# Monomial Bent Functions and Stickelberger's Theorem

Philippe Langevin

*GRIM-USTV, university of Toulon, France.*

Gregor Leander

*ITSC, university of Bochum, Germany.*

**Abstract**

In this paper we use certain results on the divisibility of Gauss Sums, mainly Stickelberger's Theorem, to study monomial bent functions. This approach turns out to be especially nice in most of the known families of monomial bent functions. As one of our main results we give an alternative proof of bentness in the case of the Kasami exponent. Using the techniques developed here this proof turns out to be very short and generalizes the results from (7) to the case where $n$ is divisible by 3. Furthermore our approach can also be used to deduce properties of the dual function. More precisely we show that the dual of the Kasami function is not a monomial Boolean function.

*Key words:* Boolean functions, Bent functions, power functions, nonlinearity, Gauss sum, Stickelberger's conruences.

## 1 Introduction

Bent functions, being exceptional combinatorial objects, play an important role in different areas in coding theory as well as in cryptography. Although many concrete constructions of bent functions are known, the general structure of bent functions is still unclear. In particular a complete classification of bent functions seems hopeless today and it can therefore be useful to focus on special families. One special family is the class of monomial bent functions, i.e. of Boolean function represented as

*Email addresses:* `langevin@univ-tln.fr` (Philippe Langevin), `leander@itsc.ruhr-uni-bochum.de` (Gregor Leander).

Table 1
All known bent exponents up to $n = 24$.

| Type | Exponent $d$ | Conditions | Proven in |
|---|---|---|---|
| Gold | $2^r + 1$ | $\gcd(d, 2^n - 1) \neq 1$ , $\alpha \notin L^d$ | ? |
| Dillon | $2^k - 1$ | $K(\alpha) = -1$ | (6) |
| Kasami | $2^{2r} - 2^r + 1$ | $\gcd(r, n) = 1$ , $\alpha \notin L^d$ | (7) (for $\gcd(n, 3) = 1$) |
| MF | $(2^r + 1)^2$ | $n = 4r$, $r$ odd , $\langle\alpha\rangle = \mathbf{F}_{2^r}^*$ | (13) |
| ? | $2^{2r} + 2^r + 1$ | $n = 6r$, $\alpha \in ?$ | conj. in (2) |

$$\begin{aligned} \mathbf{F}_{2^n} &\to \mathbf{F}_2 \\ x &\mapsto \mathrm{tr}(\alpha x^d) \end{aligned}$$

for an exponent $d$ and a fixed coefficient $\alpha \in \mathbf{F}_{2^n}$. The class of monomial bent functions is in particular interesting for mainly two reasons. The only known non-normal bent functions are monomial bent functions, demonstrating that the study of these functions leads to new classes of bent functions. Furthermore it turns out that for each of the well studied families of bent function, there is a monomial bent function belonging to these classes.

**Known Bent Exponents** There are only (see table (1)) a few exponents $d$ known that allow the construction of bent functions. The Gold case belongs to the class of quadratic bent functions and there are several easy ways to compute the Walsh spectra of these functions. The Dillon exponent was considered first by Dillon in his PhD thesis (6) as an example of a bent function in the PS-class. The Kasami exponent is particular interesting as this exponent leads to non-normal bent functions, and therefor in particular to bent functions not linear equivalent to Maiorana McFarland or PS bent functions (see (4)). Despite the similarities to the Gold exponent the proof given by Dillon and Dobbertin in (7) is rather involved. The MF exponent was found by Canteaut and it turned out that the corresponding bent functions belong to the class of Maiorana McFarland bent functions (see (13)).

In this paper we are going to concentrate on the Dillon case first to illustrate the basic ideas. This case turns out to be especially nice with respect to the approach presented here. In the following sections the notion of the $\mathcal{J}$- and $\mathcal{K}$-Set is introduced, which turns out to be powerful tools to study in particular the Gold and the Kasami case. Most notably we are able to give a very short proof for the Kasami exponent that includes the case where $n$ is not coprime to 3 and show that the dual of the bent functions of the Kasami exponent are not monomial bent functions.

## 2 Divisibility of Gauss sums

Let $n$ be an even integer, say $n = 2k$. Let $L$ be a finite extention of degree $n$ of $\mathbf{F}_2$ and let $\mu_L$ the additive character of $L$ by definition, for all $x \in L$, $\mu_L(x) = (-1)^{\mathrm{tr}_L(x)}$ where $\mathrm{tr}_L$ is the absolute trace of $L$. A binary function $f$ from $L$ into $\{-1, +1\}$ is *bent* if and only if the absolute value of all its Fourier coefficients

$$\widehat{f}(a) = \sum_{x \in L} f(x)\mu_L(ax), \quad a \in L, \tag{1}$$

are equal to $2^k$. For a such function there exists a *dual* Boolean function $f^*$ such that $\widehat{f}(a) = (-1)^{f^*(a)}2^k$. Equivalently, due to Parseval's Equation, $f$ is bent if and only if all its Fourier coefficients (except may be one) have a dyadic valuation equal to $k$. In that case, the dual of $f$ is completely determined by estimations modulo $2^{k+2}$

$$\hat{f}(a) \equiv 2^k + 2^{k+1} f^*(a) \pmod{2^{k+2}} \tag{2}$$

This is the very simple idea that we want to apply to the monomial or more precisely to the the binary function $x \mapsto \mu_L(\alpha x^d)$ where $\alpha$ a non zero element of $L$ and $d$ a positive integer, $1 \leq d < 2^n - 1$.

We will consider the bent functions as functions defined over $L^\times$ instead of $L$. For this point of view, it is natural to decompose the function in the basis of multiplicative characters of $L$. Rightly, the Gauss sums

$$\tau_L(\chi) = -\sum_{x \in L^\times} \chi(x)\mu_L(x) \tag{3}$$

are the components of $-\mu_L$ in the basis of multiplicative characters. Note that the presence of the sign is classical. In other words,

$$\mu_L(x) = \frac{1}{1 - 2^n} \sum_{\chi \in \widehat{L^\times}} \tau_L(\chi)\bar{\chi}(x) \tag{4}$$

We now apply (4) twice to express the Fourier coefficient of the monomial binary function $f(x) = \mu_L(\alpha x^d)$, at a point $a \in L^\times$.

$$\begin{aligned}
\widehat{f}(a) &= 1 + \frac{1}{(2^n - 1)^2} \sum_{x \in L^\times} \sum_{\chi_1} \sum_{\chi_2} \tau_L(\chi_1)\bar{\chi}_1(\alpha x^d)\tau_L(\chi_2)\bar{\chi}_2(ax) \\
&= 1 + \frac{1}{(2^n - 1)^2} \sum_{\chi_1} \sum_{\chi_2} \tau_L(\chi_1)\tau_L(\chi_2)\bar{\chi}_1(\alpha)\bar{\chi}_2(a) \sum_{x \in L^\times} \bar{\chi}_1^d(x)\bar{\chi}_2(x) \\
&= 1 + \frac{1}{(2^n - 1)} \sum_{\chi} \tau_L(\chi)\tau_L(\bar{\chi}^d)\bar{\chi}(\alpha)\chi(a^d)
\end{aligned}$$

Finally we obtain the starting-point formula

$$\widehat{f}(a) = 1 + \frac{1}{(2^n-1)} \sum_{\chi \in \widehat{L^\times}} \tau_L(\chi)\tau_L(\bar{\chi}^d)\bar{\chi}(\alpha)\chi(a^d). \tag{5}$$

Note that we can continue by reducing modulo $2^n$:

$$\equiv 1 - \sum_{\chi \in \widehat{L^\times}} \tau_L(\chi)\tau_L(\bar{\chi}^d)\bar{\chi}(\alpha)\chi(a^d) \pmod{2^m}$$

Since $\tau_L(1) = 1$,

$$\widehat{f}(a) \equiv - \sum_{\chi \neq 1} \tau_L(\chi)\tau_L(\bar{\chi}^d)\bar{\chi}(\alpha)\chi(a^d) \pmod{2^m}$$

Since we are interested by dyadic approximations, we will consider multiplicative characters taking values in the unramified algebraic extension of degree $n$ of $\mathbf{Q}_2$ the field of dyadic rational numbers. We know that its residue field is a finite field of order $2^n$ that we identify with $L$. The Teichmüller character of $L$ is completely defined by the relation

$$\forall a \in L, \quad a = \Big(\omega(a) \mod 2\Big). \tag{6}$$

It is a character of order $2^n - 1$. A well known result of Stickelberger (16) claims that for all integer $0 \leq j < 2^n - 1$, the following congruence holds:

$$\tau_L(\bar{\omega}^j) \equiv 2^{\mathrm{wt}(j)} \pmod{2^{1+\mathrm{wt}(j)}} \tag{7}$$

where $\mathrm{wt}(j)$ is the binary weight of the residue of $j$ modulo $2^n - 1$. The above calculation and the result of Stickelberger shows the importance of the mapping $V\colon j \mapsto \mathrm{wt}(j) + \mathrm{wt}(-jd)$ where the operations over indices are done in the set of positive residues modulo $2^n - 1$.

We are ready to rediscover a result of Dillon as an illustration of the the dyadic method concerning the *Dillon exponent* of the form $d = 2^k - 1$.

**Lemma 1** *For all residue $j$, $0 < j < 2^n - 1$, we have $\mathrm{wt}(j) + \mathrm{wt}(-j) = n$. Moreover, if $j$ is not a multiple of $2^k + 1$ then $\mathrm{wt}(-jd) = k$.*

**PROOF.** We prove the the second part. Let $r$ be the remainder of the Euclidian division of $j$ by $2^k + 1$ since $jd = rd$ thanks to the first part it suffices to prove that for any positive integer $r$ less than $2^k + 1$ we have $\mathrm{wt}(rd) = k$. Let us denote by $\bar{b}$ the complement $1 - b$ of a bit $b$. Let $i$ the position of the first nonzero bit of $b$. The result of $(2^k - 1)r$ is given by the addition of $-r$ and $2^k - 1$ by :

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $-r$ | | $1$ | $1$ | $\dots$ | $1$ | $1$ | $\dots$ | $1$ | $\bar{r}_{k-1}$ | $\dots$ | $\bar{r}_{i+1}$ | $0$ | $1$ | $\dots$ | $1$ |
| $2^k r$ | | $r_{k-1}$ | $\dots$ | $r_{i+1}$ | $1$ | $0$ | $\dots$ | $0$ | $0$ | $0$ | $\dots$ | $0$ | $0$ | $\dots$ | $0$ |
| $2^k r - r$ | $1$ | $r_{k-1}$ | $\dots$ | $r_{i+1}$ | $0$ | $1$ | $\dots$ | $1$ | $\bar{r}_{k-1}$ | $\dots$ | $\bar{r}_{i+1}$ | $0$ | $1$ | $\dots$ | $1$ |
| | $0$ | $r_{k-1}$ | $\dots$ | $r_{i+1}$ | $0$ | $1$ | $\dots$ | $1$ | $\bar{r}_{k-1}$ | $\dots$ | $\bar{r}_{i+1}$ | $1$ | $0$ | $\dots$ | $0$ |

*binary expansion*

By the above Lemma, if $j$ is not a multiple of $(2^k + 1)$ then $V(j) > k$. More precisely:

$$\widehat{f}(a) \equiv 1 - \sum_{\chi^d=1} \tau_L(\chi)\bar{\chi}(\alpha) + 2^{k+1} \sum_{\mathrm{wt}(j)=1} \omega(\alpha)\bar{\omega}^j(a) \pmod{2^{k+2}}$$

Remark that $a \mapsto \sum_{\mathrm{wt}(j)=1} \omega(\alpha)\bar{\omega}^{jd}(a) \mod 2$ is nothing but the Boolean function $a \mapsto \mathrm{tr}(\alpha a^{-d})$ and we know (5) that its degree is either zero or equal to the weight of $-d$, and by Ax theorem (1) there exists $0 \neq a \in L$ such that $\mathrm{tr}(\alpha a^{-d}) = 0$. For such $a$,

$$\widehat{f}(a) \equiv 1 - \sum_{\chi^d=1} \tau_L(\chi)\bar{\chi}(\alpha) \pmod{2^{k+2}}$$

The $\chi$ that appear in the sum are lifted characters ((14), page 197) whence using Davenport-Hasse Theorem (same reference):

$$\begin{aligned} \widehat{f}(a) &\equiv 1 - \sum_{\lambda \in \widehat{K^\times}} \tau_L(\lambda \circ \mathrm{N}_{L/K})\bar{\lambda} \circ \mathrm{N}_{L/K}(\alpha) \pmod{2^{k+2}}. \\ &\equiv 1 - \sum_{\lambda \in \widehat{K^\times}} \Big(\tau_K(\lambda)\Big)^2 \bar{\lambda}(\mathrm{N}_{L/K}(\alpha)) \pmod{2^{k+2})} \end{aligned}$$

and by Fourier analysis, see e.g. the introduction of (10)

$$\begin{aligned} &\equiv 1 - (2^k - 1)\, \mu_K * \mu_K(\mathrm{N}_{L/K}(\alpha)) \pmod{2^{k+2}} \\ &\equiv 1 - (2^k - 1)\, \mathrm{Kloos}_K(\mathrm{N}_{L/K}(\alpha)) \pmod{2^{k+2}}, \end{aligned}$$

where $*$ denotes the product of convolution in the group algebra $\mathbf{Q}_2[K^\times]$, and $\mathrm{Kloos}_K(b)$ the Kloosterman sum $\sum_{x \in K^\times} \mu_K(x^{-1} + bx)$. The monomial function is bent if and only if $1 - (2^k - 1)\mathrm{Kloos}_K(\mathrm{N}_{L/K}(\alpha)) \equiv 0 \pmod{2^{k+2}}$ and since the modulus of a Kloosterman sum is less than or equal to $2^k - 1$ this implies $\mathrm{Kloos}_K(\mathrm{N}_{L/K}(\alpha)) = -1$.

**Theorem 2 (Dillon)** *Let $n$ be an even integer and let $d = 2^{n/2} - 1$. The function*

$$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$$

*with*

$$f(x) = \mathrm{tr}(\alpha x^d)$$

*is bent if and only if* $\mathrm{Kloos}_K(\mathrm{N}_{L/K}(\alpha)) = -1$*. In that case, the* $f^*(x) = \mathrm{tr}(\alpha^{2^k} x^d)$.

**PROOF.** By the above calculation the dual is equal to

$$\mathrm{tr}(\alpha x^{-d}) = \mathrm{tr}(\alpha^{2^k} x^d).$$

Note that the existence of Kloosterman sums equal to $-1$ which is not trivial is ensured by (12).

## 3 $\mathcal{J}$-$\mathcal{K}$-sets

From Stickelberger, the monomial $x^d$ defines a bent function if and only if

$$\sum_{\substack{V(j)\leq k\\ j>0}} \tau_L(\bar{\omega}^j)\tau_L(\omega^{jd})\omega^j(\alpha)\bar{\omega}^{jd}(a) \equiv 2^k \pmod{2^{k+1}} \tag{8}$$

For the Dillon exponent, the characters implied in the sum (8) form the group of lifted characters from $K$ to $L$ and that is the reason why we (easily) succeeded in solving Dillon case. In general, it will be difficult to determine the $j$'s such that $V(j) \leq k$, moreover the determination of the dual of a monomial bent function would require more precise approximations like the Gross-Koblitz formula (11; 15).

However, in the case where the exponent $d$ satisfies the strong conditions

$$\min_{0<j<2^n-1} V(j) = k, \qquad \text{and} \qquad V(j) = k \Longrightarrow jd = 0. \tag{9}$$

we can reduce the study of the monomial $\alpha x^d$ to the determination of two subsets of $\{1, 2, \ldots, n\}$ respectively defined by

$$\mathcal{J}_d = \{j \mid V(j) = k\} \qquad \mathcal{K}_d = \{j \mid V(j) = k+1\} \tag{10}$$

Under the condition (9) the equality (5) becomes :

$$\begin{aligned}\widehat{f}(a) &\equiv -\sum_{\chi\neq 1}\tau_L(\chi)\tau_L(\bar{\chi}^d)\bar{\chi}(\alpha)\chi(a^d) \pmod{2^{t+2}}\\ &\equiv -\sum_{j\in\mathcal{J}_d}\tau_L(\bar{\omega}^j)\omega^j(\alpha)+\sum_{j\in\mathcal{K}_d}\tau_L(\bar{\omega}^j)\tau_L(\omega^{-jd})\omega^j(\alpha)\bar{\omega}^{jd}(a).\end{aligned}$$

The following Theorem summarizes the result.

**Theorem 3** *Let $d$ be an integer satisfying the conditions (9). The binary function $\mu_L(\alpha x^d)$ is bent if and only if $\sum_{j\in\mathcal{J}_d}\alpha^j=1$ and, in that case, the dual of $f$ is equal up to one to $\sum_{j\in\mathcal{K}_d}\alpha^j a^{-jd}$.*

**PROOF.** The function is bent iff the dyadic valuation of $\sum_{j\in\mathcal{J}_d}\tau_L(\bar{\omega}^j)\omega^j(\alpha)$ is constant. That implies $\sum_{j\in\mathcal{J}_d}\omega^j(\alpha)\equiv 1 \pmod{2^1}$ or by definition of the Teichmüller character $\sum_{j\in\mathcal{J}_d}\alpha^j=1$ whence there exists $\epsilon\in\{0,1\}$ such that $\sum_{j\in\mathcal{J}_d}\tau(\bar{\omega}^j)\omega^j(\alpha)\equiv 2^k+\epsilon 2^{k+1}\equiv 1 \pmod{2^{k+2}}$. Applying (2), we get :

$$f^*(a)2^{k+1}\equiv \epsilon 2^{k+1}+\sum_{j\in\mathcal{K}_d}\tau_L(\bar{\omega}^j)\tau_L(\omega^{-jd})\omega^j(\alpha)\bar{\omega}^{jd}(a) \pmod{2^{k+2}}.$$

Collecting the terms of valuation $k+1$, we obtain $f^*(a)\equiv\epsilon+\sum_{j\in\mathcal{K}_d}\omega^j(\alpha)\bar{\omega}^{jd}(a)$ $\pmod{2^1}$.

Thus on one hand, to determine the set $\mathcal{J}_d$ is equivalent to find the set of $\alpha\in L$ such that $\alpha x^d$ gives a bent function. On an other hand, to determine the polynomial expression for the dual is equivalent to find the $\mathcal{K}_d$. This theorem will be the key tool for our approach to prove the bent property in the Gold and the Kasami case.

## 4 Gold

The Gold exponent is of the form $2^r+1$, sometimes with certain conditions on $r$. As the corresponding power function has degree two only, this exponent is usually the easiest to deal with. The following theorem describes also the dual of the bent function.

**Theorem 4** *Let $\alpha\in\mathbf{F}_{2^n}$, $r\in\mathbb{N}$ and $d=2^r+1$. The function*

$$f : L\to\mathbb{F}_2$$

*with*

$$f(x)=\mathrm{tr}(\alpha x^d),$$

*is bent if and only if*

$$\alpha \notin \{x^d \mid x \in \mathbf{F}_{2^n}\}$$

*The dual of $f$ is given by*

$$f^*(a) = f(H^{-1}(a^{2^r})) + f^*(0),$$

*where*

$$H(a) = \alpha^{2^r} a^{2^{2r}} + \alpha a.$$

□

Thus for an exponent of the Gold-type there exist an $\alpha \in L$ such that the corresponding Boolean function is bent if and only if $x \mapsto x^d$ is not a bijection.

### *4.1 $\mathcal{J}$-Set*

The computation of the $\mathcal{J}$-Set is particular easy in the Gold case. The minimal value of $V(j)$ for the Gold exponent was determined in (9) to be $n/2 = k$. Thus computing the $\mathcal{J}$-set means to determine the elements $1 \leq j \leq 2^n - 2$ such that

$$\mathrm{wt}(j) + \mathrm{wt}(-(2^r + 1)j) = k,$$

and in particular we see that

$$\mathrm{wt}(j) \leq k.$$

Assuming $(2^r + 1)j \neq 0 \bmod 2^n - 1$ then $j \in \mathcal{J}_d$ iff

$$\mathrm{wt}(j) - \mathrm{wt}((2^r + 1)j) = -k$$

Furthermore

$$\mathrm{wt}((2^r + 1)j) \leq 2\mathrm{wt}(j)$$

and it follows that $\mathrm{wt}(j) = k$, a contradiction as this implies

$$\mathrm{wt}((2^r + 1)j) = 0.$$

On the other hand if $(2^r + 1)j = 0 \bmod 2^n - 1$ it follows that

$$j^{<<r} + j = 2^n - 1$$

where $j^{<<r} = \sum 2^i j_{i-r}$ is the cyclic shift of $j$ by $r$ positions. In particular at each position $i \in \{0, \ldots, n-1\}$ exactly one of the values $j_i$ and $j_{i-r}$ equals one. Thus

$$\mathrm{wt}(j^{<<r} + j) = 2\mathrm{wt}(j) = \mathrm{wt}(2^n - 1) = n$$

and we conclude that

$$(2^r + 1)j = 0 \bmod 2^n - 1 \quad \Rightarrow \quad V(j) = k$$

and furthermore

$$\mathcal{J}_d = \left\{ i\left(\frac{2^n-1}{g}\right) \mid i = 1, \ldots, g-1 \right\},$$

where $g = \gcd(s, 2^n - 1)$.

As a corollary we get that $f$ is bent iff and only if

$$\sum_{j \in \mathcal{J}_d} \alpha^j = \sum_{i=1}^{g-1} \alpha^{i(2^n-1)/g} = 1,$$

which is equivalent to

$$\alpha \notin L^d = L^g.$$

### *4.2 $\mathcal{K}$-Set*

In order to determine the dual of the bent functions in the Gold case, we have to compute the $\mathcal{K}_d$-set. Using the same arguments as before we see that the elements in $\mathcal{K}_d$ have all the same weight.

$$\forall j \in \mathcal{K}_d, \quad \mathrm{wt}(j) = k - 1$$

and

$$\mathrm{wt}((2^r + 1)j) = 2\mathrm{wt}(j).$$

**Remark 5** *Note that this in particular implies*

$$\mathrm{wt}(-(2^r + 1)j) = n - \mathrm{wt}((2^r + 1)j) = 2,$$

*and thus the well known fact, that the dual is of the (quadratic) Gold bent function is again quadratic.*

We are going to treat the case $r = 1$ only, the case $r \neq 1$ is similar. To this end we are going to apply the "digits and carry"-approach, as explained in (9). The corresponding equation for the for the Gold case is

$$2c_i + s_i = j_{i-1} + j_i + c_{i-1} \tag{11}$$

where $c_i, s_i, j_i \in \{0, 1\}$ for all $i$. For the elements in the $\mathcal{K}_d$-Set using $\mathrm{wt}((2^r + 1)j) = 2\mathrm{wt}(j)$, we see that all "carrys" $c_i$ are zero. Considering (11) obviously at most one of the positions $j_i$ and $j_{i-1}$ can be non-zero. In particular we get the implication

$$j_i = 1 \Rightarrow j_{i+1} = 0.$$

It follows that in the binary expansion of $j$ we have pairs $(j_i, j_{i+1}) = (1,0)$ for exactly $k-1$ indices $i$ and two additional zeros on arbitrary positions. Without loss of generality we assume that the binary expansion of $j$ starts with one of these additional zeros. Due to cylcotomic equivalence we can furthermore assume that the second additional zeros is at a position $i \le k$. Thus $j$ is of the following form

$$\begin{aligned}
&j = (0, 0, (1,0), (1,0), (1,0), \ldots, (1,0)) \\
&j = (0, (1,0), 0, (1,0), (1,0), \ldots, (1,0)) \\
&j = (0, (1,0), (1,0), 0, (1,0), \ldots, (1,0)) \\
&\vdots \quad \vdots
\end{aligned}$$

In other words we see that

$$[\mathcal{K}_d] = \{ \sum_{i=0}^{(t-3)/2} 2^{2i+1} + \sum_{i=0}^{k-1} 2^{2i} \mid t \le k \text{ and } odd \}.$$

is the set $\mathcal{K}_d$ reduced by cyclotomic equivalence. Its size depends on the parity of $k$.

$$\#[\mathcal{K}_d] = \begin{cases} k/2 & k \text{ even} \\ (k+1)/2 & k \text{ odd} \end{cases}$$

For the size of the complete $\mathcal{K}$-set, if we include the cyclotomic equivalent elements, we get

$$\#\mathcal{K}_d = k^2.$$

In particular we can deduce a polynomial representation of the dual of $f$.

$$f^*(x) = \sum_{j \in \mathcal{K}_d} \alpha^j x^{(2^r+1)j}.$$

If $k$ is even this can be expressed as

$$f^*(x) = \operatorname{tr}\left( \sum_{j \in [\mathcal{K}_d]} \alpha^j x^{(2^r+1)j} \right)$$

If $k$ is odd then there exists exactly one $j_0 \in \mathcal{K}_d$ such that $2^k j_0 = j_0$ and in this case the dual can be expressed as

$$f^*(x) = \operatorname{tr}\left( \sum_{j \in [\mathcal{K}_d] \setminus \{j_0\}} \alpha^j x^{(2^r+1)j} \right) + \sum_{i=0}^{k-1} \left( \alpha^{j_0} x^{(2^r+1)j_0} \right)^{2^i}.$$

## 5 Kasami

The following theorem was conjectured by Hollmann and Xiang in 1999 ((9), Conjecture 4.4) and was proven by Dillon and Dobbertin in (7).

**Theorem 6** *Let $n$ be an even integer with $\gcd(3, n) = 1$. Furthermore let $d = 2^{2r} - 2^r + 1$ with $\gcd(r, n) = 1$ and $\alpha \in \mathbf{F}_{2^n}$. The function*

$$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$$

*with*

$$f(x) = \mathrm{tr}(\alpha x^d)$$

*is bent if and only if $\alpha \notin \{x^3 | x \in \mathbf{F}_{2^n}\}$.*

The proof of this theorem given by Dillon and Dobbertin is based on quadratic forms and is rather involved. Note that there is also an alternative proof using the multivariate method proposed by Dobbertin (8).

### *5.1 A new Proof for the Kasami bent functions*

We give an alternative proof of Theorem 6 using the techniques developed above. Our approach also includes the case where $n$ is divisible by 3. We anticipate that this extension is also possible carefully studying the ideas in (7), however the technique relies heavily on the fact that in the case where $\gcd(n, 3) = 1$ the coefficient $\alpha$ can be taken without loss of generality form $\mathbf{F}_4$, which generally is false.

The minimal value of $V(j)$ for the Kasami exponent was already determined in (9) to be $k$. By extending the ideas from (9) we will be able to compute the $\mathcal{J}_d$-Set. Once knowing the $\mathcal{J}_d$-set the statement follows immediately. As explained in (9) the equation for the "digits and carry"-approach in the Kasami case is

$$2c_i + s_i = j_{i-2r} - j_{i-r} + j_i + c_{i-1}. \tag{12}$$

Adding this equation to the same equation shifted by $r$ we get

$$2(c_i + c_{i-r}) + s_i + s_{i-r} = j_{i-2r} + j_i + (c_{i-1} + c_{i-r}). \tag{13}$$

In particular, as explained by Hollmann and Xiang it follows that

$$c_i + c_{i-r} \in \{-1, 0, 1\}.$$

In the case of the Kasami exponent the "weight" of the carry values are directly connected to the value $V(j)$, namely

$$\sum c_i = \sum j_i - \sum s_i = \mathrm{wt}(j) - \mathrm{wt}(jd).$$

For the moment we will assume that there exist an $i$ such that $s_i \neq 0$ for an element in the $\mathcal{J}_d$-set. It then follows that

$$n + \sum c_i = \mathrm{wt}(j) + n - \mathrm{wt}(s) = V(j) = \frac{n}{2}$$

and thus $\sum c_i = -n/2$. Taking into account that $\sum c_i = -k$, as $c_i + c_{i-r} \in \{0, \pm 1\}$ for all $i$, it follows that $c_i \in \{0, -1\}$ for all $i$ in this case and furthermore

$$(c_i, c_{i-r}) \in \{(0, -1), (-1, 0)\}.$$

We are left with only two possible sequences $(c_0, c_r, c_{2r}, \ldots c_{r(n-1)})$ of carries, namely

$$(-1, 0, -1, 0, \ldots, -1, 0)$$

and

$$(0, -1, 0, -1 \ldots, 0, -1).$$

As $r^{-1} \bmod n$ is odd, reordering the sequences we conclude that for the sequence $(c_0, c_1, \ldots, c_{i-1})$ we obtain exactly the same two possible values. In particular we have the following implication.

$$c_i = -1 \Rightarrow c_{i-1} = c_{i-r} = c_{i-1-2r} = 0 \text{ and } c_{i-2r} = c_{i-r-1} = -1$$

Given an index $i$ such that $c_i = -1$ using equation (12) we conclude that

$$j_{i-2r} = j_i = 0\ ,\ j_{i-r} = 1 \text{ and } s_i = 1.$$

Considering (13) we see that $s_{i-r} = j_{i-3r}$ and furthermore shifting equation (12) by $-2r$, we get

$$2c_{i-2r} + s_{i-2r} = j_{i-4r} - j_{i-3r} + j_{i-2r} + c_{i-1-2r}.$$

Now again $c_{i-2r} = 1$ and $c_{i-1-2r} = 0$. Thus $j_{i-3r} = 1$ and so $s_{i-r} = 1$ as well. Finally $s_i = 1$ for all possible indices $i$. But this means nothing else, then

$$s = jd = 2^n - 1 = 0 \bmod 2^n - 1.$$

On the other hand it is easy to verify that if $jd = 0 \bmod 2^n - 1$ than $V(j) = n/2$.

Putting things together we have proven that

$$j \in \mathcal{J}_d \Leftrightarrow jd = 0 \bmod 2^n - 1,$$

in other words, as $\gcd(d, 2^n - 1) = 3$

$$\mathcal{J}_d = \left\{ \frac{2^n - 1}{3}, \frac{2(2^n - 1)}{3} \right\}.$$

Using theorem 3 we see that

$$f(x) = \mathrm{tr}(\alpha x^d)$$

is bent if and only if

$$\alpha^{\frac{2^n-1}{3}} + \left(\alpha^{\frac{2^n-1}{3}}\right)^2 + 1 = 0,$$

which is equivalent to

$$\alpha^{\frac{2^n-1}{3}} \neq 1,$$

i.e. $\alpha$ is not a 3-rd power.

### *5.2 $\mathcal{K}$-Set*

Very little is known about the dual of the bent functions with the Kasami exponent. The main result of this section is, that the dual of the Kasami is not a monomial bent function. This again shows how useful the framework developed here is. In some sense it allows to compute the terms in the trace expansion of the dual function separately.

The following lemma essentially provides all the necessary ingredients for our result.

**Lemma 7** *Let $n$ be an even integer $n = 2k$ and $r \leq k$ be an odd integer. Furthermore let $d = 2^{2r} - 2^r + 1$ then for*

$$j := \frac{2^n - 1}{3} + (2^r + 1)$$

*the following properties hold.*

*(1)* $\mathrm{wt}(j) = k + 1$      *(2)* $\mathrm{wt}(j + \frac{2^n-1}{3}) = k + 1$

*(3)* $\mathrm{wt}(j + 2\frac{2^n-1}{3}) = 2$      *(4)* $\mathrm{wt}(jd) = 2$

**PROOF.** To prove the first property we rewrite $j$ as

$$j = \left(\frac{2^n - 1}{3}\right) + (2^r + 1) \equiv \left(\sum_{i=0}^{k-1} 4^i\right) + 2^r + 1 \pmod{2^n - 1}$$

The first term consist of all $k$ "even bits", $2^r$ consists of one odd bit and finally 1 consists of one "even bit". Thus the weight of $j$ is $k+1$. The second property follows using similar arguments.

For the third claim we note that

$$j + 2\frac{2^n-1}{3} = j - \frac{2^n-1}{3} = 2^r + 1 \pmod{2^n-1}.$$

The fourth property follows easily as

$$\begin{aligned} jd &= \left(\frac{2^n-1}{3}\right)d + (2^r+1)d \pmod{2^n-1} \\ &= 0 + (2^r+1)\left(\frac{2^{3r}+1}{2^r+1}\right) \pmod{2^n-1} \\ &= 2^{3r}+1 \pmod{2^n-1} \end{aligned}$$

and $3r \neq 0 \bmod n$.

With Lemma 14 we can easily deduce that the dual of the Kasami bent function is not a monomial function. First note that the dual function is a non-quadratic function for $r > 1$. Thus in the trace expansion of the dual there is at least on non-quadratic term and it is therefor enough to prove the existence of an element $j$ in $\mathcal{K}_d$ such that $jd$ has weight 2. Furthermore we have to ensure that not all three elements (i.e. all the residues $j$ solutions of the $jd = 2^{3r}+1$)

$$j, j + \frac{2^n-1}{3}, j + 2\frac{2^n-1}{3}$$

are elements in $\mathcal{K}_d$ as (only) in this case the term $jd$ in the trace expansion will cancel out.

All these properties are exactly fulfilled by the element $-j$ specified in Lemma 14. The element $-j$ is in $\mathcal{K}_d$ as

$$\mathrm{wt}(-j) + \mathrm{wt}(-(-js)) = n - \mathrm{wt}(j) + wt(js) = k+1.$$

Noting that $3r \neq k \bmod n$ we see that in the trace expansion of the dual function we get

$$\mathrm{tr}\left(\left(\alpha^{-j} + \alpha^{-j+(2^n-1)/3}\right)x^{jd}\right) = \mathrm{tr}\left(\alpha^{-j}\left(1 + \alpha^{\frac{2^n-1}{3}}\right)x^{jd}\right)$$

Now, as seen in the last section we know that

$$\alpha^{\frac{2^n-1}{3}} + \left(\alpha^{\frac{2^n-1}{3}}\right)^2 + 1 = 0$$

Table 2
Notations of this paper

| | |
|---|---|
| $n$ | an even integer $n = 2k$ |
| $K$ | the field of order $2^k$ |
| $L$ | the field of order $2^n$ |
| $\mathrm{tr}_L$ | the absolute trace of $L$ |
| $\mathrm{tr}_{L/K}$ | the trace of $L$ over $K$ |
| $d$ | an exponent |
| $\mathbf{Q}_2$ | the field of dyadic rational numbers |
| $\mu_K$ | additive canonical character of $K$ |
| $\mu_L$ | additive canonical character of $L$ |
| $\chi$ | a multiplicative character of $L$ |
| $\lambda$ | a multiplicative character of $K$ |
| $\omega$ | the Teicmüller character of $L$ |
| $j$ | an integer, positive residue modulo $2^n - 1$ |
| $\mathrm{wt}(j)$ | the binary weight of $j$. |
| $V(j)$ | $\mathrm{wt}(j) + \mathrm{wt}(-dj)$ |
| $f * g$ | product of convolution in $K$ |
| | $f * g(z) = \sum_{xy=z\in K^*} f(x)g(y)$ |
| $\mathrm{Kloos}_K(y)$ | Kloosterman sum in $K$ |
| | $\sum_{x\in K^*} \mu_K(x^{-1} + yx)$. |

and thus we have

$$\mathrm{tr}(\alpha^{-2^r-1}x^{2^{3r}+1})$$

as one term in the trace expansion of the dual. Finally note that this term is not constant zero, as can be seen by the Weil bound (17) for example.

It should be noted that we presently cannot answer the more interesting question wether the dual is linear or affine equivalent to an monomial bent function. However, based on numerical results, we conjecture that the dual is not linear equivalent to any monomial bent function for $n > 8$.

**Problem 8** *As we saw both the Gold exponent and the Kasami exponent satisfy (9). Do there exist other exponents satisfying these very strong conditions ?*

## References


[1] J. Ax, *Zeroes of polynomials over finite fields*, American Journal of Mathematics, 86, pp 256–261, 1964.

[2] A. Canteaut, private communication, June 2004

[3] Carlitz L. and Uchiyama S., *Bounds for Exponential Sums*, Duke Math. Journal, pp 37-41, 1957.

[4] A. Canteaut, M. Daum, H. Dobbertin, G. Leander, *Finding Non-Normal Bent Functions*, special issue on Coding and Cryptography, Discrete Applied Mathematics, to appear.

[5] C.Carlet *Codes de Reed-Muller, codes de Kerdock et de Preparata*. PhD thesis, Université Paris 6, 1990.

[6] J.F. Dillon, *Elementary Hadamard Difference sets*, PhD thesis, University of Maryland, 1974.

[7] J.F. Dillon and H. Dobbertin, *New Cyclic Difference Sets with Singer Parameters*, Finite Fields And Applications, 2004, pp. 342-389.

[8] H. Dobbertin, private communication

[9] H.D.L. Hollmann and Q. Xiang, *A Proof of the Welch and Niho Conjectures on Crosscorrelations of Binary m-sequences*, Finite Fields Appl. 7 (2001), 253–286.

[10] N. M. Katz, Sommes exponentielles *SMF*, astérisque 79 , 1979.

[11] N. Koblitz, $p$-adic Analysis: a Short Course on Recent Work. *LMS*, LNS-46, 1980.

[12] G. Lachaud, J. Wolfmann, Kloosterman sums, elliptic curves and cyclic codes in characteristic 2, C. R. Acad. Sci. Paris Sr. I Math. 305, no. 20, 881–883, 1987.

[13] G. Leander *Monomial Bent Functions,* Proceedings of the Workshop on Coding and Cryptography (WCC 2005), Bergen, Norway, March 2005.

[14] R. Lidl, N. Niederreiter, *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications.* Addison-Wesley, 1983.

[15] A. Robert, The Gross-Koblitz formula revisited *Rend. Sem. Matematico Padova*, vol. 105, 2001.

[16] J. Stickelberger, Uber eine verallgemeinerung der kreistheilung. *Math. Ann.*, 37:321–367, 1890.

[17] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. USA, 34, 1948.