mathbf{F}_{2^m}$ (see (7)). We denote by $\mathcal{F}_\lambda(a)$ the Hadamard transform of $f_{\lambda,r}$ (see (1)). Then, for any $\lambda \in \mathbf{F}_{2^m}^*$,

$$\mathcal{F}_\lambda(0) = 2^m(1 - K_m(\lambda)) + K_m(\lambda). \tag{12}$$

Moreover we have for any $a \in \mathbf{F}_{2^n}^*$

$$\mathcal{F}_\lambda(a) = 2^m(-1)^{Tr(\lambda a^{r(2^m-1)})} + K_m(\lambda). \tag{13}$$

Consequently, $f_{\lambda,r}$ is bent if and only if $K(\lambda) = 0$ or, equivalently, $\mathcal{F}_\lambda(0) = 2^m$. Also, $f_{\lambda,r}$ is bent if and only if $f_{\lambda,1}$ is bent.

Proof. We denote by $\mathcal{G}$ the cyclic group of order 2^m+1. Any $x \in \mathbf{F}_{2^n}^*$ can be written $x = yz$, $y \in \mathbf{F}_{2^m}^*$ and $z \in \mathcal{G}$. Note that $y^{2^m-1} = 1$ and $z^{2^m-1} = z^{-2}$.

For readbility, we use this notation : $e(h(x)) = (-1)^{Tr(h(x))}$. So we have :

$$\begin{aligned}\mathcal{F}_\lambda(a) &= \sum_{x\in\mathbf{F}_{2^n}} e(\lambda x^{r(2^m-1)} + ax)\\ &= 1 + \sum_{z\in\mathcal{G}} \sum_{y\in\mathbf{F}_{2^m}^*} e(\lambda z^{r(2^m-1)} + ayz)\\ &= 1 + \sum_{z\in\mathcal{G}} e(\lambda z^{-2r}) \sum_{y\in\mathbf{F}_{2^m}^*} e(ayz).\end{aligned}$$

When $a = 0$, using $\gcd(r, 2^m + 1) = 1$, we get

$$\begin{aligned}\mathcal{F}_\lambda(0) &= 1 + \sum_{z\in\mathcal{G}} \sum_{y\in\mathbf{F}_{2^m}^*} e(\lambda z^{-2r})\\ &= 1 + (2^m - 1)\sum_{z\in\mathcal{G}} e(\lambda z).\end{aligned}$$

Now assume that $a \neq 0$. So, we get for any $a \in \mathbf{F}_{2^n}^*$:

$$\begin{aligned}\mathcal{F}_\lambda(a) &= 1 + \sum_{z\in\mathcal{G}} e(\lambda z^{-2r}) \left(\sum_{y\in\mathbf{F}_{2^m}} e(ayz) - 1 \right)\\ &= 1 + 2^m \sum_{z\in\mathcal{G},\ z^2=a^{2^m-1}} e(\lambda z^{-2r}) - \sum_{z\in\mathcal{G}} e(\lambda z^{-2r}),\end{aligned}$$

since $Tr(ayz) = T_1^m(y(az + a^{2^m} z^{-1}))$ so that $\sum_{y\in\mathbf{F}_{2^m}} e(ayz) \neq 0$ (and then equal to 2^m) if and only if

$$az = \frac{a^{2^m}}{z} \quad \Leftrightarrow \quad z^2 = a^{2^m-1}.$$

Then

$$\begin{aligned}\mathcal{F}_\lambda(a) &= 1 + 2^m e\left(\frac{\lambda}{a^{r(2^m-1)}}\right) - \sum_{z\in\mathcal{G}} e(\lambda z^{-2r})\\ &= 1 + 2^m e(\lambda a^{r(2^m-1)}) - \sum_{z\in\mathcal{G}} e(\lambda z),\end{aligned}$$

since $(\lambda/a^{r(2^m-1)})^{2^m} = \lambda/a^{r(1-2^m)}$. Now, it is well-known that

$$\sum_{z\in\mathcal{G}} e(\lambda z) = 1 - K_m(\lambda)$$

(different proofs can be found in [5, 9, 15, 16]). Finally

$$\mathcal{F}_\lambda(0) = 1 + (2^m - 1)(1 - K_m(\lambda)) = 2^m(1 - K_m(\lambda)) + K_m(\lambda).$$

and, for $a \in \mathbf{F}_{2^n}^*$,

$$\mathcal{F}_\lambda(a) = 1 + 2^m e(\lambda a^{r(2^m-1)}) - 1 + K_m(\lambda).$$

According to (13), $f_{\lambda,r}$ is bent if and only if $K_m(\lambda) = 0$. Indeed, it is impossible to have

$$2^m e(\lambda a^{r(2^m-1)}) + K_m(\lambda) = \pm 2^m$$

for $K_m(\lambda) \neq 0$, because $\mid K_m(\lambda) \mid < 2^m$ (see Lemma 1). And this holds for any $a \in \mathbf{F}_{2^n}^*$; further $\mathcal{F}_\lambda(0) = 2^m$.

Conversely, if $\mathcal{F}_\lambda(0) = 2^m$ then we get from (12) :

$$K_m(\lambda)(2^m - 1) = 2^m - 2^m = 0,$$

which is impossible unless $K_m(\lambda) = 0$. The proof is completed since $\mathcal{F}_\lambda(0)$ does not depend on r. ◇

Remark 2 Formula (13) is of interest for the non bent functions also. If $K_m(\lambda) \neq 0$ then $f_{\lambda,r}$ is not bent and its spectrum includes three values only which are not zero. As pointed out, the value $\mathcal{F}_\lambda(0)$ only depends on λ.

We have seen that if $f_{\lambda,r}$ is bent for some r then it is bent for any r. In the remaining of this section, we assume that $r = 1$, *i.e.,* we come back to functions f_λ defined by (11). We are going to specify the bentness of f_λ by means of properties of elements of $\mathbf{F}_{2^m}$. Recall that γ is a generator of $\mathcal{G}$, the cyclic group of order $2^m + 1$ in $\mathbf{F}_{2^n}$, $n = 2m$. Note that $\gamma^{2^m} = \gamma^{-1}$.

Lemma 3 *Let $S_i = \gamma^i \mathbf{F}_{2^m}$, $0 \leq i \leq 2^m$. The function f_λ is defined by (11). Then f_λ is constant on each S_i^*, equal to $Tr(\lambda\gamma^{-2i})$. Moreover f_λ is hyperbent if and only if*

$$\#\{\ i \mid T_1^m(\lambda(\gamma^i + \gamma^{-i})) = 1\ \} = 2^{m-1}.$$

Proof. The proof is directly deduced from Theorem 2 and its proof. One only has to observe that

$$f(\gamma^i) = Tr(\lambda\gamma^{i(2^m-1)}) = T_1^m\left(\lambda(\gamma^{2i} + \gamma^{-2i})\right).$$

◇

Remark 3 Consider again the functions $f_{\lambda,r}$, defined by (11). For any r, even not coprime with 2^m+1, it is clear that the previous result holds : $f_{\lambda,r}$ is hyperbent if and only if $N = 2^{m-1}$ where

$$N = \#\{\ i \mid T_1^m(\lambda(\gamma^{ir} + \gamma^{-ir})) = 1\ \}.$$

But if r divides 2^m+1 then $2r$ divides N with r odd. Hence $N \neq 2^{m-1}$. *We have proved that $f_{\lambda,r}$ cannot be bent when r is not coprime with 2^r+1.*

So, in order to find those λ such that f_λ is bent, we are interested by the set of the $\gamma^i + \gamma^{-i}$. The next proposition is currently known.

Proposition 2 *Let $n = 2m$ and $\mathcal{G}$ be the cyclic group of order 2^m+1 with generator γ. Then*

$$\{\ \gamma^i + \gamma^{-i} \mid 1 \leq i \leq 2^m\ \} = \{\ u \in \mathbf{F}_{2^m} \mid T_1^m(u^{-1}) = 1\ \}.$$

Proof. This was first proved by Delsarte and Goethals [7] who established that we have here the roots of

$$\begin{aligned} Q(x) &= \prod_{i=1}^{2^{m-1}} (x - (\gamma^i + \gamma^{-i})) = x^{2^{m-1}} + \sum_{j=0}^{m-1} x^{2^{m-1}-2^j} \\ &= x^{2^{m-1}} \left(1 + T_1^m(x^{-1})\right). \end{aligned}$$

Another proof can be found in [15]. ◇

Using Lemma 3, we directly deduce from the previous proposition:

Corollary 1 *The function f_λ on $\mathbf{F}_{2^n}$, $n = 2m$, is defined by (11). Then f_λ is hyperbent if and only if*

$$\#\{\ u \in \mathbf{F}_{2^m} \mid T_1^m(\lambda u) = T_1^m(u^{-1}) = 1\ \} = 2^{m-2} \tag{14}$$

Now, using (13) and (12), we have another characterization of the bentness of f_λ by its weight.

Lemma 4 *Let f_λ, defined by (6). Then the weight of f_λ is*

$$wt(f_\lambda) = (2^m - 1)\left(2^{m-1} + \frac{K_m(\lambda)}{2}\right).$$

Consequently, f_λ is hyperbent if and only if $K_m(\lambda) = 0$. Moreover,

$$\#\{\ u \in \mathbf{F}_{2^m} \mid T_1^m(\lambda u) = T_1^m(u^{-1}) = 1\ \} = 2^{m-2} + \frac{K_m(\lambda)}{4}.$$

Proof. From (12), we have

$$2^m(1 - K_m(\lambda)) + K_m(\lambda) = 2^n - 2wt(f_\lambda)$$

which gives

$$\begin{aligned} wt(f_\lambda) &= 2^{2m-1} - 2^{m-1}(1 - K_m(\lambda)) - \frac{K_m(\lambda)}{2} \\ &= 2^{m-1}(2^m - 1) + \frac{K_m(\lambda)}{2}(2^m - 1). \end{aligned}$$

We know that f_λ is constant on any S_i^* and it is hyperbent if and only if it is equal to 1 on exactly 2^{m-1} sets S_i^*. According to Lemma 3 the expression of $wt(f_\lambda)$ means that f_λ is equal to 1 on $2^{m-1} + \frac{K_m(\lambda)}{2}$ sets S_i^*. This is exactly the number

$$\#\{\ i \mid T_1^m(\lambda(\gamma^i + \gamma^{-i})) = 1\ \} = 2\#\{\ u \in \mathbf{F}_{2^m} \mid T_1^m(\lambda u) = T_1^m(u^{-1}) = 1\ \}.$$

$\diamond$

3.2 Main Result on Monomials

In this section, we are going to prove Theorem 6 (see below). Notation is as in the previous section assuming that $\lambda = 1$. We need several lemmas ; the first one directly treats the case where m is odd. In this case, since $T_1^m(1) = 1$ we can apply Lemma 2.

Lemma 5 *If m is odd then $K_m(1) \neq 0$.*

According to Corollary 1, we are going to compute the cardinality of

$$R_m = \{\ u \in \mathbf{F}_{2^m} \mid T_1^m(u) = T_1^m(u^{-1}) = 1\ \}. \tag{15}$$

From Lemma 4, we know that

$$\#R_m = 2^{m-2} + \frac{K_m(1)}{4}. \tag{16}$$

From now on we examine the case where $m = 2k$, for some integer k. We will define recursively R_m, by using a property of self reciprocal polynomials. We first present this property.

Lemma 6 *Let $m = 2k$. We denote by P_u the minimal polynomial of u over $\mathbf{F}_2$, $P_u \in \mathbf{F}_2[x]$. Assume that there is $u \in \mathbf{F}_{2^m}$ satisfying*

$$u \notin \mathbf{F}_{2^k} \quad \textit{and} \quad P_u = P_{u^{-1}}.$$

Then $\deg(P_u) = 2r$ for some $r > 0$ dividing k. Moreover, $u^{2^r} = u^{-1}$ and u is a root of the polynomial $x^{2^k+1} + 1$.

Proof. Note that the degree of P_u, denoted $\deg(P_u)$, must be even since otherwise $u \in \mathbf{F}_{2^k}$. Set $\deg(P_u) = 2r$. By definition, r is the smallest integer dividing k such that $u \in \mathbf{F}_{2^{2r}}$.

Since $P_u = P_{u^{-1}}$, there is i such that $u^{-1} = u^{2^i}$, where $1 \leq i \leq 2r - 1$. Then we have:

$$u^{2^{2i}} = \frac{1}{u^{2^i}} = u.$$

This is possible only if r divides i, because otherwise

$$u \in \mathbf{F}_{2^{2e}} \quad \text{with} \quad e = \gcd(r, i) \quad \text{and} \quad e < r.$$

If r divides i then $i < 2r$ implies $i = r$ so that $u^{2^r+1} = 1$.

Now it remains to prove that $u^{2^k+1} = 1$. We set

$$k = rs \quad \text{and} \quad t = \gcd(2^r + 1, 2^k - 1).$$

In this case, it is well-known that

$$t = \begin{cases} 1 & \text{if } s \text{ is odd} \\ 2^r + 1 & \text{otherwise} \end{cases}$$

(see a proof in [19, Lemma 11.1]). So, if s is even then $2^r + 1$ divides $2^k - 1$. But this is impossible because we suppose that $u \notin \mathbf{F}_{2^k}$. Finally, we have proved that s is odd for such u. Consequently, we have

$$2^k + 1 = (2^r + 1) \sum_{i=1}^{s} (-1)^{s-i} 2^{(s-i)r},$$

which implies that 2^r+1 divides 2^k+1 and, further, $u^{2^k+1} = 1$ since $u^{2^r+1} = 1$. ◇

Lemma 7 *For any $u \in \mathbf{F}_{2^m}$, $m = 2k$, let $P_u \in \mathbf{F}_2[x]$ be the minimal polynomial of u over $\mathbf{F}_2$. Set*

$$\begin{aligned} L_{0,m} &= \{\ u \in R_m \mid P_u = P_{u^{-1}}\ \} \\ L_{1,m} &= \{\ u \in R_m \mid P_u \neq P_{u^{-1}}\ \}. \end{aligned}$$

Then $\#R_m = \#L_{0,m} + \#L_{1,m}$, where

$$\#L_{0,m} = 2\ \#R_k,$$

where R_m is defined by (15),(16).

Proof. First note that $R_m \cap \mathbf{F}_{2^k} = \emptyset$. This is because for $u \in \mathbf{F}_{2^k}$

$$T_1^m(u) = T_1^k(u + u^{2^k}) = 0.$$

The set R_m is composed of two kinds of elements:

- The roots of pairs of polynomials $(P_u, P_{u^{-1}})$, with $P_u \neq P_{u^{-1}}$. The number of roots of such a pair equals 4δ where 2δ is the degree of P_u.
- The roots of polynomials P_u which are self-reciprocal, *i.e.,* $P_u = P_{u^{-1}}$.

Hence, we have by definition : $\#R_m = \#L_{0,m} + \#L_{1,m}$. Note that all P_u with $u \in R_m$ have degrees which divide m but not k : these degrees are even. Notably, 4 divides $\#L_{1,m}$ since $L_{1,m}$ is composed of roots of pairs of distinct polynomials.

Let $u \in R_m$ such that $P_u = P_{u^{-1}}$. Since $u \notin \mathbf{F}_{2^k}$, we deduce from Lemma 6 that the elements of $L_{0,m}$ are roots of the polynomial $x^{2^k+1} + 1$. Applying Proposition 2 to the cyclic subgroup of order $2^k + 1$ in $\mathbf{F}_{2^m}^*$, say $\mathcal{G}_k$, we get

$$\begin{aligned} L_{0,m} &= \{\ u \in \mathbf{F}_{2^m} \mid u^{2^k+1} = 1 \text{ and } T_1^m(u) = 1\ \} \\ &= \{\ u \in \mathcal{G}_k \mid T_1^k(u + u^{-1}) = 1\ \}. \end{aligned}$$

Since

$$\{\ u + u^{-1} \mid u \in \mathcal{G}_k \setminus \{1\}\ \} = \{\ v \in \mathbf{F}_{2^k}^* \mid T_1^k(v^{-1}) = 1\ \},$$

we deduce that

$$\#L_{0,m} = 2\ \#\{\ v \in \mathbf{F}_{2^k} \mid\ T_1^k(v) = T_1^k(v^{-1}) = 1\ \}.$$

We obtain $\#L_{0,m} = 2\ \#R_k$ from (15), completing the proof. ◇

Now we need more information on the divisibility of $\#L_{1,m}$.

Lemma 8 *Let $m = 2^r k$ where k is odd ($r, k \geq 1$). Then*

$$\#L_{1,m} \equiv 0 \pmod{2^{r+1}}. \tag{17}$$

Moreover $L_{1,m} \neq 0$ for any $m \geq 6$ and $L_{1,2} = L_{1,4} = 0$.

Proof. We have seen in the previous proof that the set $L_{1,m} \cap \mathbf{F}_{2^{2^{r-1}k}}$ is empty. Then any u in $L_{1,m}$ has a minimal polynomial with degree $2^r e$ where e divides k. The proof of (17) is completed since for each u belonging to $L_{1,m}$, the roots of both polynomials P_u and $P_{u^{-1}}$ belong to $L_{1,m}$ too.

Now suppose that $L_{1,m} = 0$. Then, from Lemma 7, $\#R_m = 2\#R_s$ with $s = 2^{r-1}k$. So we have

$$\#R_m = 2^{m-2} + \frac{K_m(1)}{4} = 2\#R_s.$$

Hence

$$K_m(1) = 4\#R_m - 2^m = 8\#R_s - 2^m, \quad \text{where } \#R_s \leq 2^s.$$

But the absolute value of $K_m(1)$ is less than or equal to $2^{(m+2)/2} = 2^{s+1}$ (see Lemma 1). So we must have $2^m - 2^{s+3} \leq 2^{s+1}$. This is impossible as soon as $s + 3 < m$, that is $s + 3 < 2s$ which leads to $3 < s$, *i.e.* $m > 6$. When $m = 6$ then $R_3 = \{1\}$ and we get $K_6(1) = 8 - 2^6$ which is impossible too.

When $m \in \{2, 4\}$, it is easy to check that $L_{1,m} = 0$. ◇

Theorem 6 *Let $n = 2m$ with $m \leq 2$. The Kloosterman sum*

$$K_m(1) = \sum_{y \in \mathbf{F}_{2^m}} (-1)^{T_1^m(\frac{1}{x} + x)},$$

satisfies $K_m(1) \neq 0$ unless $m = 4$. In other terms, the Boolean function $x \mapsto T_1^m(x^{-1} + x)$ is not balanced unless $m = 4$.

Consequently, the Boolean function $x \mapsto Tr(x^{2^m - 1})$, on $\mathbf{F}_{2^n}$, is not bent unless $n = 8$.

Proof. We have seen that $K_m(1) = 0$ if and only if $\#R_m = 2^{m-2}$. And this is impossible for odd m. So we assume that $m = 2^r k$, $r \geq 1$ and k odd. We have from Lemma 7:

$$\begin{aligned} \#R_m &= \#L_{0,m} + \#L_{1,m} = 2\#R_{2^{r-1}k} + \#L_{1,m} \\ &= \#L_{1,m} + 2\#L_{1,2^{r-1}k} + 2\#L_{0,2^{r-1}k}. \end{aligned}$$

By induction, one proves easily that

$$\#R_m = \#L_{1,m} + 2\#L_{1,2^{r-1}k} + \cdots + 2^{r-1}\#L_{1,2k} + 2^r\#R_k. \qquad (18)$$

It is easy to compute the first R_i. Note that $R_1 = R_3 = \{1\}$. Also $\#R_2 = 2$ and $\#R_4 = 4$. More generally we have for odd $k > 1$ (see (16)):

$$\#R_k = 2^{k-2} + \frac{K_k(1)}{4} \equiv 2\epsilon + 1 \pmod 8,$$

where $\epsilon = 0$ if $k > 3$ and $\epsilon = 1$ if $k = 3$. This is because $T_1^k(1) = 1$ implying $K_k(1) \equiv 4 \pmod 8$ (see (8)). If $r = 1$ and $k > 1$, we get

$$\#R_{2k} = 2\#R_k + \#L_{1,m} = 2^{k-1} + \frac{K_k(1)}{2} + \#L_{1,m},$$

where 4 divides $2^{k-1} + \#L_{1,m}$ but does not divide $K_k(1)/2$. Then, it is impossible to have $\#R_{2k} = 2^{2k-2}$.

From now on assume that $r > 1$ so that $m = 4,\ 8,\ 12 \ldots$. From Lemma 8, the equation (18) becomes:

$$\#R_m = 2^{r+1}M + 2^r\left(2^{k-2} + \frac{K_k(1)}{4}\right),$$

for $k > 1$ and $\#R_m = 2^{r+1}M + 2^r$ for $k = 1$, where M is some positive integer. We suppose first that $m \geq 8$ so that $M \neq 0$ (see Lemma 8) and $r < m - 2$.

In both cases ($k > 1$ or $k = 1$) 1it is easy to check that $\#R_m \neq 2^{m-2}$ since $\#R_m$ is divisible by 2^r and not by 2^{r+1}. For $k > 1$ it is sufficient to see that $K_k(1)/4$ is odd. If $m = 4$ then $\#R_4 = 4 = 2^2$, completing the proof. $\diamond$

There is an immediate consequence of the previous theorem. We consider again monomial functions of the form (11):

$$x \in \mathbf{F}_{2^n} \ \mapsto \ f_{\lambda,r}(x) = Tr(\lambda x^{r(2^m-1)}) \ , \quad \lambda \in \mathbf{F}_{2^m}^*.$$

We have proved that $f_{1,1}$ is generally non bent. From Theorem 5, this result holds for any r.

Corollary 2 *For all r with $\gcd(r, 2^m + 1) = 1$, the Boolean function $f_{1,r}(x)$ on $\mathbf{F}_{2^n}$ is not hyperbent unless $n = 8$.*

The results of this section lead naturally to a more general problem.

Open Problem 3 *Study the bentness of functions of the form (3), when $\beta_r \in \mathbf{F}_2$ for all r in E.*

4 Hyperbent Functions in Terms of Dickson Polynomials

When f is a monomial trace term, the bentness of f is established through some Kloosterman sum. However, if f is a sum of multiple trace terms, defined by (3), there is no technique which has found to dealt with this case. In this section, using the results developed in Section 3, we show that the bentness of those functions with some restriction is related to the Dickson polynomials.

4.1 Main Characterization

Dickson polynomials are here polynomials in $\mathbf{F}_2[x]$ (see Section 2.3). They are denoted by D_r where r in R, a set of representatives of the cyclotomic cosets modulo 2^m+1 of size $2m$.

Theorem 7 *Let us consider any function of type (3) on $\mathbf{F}_{2^n}$, $n=2m$, with coefficients in $\mathbf{F}_{2^m}$:*

$$f(x)=\sum_{r\in E} Tr(\beta_r x^{(2^m-1)r}) \text{ where } E\subseteq R,\ \beta_r\in\mathbf{F}_{2^m}, \tag{19}$$

and the related Boolean function on $\mathbf{F}_{2^m}$:

$$g(x)=\sum_{r\in E} T_1^m(\beta_r D_r(x)) \tag{20}$$

Then f is hyperbent if and only if

$$\#\{\ u\in\mathbf{F}_{2^m}\mid T_1^m(u^{-1})=1 \text{ and } g(u)=1\ \}=2^{m-2}.$$

Consequently, f is hyperbent if and only if

$$\sum_{x\in\mathbf{F}_{2^m}} (-1)^{T_1^m(x^{-1})+g(x)}=2^m-2wt(g). \tag{21}$$

Proof. Recall that $wt(g)$ is the weight of g and γ is a generator of the subgroup $\mathcal{G}$ of $\mathbf{F}_{2^n}$ of order 2^m+1. We have

$$f(\gamma^i)=\sum_{r\in E} Tr(\beta_r\gamma^{(2^m-1)ir})=\sum_{r\in E} T_1^m\left(\beta_r(\gamma^{2ri}+\gamma^{-2ri})\right).$$

Then, applying Theorem 2, f is hyperbent if and only if $N = 2^{m-1}$ where

$$N = \#\{\ j \mid \sum_{r \in E} T_1^m(\beta_r(\gamma^{rj} + \gamma^{-rj})) = 1\ \}. \tag{22}$$

For $u = \gamma + \gamma^{-1}$, we now use basic properties of Dickson polynomials (see Proposition 1).

$$\gamma^{rj} + \gamma^{-rj} = D_{rj}(u) = D_r(\gamma^j + \gamma^{-j}),\ 1 \leq j \leq 2^m.$$

Using Proposition 2, we rewritte (22) as follows :

$$\begin{aligned} N &= \#\{\ j \mid \sum_{r \in E} T_1^m(\beta_r D_r(\gamma^j + \gamma^{-j})) = 1\ \} \\ &= 2\ \#\{\ u \in \mathbf{F}_{2^m} \mid T_1^m(u^{-1}) = 1 \text{ and } g(u) = 1\ \}, \end{aligned}$$

where $g(x)$ is defined by (20).

Denote by h the function $x \mapsto T_1^m(x^{-1})$. To prove (21), we have to compute the Hadamard transform of the function $h+g$ in point 0, say $\mathcal{F}(0)$. We know that $\mathcal{F}(0) = 2^m - 2wt(h+g)$. By definition of the Hamming weight, we have:

$$wt(h+g) = wt(h) + wt(g) - 2wt(hg) = 2^{m-1} - 2wt(hg) + wt(g).$$

Note that $wt(h) = 2^{m-1}$ since the inverse function is a permutation. By definition, $hg(x) = 1$ if and only if $h(x) = g(x) = 1$ providing $wt(hg) = N/2$. Then f is hyperbent if and only if $wt(hg) = 2^{m-2}$ or, equivalently, $\mathcal{F}(0) = 2^m - 2wt(g)$. $\diamond$

4.2 A Class of Binomial Functions

The results in Theorem 7 provide a way to transfer the evaluation of the weight of the function f in the cyclic group $\mathcal{G}$ to the evaluation of the weight of some Boolean function on $\mathbf{F}_{2^m}$. The later problem is easier than the former one, since we could use the divisibility of some cyclic codes, especially, for special classes of functions of type (19). To illustrate our purpose we are going to treat some binomial functions of type (19). Let, for any $\lambda \in \mathbf{F}_{2^m}^*$,

$$f(x) = Tr\left(\lambda(x^{(2^r-1)(2^m-1)} + x^{(2^r+1)(2^m-1)})\right),\ 0 < r < m. \tag{23}$$

Then, according to Theorem 7, we have

$$g(x) = T_1^m(\lambda(D_{2^r-1}(x) + D_{2^r+1}(x))).$$

We apply the recursive definition of Dickson polynomials (see Section 2.3) :

$$D_{2^r+1}(x) = xD_{2^r}(x) + D_{2^r-1}(x) = x^{2^r+1} + D_{2^r-1}(x),$$

leads to $g(x) = T_1^m(\lambda x^{2^r+1})$. Hence, we can study the bentness of f, defined by (23), if we can exhibit some property on the Hadamard transform of the function $x \mapsto T_1^m(x^{-1} + \lambda x^{2^r+1})$. For instance, we have to prove that this function is balanced when g is balanced too (according to (21)). We obtain directly the following characterization which could be seen as a generalization of Theorem 3.

Theorem 8 *Let $n = 2m$. Consider any function f defined by (23), with $\lambda \in \mathbf{F}_{2^m}^*$. Assume that the function $x \mapsto T_1^m(\lambda x^{2^r+1})$ is balanced on $\mathbf{F}_{2^m}$.*

Then f is hyperbent if and only if

$$\sum_{x \in \mathbf{F}_{2^m}} (-1)^{T_1^m(x^{-1} + \lambda x^{2^r+1})} = 0$$

Note that the previous equality is valid for any r such that $\gcd(2^r + 1, 2^m - 1) = 1$. So we are expecting a number of hyperbent functions of type (23). To describe a subset of such functions is, in particular, to solve the next problem.

Open Problem 4 *Describe the set of $\lambda \in \mathbf{F}_{2^m}^*$ such that the function on $\mathbf{F}_{2^m}$, $x \mapsto T_1^m(x^{-1} + \lambda x^{2^r+1})$, where $2^r + 1$ is coprime to $2^m - 1$, is balanced.*

The simplest case is $r = 1$. Before we present the result about the case $r = 1$, we introduce a lemma on the divisibility of the *inverse cubic* sums, which is established by Charpin, Helleseth and Zinoviev recently. It turns out that this result is essential for proving the next proposition.

Lemma 9 [5, Lemma 5] *Let m be odd, $m \geq 5$. Define, for any $a \in \mathbf{F}_{2^m}^*$, the Boolean function over $\mathbf{F}_{2^m}$: $h_a(x) = T_1^m(a(x^{-3} + x))$. Then*

$$\sum_{x \in \mathbf{F}_{2^m}} (-1)^{h_a(x)} \equiv \begin{cases} 8 \pmod{16}, & \text{if } T_1^m(a) = 1, \\ 0 \pmod{16}, & \text{if } T_1^m(a) = 0. \end{cases}$$

Proposition 3 *Let $n = 2m$ with m odd. Let, for any $\lambda \in \mathbf{F}_{2^m}^*$, the Boolean function on $\mathbf{F}_{2^n}$*

$$f(x) = Tr\left(\lambda(x^{2^m-1} + x^{3(2^m-1)})\right). \tag{24}$$

Then we have :

(i) *If $m = 3$ then f is hyperbent unless $\lambda = 1$.*

(ii) *Let $m \geq 5$. If $T_1^m(\lambda) = 1$ then f is not hyperbent.*

Proof. Note that $x \mapsto x^3$ is a permutation on $\mathbf{F}_{2^m}$ for odd m. Hence, the function $x \mapsto T_1^m(\lambda x^3)$ is balanced for any λ. According to Theorem 8, f is hyperbent if and only if

$$\sum_{x \in \mathbf{F}_{2^m}} (-1)^{T_1^m(x^{-1}+\lambda x^3)} = 0.$$

Denote by A the left-hand-side of the above identity. For $m \geq 5$, we use Lemma 9 with $a = \lambda$. We have :

$$\begin{aligned}
\sum_{x \in \mathbf{F}_{2^m}} (-1)^{h_\lambda(x)} &= \sum_{x \in \mathbf{F}_{2^m}} (-1)^{T_1^m(\lambda x^{-3}+\lambda x)} \\
&= \sum_{x \in \mathbf{F}_{2^m}} (-1)^{T_1^m(\lambda x^3+\lambda x^{-1})} \\
&= \sum_{y \in \mathbf{F}_{2^m}} (-1)^{T_1^m(\lambda^4 y^3+y^{-1})} \\
&= \sum_{z \in \mathbf{F}_{2^m}} (-1)^{T_1^m(\lambda z^3+z^{-1})} = A
\end{aligned}$$

where $y = x/\lambda$ and, further, $z = y^{2^{m-2}}$. From Lemma 9, A is congruent to 8 modulo 16 as soon as $T_1^m(\lambda) = 1$. Thus, in this case $A \neq 0$.

Now, if $m = 3$ then $x^{-1} = x^{2^m-2} = (x^3)^2$ for $x \in \mathbf{F}_{2^m}$. In this case,

$$T_1^m(x^{-1} + \lambda x^3) = T_1^m(x^3(1 + \lambda)).$$

The function $x \mapsto T_1^m(x^3(1 + \lambda))$ is balanced unless $\lambda = 1$. In other terms, $A = 0$ for any $\lambda \neq 1$, completing the proof. ◇

Bent functions of the form (24) exist for $m > 3$, as it is proved by the next example.

Example 1 Let $m = 9$. In $\mathbf{F}_{2^9}$, we have $x^{-1} = (x^{255})^2$. Also,

$$\sum_{x \in \mathbf{F}_{2^9}} (-1)^{T_1^m(x^{255} + \lambda x^3)} = \sum_{y \in \mathbf{F}_{2^9}} (-1)^{T_1^m(y^{85} + \lambda y)},$$

where y replaces x^3. There are 57 values of $\lambda \in \mathbf{F}_{2^9}^*$ for which the sum above is zero[1]. Therefore, there are 57 functions f, as defined in Proposition 3, which are hyperbent for $m = 9$.

We also computed the number of hyperbent functions for $m = 15$, using the same method, and found 595 such functions.

The previous result leads to a more specific research problem.

Open Problem 5 *Let $m = 3k$, k odd. Find an infinite class of balanced functions on $\mathbf{F}_{2^m}$ of the form*

$$y \ \mapsto \ T_1^m(y^d + \lambda y), \ \lambda \in \mathbf{F}_{2^m}^*, \ d = \frac{2^{m-1} - 1}{3}.$$

4.3 Monomial Hyperbent Functions in Terms of Dickson Polynomials

In this section, we show another interesting consequence of Theorem 7. If $E = \{r\}$ in Theorem 7, then $g(x) = T_1^m(\beta_r D_r(x))$. We consider again any monomial function defined by (11),

$$f_{\lambda,r}(x) = Tr(\lambda x^{r(2^m-1)}),$$

with $\lambda \in \mathbf{F}_{2^m}^*$ and $\gcd(r, 2^m + 1) = 1$. We have proved that the bentness of $f_{\lambda,r}$ depends on λ only. Thus Theorem 7, together with Theorem 5, yields the following result about the monomial functions.

Corollary 3 *For any integer r, $r > 0$, let*

$$g_r \ : \ x \in \mathbf{F}_{2^m} \ \mapsto \ T_1^m(\lambda D_r(x))$$

where D_r is the Dickson polynomial of degree r. Then, the function $f_{\lambda,1}$ is hyperbent if and only if there is r coprime to $2^m + 1$ such that

$$\#\{ \ u \in \mathbf{F}_{2^m} \mid T_1^m(u^{-1}) = 1 \text{ and } g_r(u)) = 1 \ \} = 2^{m-2}. \tag{25}$$

[1]The weight enumerators of cyclic codes of length 511 with two non zeros, α and α^ℓ are listed in [4, p. 1028-29]

This is equivalent to : there is r coprime to 2^m+1 such that

$$\sum_{x\in\mathbf{F}_{2^m}} (-1)^{T_1^m(x^{-1})+g_r(x)} = 2^m - 2wt(g_r). \tag{26}$$

Note that g is balanced when D_r is a permutation polynomial, *i.e.,* when $\gcd(r, 2^n-1) = 1$ (see Section 2.3). In this case $2^m - 2wt(g_r) = 0$. Thus we have proved the next surprising property.

Proposition 4 *Recall that K_m denotes the Kloosterman sum over $\mathbf{F}_{2^m}$ (see (7)) and Dickson polynomials D_r are defined in Section 2.3. Let $\lambda \in \mathbf{F}_{2^m}^*$ be such that $K_m(\lambda) = 0$. Then, for any r coprime to $2^{2m}-1$ with $r \leq 2^m$:*

$$\sum_{x\in\mathbf{F}_{2^m}} (-1)^{T_1^m(x^{-1}+\lambda D_r(x))} = 0. \tag{27}$$

This is to say that the function $x \mapsto T_1^m(x^{-1}+\lambda D_r(x))$ is balanced.

Remark 4 In this remark, we show a couple of unusual consequences related to Corollary 3. For clarity we only consider r satisfying $\gcd(r, 2^{2m}-1) = 1$. In this case D_r is a permutation on $\mathbf{F}_{2^m}$.

1. We denote the left hand side of (27) by $T(\lambda, r)$. From Corollary 3, $f_{\lambda,r}$ is hyperbent if and only if $T(\lambda, r) = 0$ which depends on r. On the other hand, from Theorem 5, $f_{\lambda,r}$ is hyperbent if and only if $K_m(\lambda) = 0$ which is independent of r.

2. Another fascinating result from Corollary 3 is related to the result of Theorem 6 where we showed that $K_m(1) \neq 0$ for $m \neq 8$. Thus, $f_{1,r}$ is not hyperbent for any r relatively coprime with 2^m+1. Therefore, we have that $T(1, r) \neq 0$ in (27). However the function

$$x \quad \mapsto \quad T_1^m(x^{-1} + D_r(x))$$

has multiple trace terms, since D_r has multiple terms. Usually, it is not easy to determine whether such a function is balanced or not. However, through this hyperbent connection, we know that this exponential sum is not equal to zero, since it is determined by $K_m(1)$, the Kloosterman sum at 1. The case $m = 4$ is explained in the next example.

Example 2 We know that $K_4(1) = 0$ (see Theorem 6). The Dickson polynomials which are permutations are here, up to equivalence, those D_r with $r \in \{1,\ 7,\ 11,\ 13\}$. They are

$$x,\ x^7 + x^5 + x,\ x^{11} + x^9 + x^5 + x^3 + x,\ x^{13} + x^{11} + x^3 + x.$$

Note that in $\mathbf{F}_{16}$ we have $T_1^4(x^{-1}) = T_1^4(x^7)$. It is easy to check directly (27).

5 Conclusion

A number of recent papers are devoted to bent Boolean functions expressed by means of trace-functions [1, 2, 3, 6, 11, 16, 17]. In this paper, we contribute to the knowledge of this fascinating class of functions, by studying a subclass of the so-called $\mathcal{PS}^-$ class. Such functions are not yet classified , even when they are monomials (see Open problem 1). We show the nonbentness of an infinite class of monomials by means of a property of some Kloosterman sums.

Kloosterman sums appear in many problems where it is crucial to determine the sums $K_m(a)$ for specific a (see [12], for instance). Also, in a number of recent papers, Dickson polynomials were fruitfully used. We follow in particular [11] and [12]. In this paper, we show that the link between the monomials and some Kloosterman sums is generalized in a link between multiple trace terms functions and some exponential sums where Dickson polynomials are involved. We emphasize that we have here introduced a new method for exploring the possibly hyperbent functions.

Considering our first results on monomials and binomials, it seems to us that our work has several expansions. The results of Section 4.3 are surprising. For instance, as soon as we have characterized one monomial bent function we can then generate a sequence of balanced functions using the Dickson permutation polynomials. We are mainly interested by the bentness, but to have properties on the full spectrum is of interest also. In particular, some formula in this paper can be seen as approximations of the components of the inverse function. To conclude, note that we only use Dickson polynomials of $\mathbf{F}_2[x]$, while Dickson polynomials of $\mathbf{F}_{2^m}[x]$ could be considered.

References

[1] A. Canteaut, P. Charpin, and G. Kyureghyan, "A new class of monomial bent functions", *Finite Fields and Their Applications*, in press.

[2] A. Canteaut, M. Daum, G. Leander and H. Dobbertin, "Normal and non normal bent functions," *Discrete Applied Mathematics*, Vol. 154, Issue 2, pp. 202-18, February 2006.

[3] C. Carlet and P. Gaborit, "Hyperbent functions and cyclic codes," *Jour. Comb. Theory*, Series A, 113(2006), Issue 3, pp. 466-82.

[4] P. Charpin, *Open problems on cyclic codes*, In "Handbook of Coding Theory", Part 1, chapter 11, V. S. Pless, W. C. Huffman, Eds, R. A. Brualdi, assistant editor, Amsterdam, the Netherlands: Elsevier, 1998.

[5] P. Charpin, T. Helleseth, and V. Zinoviev, "The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd", *Jour. Comb. Theory, Series A*, 114(2007), Issue 2, pp. 322-338.

[6] P. Charpin and G. Kyureghyan, "Cubic monomial bent functions: a subclass of $\mathcal{M}$" . SIAM J. of Discrete Math., to appear.

[7] P. Delsarte and J.M. Gœthals, *Irreducible binary cyclic codes of even dimension*, in: Combinatorial Mathematics and its Applications, Proc. Second Chapel Hill Conference, May 70 (Univ. of North Carolina, Chapel Hill, N.C.,1970) pp. 100-113.

[8] L.E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover Publication, Inc., 1958.

[9] J.F. Dillon, "Elementary Hadamard Difference sets," Ph.D. dissertation, University of Maryland, 1974.

[10] J.F. Dillon, Elementary Hadamard difference sets. In Proc. *6-th S-E Conf. Combinatorics, Graph theory, and Computing.* Congress Number XIV, 1975, pp. 237-249.

[11] J.F. Dillon and H. Dobbertin, "New cyclic difference sets with Singer parameters", *Finite Fields and Their Applications*, 10(2004), pp. 342-389.

[12] H. Dobbertin, P. Felke, T. Helleseth and P. Rosendalh. "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums", *IEEE Trans. on Inform. Theory*, vol. 52, No. 2, pp. 613 - 627, February 2006.

[13] S.W. Golomb and G. Gong, "Transform domain analysis of DES", *IEEE Trans. Inform. Theory*, vol. 45, No. 6, pp. 2065-2073, February 1999.

[14] T. Helleseth and V.A. Zinoviev, "On Z_4-Linear Goethals Codes and Kloosterman Sums", Designs, Codes and Cryptography, vol. 17, No. 1-3, pp. 246-262, 1999.

[15] G. Lachaud and J. Wolfmann, "The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes," *IEEE Trans. Inform. Theory*, vol. 36, No. 3, pp. 686-692, May 1990.

[16] N.G. Leander, "Monomial bent functions," *IEEE Trans. Inform. Theory*, vol. 52, No. 2, pp. 738-743, February 2006.

[17] N.G. Leander and A. Kholosha, "Bent functions with 2^r Niho exponents," *IEEE Trans. Inform. Theory*, vol. 52, No. 12, pp. 5529-5532, December 2006.

[18] R. Lidl, G.L. Mullen and G. Turnwald, *Dickson Polynomials*, Pitman Monographs in Pure and Applied Mathematics, Vol. 65, Addison-Wesley, Reading, MA 1993.

[19] R.J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Boston: Kluwer, 1987.

[20] A.M. Youssef and G. Gong, "Hyper-Bent Functions", Advances in Cryptology – Eurocrypt'2001, Lecture Notes in Computer Science, 2045, Springer, 2001, pp. 406-419.