Hyperbent functions, Kloosterman sums and Dickson polynomials

Pascale Charpin
INRIA, Codes
Domaine de Voluceau-Rocquencourt
BP 105 - 78153, Le Chesnay
France
Email: pascale.charpin@inria.fr

Guang Gong
Department of Electrical
and Computer Engineering,
University of Waterloo, Waterloo,
Ontario, N2L3G1, CANADA,
Email: 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. It implies notably that Kloosterman sums at point 1 on $\mathbf{F}_{2^m}$ cannot be zero, unless $m=4$. Further, we show that hyperbent functions with multiple trace terms can be described by means of Dickson polynomials.**

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

I. Introduction

Hyperbent functions were introduced by Youssef and Gong in [18]. 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 to 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 [12] (see (2) below). In [12], the authors proposed that *S*-boxes should not be approximated by a bijective monomial, providing a new criterion for the *S*-box design.

Further, Carlet and Gaborit established that hyperbent functions can be seen as some codewords of a cyclic code fully characterized by its non zeroes [2]. However, the classification of hyperbent functions is not achieved and many problems remain open.

In this paper we consider functions on $\mathbf{F}_{2^n}$, with $n=2m$, or on any subfield of $\mathbf{F}_{2^n}$. Section II is a preliminary section. Section III is devoted to monomial hyperbent functions. These famous bent functions, discovered by Dillon [8](1974), are strongly related with Kloosterman sums K_m. We focus on such function f_λ with $\lambda=1$. 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 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 the monomials, providing surprising results.

This paper is an extended abstract. All the proofs have to be found in our full paper [5].

II. 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 $\mathbf{F}_{2^r}$:

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

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 :

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

and its *extended Hadamard transform*

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

where $\gcd(k,2^n-1)=1$. Recall that, for even n, f is *bent* if and only if $\mathscr{F}(a)=\pm 2^{\frac{n}{2}}$ for all a. Also, f is said to be *balanced* if and only if $\mathscr{F}(0)=0$.

A. Hyperbent Functions

Youssef and Gong proposed in [18] to strength the bent concept by using the extended Hadamard transform.

Definition 1: Any Boolean function f on $\mathbf{F}_{2^n}$, $n=2m$, is said *hyperbent* if, for all a and for all k, $\mathscr{F}(a,k)\in\{\pm 2^m\}$.

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

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 $\mathbf{F}_{2^n}$ of the form:

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

Any hyperbent function of the form (3) belongs to the class $\mathscr{PS}_{ap}$, a subclass of the partial spread family $\mathscr{PS}^-$ introduced by Dillon [8, pp. 95-100].

Theorem 1: [8] 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 $\mathscr{PS}^-$, 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 [18, Theorem 1].

Theorem 2: Let γ be a generator of $\mathscr{G}$, the cyclic subgroup of $\mathbf{F}_{2^n}^*$ of order 2^m+1. 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.

To express precisely some 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 β_r.

B. Monomial hyperbent functions

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

$$f_\lambda(x) = Tr(\lambda x^{2^m-1})\ ,\quad \lambda \in \mathbf{F}_{2^m}. \tag{4}$$

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

$$K_m(\lambda) = \sum_{y \in \mathbf{F}_{2^m}} (-1)^{T_1^m(\frac{1}{y}+\lambda y)}, \tag{5}$$

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 [8], [9]:

Theorem 3: The function f_λ, defined by (4) 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 [14] for any m (even or odd). As a consequence, these authors proved that there are some λ such that $K_m(\lambda)=0$, for any m. But this proves the existence of such λ only, 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 III-B we present our main result in this context : we completely solve the case $\lambda=1$. Open Problem 2 can be restricted as follows (from a divisibility property of K_m [13]).

Lemma 1: If $T_1^m(\lambda)=1$ then $K_m(\lambda)\neq 0$, *i.e.*, the function f_λ, defined by (4) is not bent.

C. Dickson Polynomials

An excellent presentation of the work of Dickson can be found in [16]. In our approach, we follow several recent papers where the reader can find a basic overview [10], [11]. Here we introduce some useful properties, restricting ourselves to our context.

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

$$\begin{array}{l} D_0(x)=0 \text{ and } D_1(x)=x\ ; \\ D_{i+2}(x) = xD_{i+1}(x)+D_i(x). \end{array} \tag{6}$$

Using this definition, some basic properties are easily proved.

Proposition 1: The polynomials defined by (6) 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 $\gcd(i,2^{2m}-1)=1$.

III. Hyperbent Functions and Zeroes of Kloosterman sums

In this section, we study the monomial functions $x \mapsto Tr(x^{r(2^m-1)})$ over $\mathbf{F}_{2^n}$, $n=2m$. First, we are going to show that it is sufficient to treat the case $r=1$.

A. Monomial Functions

Recently, Leander [15] proposed another proof of Theorem 3, giving more informations on the spectrum of functions f_λ defined by (4). The next theorem (and its proof) is principally due to Leander. In our proof, we include the case $a=0$; we also consider the general form, $f_{\lambda,r}$ instead of f_λ.

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

$$f_{\lambda,r}(x) = Tr(\lambda x^{r(2^m-1)})\ ,\quad \lambda \in \mathbf{F}_{2^m}^*. \tag{7}$$

Recall that K_m is the Kloosterman sum on $\mathbf{F}_{2^m}$ (see (5)). We denote by $\mathscr{F}_\lambda(a)$ the Hadamard transform of $f_{\lambda,r}$ (see (1)). Then, for any $\lambda \in \mathbf{F}_{2^m}^*$,

$$\mathscr{F}_\lambda(0) = 2^m(1-K_m(\lambda))+K_m(\lambda). \tag{8}$$

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

$$\mathscr{F}_\lambda(a) = 2^m(-1)^{Tr(\lambda a^{r(2^m-1)})}+K_m(\lambda). \tag{9}$$

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

In the remaining of this section, we assume that $r=1$. We denote $f_{\lambda,1}$ by f_λ, *i.e.*, we come back to functions f_λ defined by (4). We begin by some preliminaries.

Lemma 2: Let $S_i=\gamma^i\mathbf{F}_{2^m}$, $0\le i\le 2^m$. The function f_λ is defined by (4). Then f_λ is constant on each S_i^*, equal to $Tr(\lambda\gamma^{-2i})$. Moreover f_λ is hyperbent if and only if

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

Remark 1: Consider again the functions $f_{\lambda,r}$, defined by (7). 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.*

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

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

Using Lemma 2, we deduce :

Corollary 1: The function f_λ on $\mathbf{F}_{2^n}$, $n = 2m$, is defined by (4). Then f_λ is hyperbent if and only if

$$\#\{\ u \in \mathbf{F}_{2^m} \mid T_1^m(\lambda u) = T_1^m(u^{-1}) = 1\ \} = 2^{m-2} \qquad (10)$$

We also can characterize the bentness of f_λ by its weight.

Lemma 3: Let f_λ, defined by (4). 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,

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

B. 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, we apply Lemma 1.

Lemma 4: If m is odd then $K_m(1) \neq 0$.

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

$$R_m = \{\ u \in \mathbf{F}_{2^m} \mid T_1^m(u) = T_1^m(u^{-1}) = 1\ \}. \qquad (11)$$

From Lemma 3, we know that

$$\#R_m = 2^{m-2} + \frac{K_m(1)}{4}. \qquad (12)$$

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 5: 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

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

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 $x^{2^k+1}+1$.

Lemma 6: 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 (11),(12).

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 5 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 $\mathscr{G}_k$, we get

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

Since

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

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 (11), completing the proof. ■

Lemma 7: Let $m = 2^r k$ where k is odd ($r, k \ge 1$). Then

$$\#L_{1,m} \equiv 0 \pmod{2^{r+1}}. \qquad (13)$$

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

Now, we are able to prove :

Theorem 6: Let $n = 2m$ with $m \le 2$. The Kloosterman sum

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

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 $m = 2^r k$, $r \ge 1$ and k odd. We have from Lemma 6:

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

By induction, one proves easily that

$$\#R_m = \#L_{1,m} + 2\#L_{1,2^{r-1}k} + \ldots + 2^{r-1}\#L_{1,2k} + 2^r\#R_k. \qquad (14)$$

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 (12)):

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

where $\varepsilon = 0$ if $k > 3$ and $\varepsilon = 1$ if $k = 3$. This is because $T_1^k(1) = 1$ implying $K_k(1) \equiv 4 \pmod 8$ (see [13]). 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 7, the equation (14) 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 7) and $r < m - 2$.

In both cases ($k > 1$ or $k = 1$) it 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. ∎

There is an immediate consequence of the previous theorem, considering again monomial functions of the form (7).

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 $n = 8$.

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 which has found to dealt 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 denoted $D_r \in \mathbf{F}_2[x]$ 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 $\mathbf{F}_{2^m}$:

$$f(x) = \sum_{r \in E} Tr(\beta_r x^{(2^m-1)r}) \text{ where } E \subseteq R,\ \beta_r \in \mathbf{F}_{2^m}, \quad (15)$$

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

$$g(x) = \sum_{r \in E} T_1^m(\beta_r D_r(x)) \quad (16)$$

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

$$\sum_{x \in \mathbf{F}_{2^m}} (-1)^{T_1^m(x^{-1}) + g(x)} = 2^m - 2wt(g). \quad (17)$$

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

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

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

$$N = \#\{\ j \mid \sum_{r \in E} T_1^m(\beta_r(\gamma^{rj} + \gamma^{-rj})) = 1\ \}. \quad (18)$$

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 (18) 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 (16).

Denote by h the function $x \mapsto T_1^m(x^{-1})$. To prove (17), we have to compute the Hadamard transform of the function $h + g$ in point 0, say $\mathscr{F}(0)$. We know that $\mathscr{F}(0) = 2^m - 2wt(h+g)$. 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, $\mathscr{F}(0) = 2^m - 2wt(g)$. ∎

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 $\mathscr{G}$ 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 (15). To illustrate our purpose we are going to treat some binomial functions of type (15). Let, for any $\lambda \in \mathbf{F}_{2^m}^*$,

$$f(x) = Tr\left(\lambda\left(x^{(2^r-1)(2^m-1)} + x^{(2^r+1)(2^m-1)}\right)\right) \quad (19)$$

with $0 < r < m$. Then, according to Theorem 7, we have

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

We apply the recursive definition of Dickson polynomials (see Section II-C) :

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

leads to $g(x) = T_1^m(\lambda x^{2^r+1})$. Hence, we can study the bentness of f, defined by (19), 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 (17)). 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 (19), 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 (19). To describe a subset of such functions is, in particular, to solve the next problem.

Open Problem 3: 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 $r=1$. For our next result, we use a property on the divisibility of the *inverse cubic* sums [4, Lemma 5].

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

$$f(x) = Tr\left(\lambda (x^{2^m-1} + x^{3(2^m-1)})\right). \qquad (20)$$

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.

C. Monomial Hyperbent Functions in Terms of Dickson Polynomials

Another interesting consequence of Theorem 7 concerns monomial functions defined by (7), $f_{\lambda,r}$ with $\lambda \in \mathbf{F}_{2^m}^*$. We assume that $\gcd(r, 2^{2m}-1))=1$ so that D_r is a permutation polynomial. Our main result is :

Theorem 9: Recall that K_m denotes the Kloosterman sum over $\mathbf{F}_{2^m}$ (see (5)). Dickson polynomials D_r (see Section II-C) are defined for any r coprime to $2^{2m}-1$ and $r \leq 2^m$. Let $\lambda \in \mathbf{F}_{2^m}^*$ be fixed. Then the functions $f_{\lambda,r}$ are bent if and only if one of these statements is satisfied :

(1) - $K_m(\lambda)=0$;

(2) - One proves for only one r that

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

(2) - All functions $x \mapsto T_1^m(x^{-1}+\lambda D_r(x))$ are balanced.

V. Conclusion

A number of recent papers are devoted to bent Boolean functions expressed by means of trace-functions [1], [2], [6], [10], [15]. In this paper, we contribute to the knowledge of this fascinating class of functions, by studying a subclass of the so-called $\mathscr{PS}^-$ class. Such functions are not yet classified, even when they are monomials.

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.

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 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.

References

[1] A. Canteaut, P. Charpin, and G. Kyureghyan, "A new class of monomial bent functions", *Finite Fields and Their Applications*, 14(1):221–241, January 2008.

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

[3] 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.

[4] 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.

[5] P. Charpin and G. Gong, "Hyperbent functions, Kloosterman sums and Dickson polynomials", submitted. Research report of the *Center for Applied Cryptographic Research* at University of Waterloo, CACR 2007-29.

[6] P. Charpin and G. Kyureghyan, "Cubic monomial bent functions: a subclass of $\mathscr{M}$" . *SIAM J. of Discrete Math.*, Vol. 22, N. 2, pp. 650-665, 2008.

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

[9] 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.

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

[11] 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.

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

[13] 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.

[14] 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.

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

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

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

[18] 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.