On bent and hyper-bent functions via Dillon-like exponents

Sihem Mesnager[1] **and Jean-Pierre Flori** [2]

[1]University of Paris VIII and University of Paris XIII
Department of mathematics,
LAGA (Laboratory Analysis, Geometry and Application),
France
[2] ANSSI (Agence nationale de la sécurité des systemes d'information), France

Code-based Cryptography Workshop 2012
Lyngby, Copenhagen, May 9, 2012

Outline

1. Background on bent functions and hyper-bent functions
2. New results on bent and hyper-bent functions with multiple trace terms via Dillon-like exponents
3. Conclusion

Background on Boolean functions : representation

$f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ an n-variable Boolean function.

☞ We identify the vectorspace $\mathbb{F}_2^n$ with the Galois field $\mathbb{F}_{2^n}$

Definition

Let n be a positive integer. Every Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion called its **polynomial form :**

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

Definition (Absolute trace over $\mathbb{F}_2$)

Let k be a positive integer. For $x \in \mathbb{F}_{2^k}$, the (absolute) trace $Tr_1^k(x)$ of x over $\mathbb{F}_2$ is defined by :

$$Tr_1^k(x) := \sum_{i=0}^{k-1} x^{2^i} = x + x^2 + x^{2^2} + \cdots + x^{2^{k-1}} \in \mathbb{F}_2$$

Background on Boolean functions : representation

DEFINITION

Let n be a positive integer. Every Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion called its **polynomial form :**

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

- Γ_n is the set obtained by choosing one element in each cyclotomic class of 2 modulo $2^n - 1$,
- $o(j)$ is the size of the cyclotomic coset containing j (that is, $o(j)$ is the smallest positive integer such that $j2^{o(j)} \equiv j \pmod{2^n - 1}$),
- $\epsilon = wt(f)$ modulo 2.

Recall :

DEFINITION (THE HAMMING WEIGHT OF A BOOLEAN FUNCTION)

$$wt(f) = \#supp(f) := \#\{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$$

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ a Boolean function.

- **General upper bound on the nonlinearity of any n-variable Boolean function : $\mathrm{nl}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$**

DEFINITION (BENT FUNCTION [ROTHAUS 1976])

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be a bent function if $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$

DEFINITION (THE DISCRETE FOURIER (WALSH) TRANSFORM)

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

where "Tr_1^n" is the absolute trace function on $\mathbb{F}_{2^n}$.

- **A main characterization of bentness :**

$$(f \text{ is bent }) \iff \widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}, \quad \forall \omega \in \mathbb{F}_{2^n}$$

Notation : in this talk we use sometime $\chi(*) := (-1)^*$

Bent and "hyper-bent "Boolean functions

Definition (hyper-bent Boolean function [Youssef-Gong 2001])

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be a hyper-bent if the function $x \mapsto f(x^i)$ is bent , for every integer i co-prime to $2^n - 1$.

- (f is hyper-bent) $\Rightarrow$ (f is bent)
- Hyper-bent functions have properties still stronger than the well-known bent functions which were already studied by Dillon [Dillon 1974] and Rothaus [Rothaus 1976] more than three decades ago. They are interesting in cryptography, coding theory and from a combinatorial point of view.
- Hyper-bent functions were initially proposed by Golomb and Gong [Golomb-Gong 1999] as a component of S-boxes to ensure the security of symmetric cryptosystems.
- Hyper-bent functions are rare and whose classification is still elusive.

☞ Therefore, not only their characterization, but also their generation are challenging problems.

For any bent/hyper-bent Boolean function f defined over $\mathbb{F}_{2^n}$:

- Polynomial form :

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

  - Γ_n is the set obtained by choosing one element in each cyclotomic class of 2 modulo $2^n - 1$,
  - $o(j)$ is the size of the cyclotomic coset containing j,

PROBLEM (HARD)

Characterize classes of bent / hyper-bent functions in polynomial form, by giving explicitly the coefficients a_j.

(Hyper)-bentness can be characterized by means of Kloosterman sums :
$K_n(a) := \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(ax+\frac{1}{x})}$

- It is known since 1974 that the zeros of Kloosterman sums give rise to (hyper)-bent functions.
  [Dillon 1974] ($r=1$)[Charpin-Gong 2008] (r such that $gcd(r, 2^m+1)=1$) :
  Let $n=2m$. Let $a \in \mathbb{F}_{2^m}^\star$

$$\begin{array}{rcccl} f_a^{(r)} & : & \mathbb{F}_{2^n} & \longrightarrow & \mathbb{F}_2 \\ & & x & \longmapsto & Tr_1^n(ax^{r(2^m-1)}) \end{array}$$

  then : f_a is (hyper)-bent if and only if $K_m(a)=0$.

- In 2009 we have shown that the value 4 of Kloosterman sums leads to constructions of (hyper-)bent functions.
  [Mesnager 2009] : Let $n=2m$ (m odd). Let $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_4^\star$.

$$\begin{array}{rcccl} f_{a,b}^{(r)} & : & \mathbb{F}_{2^n} & \longrightarrow & \mathbb{F}_2 \\ & & x & \longmapsto & Tr_1^n\left(ax^{r(2^m-1)}\right) + Tr_1^2\left(bx^{\frac{2^n-1}{3}}\right) ; gcd(r, 2^m+1) = 1 \end{array}$$

  then : $f_{a,b}^{(r)}$ is (hyper)-bent if and only if $K_m(a)=4$.

• [Charpin-Gong 2008] have studied the hyper-bentness of Boolean functions which are sum of several Dillon-like monomial functions :
Let $n = 2m$. Let E' be a set of representatives of the cyclotomic cosets modulo $2^m + 1$ for which each coset has the maximal size n. Let f_{a_r} be the function defined on $\mathbb{F}_{2^n}$ by

$$f_{a_r}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) \qquad (1)$$

where $a_r \in \mathbb{F}_{2^m}$ and $R \subseteq E'$.

- ☞ when r is co-prime with $2^m + 1$, the functions f_{a_r} are the sum of several Dillon monomial functions.
- ☞ characterization of hyper-bent functions of the form (1) has been given by means of Dikson polynomials.

Definition

The Dickson polynomials $D_r(X) \in \mathbb{F}_2[X]$ is defined by

$$D_r(X) = \sum_{i=0}^{\lfloor \frac{r}{2} \rfloor} \frac{r}{r-i} \binom{r-i}{i} X^{r-2i}, \quad r = 2, 3, \cdots$$

- In 2010, we have extended such an approach to treat Charpin-Gong like function with an additional trace term over $\mathbb{F}_4$:

Theorem ([Mesnager 2010])

Let $n = 2m$ with m odd. Let $b \in \mathbb{F}_4^\star$ and β be a primitive element of $\mathbb{F}_4$. Let $f_{a_r,b}$ defined on $\mathbb{F}_{2^n}$ by

$$f_{a_r,b}(x) = \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$$

where $a_r \in \mathbb{F}_{2^m}$. Let g_{a_r} defined on $\mathbb{F}_{2^m}$ by $\sum_{r\in R} Tr_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r.

1. $f_{a_r,\beta}$ is (hyper-)bent if and only if, $\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g_{a_r}(D_3(x))\Big) = -2$; equivalently, $\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(Tr_1^m(x^{-1}) + g_{a_r}(D_3(x))\Big) = 2^m - 2wt(g_{a_r} \circ D_3) + 4$.
2. $f_{a_r,1}$ is (hyper-)bent if and only if, $2\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g_{a_r}(D_3(x))\Big) - 3\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g_{a_r}(x)\Big) = 2.$

• In 2010, we have extended such an approach to treat Charpin-Gong like function with an additional trace term over $\mathbb{F}_4$ with m odd (i.e. $m \equiv 1 \pmod 2$).
• Adopting the approach developed by Mesnager [Mesnager 2010], Wang et al. [Wang-Tang-Qi-Yang-Xu 2011] studied in late 2011 the following family with an additional trace term on $\mathbb{F}_{16}$:

$$f_{a,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^4(bx^{\frac{2^n-1}{5}})$$

where some further restrictions lie on the coefficients a_r, the coefficient b is in $\mathbb{F}_{16}$ and m must verify $m \equiv 2 \pmod 4$.

☞ Both these approaches are quite similar and crucially depend on the fact that the hypothesis made on m implies that 3 or 5 do not only divide $2^n - 1$, but also $2^m + 1$.

Here, we show how such approaches can be extended to an infinity of different trace terms, covering all the possible Dillon-like exponents. In particular, we show that they are valid for an infinite number of other denominators, e.g 9, 11, 13,17, 33 etc. To this end, we consider a function of the general form

$$f_{a,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^t(bx^{s(2^m-1)})$$

where

- $n = 2m$ is an even integer,
- R is a set of representatives of the cyclotomic classes modulo $2^m + 1$,
- the coefficients a_r are in $\mathbb{F}_{2^m}$,
- s divides $2^m + 1$, i.e $s(2^m - 1)$ is a Dillon-like exponent. Set $\tau = \frac{2^m+1}{s}$.
- $t = o(s(2^m - 1))$, i.e t is the size of the cyclotomic coset of s modulo $2^m + 1$,
- the coefficient b is in $\mathbb{F}_{2^t}$.

☞ Our objective is to show how we can treat the property of hyper-bentness in this general case.

The following partial exponential sums are a classical tool to study hyper-bentness.

DEFINITION

Let $U = \{u \in \mathbb{F}_{2^n}^* \mid u^{2^m+1} = 1\}$. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function. We define $\Lambda(f)$ as :

$$\Lambda(f) = \sum_{u \in U} \chi_f(u)$$

THEOREM

Let $f_{a,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^t(bx^{s(2^m-1)})$. Then

$f_{a,b}$ is (hyper)-bent if and only if $\Lambda(f_{a,b}) = 1$.

Let

- $V = \{v \in \mathbb{F}_{2^n}^* \mid v^s = 1\}$,
- $U = \left\{u \in \mathbb{F}_{2^n}^* \mid u^{2^m+1} = 1\right\}$ and ζ is a generator of U,
- $W = \{w \in \mathbb{F}_{2^n}^* \mid w^\tau = 1\}$.

The set U can be decomposed as $U = \bigcup_{i=0}^{\tau-1} \zeta^i V = \bigcup_{i=0}^{s-1} \zeta^i W$.

Definition

Let $f_a(x) = \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)})$ and $\overline{f}_a(x) = \sum_{r\in R} Tr_1^n(a_r x^r)$. For $i \in \mathbb{Z}$, define $S_i(a)$ and $\overline{S}_i(a)$ to be the partial exponential sums :

$$S_i(a) = \sum_{v\in V} \chi\left(f_a(\zeta^i v)\right) \text{ and } \overline{S}_i(a) = \sum_{v\in V} \chi\left(\overline{f}_a(\zeta^i v)\right).$$

Note that ζ is of order τ so that $S_i(a)$ and $\overline{S}_i(a)$ only depend on the value of i modulo $\tau := \frac{2^m+1}{s}$.

Definition

Let $f_a(x) = \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)})$ and $\overline{f}_a(x) = \sum_{r\in R} Tr_1^n(a_r x^r)$. For $i \in \mathbb{Z}$, define $S_i(a)$ and $\overline{S}_i(a)$ to be the partial exponential sums

$$S_i(a) = \sum_{v\in V} \chi\left(f_a(\zeta^i v)\right) \text{ and } \overline{S}_i(a) = \sum_{v\in V} \chi\left(\overline{f}_a(\zeta^i v)\right).$$

Theorem

- $\sum_{i=0}^{\tau-1} S_i(a) = 1 + 2T_1(g_a)$ where $T_1(f) = \sum_{x\in\{x\in\mathbb{F}_{2^m} \mid Tr_1^m(1/x)=1\}} \chi_f(x)$ and g_a be the Boolean function defined on $\mathbb{F}_{2^m}$ as $g_a(x) = \sum_{r\in R} Tr_1^m a_r D_r(x)$.
- For $0 \le i \le \tau - 1$, then $S_i(a) = \overline{S}_{-2i \pmod{\tau}}(a)$.
- For r is co-prime with $2^m + 1$ then $\sum_{i=0}^{\tau-1} S_i(a) = 1 - K_m(a)$
- For l be a divisor of τ and let k the integer such that $k = \tau/l$, then $\sum_{i=0}^{k-1} S_{il}(a) = \sum_{i=0}^{k-1} \overline{S}_{il}(a) = \frac{1}{l}\left(1 + 2T_1(g_a \circ D_l)\right)$
- Let $k = m/l$. Suppose that the coefficients a_r lie in $\mathbb{F}_{2^l}$ and that $2^l \equiv j \pmod{\tau}$, where j is a k-th root of -1 modulo τ. Then $\overline{S}_i(a) = \overline{S}_{ij}(a)$

☞ We express $\Lambda(f_{a,b})$ by means of the partial exponential sums $\overline{S}_i(a)$:

we deduce :

THEOREM

$$\Lambda(f_{a,b}) = \chi\left(Tr_1^t b\right)\overline{S}_0(a) + \sum_{i=1}^{\frac{\tau-1}{2}}\left(\chi\left(Tr_1^t b\xi^i\right) + \chi\left(Tr_1^t b\xi^{-i}\right)\right)\overline{S}_i(a)$$

Recall that

$f_{a,b}$ is (hyper)-bent if and only if $\Lambda(f_{a,b}) = 1$.

REMARK

It is a difficult problem to deduce a completely general characterization of hyper-bentness in terms of complete exponential sums from our results. Nevertheless, several powerful applications of our results, valid for infinite families of Boolean functions can be described.

Building infinite families of extension degrees

- In the first approach, we set an extension degree m and studied the corresponding exponents s dividing $2^m + 1$.
- It is however customary to go the other way around, i.e. set an exponent s, or a given form of exponents, which is valid for an infinite family of extension degrees m and devise characterizations valid for this infinity of extension degrees.

☞ We provide the link between these two approaches.

Building infinite families of extension degrees

We fix a value for τ and devise the extension degrees m for which τ divides $2^m + 1$.

☞ We have study the values of τ for which an infinite number of such extension degrees m exists

1. case of an odd prime number :$\tau = p$ (p prime).
2. case of a prime power : $\tau = p^k$ (p prime).
3. case of an odd composite number : $\tau = p_1^{k_1} \cdots p_r^{k_r}$ is a product of $r \geq 2$ distinct prime powers.

Application :

- The case $\tau = 3$: we recover the characterizations of hyper-bentness of functions of the family of [Mesnager 2010]

$$f_{a_r,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}}), b \in \mathbb{F}_4^\star, m \equiv 1 \pmod 2$$

- The case $\tau = 5$: we recover the characterizations of hyper-bentness of functions of the family of [Wang et al. 2011]

$$f_{a_r,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^4(bx^{\frac{2^n-1}{5}}), b \in \mathbb{F}_{16}^\star, m \equiv 2 \pmod 4$$

- The case $\tau = 9$: we characterize the hyper-bentness for a new family

$$f_{a_r,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^6(bx^{\frac{2^n-1}{9}}), b \in \mathbb{F}_{64}^\star, m \equiv 3 \pmod 6$$

- The case $\tau = 11$: we characterize the hyper-bentness for a new family

$$f_{a_r,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^{10}(bx^{\frac{2^n-1}{11}}), b \in \mathbb{F}_{2^{10}}^\star, m \equiv 5 \pmod{10}$$

Application :

- The case $\tau = 13$: we characterize the hyper-bentness for a new family

$$f_{a_r,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^{12}(bx^{\frac{2^n-1}{13}}), b \in \mathbb{F}^{\star}_{2^{12}}, m \equiv 6 \pmod{12}$$

- The case $\tau = 17$: we characterize the hyper-bentness for a new family

$$f_{a_r,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^{8}(bx^{\frac{2^n-1}{17}}), b \in \mathbb{F}^{\star}_{2^{8}}, m \equiv 4 \pmod{8}$$

- The case $\tau = 33$: we characterize the hyper-bentness for a new family

$$f_{a_r,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^{10}(bx^{\frac{2^n-1}{33}}), b \in \mathbb{F}^{\star}_{2^{10}}, m \equiv 5 \pmod{10}$$

Conclusion :

- We study hyper-bent functions with multiple trace terms (including binomial functions) via Dillon-like exponents :

$$f_{a,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^t(b x^{s(2^m-1)})$$

- We show how the approach developed by Mesnager to extend the Charpin–Gong family (and subsequently slightly extended by Wang et al) fits in a much more general setting.
- We tackle the problem of devising infinite families of extension degrees for which a given exponent is valid and apply these results not only to reprove straightforwardly the results of Mesnager and Wang et. al, but also to characterize the hyper-bentness of several new infinite classes of Boolean functions.
- We also propose a reformulation of such characterizations in terms of hyperelliptic curves and use it to actually build hyper-bent functions.