Hyperbent Functions, Kloosterman Sums, and Dickson Polynomials

Pascale Charpin and Guang Gong, *Senior Member, IEEE*

***Abstract*—This paper is devoted to the study of hyperbent functions in n variables, i.e., bent functions which are bent up to a change of primitive roots in the finite field $GF(2^n)$. Our main purpose is to obtain an explicit trace representation for some classes of hyperbent functions. We first exhibit an infinite class of monomial functions which is not hyperbent. This result indicates that Kloosterman sums on $\boldsymbol{F}_{2^m}$ cannot be zero at some points. For functions with multiple trace terms, we express their spectra by means of Dickson polynomials. We then introduce a new tool to describe these hyperbent functions. The effectiveness of this new method can be seen from the characterization of a new class of binomial hyperbent functions.**

***Index Terms*—Bent function, Boolean function, Dickson polynomial, hyperbent function, Kloosterman sum, permutation polynomial, quadratic function.**

I. Introduction

HYPERBENT functions were introduced by Youssef and Gong in [23]. A Boolean bent function f, on $\boldsymbol{F}_{2^n}$, is said to be hyperbent if $f(x^k)$ is bent for any k coprime with 2^n-1. 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 [15] (see (2) below). In [15], 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 [23] are those elements of the $\mathcal{PS}_{ap}$ class due to Dillon [11]. They also established that hyperbent functions can be seen as a partial set of codewords of a cyclic code fully determined by its nonzeroes. However, the classification of hyperbent functions and many related problems remain open. This fact has also been made clear in a more recent paper due to Kuzmin *et al.* [17].

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, where we introduce new tools mainly for the description of hyperbent functions.

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

Section III concerns monomial hyperbent functions. These famous bent functions, discovered by Dillon [11] (1974), are strongly related to Kloosterman sums. We give a completed version of a result of Leander [19], which specifies the spectrum of such a function f_λ by means of $K_m(\lambda)$, the Kloosterman sum on $\boldsymbol{F}_{2^m}t$ at point λ (Theorem 5). After several general properties, we focus on specific families of λ such that $K_m(\lambda)\neq 0$. This is equivalent to saying that for such λ the function f_λ cannot be bent. In particular, we prove that $K_m(1)\neq 0$ unless $m=4$. In other terms, we prove that f_1, defined on $\boldsymbol{F}_{2^n}$, is not bent unless $n=8$. We then solve a problem which was proposed by Dillon to the second author several years ago.

In Section IV, 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 a class of monomial functions, providing surprising results. By Theorem 8, we characterize a class of binomial hyperbent functions. Proposition 4 is a generalization. Monomial hyperbent functions, which are related to the zeros of some Kloosterman sums, are here described by means of Dickson permutation polynomials.

II. The Main Objectives

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

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

Any Boolean function f over $\boldsymbol{F}_{2^n}$ is a function from $\boldsymbol{F}_{2^n}$ to $\boldsymbol{F}_2$. The *weight* of f, denoted $\mathrm{wt}(f)$, 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 $\boldsymbol{F}_{2^n}$ we state its Hadamard transform

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

and its *extended Hadamard transform*

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

where $a\in\boldsymbol{F}_{2^n}$ and $\gcd(k,2^n-1)=1$. 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 $\mathcal{F}(0)=0$.

Manuscript received September 12, 2007; revised April 14, 2008. Published August 27, 2008 (projected).

P. Charpin is with INRIA—Rocquencourt, Domaine de Voluceau, B.P. 105 F-78153 Le Chesnay Cedex, France (e-mail: Pascale.Charpin@inria.fr).

G. Gong is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L3G1, Canada (e-mail: ggong@calliope.uwaterloo.ca).

Communicated by I. Dumer, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2008.928273

A. Hyperbent Functions

Youssef and Gong proposed in [23] to strengthen the bent concept by using the extended Hadamard transform and stated the following.

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

They later introduced 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 $2m$. Define the Boolean functions on $\boldsymbol{F}_{2^n}$ of the form

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

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 [11, pp. 95–100)]. We first recall the definition of $\mathcal{PS}^-$.

Theorem 1: [11] Let f be a Boolean function over $\boldsymbol{F}_{2^n}, n = 2m$, and set

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

Denote by $\{S_i, i = 1, 2, \ldots, N\}$ a set of subspaces of $\boldsymbol{F}_{2^n}$ of dimension m satisfying

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

Assume that f is such that

$$E_f = \bigcup_{i=1}^{N} S_i^*$$

where $S_i^* = S_i \setminus \{0\}$. Then, the function f is bent if and only if $N = 2^{m-1}$. In this case, f is said to be in $\mathcal{PS}^-$.

According to the preceding theorem, we give now a slightly different version of [23, Theorem 1]. Although the result is known, we present a brief proof of the next theorem, giving some elements which we will use later.

Theorem 2: Denote by $\mathcal{G}$ the cyclic subgroup of $\boldsymbol{F}_{2^n}{}^*$ 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

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

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

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

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

Now, define subspaces

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

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 $N = 2^{m-1}$ (I has cardinality 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 $\mathcal{G}$. □

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 explicitly the coefficients β_r.

B. Monomial Hyperbent Functions

For the monomial 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 $\boldsymbol{F}_{2^n}$ to $\boldsymbol{F}_2$

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

Define the Kloosterman sums over $\boldsymbol{F}_{2^m}$

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

where $T_1^m(a)$ is the absolute trace on $\boldsymbol{F}_{2^m}$. Note that we assume

$$T_1^m\left(\frac{1}{0}\right) = T_1^m\left(0^{2^{m-1}-1}\right) = 0.$$

The following characterization is due to Dillon [11], [12].

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 [18] for any m (even or odd).

Lemma 1: The set $\{K_m(\lambda), \lambda \in \boldsymbol{F}_{2^m}\}$ is the set of all the integers $s \equiv 0 \pmod 4$ in the range

$$\left[-2^{(m+2)/2} + 1,\ 2^{(m+2)/2} + 1\right].$$

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 the following Open Problem.

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

The preceding problem appeared as a very difficult problem. Through numerical results it is possible to introduce some conjecture concerning a partial problem. In Section III-B, we present our main results in this context. In particular, 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 [16]: For any $m\geq 3$

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

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

Remark 1: We can take $\lambda\in\boldsymbol{F}_{2^m}$ 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 $\lambda\in\boldsymbol{F}_{2^n}$ can be written $\lambda=uv$ with $u\in\boldsymbol{F}_{2^m}$ and v in the subgroup of $\boldsymbol{F}_{2^n}$ of order 2^m+1. Then f_λ has the same spectrum as f_u.

C. Dickson Polynomials

The main reference on Dickson polynomials is Dickson's book [10]. An excellent presentation of the work of Dickson can be found in [21]. In our approach, we follow several recent papers where the reader can find a basic overview [13], [14]. A Dickson polynomial is defined by

$$D_r(x)=\sum_{i=0}^{r/2}\frac{r}{r-i}\binom{r-i}{i}x^{r-2i},\quad r=2,3,\ldots. \tag{9}$$

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

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

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

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

for any integer $i,j>0$.

We also have the following fundamental result.

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

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

III. Hyperbent Functions and Zeroes of Kloosterman Sums

In this section, we study the bentness of monomial functions $x\mapsto \mathrm{Tr}(\lambda x^{r(2^m-1)})$ over $\boldsymbol{F}_{2^n}$, $n=2m$, by means of properties of Kloosterman sums. In the following subsection, we are going to show that it is sufficient to treat the case $r=1$.

A. Monomial Functions

Recently, Leander [19] proposed another proof of Theorem 3, giving more information 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 [19, Theorem 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 with 2^m+1, define the Boolean functions on $\boldsymbol{F}_{2^n}, n=2m$

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

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

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

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

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

Consequently, $f_{\lambda,r}$ is bent if and only if $K_m(\lambda)=0$ 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 $x\in\boldsymbol{F}_{2^n}{}^*$ can be written $x=yz, y\in\boldsymbol{F}_{2^m}{}^*$ and $z\in\mathcal{G}$. Note that $y^{2^m-1}=1$ and $z^{2^m-1}=z^{-2}$. For readability, we use this notation :$e(h(x))=(-1)^{\mathrm{Tr}(h(x))}$. So we have

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

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

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

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

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

Indeed

$$\mathrm{Tr}(ayz)=T_1^m\left(y(az+a^{2^m}z^{-1})\right)$$

so that $\sum_{y\in\boldsymbol{F}_{2^m}}e(ayz)\neq 0$ (and then equal to 2^m) if and only if

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

Then

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

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 [7], [11], [18], [19]). Finally

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

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

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

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

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

for $K_m(\lambda) \neq 0$, because $|K_m(\lambda)| < 2^m$ (see Lemma 1). And this holds for any $a \in \boldsymbol{F}_{2^n}{}^*$; 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 exactly three values 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 remainder of this section, we assume that $r = 1$, i.e., we come back to functions f_λ defined by (6). We are going to specify the bentness of f_λ by means of properties of elements of $\boldsymbol{F}_{2^m}$. Recall that γ is a generator of $\mathcal{G}$, the cyclic group of order $2^m + 1$ in $\boldsymbol{F}_{2^n}, n = 2m$. Note that $\gamma^{2^m} = \gamma^{-1}$.

Lemma 3: Let $S_i = \gamma^i \boldsymbol{F}_{2^m}, 0 \leq i \leq 2^m$. The function f_λ is defined by (6). Then f_λ is constant on each S_i^*, equal to $\mathrm{Tr}(\lambda\gamma^{-2i})$. Moreover, f_λ is hyperbent if and only if

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

Proof: The lemma follows from Theorem 2 and its proof, together with the following observation:

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

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

$$N = \#\left\{i \in [1, 2^m] \,|\, T_1^m(\lambda(\gamma^{ir} + \gamma^{-ir})) = 1\right\}.$$

If $\gcd(r, 2^m + 1) = d$ with $d > 1$ and d odd, then $2d$ divides N and thus $N \neq 2^{m-1}$. 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

$$\{\gamma^i + \gamma^{-i} \,|\, 1 \leq i \leq 2^m\} = \left\{u \in \boldsymbol{F}_{2^m} \,|\, T_1^m(u^{-1}) = 1\right\}.$$

Proof: This was first proved by Delsarte and Goethals [9] who established that we have here the roots of

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

Another proof can be found in [18]. □

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

Corollary 1: The function f_λ on $\boldsymbol{F}_{2^n}, n = 2m$ is defined by (6). Then f_λ is hyperbent if and only if

$$\#\left\{u \in \boldsymbol{F}_{2^m} \,|\, T_1^m(\lambda u) = T_1^m(u^{-1}) = 1\right\} = 2^{m-2}. \quad (14)$$

Now, using (12) and (13), 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

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

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

$$\#\left\{u \in \boldsymbol{F}_{2^m} \,|\, T_1^m(\lambda u) = T_1^m(u^{-1}) = 1\right\} = 2^{m-2} + \frac{K_m(\lambda)}{4}.$$

Proof: From (12), we have

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

which gives

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

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 $\mathrm{wt}(f_\lambda)$ 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

$$\#\left\{i \,|\, T_1^m(\lambda(\gamma^i+\gamma^{-i}))=1\right\}$$

which is equal to

$$2\#\left\{u\in \boldsymbol{F}_{2^m} \,|\, T_1^m(\lambda u)=T_1^m(u^{-1})=1\right\}. \qquad \square$$

B. Non-Bent Monomials

In this subsection, we exhibit an infinite set of monomial functions of type (6) which are not bent. We also explain the special case $n=8$, where monomial bent functions can be defined explicitly. We use Theorem 3 and thus study the values $K_m(\lambda)$. There are some specific results which can be obtained directly from Lemma 2.

Lemma 5: If m is odd then $K_m(1)\neq 0$. Let $m=2k$ with k odd. Then

$$K_m(\lambda)\neq 0, \quad \text{for } \lambda\in \boldsymbol{F}_4\setminus\{0,1\}.$$

Proof: According to Lemma 2, we simply have to prove that $T_1^m(\lambda)=1$. It is clear for m odd and $\lambda=1$.

Let $m=2k$ with k odd then $\boldsymbol{F}_4=\{0,1,\lambda,\lambda^2\}$ and

$$T_1^m(\lambda)=T_1^k(\lambda+\lambda^2)=T_1^k(1)=1. \qquad \square$$

Now we want to have more results, especially to complete the case $\lambda=1$. We will show that for m even, $m=2k$, $K_m(\lambda)$ cannot be 0 for almost all $\lambda\in \boldsymbol{F}_{2^k}^*$.

Lemma 6: Let $m=2k$ with $k>1$. If $m\neq 4$, then

$$K_m(\lambda)\neq 0, \quad \text{for } \lambda\in \boldsymbol{F}_{2^k}^*.$$

Moreover, $K_4(\lambda)=0$ for $\lambda=1 (\lambda\in \boldsymbol{F}_4^*)$ only.

Proof: Assume that, more generally, $m=sk$. Carlitz proved that the Kloosterman sum $K_{ks}(a)$ where $\lambda\in \boldsymbol{F}_{2^k}^*$ can be expressed as a polynomial in $K_k(\lambda)$ (see [4, eq. (5.10)]). For $s=2$, this expression becomes very simple

$$K_{2k}(\lambda)=-(K_k(\lambda))^2+2K_k(\lambda)+2^{k+1}. \qquad (15)$$

Note that we rewrite here the formula due to Carlitz, considering any Kloosterman sum as a sum on the full field (including 0).

Suppose that $K_{2k}(\lambda)=0$ for some $\lambda\in \boldsymbol{F}_{2^k}^*$. Then $K_k(\lambda)\neq 0$ and we get

$$(K_k(\lambda))^2-2K_k(\lambda)=K_k(\lambda)(K_k(\lambda)-2)=2^{k+1}.$$

Thus, $K_k(\lambda)-2$ must be a power of 2. Since $K_k(\lambda)$ is divisible by 4 (see Lemma 1), this is impossible unless $K_k(\lambda)=4$ so that $2^{k+1}=8$.

Now, assume that $k=2$. Then (15) becomes for $\lambda\in \boldsymbol{F}_4^*$

$$K_4(\lambda)=-(K_2(\lambda))^2+2K_2(\lambda)+2^3$$

with

$$K_2(\lambda)=\sum_{x\in \boldsymbol{F}_4}(-1)^{T_1^2(x(1+\lambda))}.$$

Thus, $K_2(\lambda)=4$ for $\lambda=1$; otherwise, $K_2(\lambda)=0$. Therefore, $K_4(\lambda)=0$ for $\lambda=1$; otherwise, $K_4(\lambda)=8$. $\square$

We now summarize our results. Denote by $\mathcal{T}_m$ the set of those $\lambda\in \boldsymbol{F}_{2^m}$, which we described in Lemmas 5 and 6. That is

$$\mathcal{T}_m=\begin{cases}\{1\}, \text{ if } m \text{ is odd}\\ \boldsymbol{F}_{2^k}^* \text{ if } m=2k \text{ with } k \text{ even}, \ k>2\\ \boldsymbol{F}_4\setminus\{0,1\}, \text{ if } m=4\\ (\boldsymbol{F}_{2^k}\cup \boldsymbol{F}_4)^*, \text{ if } m=2k \text{ with } k \text{ odd.}\end{cases} \qquad (16)$$

Theorem 6: Let $n=2m$ with $m\geq 3$. For any $\lambda\in\mathcal{T}_m$, the Kloosterman sum

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

satisfies $K_m(\lambda)\neq 0$. Consequently,

- the Boolean functions $y\mapsto T_1^m(y^{-1}+\lambda y)$, on $\boldsymbol{F}_{2^m}$, are not balanced;
- the Boolean functions $x\mapsto \mathrm{Tr}(\lambda x^{r(2^m-1)})$, on $\boldsymbol{F}_{2^n}$, are not bent, for any r coprime with 2^m+1.

Note that the previous theorem holds for any $\lambda\in \boldsymbol{F}_{2^m}$ such that $T_1^m(\lambda)=1$, according to Lemma 2. Also, there are immediate consequences of our previous results that we explain now.

Corollary 2: Let $n=2m$ with $m\geq 2$. Then the Boolean functions on $\boldsymbol{F}_{2^n}$

$$f_{1,r}(x)=\mathrm{Tr}\left(x^{r(2^m-1)}\right), \quad \gcd(r,2^m+1)=1$$

are not hyperbent unless $n=8$. In other terms, $K_m(1)\neq 0$ unless $m=4$.

We proved that $K_m(1)\neq 0$ for any $m>4$ by another way in [6], using properties of the self-reciprocal polynomials. The preceding corollary leads naturally to the problem of the existence of binary hyperbent functions.

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

We proved that $K_4(1)=0$. So we deduce from (15) that $K_8(1)=2^5$. Then, using Theorem 5, we can give the values of the Hadamard transform of the corresponding $f_{1,r}$.

Corollary 3: The Boolean functions on $\boldsymbol{F}_{2^8}$

$$x\mapsto \mathrm{Tr}\left(x^{r(2^4-1)}\right), \quad 1\leq r<17$$

are bent. Consider the functions on $\boldsymbol{F}_{2^{16}}$

$$x\mapsto \mathrm{Tr}\left(x^{r(2^8-1)}\right), \quad \gcd(r,2^8+1)=1.$$

They are not bent and the values of its Hadamard transform are

$$\{2^5(1+2^3-2^8),2^5\pm 2^8\}.$$

TABLE I
THE ZEROES OF $K_m(\lambda)$ FOR $m < 14$

m	Coset Leaders	$(c_0, c_1, \cdots, c_{m-1})$
4	$\{0, 1\}$	1100
5	$\{15\}$	10010
6	$\{1, 7\}$	110000
7	$\{1, 29\}$	1100000
8	$\{13, 31\}$	10111000
9	$\{1, 61\}$	100010000
10	$\{1, 9, 23, 117, 205, 511\}$	1001000000
11	$\{1, 59, 95, 315, 363\}$	10100000000
12	$\{23, 55, 91, 427, 505, 731\}$	110010100000
13	$\{199, 621, 915, 921\}$	1101100000000
14	$\{409, 509, 1333, 1355, 1735, 2399, 2647, 3061\}$	11010100000000

To illustrate our purpose, we list in Table I the zeroes of $K_m(\lambda)$ for small values of m

Explanation of Table I: in the second column, we list coset leaders i such that $K_m(\alpha^i) = 0$ for $4 \leq m \leq 14$. In the third column of Table I, we list a primitive polynomial

$$f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0$$

as a vector $(c_0, c_1, \ldots, c_{m-1})$ for defining $\boldsymbol{F}_{2^m}$. For example, for $m = 4$, the entries in the second column correspond to $K_4(\alpha^i) = 0$ for $i \in C_0 \cup C_1$, where C_i is a cyclotomic cosets modulo $2^m - 1$. For $m = 4, C_0 = \{0\}, C_1 = \{1, 2, 4, 8\}$, and the primitive polynomial is $f(x) = x^4 + x + 1$.

IV. 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 to deal with this case. In this section, using the results developed in Section III, we show that the bentness of those functions with some restriction is related to the Dickson polynomials.

A. Main Characterization

Dickson polynomials are defined here as polynomials in $\boldsymbol{F}_2[x]$ (see Section II-C). They are denoted by D_r where r in R. Recall that R is a set of representatives of the cyclotomic cosets modulo $2^m + 1$ of size $2m$.

Theorem 7: Let $n = 2m$. Consider any function of type (3) on $\boldsymbol{F}_{2^n}$ with coefficients in $\boldsymbol{F}_{2^m}$

$$f(x) = \sum_{r \in E} \mathrm{Tr}\left(\beta_r x^{r(2^m-1)}\right), \quad \beta_r \in \boldsymbol{F}_{2^m} \tag{17}$$

where $E \subseteq R$. Define the related Boolean function on $\boldsymbol{F}_{2^m}$

$$g(x) = \sum_{r \in E} T_1^m(\beta_r D_r(x)). \tag{18}$$

Then f is hyperbent if and only if

$$\#\{u \in \boldsymbol{F}_{2^m} \,|\, T_1^m(u^{-1}) = 1 \quad \text{and} \quad g(u) = 1\} = 2^{m-2}.$$

Consequently, f is hyperbent if and only if

$$\sum_{x \in \boldsymbol{F}_{2^m}} (-1)^{T_1^m(x^{-1}) + g(x)} = 2^m - 2\mathrm{wt}(g). \tag{19}$$

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

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

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

$$N = \#\left\{ j \,|\, \sum_{r \in E} T_1^m(\beta_r(\gamma^{rj} + \gamma^{-rj})) = 1 \right\}. \tag{20}$$

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

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

Using Proposition 2, we rewrite (20) as follows:

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

where $g(x)$ is defined by (18).

Denote by h the function $x \mapsto T_1^m(x^{-1})$. To prove (19), we have to compute the Hadamard transform of the function $h + g$ at point 0, say $\mathcal{F}(0)$. We know that $\mathcal{F}(0) = 2^m - 2\mathrm{wt}(h + g)$. By definition of the Hamming weight, we have

$$\begin{aligned} \mathrm{wt}(h + g) &= \mathrm{wt}(h) + \mathrm{wt}(g) - 2\mathrm{wt}(hg) \\ &= 2^{m-1} - 2\mathrm{wt}(hg) + \mathrm{wt}(g). \end{aligned}$$

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

As a consequence of the previous theorem, we obtain an analogue of Theorem 3. If the function g is balanced in (19) then $2^m - 2\mathrm{wt}(g) = 0$. So we have the following.

Corollary 4: Let f and g be the Boolean functions defined in Theorem 7. Assume that g is balanced. Then f is bent if and only if

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

B. 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 $\boldsymbol{F}_{2^m}$. The latter problem is easier than the former, since we could use the divisibility of some cyclic codes, especially for special classes of functions of type (17). To illustrate, we are going to treat some binomial functions of type (17). Let, for any $\lambda \in \boldsymbol{F}_{2^m}{}^*$

$$f(x) = \mathrm{Tr}\left(\lambda\left(x^{(2^r-1)(2^m-1)} + x^{(2^r+1)(2^m-1)}\right)\right) \qquad (21)$$

where $0 < r < m$ and $\{2^r-1, 2^r+1\} \subset R$. 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 II-C)

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

that leads to $g(x) = T_1^m(\lambda x^{2^r+1})$. Hence, we can study the bentness of f, defined by (21), 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 if g is balanced as well (according to Corollary 4). Thus, we characterize directly a *new* class of bent functions. We obtain here binomial bent functions defined by means of the zeros of (so-called) *inverse-quadratic* exponential sums while by Theorem 3, monomial bent functions and Kloosterman sums were considered.

Theorem 8: Let $n = 2m$. Consider any function f defined by (21), with $\lambda \in \boldsymbol{F}_{2^m}{}^*$. Assume that the function $x \mapsto T_1^m(\lambda x^{2^r+1})$ is balanced on $\boldsymbol{F}_{2^m}$.

Then f is hyperbent if and only if

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

Note that for any r such that $\gcd(2^r+1, 2^m-1) = 1$, the function $x \mapsto x^{2^r+1}$ is a permutation on $\boldsymbol{F}_{2^m}$ so that the Boolean function $x \mapsto T_1^m(\lambda x^{2^r+1})$ is balanced for any λ. So we are expecting a number of hyperbent functions of type (21). To describe a subset of such functions is, in particular, to solve the next problem.

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

Remark 4: The functions of type (21) are defined under the condition

$$0 < r < m \quad \text{and} \quad \{2^r-1, 2^r+1\} \subset R.$$

Thus, we have to guarantee that 2^r-1 and 2^r+1 each belongs to a cyclotomic coset modulo 2^m+1 of size $2m$. This is to say that, with $a_1 = (2^r-1)(2^m-1)$ and $a_2 = (2^r+1)(2^m-1)$, it is impossible to have k dividing n such that

$$x^{a_i} \in \boldsymbol{F}_{2^k}, \quad \forall x \in \boldsymbol{F}_{2^n}$$

for $i = 1$ or 2. In other words, there is no $k < m$ such that

$$(2^k-1)(2^r \triangle 1) \equiv 0 \,(\mathrm{mod}\, 2^m+1),\ \triangle \in \{+,-\}. \qquad (22)$$

The simplest case is $r = 1$; thus, $2^r-1 = 1$ and $2^r+1 = 3$. In this case, there is no k such that (22) holds for $m > 3$. Indeed

$$3(2^k-1) = 2^{k+1} + 2^k - 3 \equiv 0 \,(\mathrm{mod}\, 2^m+1)$$

is impossible unless $k = m-1$ and $m = 3$. Before we present the result about the case $r = 1$, we introduce a lemma on the divisibility of the *inverse cubic* sums, which has been recently established by Charpin, Helleseth, and Zinoviev. It turns out that this result is essential for proving the next proposition.

Lemma 7: [7, Lemma 5] Let m be odd, $m \geq 5$. Define, for any $a \in \boldsymbol{F}_{2^m}{}^*$, the Boolean function over $\boldsymbol{F}_{2^m}$

$$h_a(x) = T_1^m(a(x^{-3} + x)).$$

Then

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

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

$$f(x) = \mathrm{Tr}\left(\lambda\left(x^{2^m-1} + x^{3(2^m-1)}\right)\right). \qquad (23)$$

Then we have the following.

(i) If $m = 3$ and $\lambda + \lambda^2 + \lambda^{2^2} = 0$ then f is monomial hyperbent.

(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 $\boldsymbol{F}_{2^m}$ 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

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

Denote by A the left-hand side of the above identity. For $m \geq 5$, we use Lemma 7 with $a = \lambda$. We have

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

where $y = x/\lambda$ and, further, $z = y^{2^{m-2}}$. From Lemma 7, 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 we have seen that (22) holds. Actually (23) becomes

$$f(x) = \mathrm{Tr}(\lambda x^7) + T_1^2\left(T_2^6(\lambda)x^{21}\right).$$

If $T_2^6(\lambda) = 0$ then $f(x) = \mathrm{Tr}(\lambda x^7)$. Note that, since $\lambda \in \boldsymbol{F}_{2^3}$ then

$$T_2^6(\lambda) = \lambda + \lambda^4 + \lambda^2.$$

Thus, if $\lambda + \lambda^2 + \lambda^4 = 0$, we get a monomial function of type (6). Such function f is bent if and only if $K_3(\lambda) = 0$. Since $m = 3$ we have

$$x^{-1} = x^{2^m-2} = (x^3)^2, \quad \text{for } x \in \boldsymbol{F}_{2^m}.$$

Thus

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

It is well known that the function $x \mapsto T_1^m(x^3+\lambda x)$ is balanced if and only if

$$T_1^3(\lambda) = \lambda + \lambda^2 + \lambda^4 = 0,$$

This completes the proof. □

Bent functions of the form (23) exist for $m > 3$, as it is proved by the next example.

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

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

where y replaces x^3. There are 57 values of $\lambda \in \boldsymbol{F}_{2^9}^*$ 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 $\boldsymbol{F}_{2^m}$ of the form

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

C. Monomial Hyperbent Functions in Terms of Dickson Polynomials

In this subsection, 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)

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

with $\lambda \in \boldsymbol{F}_{2^m}{}^*$ 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.

[1]The weight enumerators of cyclic codes of length 511 with two non-zeros, α and α^ℓ, are listed in [5, pp. 1028–1029].

Corollary 5: For any integer $r, r > 0$, let

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

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 with $2^m + 1$ such that

$$\#\left\{u \in \boldsymbol{F}_{2^m} \mid T_1^m(u^{-1}) = 1 \text{ and } g_r(u)) = 1\right\} = 2^{m-2}.$$

This is equivalent to the following: there is r coprime with $2^m + 1$ such that

$$\sum_{x\in\boldsymbol{F}_{2^m}} (-1)^{T_1^m(x^{-1})+g_r(x)} = 2^m - 2\mathrm{wt}(g_r). \tag{24}$$

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

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

$$\sum_{x\in\boldsymbol{F}_{2^m}} (-1)^{T_1^m(x^{-1}+\lambda D_r(x))} = 0. \tag{25}$$

This is to say that the function $x \mapsto T_1^m(x^{-1} + \lambda D_r(x))$ is balanced on $\boldsymbol{F}_{2^m}$.

We can formulate differently the results of this section.

Proposition 5: Let $\lambda \in \boldsymbol{F}_{2^m}$. Then the functions $f_{\lambda,r}$, where $\gcd(r, 2^{2m}-1) = 1$, are bent if and only if one of the following equivalent conditions is satisfied:

- $K_m(\lambda) = 0$;
- there is an r such that (25) is satisfied;
- all functions $x \mapsto T_1^m(x^{-1} + \lambda D_r(x))$ are balanced.

Remark 5: In this remark, we show some unusual consequences related to Corollary 5. For clarity, we only consider r satisfying $\gcd(r, 2^{2m}-1) = 1$. In this case, D_r is a permutation on $\boldsymbol{F}_{2^m}$.

1) We denote the left-hand side of (25) by $T(\lambda, r)$. From Corollary 5, $f_{\lambda,r}$ 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 5 is related with Corollary 2, where we proved that $K_m(1) \neq 0$ for $m \neq 4$. 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 (25). However the function

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

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 $K_4(1) = 0$. The Dickson polynomials which are permutations on $\boldsymbol{F}_{16}$ are, 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 $\boldsymbol{F}_{16}$ we have $T_1^4(x^{-1}) = T_1^4(x^7)$. It is easy to check directly (25).

V. Conclusion

A number of recent papers has dealt with the subject of the trace representation of bent Boolean functions [1]–[3], [8], [13], [19], [20]. 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 in the monomial case (see Open Problem 1). First, 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 [14], for example). Also, in a number of recent papers, Dickson polynomials have been effectively used. We follow this approach; in particular, that of [13] and [14]. In this paper, we show that the link between the monomials and some Kloosterman sums can be generalized to a link between multiple trace terms functions and some exponential sums where Dickson polynomials are involved. We emphasize that we have introduced here a new method for exploring possible hyperbent functions.

Considering our first results on monomials and binomials, it seems that our work has several extensions. The results of Section IV-C 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 in the bentness, but also in properties of the full spectrum. In particular, some formulas in this paper can be seen as approximations of the components of an inverse function. Note that only basic properties of Dickson polynomials of $\boldsymbol{F}_2[x]$ have been used in the questions on Dickson polynomials, which appear throughout our paper. For instance, by Theorem 7 we see that any property of linear combinations of Dickson polynomials could be of interest. We study the simplest such combination in Section IV-B.

Acknowledgment

The authors wish to thank Victor Zinoviev who indicated that the paper of Carlitz [4] could be effectively used to prove the results of Section III. The authors also wish to thank an anonymous referee who indicated [17] and proposed several improvements.

References

[1] A. Canteaut, P. Charpin, and G. Kyureghyan, "A new class of monomial bent functions," *Finite Fields Their Applic.*, vol. 14, pp. 221–241, 2008.

[2] A. Canteaut, M. Daum, G. Leander, and H. Dobbertin, "Normal and non normal bent functions," *Discr. Appl. Math.*, vol. 154, no. 2, pp. 202–18, Feb. 2006.

[3] C. Carlet and P. Gaborit, "Hyperbent functions and cyclic codes," *J. Comb. Theory*, ser. A, vol. 113, no. 3, pp. 466–82, 2006.

[4] L. Carlitz, "Kloosterman sums and finite field extensions," *Acta Arithmetica*, vol. XVI, no. 2, pp. 179–193, 1969.

[5] P. Charpin, "Open problems on cyclic codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, ch. 11, pt. 1, R. A. Brualdi, Assistant Editor.

[6] P. Charpin and G. Gong, Hyperbent Functions, Kloosterman Sums and Dickson Polynomials Univ. Waterloo, Waterloo, ON, Canada, Rep. CACR 2007-29, Research Report of the Center for Applied Cryptographic Research at the University of Waterloo.

[7] P. Charpin, T. Helleseth, and V. Zinoviev, "The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd," *J. Comb. Theory*, ser. A, vol. 114, no. 2, pp. 322–338, 2007.

[8] P. Charpin and G. Kyureghyan, "Cubic monomial bent functions: A subclass of $\mathcal{M}$," *SIAM J. Discr. Math.*, vol. 22, no. 2, pp. 650–665.

[9] P. Delsarte and J. M. Gœthals, "Irreducible binary cyclic codes of even dimension," in *Combinatorial Mathematics and Its Applications, Proc. 2nd Chapel Hill Conf.*, Univ. North Carolina, Chapel Hill, NC, May 1970, pp. 100–113.

[10] L. E. Dickson, *Linear Groups With an Exposition of the Galois Field Theory*. New York: Dover, 1958.

[11] J. F. Dillon, "Elementary Hadamard Difference Sets," Ph.D. dissertation, Univ. Maryland, College Park, 1974.

[12] J. F. Dillon, "Elementary Hadamard difference sets.," in *Proc. 6th S-E Conf. Combinatorics, Graph Theory, and Computing*, Boca Raton, FL, Feb. 1975, pp. 237–249, Congress Number XIV.

[13] J. F. Dillon and H. Dobbertin, "New cyclic difference sets with singer parameters," *Finite Fields Their Applic.*, vol. 10, pp. 342–389, 2004.

[14] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendalh, "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 613–627, Feb. 2006.

[15] S. W. Golomb and G. Gong, "Transform domain analysis of DES," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 2065–2073, Sep. 1999.

[16] T. Helleseth and V. A. Zinoviev, "On Z_4-linear Goethals codes and Kloosterman sums," *Des., Codes Cryptogr.*, vol. 17, no. 1–3, pp. 246–262, 1999.

[17] A. S. Kuzmin, V. T. Markov, A. A. Nechaev, and A. B. Shishkov, "Approximation of Boolean functions by monomial ones," *Discr. Math. Applic.*, vol. 16, no. 1, pp. 7–28, 2006.

[18] G. Lachaud and J. Wolfmann, "The weights of the orthogonals of the extended quadratic binary Goppa codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 3, pp. 686–692, May 1990.

[19] N. G. Leander, "Monomial bent functions," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 738–743, Feb. 2006.

[20] N. G. Leander and A. Kholosha, "Bent functions with 2^r Niho exponents," *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5529–5532, Dec. 2006.

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

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

[23] A. M. Youssef and G. Gong, "Hyper-Bent Functions," in *Advances in Cryptology—Eurocrypt'2001 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2001, vol. 2045, pp. 406–419.