A note on hyper-bent functions via Dillon-like exponents

Sihem Mesnager * Jean-Pierre Flori †

Monday 23rd January, 2012

Abstract

This note is devoted to hyper-bent functions with multiple trace terms (including binomial functions) via Dillon-like exponents. We show how the approach developed by Mesnager to extend the Charpin–Gong family and subsequently extended by Wang et al. fits in a much more general setting.

To this end, we first explain how the original restriction for Charpin–Gong criterion can be weakened before generalizing the Mesnager approach to arbitrary Dillon-like exponents. Afterward, 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 new infinite classes of Boolean functions.

Keywords. Boolean functions, hyper-bent functions, Walsh–Hadamard transform, exponential sums, Kloosterman sums, Dickson polynomials, Dillon exponents.

1 Introduction

Hyper-bent functions were defined by Youssef and Gong [21] in 2001 and are both of theoretical and practical interest. In fact, they were initially proposed by Golomb and Gong [8] as a component of S-boxes to ensure the security of symmetric cryptosystems. But such functions are rare, and in particular they are interesting from a combinatorial point of view: they indeed have stronger properties than the well-known bent functions which were already studied by Dillon [6] and Rothaus [17] more than three decades ago and whose classification is still elusive. Therefore, not only their characterization, but also their generation are challenging problems.

In 2008, Charpin and Gong [2] studied the hyper-bentness of Boolean functions in the following form:

$$f_a(x) = \sum_{r \in R} \mathrm{Tr}_1^n \left(a_r x^{r(2^m-1)} \right)$$

where $n = 2m$ is an even integer, R is a set of representatives of the cyclotomic classes modulo $2^m + 1$ of full size n and the coefficients a_r live in the subfield $\mathbb{F}_{2^m}$.

Such an approach was first extended by Mesnager (in 2009 for the binomial case [15] and further in 2010 for the general case [14]) to treat Charpin–Gong like functions with an additional

*LAGA (Laboratoire Analyse, Géometrie et Applications), UMR 7539, CNRS, Department of Mathematics, University of Paris XIII and University of Paris VIII, 2, rue de la liberté, 93526 Saint-Denis Cedex, France. smesnager@univ-paris8.fr

†ANSSI (Agence nationale de la sécurité des sytèmes d'information), 51, boulevard de la Tour-Maubourg, 75007 Paris SP, France. jean-pierre.flori@ssi.gouv.fr

trace term over $\mathbb{F}_4$:

$$f_{a,b}(x) = \sum_{r \in R} \mathrm{Tr}_1^n \left(a_r x^{r(2^m-1)} \right) + \mathrm{Tr}_1^2 \left(b x^{\frac{2^n-1}{3}} \right)$$

where the same restriction lies on the coefficient a_r, the coefficient b is in $\mathbb{F}_4$ and m must verify $m \equiv 1 \pmod 2$, i.e. m is odd.

Adopting the approach developed by Mesnager, Wang et al. studied in late 2011 (for the general case [20], but also specific treatments for the binomial case [19, 18]) the following family with an additional trace term on $\mathbb{F}_{16}$:

$$f_{a,b}(x) = \sum_{r \in R} \mathrm{Tr}_1^n \left(a_r x^{r(2^m-1)} \right) + \mathrm{Tr}_1^4 \left(b x^{\frac{2^n-1}{5}} \right)$$

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 $2^m + 1$. In this note, 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 or 11. To this end, we consider a function of the general form

$$f_{a,b}(x) = \sum_{r \in R} \mathrm{Tr}_1^n \left(a_r x^{r(2^m-1)} \right) + \mathrm{Tr}_1^t \left(b x^{s(2^m-1)} \right)$$

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, $t = o(s(2^m - 1))$, i.e. t is the size of the cyclotomic coset of s modulo $2^m + 1$, and 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.

In Section 2, we provide some background on the different objects we manipulate in the following sections, namely Boolean functions, Walsh-Hadamard transform, Dickson polynomials, exponential sums.Section 3 and 4 build the core of this paper: in the former one, we study general Dillon-like exponents; in the latter one, we devise for which extension degrees a given exponent is valid. Section 5 then provides both known and new applications of the developed theory.

2 Notation and preliminaries

Throughout this paper, $m \geq 0$ is a positive integer and $n = 2m$ is an even integer. The base field for our work will be $\mathbb{F}_{2^m}$, but our final motivation is the study of Boolean functions defined over $\mathbb{F}_{2^n}$. The element α denote a primitive element of $\mathbb{F}_{2^n}$. While working over finite fields, we use the shorthand notation $1/0 = 0$. For any set S such that $0 \in S$, S^* denotes $S^* = S \setminus \{0\}$ and $|S|$ denotes the cardinality of S.

2.1 Boolean functions and polynomial forms

Let n be a positive integer. A Boolean function f on $\mathbb{F}_{2^n}$ is an $\mathbb{F}_2$-valued function. The *weight* of f, denoted by $\mathrm{wt}(f)$, is the *Hamming weight* of the image vector of f, i.e. the cardinality of its support $\mathrm{supp}(f) = \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.

For any positive integer k, and r dividing k, the field trace from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$, denoted by Tr_r^k, can be explicitely defined as $\mathrm{Tr}_r^k(x) = \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}}$. In particular, we denote the *absolute trace* of

an element $x \in \mathbb{F}_{2^n}$ by $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. Recall that, for every integer l dividing k, the trace function Tr_l^k is surjective and satisfies the transitivity property, that is $\mathrm{Tr}_1^k = \mathrm{Tr}_1^l \circ \mathrm{Tr}_l^k$.

Every non-zero Boolean function f defined on $\mathbb{F}_{2^n}$ has a trace expansion of the form

$$f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_1^n\left(a_j x^j\right) + \epsilon(1 + x^{2^n-1})$$

where Γ_n is a set of representatives of the cyclotomic classes modulo $2^n - 1$, the coefficients a_j are in $\mathbb{F}_{2^n}$, and $\epsilon = \mathrm{wt}(f)$ modulo 2. Such a representation can be made unique by restricting the fields of definition of the coefficients a_j to $\mathbb{F}_{2^{o(j)}}$ and by writing f as

$$f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_1^{o(j)}\left(a_j x^j\right) + \epsilon(1 + x^{2^n-1})$$

where $o(j)$ is the size of the cyclotomic coset of j modulo $2^n - 1$. It is then called the polynomial form of f.

Going from the non-unique trace representation to the unique one basically amounts to take the traces of the coefficients from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^{o(j)}}$. Going the other way around relies on the surjectivity of the trace map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^{o(j)}}$.

2.2 Walsh–Hadamard transform and bentness

The *"sign" function* of a Boolean function f is the integer-valued function $\chi_f = \chi(f) = (-1)^f$, i.e. f composed with the additive character of $\mathbb{F}_2$.

The *Walsh–Hadamard transform* of f is the discrete Fourier transform of χ_f, whose value at $\omega \in \mathbb{F}_{2^n}$ is defined as

$$\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n(\omega x)} \ .$$

The *extended Walsh–Hadamard transform* of f is defined as

$$\widehat{\chi_f}(\omega, k) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n\left(\omega x^k\right)} \ ,$$

for $\omega \in \mathbb{F}_{2^n}$ and k an integer co-prime with $2^n - 1$.

Bent functions are functions with maximum nonlinearity.

Definition 2.1. *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be bent if $\widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}$ for all $\omega \in \mathbb{F}_{2^n}$.*

Hyper-bent functions have even stronger properties than bent functions. More precisely, hyper-bent functions can be defined as follows.

Definition 2.2. *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be hyper-bent if its extended Walsh–Hadamard transform only takes the values $\pm 2^{\frac{n}{2}}$.*

Note that bent and hyper-bent functions only exist for n even. Moreover, it is well-known that their Hamming weight is even. Therefore, their polynomial forms are of the form

$$f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_1^{o(j)}\left(a_j x^j\right) \ .$$

It is well-known that the algebraic degree of a bent function is at most $n/2$ [17]. If it is moreover hyper-bent, then it is exactly $n/2$ [1, Theorem 1].

2.3 A characterization of hyper-bentness

Dillon [6] introduced a convenient criterion for bentness involving the support of a Boolean function, forming the so-called Partial Spreads class $\mathcal{PS}^-$ of Boolean functions.

Theorem 2.3 ($\mathcal{PS}^-$ class [6]). *Let E_i, $i = 1, 2, \cdots, N$, be N subspaces of $\mathbb{F}_{2^n}$ of dimension m satisfying $E_i \cap E_j = \{0\}$ for all $i, j \in \{1, 2, \cdots, N\}$ with $i \neq j$. Let f be a Boolean function on $\mathbb{F}_{2^n}$. Assume that the support of f can be written as $\mathrm{supp}(f) = \bigcup_{i=1}^{N} E_i^*$. Then f is bent if and only if $N = 2^{m-1}$. In this case, f is said to belong to the $\mathcal{PS}^-$ class.*

Dillon also exhibited a subclass of $\mathcal{PS}^-$, denoted by $\mathcal{PS}_{ap}$, whose elements are defined in an explicit form as follows. To this end, consider $\mathbb{F}_{2^n}$ as a $\mathbb{F}_{2^m}$-vectorspace of dimension 2 with basis $\{1, w\}$; then every element $z \in \mathbb{F}_{2^n}$ can be decomposed as $z = x + wy$ with $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

Definition 2.4 ($\mathcal{PS}_{ap}$ class [6]). *The $\mathcal{PS}_{ap}$ class consists of all Boolean functions f defined as follows. Let g be a balanced Boolean function on $\mathbb{F}_{2^m}$ such that $g(0) = 0$. Then define the Boolean function f on $\mathbb{F}_{2^n} \simeq \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ as $f(x, y) = g(xy^{2^m-2})$ for every $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.*

A similar result for hyper-bentness was provided by Youssef and Gong [21] who showed that hyper-bent functions actually exist. They partially state this main result in terms of sequences. The following proposition is an easy translation of their result stated using only the terminology of Boolean functions as it was given by Carlet and Gaborit [1].

Proposition 2.5 ($\mathcal{PS}_{ap}^{\#}$ class [21, Theorem 1], [1, Proposition 3]). *Let α be a primitive element of $\mathbb{F}_{2^n}$. Let f be a Boolean function defined on $\mathbb{F}_{2^n}$ such that $f(\alpha^{2^m+1}x) = f(x)$ for every $x \in \mathbb{F}_{2^n}$ and $f(0) = 0$. Then f is a hyper-bent function if and only if the weight of the vector $(f(1), f(\alpha), f(\alpha^2), \cdots, f(\alpha^{2^m}))$ equals 2^{m-1}. In this case f is said to belong to the $\mathcal{PS}_{ap}^{\#}$ class.*

Charpin and Gong [2] have derived a slightly different version of the preceding proposition.

Proposition 2.6 ([2, Theorem 2]). *Let α be a primitive element of $\mathbb{F}_{2^n}$. Let f be a Boolean function defined on $\mathbb{F}_{2^n}$ such that $f(\alpha^{2^m+1}x) = f(x)$ for every $x \in \mathbb{F}_{2^n}$ and $f(0) = 0$. Denote by U the cyclic subgroup of $\mathbb{F}_{2^n}^*$ of order $2^m + 1$. Let $\zeta = \alpha^{2^m-1}$ be a generator of U. Then f is a hyper-bent function if and only if the cardinality of the set $\left\{i \mid f(\zeta^i) = 1, 0 \leq i \leq 2^m\right\}$ equals 2^{m-1}.*

Remark 2.7. *It is important to point out that bent functions f defined on $\mathbb{F}_{2^n}$ such that $f(\alpha^{2^m+1}x) = f(x)$ for every $x \in \mathbb{F}_{2^n}$ and $f(0) = 0$ are always hyper-bent. A proof of this claim can be found in the paper of Charpin and Gong [2, Proof of Theorem 2] or it can be directly observed that the support $supp(f)$ of such a Boolean function f can be decomposed as $\mathrm{supp}(f) = \bigcup_{i \in S} \alpha^i \mathbb{F}_{2^m}^*$, where $S = \left\{i \mid f(\alpha^i) = 1\right\}$, that is, thanks to Theorem 2.3, f is bent if and only if $|S| = 2^{m-1}$, proving that such bent functions are actually hyper-bent functions according to Proposition 2.5.*

Finally, Carlet and Gaborit have proved the following more precise statement about the functions considered in Proposition 2.5.

Proposition 2.8 ([1, Proposition 4]). *Hyper-bent functions as in Proposition 2.5 such that $f(1) = 0$ are the elements of the $\mathcal{PS}_{ap}$ class. Those such that $f(1) = 1$ are the functions of the form $f(x) = g(\delta x)$ for some $g \in \mathcal{PS}_{ap}$ and $\delta \in \mathbb{F}_{2^n} \setminus \{1\}$ such that $g(\delta) = 1$.*

2.4 Dickson polynomials

Recall that the family of binary Dickson polynomials $D_r(x) \in \mathbb{F}_2[x]$ is defined by

$$D_r(x) = \sum_{i=0}^{\frac{r}{2}} \frac{r}{r-i} \binom{r-i}{i} x^{r-2i} \ .$$

Moreover, the family of Dickson polynomials $D_r(x) \in \mathbb{F}_2[x]$ can also be defined by the recurrence relation

$$D_{i+2}(x) = xD_{i+1}(x) + D_i(x)$$

with initial values

$$D_0(x) = 0, \quad D_1(x) = x \ .$$

The reader can refer to the monograph of Lind, Mullen and Turnwald [13] for many useful properties and applications of Dickson polynomials. In particular, for any non-zero positive integers r and s, Dickson polynomials satisfy

1. $\deg(D_r(x)) = r$,
2. $D_{rs}(x) = D_r(D_s(x))$,
3. $D_r(x + x^{-1}) = x^r + x^{-r}$.

A well-known result by Chou, Gomez-Calderon and Mullen [3] describes the cardinality of the preimage of an arbitraty element.

Theorem 2.9 ([3, Theorem 9'], [13, Theorem 3.26'])**.** *Let $\mathbb{F}_{2^m}$ be the finite field with 2^m elements and $1 \leq r \leq 2^n - 1$ be an integer. Let*

$$k = \gcd(r, 2^m - 1), \ \ l = \gcd(r, 2^m + 1) \ .$$

Let $x, y \in \mathbb{F}_{2^m}$ be two elements such that $D_r(x) = y$. Then

$$\left|D_r^{-1}(y)\right| = \begin{cases} \frac{k+l}{2} & \text{if } y = 0 \ , \\ k & \text{if } y \neq 0 \text{ and } \mathrm{Tr}_1^m(1/x) = 0 \ , \\ l & \text{if } y \neq 0 \text{ and } \mathrm{Tr}_1^m(1/x) = 1 \ . \end{cases}$$

Furthermore, a finer analysis of this result shows that Dickson polynomials leave stable the trace of the inverse of an arbitrary element.

Lemma 2.10 ([5, pp 355–356])**.** *Let $r \geq 0$ be an integer and $x \in \mathbb{F}_{2^m}$. Then*

$$\mathrm{Tr}_1^m\left(\frac{1}{D_r(x)}\right) = \mathrm{Tr}_1^m\left(\frac{1}{x}\right) \ .$$

We therefore denote the subsets of elements with a given trace of inverse as follows.

Definition 2.11. *For $i \in \mathbb{F}_2$, let $\mathcal{T}_i$ denote the set*

$$\mathcal{T}_i = \{x \in \mathbb{F}_{2^m} \mid \mathrm{Tr}_1^m(1/x) = i\} \ .$$

The following property is then a corollary to the above results.

Corollary 2.12. *Let $1 \leq r \leq 2^n - 1$ be an integer. Then the map $x \mapsto D_r(x)$ induces a permutation of*

- *$\mathcal{T}_0$ if and only if $k = \gcd(r, 2^m - 1) = 1$;*
- *$\mathcal{T}_1$ if and only if $l = \gcd(r, 2^m + 1) = 1$.*

2.5 Exponential sums

Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function. We denote the exponential sum associated with f by $\Xi(f)$, that is

$$\Xi(f) = \sum_{x \in \mathbb{F}_{2^m}} \chi_f(x) \ .$$

The classical binary Kloosterman sums on $\mathbb{F}_{2^m}$ are then defined as follows.

Definition 2.13 (Kloosterman sums)**.** *Let $a \in \mathbb{F}_{2^m}$. The binary Kloosterman sums associated with a is*

$$K_m(a) = \Xi\left(\mathrm{Tr}_1^m\left(ax + \frac{1}{x}\right)\right) \ .$$

The values of Kloosterman sums have been explicitely determined.

Proposition 2.14 ([12, Theorem 3.4])**.** *The Kloosterman sums $K_m(a)$ on $\mathbb{F}_{2^m}$ takes all the integer values divisible by 4 in the range $[-2^{(m+2)/2} + 1, 2^{(m+2)/2} + 1]$.*

The following partial exponential sums are a classical tool to study hyper-bentness. Beware that the Boolean function is defined on $\mathbb{F}_{2^n}$ in the first definition and $\mathbb{F}_{2^m}$ in the second one.

Definition 2.15. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function and U be the set of $(2^m + 1)$-th roots of unity in $\mathbb{F}_{2^n}$. We define $\Lambda(f)$ as*

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

Definition 2.16. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function and, for $i \in \mathbb{F}_2$, denote by $T_i(f)$ the partial exponential sum on $\mathcal{T}_i$ associated with f, that is*

$$T_i(f) = \sum_{x \in \mathcal{T}_i} \chi_f(x) \ .$$

The following lemma is easily deduced from the equality $(-1)^{\mathrm{Tr}_1^m(x)} = 1 - 2\,\mathrm{Tr}_1^m(x)$ where the values of the trace are understood as the integers 0 and 1.

Lemma 2.17. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function. Then*

$$T_i(f) = \frac{1}{2}\left(\Xi(f) + (-1)^i \Xi\left(\mathrm{Tr}_1^m(1/x) + f(x)\right)\right) \ .$$

Applying furthermore Corollary 2.12 gives the following result.

Corollary 2.18. *Let $1 \le r \le 2^n - 1$ be an integer and $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function. Suppose moreover that $k = \gcd(r, 2^m - 1) = 1$. Then*

$$\begin{aligned} T_0(f \circ D_r) &= T_0(f) \ , \\ T_1(f \circ D_r) &= \Xi(f \circ D_r) - T_0(f) \ . \end{aligned}$$

Finally, we have the following relation between Kloosterman sums and the above partial exponential sums.

Corollary 2.19. *Let $a \in \mathbb{F}_{2^m}^*$. Then*

$$\begin{aligned} K_m(a) &= -2T_1(\mathrm{Tr}_1^m(ax)) \ , \\ &= 2T_0(\mathrm{Tr}_1^m(ax)) \ . \end{aligned}$$

Proof. According to Lemma 2.17,

$$T_0(\mathrm{Tr}_1^m(ax)) - T_1(\mathrm{Tr}_1^m(ax)) = K_m(a) \ .$$

Moreover,

$$T_0(\mathrm{Tr}_1^m(ax)) + T_1(\mathrm{Tr}_1^m(ax)) = \Xi(\mathrm{Tr}_1^m(ax)) = 0 \ .$$

□

3 Hyper-bent Boolean functions with Dillon-like exponents: a generic approach

3.1 Extending the Charpin–Gong criterion

The family of Boolean functions $\mathcal{F}_n$ consists of the functions f_a given in trace representation by Dillon-like only exponents, that is

$$f_a(x) = \sum_{r \in R} \mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) \tag{1}$$

where R is a set of representatives of the cyclotomic classes modulo 2^m+1 (hence the elements $r(2^m-1)$ yield a set of representatives of the cyclotomic classes modulo 2^n-1 of the form $[i(2^m-1)]$) and the coefficients a_r live in the field $\mathbb{F}_{2^n}$. Departing from the approach of Charpin and Gong, we do not require that the cyclotomic classes are of maximal size $n = 2m$.

Lemma 3.1. *Let f_a be a Boolean function in $\mathcal{F}_n$. Then $f_a(\alpha^{2^m+1}x) = f_a(x)$.*

Proof. We indeed have

$$\begin{aligned} f_a(\alpha^{2^m+1}x) &= \sum_{r \in R} \mathrm{Tr}_1^n\left(a_r(\alpha^{2^m+1}x)^{r(2^m-1)}\right) \\ &= \sum_{r \in R} \mathrm{Tr}_1^n\left(a_r\alpha^{r(2^n-1)}x^{r(2^m-1)}\right) \\ &= f_a(x) \ . \end{aligned}$$

□

Proposition 2.6 can therefore be directly applied to characterize the hyper-bentness of f_a with the partial exponential sum $\Lambda(a) = \Lambda(f_a)$.

Proposition 3.2. *Let f_a be a Boolean function in $\mathcal{F}_n$. The function f_a is hyper-bent if and only if $\Lambda(a) = 1$.*

Proof. According to Proposition 2.6, f_a is hyper-bent if and only if its restriction to U has Hamming weight 2^{m-1}. Now $\Lambda(a) = |U| - 2\,\mathrm{wt}(f_a|_U) = 2^m + 1 - 2\,\mathrm{wt}(f_a|_U)$. Thus f_a is hyper-bent if and only if $\Lambda(a) = 1$. □

Remark 3.3. *An hyper-bent function $f_a \in \mathcal{F}_n$ is in $\mathcal{PS}_{ap}$ if and only if $\sum_{r \in R} \mathrm{Tr}_1^n(a_r) = 1$.*

In fact, the complete extended Walsh–Hadamard spectrum of f_a can be expressed with $\Lambda(a)$.

Proposition 3.4. *Let f_a be a Boolean function in $\mathcal{F}_n$. For $\omega = 0$,*

$$\widehat{\chi_{f_a}}(0,k) = 1 + \Lambda(a)\left(-1 + 2^m\right) \ ,$$

and, for $\omega \in \mathbb{F}_{2^n}^*$ non-zero,

$$\widehat{\chi_{f_a}}(\omega,k) = 1 - \Lambda(a) + 2^m(-1)^{f_a(\omega^{(2^m-1)/(2k)})} \ .$$

Proof. It is a well-known fact that every non-zero element $x \in \mathbb{F}_{2^n}^*$ has a unique polar decomposition as a product $x = yu$ where y lies in the subfield $\mathbb{F}_{2^m}$ and $u \in U$.

The extended Walsh–Hadamard transform of f_a at (ω, k) can consequently be expressed as

$$\begin{aligned}
\widehat{\chi_{f_a}}(\omega,k) &= \sum_{x\in\mathbb{F}_{2^n}} \chi\left(f_a(x) + \mathrm{Tr}_1^n\left(\omega x^k\right)\right) \\
&= 1 + \sum_{x\in\mathbb{F}_{2^n}^*} \chi\left(f_a(x) + \mathrm{Tr}_1^n\left(\omega x^k\right)\right) \\
&= 1 + \sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^*} \chi\left(f_a(yu) + \mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right) \ .
\end{aligned}$$

But

$$\begin{aligned}
f_a(yu) &= \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r (yu)^{r(2^m-1)}\right) \\
&= \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r y^{r(2^m-1)} u^{r(2^m-1)}\right) \\
&= \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r u^{r(2^m-1)}\right) \\
&= f_a(u) \ ,
\end{aligned}$$

so that

$$\begin{aligned}
\widehat{\chi_{f_a}}(\omega,k) &= 1 + \sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^*} \chi\left(f_a(u) + \mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right) \\
&= 1 + \sum_{u\in U} \chi_{f_a}(u) \sum_{y\in\mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right) \\
&= 1 + \sum_{u\in U} \chi_{f_a}(u) \left(-1 + \sum_{y\in\mathbb{F}_{2^m}} \chi\left(\mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right)\right) \\
&= 1 - \Lambda(a) + \sum_{u\in U} \chi_{f_a}(u) \sum_{y\in\mathbb{F}_{2^m}} \chi\left(\mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right) \ .
\end{aligned}$$

If $\omega = 0$, then $\widehat{\chi_f}(\omega,k) = 1 + \Lambda(a)\left(-1 + 2^m\right)$ as desired.

If $\omega \neq 0$, then the transitivity of the trace yields

$$\begin{aligned}
\mathrm{Tr}_1^n\left(\omega y^k u^k\right) &= \mathrm{Tr}_1^m\left(\mathrm{Tr}_m^n\left(\omega y^k u^k\right)\right) \\
&= \mathrm{Tr}_1^m\left(\omega y^k u^k + \left(\omega y^k u^k\right)^{2^m}\right) \\
&= \mathrm{Tr}_1^m\left(\omega y^k u^k + \omega^{2^m} y^k u^{-k}\right) \\
&= \mathrm{Tr}_1^m\left(y^k\left(\omega u^k + \omega^{2^m} u^{-k}\right)\right) \ .
\end{aligned}$$

As a consequence of this equality and of the fact that k is co-prime with 2^m+1, the sum over $\mathbb{F}_{2^m}$ is non-zero if and only if $u^{2k}=\omega^{2^m-1}$. Therefore

$$\widehat{\chi_{f_a}}(\omega,k)=1-\Lambda(a)+2^m(-1)^{f_a(\omega^{(2^m-1)/(2k)})} \ .$$

□

In particular, Proposition 3.2 is a direct corollary to the above proposition.

Remark 3.5. *Set*

$$\overline{f}_a(x)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^r\right) \ ,$$

and let $\overline{\Lambda}(a)=\Lambda(\overline{f}_a)$. *The integers* 2^m-1 *and* 2^m+1 *are co-prime and so the* (2^m-1)*-power map induces a permutation of* U. *In particular, one has* $\Lambda(a)=\overline{\Lambda}(a)$.

We now restrict to the family $\mathcal{G}_n$ of Boolean functions defined as above, but where the coefficients a_r are restricted to the subfield $\mathbb{F}_{2^m}$. The following remark shows that it is enough to restrict to Dillon-like exponents whose cyclotomic coset sizes do not divide m.

Remark 3.6. *If* $t=o(r(2^m-1))$, *then*

$$\mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right)=\mathrm{Tr}_1^t\left(\mathrm{Tr}_t^n\left(a_r\right)x^{r(2^m-1)}\right) \ .$$

Suppose now that $a_r\in\mathbb{F}_{2^m}$, *e.g.* $f_a\in\mathcal{G}_n$. *If* t *divides* m, *then* $\mathrm{Tr}_t^n\left(a_r\right)=\mathrm{Tr}_t^m\left(a_r+a_r^{2^m}\right)=0$ *and*

$$\mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right)=0 \ .$$

Otherwise, if $k=\gcd(t,m)$, *then* $\mathrm{Tr}_t^n\left(a_r\right)\in\mathbb{F}_{2^k}$.

Furthermore, Proposition 3.4 can be used to compute the dual of f_a in the case where f_a is hyper-bent.

Proposition 3.7. *Suppose that* $f_a\in\mathcal{G}_n$ *is hyper-bent. Then it is its own dual, i.e. we have*

$$\widehat{\chi_{f_a}}(\omega)=2^m\chi_{f_a}(\omega) \ .$$

Proof. If f_a is hyper-bent, then $\Lambda(a)=1$ and one has

$$\widehat{\chi_{f_a}}(\omega)=2^m\chi_{f_a}(u) \ ,$$

where $u^{1-2^m}=\omega^{2^m-1}$. In particular, one has $f_a(u)=f_a(\omega^{-1})$. One then concludes that $f_a(\omega^{-1})=f_a(\omega)$ using the facts that $a_r^{2^m}=a_r$ and that $2^m(1-2^m)\equiv 2^m-1 \pmod{2^n-1}$. □

For functions f_a in $\mathcal{G}_n$, Remark 3.5 combined with the transitivity of the trace yields a useful expression of $\Lambda(a)$ using the partial exponential sum T_1 whose proof we recall here.

Lemma 3.8 ([14, Lemma 12])**.** *Let* f_a *be a Boolean function in* $\mathcal{G}_n$ *and* l *be any positive integer. Let* g_a *be the Boolean function defined on* $\mathbb{F}_{2^m}$ *as* $g_a(x)=\sum_{r\in R}\mathrm{Tr}_1^m\left(a_r D_r(x)\right)$. *Then* $\Lambda(f_a(x^l))=1+2T_1(g_a\circ D_l)$.

Proof. Using the facts that the (2^m-1)-power map induces a permutation of U, that $a_r^{2^m} = a_r$ and that $D_r(x+x^{-1}) = x^r + x^{-r}$ for any $x \in \mathbb{F}_{2^n}$, one gets

$$\begin{aligned}
\Lambda(f_a(x^l)) &= \sum_{u\in U} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^n\left(a_r\left(u^{2^m-1}\right)^{lr}\right)\right) \\
&= \sum_{u\in U} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^n\left(a_r u^{lr}\right)\right) \\
&= \sum_{u\in U} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^m\left(\left(a_r u^{lr}\right) + \left(a_r u^{lr}\right)^{2^m}\right)\right) \\
&= \sum_{u\in U} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^m\left(a_r\left(u^{lr} + u^{-lr}\right)\right)\right) \\
&= \sum_{u\in U} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^m\left(a_r D_r(D_l(u+u^{-1}))\right)\right) \ .
\end{aligned}$$

To conclude, recall that the map $x \mapsto x + x^{-1}$ is 2-to-1 from $U \setminus \{1\}$ to $\mathcal{T}_1$ to obtain

$$\begin{aligned}
\Lambda(f_a(x^l)) &= 1 + 2\sum_{t in \mathcal{T}_1} g_a(D_l(t)) \\
&= 1 + 2T_1(g_a \circ D_l) \ .
\end{aligned}$$

□

The following extension of the Charpin–Gong criterion is then straightforward.

Theorem 3.9 (Extension of the Charpin–Gong criterion [2, Theorem 7])**.** *Let f_a be a Boolean function in $\mathcal{G}_n$. Let g_a be the Boolean function defined on $\mathbb{F}_{2^m}$ as $g_a(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x))$. Then f_a is hyper-bent if and only if $T_1(a) = T_1(g_a) = 0$. Moreover, if f_a is hyper-bent, then it is in the $\mathcal{PS}_{ap}$ class.*

Proof. This is a direct consequence of Proposition 3.2 and Lemma 3.8. □

3.2 Extending the Mesnager criterion

The above approach yields a satisfactory criterion for Boolean functions f_a in the family $\mathcal{G}_n$. In particular, using Lemma 2.17, one gets a characterization of the hyper-bentness of f_a involving only complete exponential sums, or equivalently the Hamming weight of f_a and that of g_a.

Nonetheless, the restriction that lies on the coefficients a_r is not satisfying, namely they should live in the field $\mathbb{F}_{2^n}$. In this subsection, we extend the approach of Mesnager to partially address this issue.

We therefore consider a different family of Boolean functions defined as follows. The family of Boolean functions $\mathcal{H}_n$ consists of the functions $f_{a,b}$ defined as

$$f_{a,b}(x) = \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) + \mathrm{Tr}_1^t\left(b x^{s(2^m-1)}\right) \tag{2}$$

where 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, $t = o(s(2^m-1))$, i.e. t is the size

of the cyclotomic coset of s modulo 2^m+1, and the coefficient b is in $\mathbb{F}_{2^t}$. Moreover, let $\tau = \frac{2^m+1}{s}$. Remark that $f_{a,0} = f_a$ where $f_a \in \mathcal{G}_n$ is the function defined in the previous subsection. Set

$$\overline{f}_{a,b}(x) = \sum_{r \in R} \mathrm{Tr}_1^n\left(a_r x^r\right) + \mathrm{Tr}_1^t\left(b x^s\right) \ .$$

Remark 3.10. *According to Remark 3.6, the family $\mathcal{H}_n$ is always strictly larger than the family $\mathcal{G}_n$.*

Let $U = \left\{u \in \mathbb{F}_{2^n}^* \mid u^{2^m+1} = 1\right\}$ be the subgroup of $\mathbb{F}_{2^n}^*$ of order 2^m+1, $V = \left\{v \in \mathbb{F}_{2^n}^* \mid v^s = 1\right\}$ its subgroup of order s and $W = \left\{w \in \mathbb{F}_{2^n}^* \mid w^\tau = 1\right\}$ its subgroup of order τ. Denote by α a primitive element of $\mathbb{F}_{2^n}$. Then $\zeta = \alpha^{2^m-1}$ is a generator of U, $\rho = \zeta^\tau$ is a generator of V and $\xi = \zeta^s$ is a generator of W.

Remark 3.11. *Note that $\mathbb{F}_{2^t}^* \supset W$. Indeed, by definition $s(2^m-1) \equiv 2^t s(2^m-1) \pmod{2^n-1}$. Thus $(2^t-1)s \equiv 0 \pmod{2^m+1}$, which implies that $2^t-1 \equiv 0 \pmod{\tau}$, that is τ divides 2^t-1.*

Remark 3.12. *Let us consider the τ-power homomorphism $\phi: \ x \in \mathbb{F}_{2^n}^* \mapsto x^\tau \in \mathbb{F}_{2^n}^*$. Its kernel is W and so it is τ-to-1.*

Furthermore, V and W are subsets of U, so that the restriction of ϕ to U maps U onto V and is again τ-to-1.

A similar statement is clearly true for s, switching the sets V and W.

Remark 3.13. *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 3.14. *For $0 \le i \le \tau-1$, define $S_i(a)$ and $\overline{S}_i(a)$ to be the partial exponential sums*

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

Moreover, define $\Lambda(a,b) = \Lambda(f_{a,b})$ and $\overline{\Lambda}(a,b) = \Lambda(\overline{f}_{a,b})$.

Remark 3.15. *The Boolean function $f_{a,b}$ is hyper-bent if and only if $\Lambda(a,b) = 1$. Moreover, Remark 3.5 can be extended to $f_{a,b}$ and $\overline{f}_{a,b}$ and yields $\Lambda(a,b) = \overline{\Lambda}(a,b)$. Finally, Proposition 3.7 can be extended to show that, if $f_{a,b}$ is hyper-bent, then its is $f_{a,b^{2^m}}$.*

Remark 3.16. *One obviously has*

$$\sum_{i=0}^{\tau-1} S_i(a) = \Lambda(a,0) = \Lambda(a) \ .$$

In particular, Lemma 3.8 yields

$$\sum_{i=0}^{\tau-1} S_i(a) = 1 + 2T_1(a) \ .$$

In the particular case where f_a is a monomial function, i.e. $f_a(x) = \mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$, Remark 3.16 can be further refined.

Lemma 3.17. *Suppose that r is co-prime with 2^m+1. One has*

$$\sum_{i=0}^{\tau-1} S_i(a) = 1 - K_m(a) \ .$$

Proof. The function $u \mapsto u + u^{-1}$ being onto and 2-to-1 from $U \setminus \{1\}$ to $\mathcal{T}_1$, one gets

$$\begin{aligned} K_m(a) &= -2T_1(\mathrm{Tr}_1^m(ax)) \\ &= -\sum_{u\in U,\ u\neq 1} \chi\left(\mathrm{Tr}_1^m\left(a\left(u+u^{-1}\right)\right)\right) \\ &= -\sum_{u\in U,\ u\neq 1} \chi\left(\mathrm{Tr}_1^n(au)\right) \\ &= 1 - \sum_{u\in U} \chi\left(\mathrm{Tr}_1^n(au)\right) \ . \end{aligned}$$

Furthermore, the r-power map induces a permutation of U and thus

$$\begin{aligned} \sum_{u\in U} \chi\left(\mathrm{Tr}_1^n(au)\right) &= \sum_{u\in U} \chi\left(\mathrm{Tr}_1^n(au^r)\right) \\ &= \overline{\Lambda}(a) \\ &= \Lambda(a) \ . \end{aligned}$$

□

The two partial exponential sums S_i and $\overline{S}_i$ defined above are closely related.

Lemma 3.18. *For $0 \le i \le \tau - 1$, one has*

$$S_i(a) = \overline{S}_{-2i}(a) \ .$$

Proof. First, one has

$$\begin{aligned} S_i(a) &= \sum_{v\in V} \chi\left(f_a(\zeta^i v)\right) \\ &= \sum_{v\in V} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^n\left(a_r\left(\zeta^i v\right)^{r(2^m-1)}\right)\right) \\ &= \sum_{v\in V} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^n\left(a_r\left(\zeta^{i(2^m-1)} v^{2^m-1}\right)^r\right)\right) \ . \end{aligned}$$

But $2^m - 1$ is co-prime with s, so that the (2^m-1)-power map induces a permutation of V, as does multiplication by ζ^τ. Moreover, $2^m + 1 \equiv 0 \pmod{\tau}$ implies that $2^m - 1 \equiv -2 \pmod{\tau}$. Hence,

$$S_i(a) = \sum_{v\in V} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^n\left(a_r\left(\zeta^{-2i} v\right)^r\right)\right) \ .$$

□

Remark 3.16 can then be extended to express $\Lambda(a,b)$ as a linear combination of the sums S_i.

Proposition 3.19. *One has*

$$\Lambda(a,b) = \sum_{i=0}^{\tau-1} \chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right) \overline{S}_i(a) \quad .$$

Proof. One has

$$\begin{aligned}
\Lambda(a,b) &= \overline{\Lambda}(a,b) \\
&= \sum_{u\in U} \chi\left(\overline{f}_a(u) + \mathrm{Tr}_1^t\left(bu^s\right)\right) \\
&= \sum_{u\in U} \chi\left(\overline{f}_a(u)\right) \chi\left(\mathrm{Tr}_1^t\left(bu^s\right)\right) \\
&= \sum_{i=0}^{\tau-1} \sum_{v\in V} \chi\left(\overline{f}_a(\zeta^i v)\right) \chi\left(\mathrm{Tr}_1^t\left(b\left(\zeta^i v\right)^s\right)\right) \\
&= \sum_{i=0}^{\tau-1} \chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right) \sum_{v\in V} \chi\left(\overline{f}_a(\zeta^i v)\right) \\
&= \sum_{i=0}^{\tau-1} \chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right) \overline{S}_i(a) \quad .
\end{aligned}$$

□

We now devise an additional relation between the partial exponential sums S_i and the partial exponential sum T_1. In particular, we express the partial exponential sum S_0 using T_1.

Lemma 3.20. *Let l be a divisor of τ and let k be the integer $k = \tau/l$. Then*

$$\sum_{i=0}^{k-1} S_{il}(a) = \sum_{i=0}^{k-1} \overline{S}_{il}(a) = \frac{1}{l}\left(1 + 2T_1(g_a \circ D_l)\right) \quad .$$

For $l = 1$, it reads

$$\sum_{i=0}^{\tau-1} S_i(a) = \sum_{i=0}^{\tau-1} \overline{S}_i(a) = \left(1 + 2T_1(g_a)\right) \quad ,$$

which is nothing but Remark 3.16. For $l = \tau$, it reads

$$S_0(a) = \overline{S}_0(a) = \frac{1}{\tau}\left(1 + 2T_1(g_a \circ D_\tau)\right) \quad .$$

Proof. According to a straightforward extension of Remark 3.11, the l-power map is l-to-1 from U onto $\bigcup_{i=0}^{k-1} \zeta^{il} V$. Therefore,

$$\begin{aligned}
\sum_{i=0}^{k-1} S_{il}(a) &= \sum_{i=0}^{k-1} \sum_{v\in V} \chi\left(f_a(\zeta^{il} v)\right) \\
&= \frac{1}{l} \sum_{u\in U} \chi\left(f_a(u^l)\right) \quad .
\end{aligned}$$

One then concludes with Lemma 3.8.

The results for $\overline{S}_i$ readily follows from the fact multiplication by -2 induces a permutation of $\{il\}_{i=0}^{k-1}$ and Lemma 3.18. □

Remark 3.21. *Recall that τ divides 2^m+1, and so does l. Therefore, τ and l are co-prime with 2^m-1. According to Corollary 2.12, D_l induces a permutation of $\mathcal{T}_0$, whence the validity of the equality*

$$\sum_{i=0}^{k-1} S_{il}(a) = \sum_{i=0}^{k-1} \overline{S}_{il}(a) = \frac{1}{l}\left(1 + 2\Xi\left(g_a \circ D_l\right) - 2T_0(a)\right) \ .$$

In the case where $l=\tau$, it reads

$$S_0(a) = \overline{S}_0(a) = \frac{1}{\tau}\left(1 + 2\Xi\left(g_a \circ D_\tau\right) - 2T_0(a)\right) \ .$$

To conclude this section, we show how further identities involving the partial exponential sums S_i can be obtained by restricting the field of definition of the coefficients a_r to a strict subfield of $\mathbb{F}_{2^m}$.

Lemma 3.22. *Let l be a divisor of m and $k=m/l$. 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*

$$\overline{S}_i(a) = \overline{S}_{ij}(a) \ .$$

Proof. Recall that $2^m \equiv -1 \pmod{\tau}$. Hence, if $2^l \equiv j \pmod{\tau}$, then j is a k-th root of -1 modulo τ.

Since $a_r \in \mathbb{F}_{2^l}$, one has $a_r^{2^l} = a_r$. Recall that $\mathrm{Tr}_1^m\left(x^2\right) = \mathrm{Tr}_1^m(x)$, so that

$$\begin{aligned}
\overline{S}_i(a) &= \sum_{v\in V} \chi\left(\overline{f}_a(\zeta^i v)\right) \\
&= \sum_{v\in V} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^m\left(a_r(\zeta^i v)^r\right)\right) \\
&= \sum_{v\in V} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^m\left(a_r^{2^l}(\zeta^{2^l i} v^{2^l})^r\right)\right) \\
&= \sum_{v\in V} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^m\left(a_r(\zeta^{ij}\zeta^{i(2^l-j)} v^{2^l})^r\right)\right) \ .
\end{aligned}$$

But the (2^l)-power map and multiplication by $\zeta^{i(2^l-j)}$ induce permutations of V and therefore

$$\begin{aligned}
\overline{S}_i(a) &= \sum_{v\in V} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^m\left(a_r(\zeta^{ij} v)^r\right)\right) \\
&= \overline{S}_{ij}(a) \ .
\end{aligned}$$

□

Remark 3.23. *In the particular case where $l=m$, note that $2^m \equiv -1 \pmod{\tau}$. Therefore, one has*

$$\overline{S}_i(a) = \overline{S}_{-i}(a) \ .$$

One then deduces from Proposition 3.19 that

$$\Lambda(a,b) = \chi\left(\mathrm{Tr}_1^t(b)\right)\overline{S}_0(a) + \sum_{i=1}^{\frac{\tau-1}{2}} \left(\chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right) + \chi\left(\mathrm{Tr}_1^t\left(b\xi^{-i}\right)\right)\right)\overline{S}_i(a) \ .$$

Remark 3.24. *It is a difficult problem to deduce a completely general characterization of hyper-bentness in terms of complete exponential sums from the results of the current section, that is a characterization valid for any m, s and b. Nevertheless, several powerful applications of these results, valid for infinite families of Boolean functions, will be described in Section 5.*

3.3 An alternate proof

To provide an alternate proof of Proposition 3.19, we introduce *inverse exponential sums*.

Proposition 3.25. *For $c \in \mathbb{F}_{2^t}$, let $\widetilde{\Lambda}(a,c)$ be the exponential sum*

$$\widetilde{\Lambda}(a,c) = \sum_{b \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \Lambda(a,b) \ .$$

1. *For all $c \in \mathbb{F}_{2^t}$, one has*
$$\widetilde{\Lambda}(a,c) = 2^t \sum_{u \in U,\ u^s = c} \chi\left(\overline{f}_a(u)\right) \ .$$

2. *If $c \in \mathbb{F}_{2^t} \setminus W$, then $\widetilde{\Lambda}(a,c) = 0$. If $c \in W$, that is if $c = \xi^i$ for some i, then*
$$\widetilde{\Lambda}(a,\xi^i) = 2^t \overline{S}_i(a) \ .$$

Proof. 1. Switching the summations on U and $\mathbb{F}_{2^t}$ yields

$$\begin{aligned}
\widetilde{\Lambda}(a,c) &= \sum_{b \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \sum_{u \in U} \chi\left(f_{a,b}(u)\right) \\
&= \sum_{b \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \sum_{u \in U} \chi\left(f_a(u)\right) \chi\left(\mathrm{Tr}_1^t\left(bu^{s(2^m-1)}\right)\right) \\
&= \sum_{u \in U} \chi\left(f_a(u)\right) \sum_{b \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t\left(b\left(c + u^{s(2^m-1)}\right)\right)\right) \ .
\end{aligned}$$

The sum over $\mathbb{F}_{2^t}$ is non-zero if and only if $c = u^{s(2^m-1)}$ so that

$$\begin{aligned}
\widetilde{\Lambda}(a,c) &= 2^t \sum_{u \in U,\ u^{s(2^m-1)} = c} \chi\left(f_a(u)\right) \\
&= 2^t \sum_{u \in U,\ u^s = c} \chi\left(\overline{f}_a(u)\right) \ .
\end{aligned}$$

2. According to Remark 3.11, if $c \in \mathbb{F}_{2^t} \setminus W$, then the equation $u^s = c$ has no solutions in U. Therefore, $\widetilde{\Lambda}(a,c) = 0$.

   Suppose now that $c \in W$ and that $c = \xi^i = \zeta^{is}$ for some i. The kernel of the s-power map is V so that $u^s = \zeta^{is}$ if and only if $u \in \zeta^i V$. Thus

$$\widetilde{\Lambda}(a,c) = 2^t \sum_{v \in V} \chi\left(\overline{f}_a(\zeta^i v)\right) \ .$$

□

The partial exponential sum $\Lambda(a,b)$ can now be expressed with $\widetilde{\Lambda}(a,c)$.

Lemma 3.26. *One has*

$$\Lambda(a,b) = \frac{1}{2^t} \sum_{c \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \widetilde{\Lambda}(a,c) \ .$$

Proof. Going back to the definition of $\widetilde{\Lambda}(a,c)$, one has

$$\begin{aligned}
\sum_{c \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \widetilde{\Lambda}(a,c) &= \sum_{c \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \sum_{d \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(dc)\right) \Lambda(a,d) \\
&= \sum_{d \in \mathbb{F}_{2^t}} \Lambda(a,d) \sum_{c \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \chi\left(\mathrm{Tr}_1^t(dc)\right) \\
&= \sum_{d \in \mathbb{F}_{2^t}} \Lambda(a,d) \sum_{c \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t((b+d)c)\right) \ .
\end{aligned}$$

But $\sum_{c \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t((b+d)c)\right) = 0$ if $b \neq d$ and 2^t otherwise. Therefore

$$\sum_{c \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \widetilde{\Lambda}(a,c) = 2^t \Lambda(a,b) \ .$$

□

Remark 3.27. *Proposition 3.25 and Lemma 3.26 provide an alternate proof of Proposition 3.19:*

$$\begin{aligned}
\Lambda(a,b) &= \frac{1}{2^t} \sum_{c \in \mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \widetilde{\Lambda}(a,c) \\
&= \frac{1}{2^t} \left(\sum_{c \in \mathbb{F}_{2^t} \setminus W} \chi\left(\mathrm{Tr}_1^t(bc)\right) \widetilde{\Lambda}(a,c) + \sum_{c \in W} \chi\left(\mathrm{Tr}_1^t(bc)\right) \widetilde{\Lambda}(a,c) \right) \\
&= \frac{1}{2^t} \sum_{c \in W} \chi\left(\mathrm{Tr}_1^t(bc)\right) \widetilde{\Lambda}(a,c) \\
&= \frac{1}{2^t} \sum_{i=0}^{\tau-1} \chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right) \widetilde{\Lambda}(a,\xi^i) \\
&= \frac{1}{2^t} \sum_{i=0}^{\tau-1} \chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right) 2^t \overline{S}_i(a) \\
&= \sum_{i=0}^{\tau-1} \chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right) \overline{S}_i(a) \ .
\end{aligned}$$

4 Building infinite families of extension degrees

In the previous subsection, we set an extension degree m and studied the corresponding exponents s. It is however customary to go the opposite way around, i.e. set an exponent, or a given form of exponent, which is valid for an infinite family of extension degree and devise characterizations valid for this inifinity of extension degrees. In this section we provide the link between these two approaches.

The above construction relies on the fact that τ divides $2^m + 1$, that is $2^m \equiv -1 \pmod{\tau}$ or equivalently that -1 is in the cyclotomic coset of 1 modulo $2^m + 1$. We now focus on the construction of values of τ for which an infinite number of such m exists. Recall that the integers s and τ of the previous section verify $s = \frac{2^m+1}{\tau}$.

4.1 Prime case

Let p be an odd prime number.

The set of modular integers $\mathbb{Z}/p\mathbb{Z}$ is a field and there exists i such that $2^i \equiv -1 \pmod{p}$ if and only if the multiplicative order of 2 modulo p is even. In this case, taking $m \equiv l \pmod{2l}$, where $2l$ is the multiplicative order of 2 modulo p, yields an infinite family of values of m for which $2^m \equiv -1 \pmod{p}$. The corresponding denominator is $\tau = p$. The size $t = o(s)$ of the cyclotomic coset of $s = (2^m + 1)/\tau$ modulo $2^m + 1$, is then

$$t = 2l \ .$$

Furthermore, one has

$$2^m \equiv 2^l \pmod{2^t - 1} \ ,$$

so that if $f_{a,b} \in \mathcal{H}_n$ is hyper-bent, then its dual is $f_{a,b^{2^l}}$.

To actually devise such prime numbers, we now focus on the specific case where the multiplicative order of 2 modulo p is maximal, that is where 2 is a primitive root modulo p. In this situation, the above condition becomes

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p} \ .$$

This implies that the Legendre symbol $\left(\frac{2}{p}\right)$ of 2 modulo p is -1 and that 2 is a quadratic nonresidue modulo p. It is well-known that the Legendre symbol of 2 modulo an odd prime p is

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \ , \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \ . \end{cases}$$

Therefore, if 2 is a primitive root modulo p, then one must have $p \equiv \pm 3 \pmod{8}$. This gives a practical criterion to discard prime numbers such that 2 is not a primitive element. Further characterizations of primes p such that 2 is a primitive root modulo p can be found in a paper of Park, Park and Kim [16].

For such a prime number p, taking $m \equiv \frac{p-1}{2} \pmod{p-1}$ yields an infinite family of values of m for which $2^m \equiv -1 \pmod{p}$, the corresponding denominator being $\tau = p$. The size $t = o(s)$ of the cyclotomic coset of $s = (2^m + 1)/\tau$ modulo $2^m + 1$, is then

$$t = p - 1 = \tau - 1 \ .$$

Finding an inifinite number of odd prime numbers for which 2 is a primitive element would thus give an elegant solution to our problem, i.e. finding an infinite family of denominators τ associated with infinite families of extension degrees m. This question is however difficult; it is a special case of Artin's conjecture on primitive roots.

Conjecture 4.1 (Artin's conjecture on primitive roots)**.** *Let a be an integer which is neither a perfect square nor -1. Then the number of primes numbers p such that a is a primitive element modulo p is infinite.*

It should be noted that Artin's conjecture has been proved by Hooley [10] under the Generalized Riemann Hypothesis. Heath-Brown [9] has proved unconditionally that there exist at most two exceptional primes for which Artin's conjecture fails; nonetheless, this proof is non-constructive.

From a more computational perspective, the first elements of the sequence of primes such that 2 is a primitive element is sequence `A001122` in OEIS [11] and begins with

$$3,\ 5,\ 11,\ 13,\ 19,\ 29,\ 37,\ 53,\ 59,\ 61,\ 67,\ 83 \ .$$

As mentioned in the beginning of this section, it is not necessary that 2 is a primitive root modulo 2 for 1 and -1 to lie in the same cyclmotomic coset modulo p. The list of odd primes p smaller than 100 such that the multiplicative order of 2 modulo p is even and a strict divisor of $p-1$, together with half the order l of 2, i.e. the smallest integer l such that $2^l \equiv -1 \pmod{p}$, is

$$(17,4),\ (41,10),\ (43,7),\ (97,24)\ .$$

Finally, there exist as well odd primes for which 1 and -1 are not in the same cyclotomic coset modulo p. The list of such primes smaller than 100 is

$$7,\ 23,\ 31,\ 47,\ 71,\ 73,\ 79,\ 89\ .$$

4.2 Prime power case

Let p be an odd prime number and $k \geq 2$ a positive integer. The multiplicative group of units modulo p^k is once again cyclic and isomorphic to

$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times \simeq (\mathbb{Z}/(p-1)\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^{k-1}\ .$$

The condition for the prime case is thus still valid; there exists i such that $2^i \equiv -1 \pmod{p^k}$ if and only if the multiplicative order of 2 modulo p^k is even. In this case, taking $m \equiv l \pmod{2l}$, where $2l$ is the multiplicative order of 2 modulo p^k, yields an infinite family of values of m for which $2^m \equiv -1 \pmod{p}$. The corresponding denominator is $\tau = p^k$. The size $t = o(s)$ of the cyclotomic coset of $s = (2^m+1)/\tau$ modulo 2^m+1, is then

$$t = 2l\ .$$

If $f_{a,b} \in \mathcal{H}_n$ is hyper-bent, then its dual is $f_{a,b2^l}$.

It is a classical result [4, Lemma 1.4.5 and following remarks], that if an integer a is a primitive root modulo p, then a or $a+p$ is a primitive root modulo p^2. Furthermore, if a is a primitive root modulo p^2, then it is modulo p^k for any $k \geq 2$. Conversely, if a is not a primitive root modulo p^i, then it is not a primitive root modulo p^k for any $k \geq i$. The approach of the previous subsection can therefore be extended to any prime power p^k with $k \geq 2$ by just checking that 2 is a primitive root modulo p^2. If it is, then

$$2^{\frac{\phi(p^k)}{2}} \equiv -1 \pmod{\phi(p^k)}$$

for any $k \geq 2$, where ϕ denotes Euler's totient function. In particular, $\phi(p^k) = (p-1)p^k$. In this case, one would choose $m \equiv \frac{\phi(p^k)}{2} \pmod{\phi(p^k)}$, the corresponding denominator being $\tau = p^k$. The size $t = o(s)$ of the cyclotomic coset of $s = (2^m+1)/\tau$ modulo 2^m+1, is then

$$t = \phi(p^k)\ .$$

The primes smaller than 100 such that 2 is a primitive root modulo p^2 are

$$3,\ 5,\ 11,\ 13,\ 19,\ 29,\ 37,\ 53,\ 59,\ 61,\ 67,\ 83\ .$$

From a computational perspective, more can be said. Indeed, if 2 is primitive root modulo p, but is not modulo p^2, a simple calculation shows that $2^{p-1} \equiv 1 \pmod{p^2}$, that is p is a *Wieferich prime*. The sequence of such primes is sequence `A001220` in the OEIS [11]. Only two of them are currently known: 1093 and 3511; and 2 is not a primitive root for both of these primes. Checking that 2 is a primitive root modulo p is therefore enough to ensure that it is modulo any power of p as long as p is not too large, less than fifteen decimal digits according to Dorais and Klyve [7].

The list of odd primes p smaller than 100 such that the multiplicative order of 2 modulo p^2 is even and a strict divisor of $\phi(p^2)$, together with half the order l of 2, i.e. the smallest integer l such that $2^l \equiv -1 \pmod{p^2}$, is

$$(17, 68),\ (41, 410),\ (43, 301),\ (97, 2328)\ .$$

Finally, the list of odd primes p smaller than 100 such that 1 and -1 do not lie in the same cyclotomic coset modulo p^2 is

$$7,\ 23,\ 31,\ 47,\ 71,\ 73,\ 79,\ 89\ .$$

4.3 Composite case

We now consider the general case of an odd composite number. Let's say that $\tau = p_1^{k_1} \cdots p_r^{k_r}$ is a product of $r \geq 2$ distinct prime powers.

The multiplicative group of units modulo τ is not cyclic anymore and is isomorphic to the product of the cyclic groups corresponding to each prime power:

$$(\mathbb{Z}/\tau\mathbb{Z})^\times \simeq \left(\mathbb{Z}/p_1^{k_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_r^{k_r}\mathbb{Z}\right)^\times\ .$$

The multiplicative order of 2 modulo τ is the least common multiple of its multiplicative orders modulo the prime powers dividing n. There exists an integer i such that $2^i \equiv -1 \pmod{\tau}$ if and only if there exists such integers for each prime power dividing τ, that is if the multiplicative order of 2 modulo $p_j^{k_j}$ is even for $1 \leq j \leq r$, and if moreover their least common multiple is an odd multiple of each of them, that is if they all have the same 2-adic valuation. In such a situation, taking $m \equiv l \pmod{2l}$, where $2l$ is the multiplicative order of 2 modulo τ, yields an infinite family of values of m for which $2^m \equiv -1 \pmod{\tau}$. Recall that the corresponding denominator is τ. The size $t = o(s)$ of the cyclotomic coset of $s = (2^m + 1)/\tau$ modulo $2^m + 1$, is then

$$t = 2l\ .$$

If $f_{a,b} \in \mathcal{H}_n$ is hyper-bent, then its dual is $f_{a,b^{2^l}}$.

In particular, if 2 is a primitive root modulo each prime power dividing τ, then the multiplicative order of 2 modulo τ is

$$2l = \mathrm{lcm}(\phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r}))\ ,$$

and $2^l \equiv -1 \pmod{\tau}$ if and only if $\nu_2(p_1 - 1) = \cdots = \nu_2(p_r - 1)$, where ν_2 denotes the 2-adic valuation. Conditioned by the fact that there exists an infinite number of primes p such that 2 is a primitive root modulo p or modulo p^2 and such that $p - 1$ has a given 2-adic valuation, we can construct an infinite number of composite odd numbers addressing our original problem.

The list of suitable odd composite numbers τ smaller than 100, together with half the multiplicative order l of 2 modulo τ, that is the smallest integer such that $2^l \equiv -1 \pmod{\tau}$, is

$$(33, 5),\ (57, 9),\ (65, 6),\ (99, 15)\ .$$

5 Applications

In this section, we show how the results of Section 3 can be applied to several infinite families of Boolean functions in order to obtain characterizations of their hyper-bentness in terms of complete exponential sums. Much of these applications can be straightforwardly extended to other cases.

5.1 The case $b = 1$

We first apply results of Subsections 3.1 and 3.2 to $f_{a,1}$ defined as in Equation (2) in the specific case where $b = 1$.

Since 1 lies in $\mathbb{F}_2$, there exists $\beta \in \mathbb{F}_{2^m}$ such that $\mathrm{Tr}_t^n(\beta) = 1$. In particular, $f_{a,1}$ belongs to both families $\mathcal{G}_n$ and $\mathcal{H}_n$. Applying Theorem 3.9 shows that $f_{a,1}$ is hyper-bent if and only if

$$\sum_{t \in \mathcal{T}_1} \chi\left(\sum_{r \in R} a_r D_r(t) + \beta D_s(t)\right) = 0 \ .$$

Applying Lemma 2.17, this condition is straightforwardly expressed in terms of complete exponential sums, or of the Hamming weights of $f_{a,\beta}$ and $g_{a,\beta}$.

We now show how the results of Subsection 3.2 can be applied to obtain a different characterization ot the hyper-bentness of $f_{a,1}$. According to Proposition 3.2, $f_{a,1}$ is hyper-bent if and only if

$$\Lambda(a, 1) = 1 \ .$$

Let ξ be a primitive τ-th root of unity. First, recall that ξ lies in $\mathbb{F}_{2^t}$, that $\mathrm{Tr}_1^t\left(\xi^2\right) = \mathrm{Tr}_1^t(\xi)$ and that

$$\sum_{i=0}^{\tau-1} \xi^i = 0 \ .$$

Second, remark that the results of Section 4 imply that t is even, so that $\mathrm{Tr}_1^t(1) = 0$. Moreover, ξ is a $(2^{t/2} + 1)$-th root of unity so that $\xi + \xi^{-1} \in \mathbb{F}_{2^{t/2}}$ which implies that

$$\mathrm{Tr}_1^t\left(\xi^i\right) = \mathrm{Tr}_1^t\left(\xi^{-i}\right) \ .$$

Finally, Proposition 3.19 reads

$$\Lambda(a, 1) = \overline{S}_0(a) + 2\sum_{i=1}^{\frac{\tau-1}{2}} \chi\left(\mathrm{Tr}_1^t\left(\xi^i\right)\right) \overline{S}_i(a) \ .$$

Nonetheless, the trace of ξ^i for $i \neq 0$ depends on the exact value of τ. In the sequel, we deal with some specific cases.

5.1.1 Prime case

For simplicty, we first suppose that $\tau = p$ is a prime and that 2 is a primitive root modulo p. In this case, $t = p - 1$ and i is co-prime with p, so that

$$\mathrm{Tr}_1^{p-1}\left(\xi^i\right) = \sum_{j=0}^{p-2} \xi^{i2^j} = \sum_{j=1}^{p-1} \xi^{ij} = \sum_{j=1}^{p-1} \xi^j = 1 \ .$$

Therefore

$$\Lambda(a, 1) = 2\overline{S}_0(a) - \sum_{i=1}^{\tau-1} \overline{S}_i(a) \ .$$

Applying Lemma 3.20 with $l = 1$ and $l = \tau$ yields

$$\Lambda(a, 1) = \frac{2}{\tau}(1 + 2T_1(g_a \circ D_\tau)) - (1 + 2T_1(g_a)) \ .$$

Consequently, we get the following characterization.

Proposition 5.1. *Suppose that $\tau = p$ is a prime and that 2 is a primitive root modulo p. Then*

$$\tau\Lambda(a,1) = 4T_1(g_a \circ D_\tau) - 2\tau T_1(g_a) - \tau + 2 \ .$$

In particular, $f_{a,1}$ is hyper-bent if and only if

$$2T_1(g_a \circ D_\tau) - \tau T_1(g_a) = \tau - 1 \ .$$

5.1.2 Prime power case

We now treat the case where $\tau = p^k$ is a prime power and that 2 is a primitive root modulo p^k, including the case where $k = 1$. Then $t = \phi(p^k) = (p-1)p^{k-1}$. Remark that in this situation, for every positive integers $i \geq 0$ and $j > 0$ such that $i + j = k$, one has $\left(\xi^{p^i}\right)^{p^j} = \xi^{p^k} = 1$, so that

$$\sum_{l=0}^{p^j-1} \xi^{lp^i} = 0 \ . \tag{3}$$

Then

$$\mathrm{Tr}_1^{\phi(p^k)}\left(\xi^i\right) = \sum_{j=0}^{\phi(p^k)-1} \xi^{i2^j} = \sum_{1\leq j\leq p^k-1,\ p\nmid j} \xi^{ij} \ .$$

If $p^e \,||\, i$ with $0 \leq e \leq k-1$, then $i = lp^e$ with l co-prime with $p-1$ and

$$\begin{aligned}
\mathrm{Tr}_1^{\phi(p^k)}\left(\xi^i\right) &= \sum_{1\leq j\leq p^k-1,\ p\nmid j} \xi^{jlp^e} \\
&= \sum_{1\leq j\leq p^k-1,\ p\nmid j} \xi^{jp^e} \\
&= \sum_{j=0}^{p^k-1} \xi^{jp^e} + \sum_{j=0}^{p^{k-1}-1} \xi^{jp^{e+1}} \\
&= \sum_{j=0}^{p^k-1} \xi^{jp^e} + \sum_{j=0}^{p^k-1} \xi^{jp^{e+1}} + \sum_{j=p^{k-1}}^{p^k-1} \xi^{jp^{e+1}} \ .
\end{aligned}$$

Equation (3) shows that the first two sums of the right hand side of the last equality can be splitted into a multiple of sums equal to zero. If $0 \leq e \leq k-2$, then the third sum is zero as well, so that

$$\mathrm{Tr}_1^{\phi(p^k)}\left(\xi^i\right) = 0 \ .$$

If $e = k-1$, then the third sum reads

$$\sum_{j=p^{k-1}}^{p^k-1} \xi^{jp^k} = \sum_{j=p^{k-1}}^{p^k-1} \xi^j = 1 \ .$$

Therefore

$$\mathrm{Tr}_1^{\phi(p^k)}\left(\xi^i\right) = 1 \ .$$

Summing up the above observations yields

$$\begin{aligned}\Lambda(a,1) &= \sum_{i=0}^{p^k-1} \overline{S}_i(a) - 2\sum_{i=1}^{p-1} \overline{S}_{ip^{k-1}}(a) \\ &= 2\overline{S}_0(a) + \sum_{i=0}^{p^k-1} \overline{S}_i(a) - 2\sum_{i=0}^{p-1} \overline{S}_{ip^{k-1}}(a) \ .\end{aligned}$$

Applying Lemma 3.20 with $l = 1$, $l = p^{k-1}$ and $l = p^k$ then gives

$$\Lambda(a,1) = \frac{2}{p^k}(1 + 2T_1(g_a \circ D_{p^k})) - \frac{2}{p^{k-1}}(1 + 2T_1(g_a \circ D_{p^{k-1}})) + (1 + 2T_1(g_a)) \ .$$

Consequently, we get the following characterization.

Proposition 5.2. *Suppose that $\tau = p^k$ is a prime power and that 2 is a primitive root modulo p^k. Then*

$$p^k\Lambda(a,1) = 4T_1(g_a \circ D_{p^k})) - 4pT_1(g_a \circ D_{p^{k-1}}) + 2p^kT_1(g_a) + p^k - 2p + 2 \ .$$

In particular, $f_{a,1}$ is hyper-bent if and only if

$$2T_1(g_a \circ D_{p^k}) - 2pT_1(g_a \circ D_{p^{k-1}}) + p^kT_1(g_a) = p - 1 \ .$$

5.1.3 Other cases

The cases where τ is an odd composite number or where 2 is not a primitive root modulo τ are more involved and will be treated in subsequent works.

5.2 Explicit values for τ

The previous subsection dealt with a fixed value of $b \in \mathbb{F}_{2^t}^*$ casting as few restictions as possible on τ. In this subsection we go the other way around and treat the first few possible values of τ for all values of b with as few restrictions as possible on the corresponding infinite family of Boolean functions.

5.2.1 The case $\tau = 3$

The smallest possible value for τ is $\tau = 3$. This case was originally addressed by Mesnager in 2009 for the binomial case [15] and further in 2010 for the general case [14]. We now show how the characterizations for the general case can be directly deduced from the results of Section 3.

In this case, $t = 2$ and $m \equiv 1 \pmod 2$. In particular, $t < 2m$ as soon as $m \neq 1$. Furthermore, if $f_{a,b}$ is hyper-bent, then its dual is f_{a,b^2}.

According to Remark 3.23,

$$\Lambda(a,b) = \chi\left(\mathrm{Tr}_1^2(b)\right)\overline{S}_0(a) + \left(\chi\left(\mathrm{Tr}_1^2(b\xi)\right) + \chi\left(\mathrm{Tr}_1^2\left(b\xi^{-1}\right)\right)\right)\overline{S}_1(a) \ .$$

Note that ξ is a 3-rd root of unity and that $\xi + \xi^{-1} = 1$, so that

$$\Lambda(a,b) = \chi\left(\mathrm{Tr}_1^2(b)\right)\overline{S}_0(a) + \chi\left(\mathrm{Tr}_1^2(b\xi)\right)\left(1 + \chi\left(\mathrm{Tr}_1^2(b)\right)\right)\overline{S}_1(a) \ .$$

Moreover, $\mathbb{F}_4^* = \langle\xi\rangle$. Thus, if $b = 1$, then $\Lambda(a,1) = \overline{S}_0(a) - 2\overline{S}_1(a)$, and if $b = \xi$ or $b = \xi^{-1}$, that is if b is a 3-rd root of unity or equivalently a primitive element of $\mathbb{F}_4$, then $\Lambda(a,b) = -\overline{S}_0(a)$. Applying Lemma 3.20 with $l = 1$ and $l = 3$ then gives the following theorem and the corresponding characterizations for hyper-bentness.

$j\backslash i$	0	1	2	3	4
0	0	1	1	1	1
1	0	0	1	0	1
2	0	0	0	1	1
3	1	1	1	1	0
4	0	1	0	1	0
5	0	0	1	1	0
6	1	1	1	0	1
7	1	0	1	0	0

$j\backslash i$	0	1	2	3	4
8	0	1	1	0	0
9	1	1	0	1	1
10	0	1	0	0	1
11	1	1	0	0	0
12	1	0	1	1	1
13	1	0	0	1	0
14	1	0	0	0	1

Table 1: Traces for $\tau = 5$

Theorem 5.3 ([15]). *Let $\tau = 3$ and $m \equiv 1 \pmod 2$. Then*

1. *If $b = 1$, then $3\Lambda(f_{a,1}) = 4T_1(g_a \circ D_3) - 6T_1(g_a) - 1$.*
2. *If b is a primitive element of $\mathbb{F}_4$, then $3\Lambda(f_{a,b}) = 2T_1(g_a \circ D_3) + 1$.*

5.2.2 The case $\tau = 5$

The next possible value for τ is $\tau = 5$. This case was originally addressed by Wang et al. in late 2011 for the general case [20], but they also gave specific treatments for the binomial case [19, 18]. We now show how their characterizations for the general case can be directly deduced from the results of Section 3.

In this case, $t = 4$ and $m \equiv 2 \pmod 4$. In particular, $t < 2m$ as soon as $m \neq 2$. Furthermore, if $f_{a,b}$ is hyper-bent, then its dual is f_{a,b^4}.

According to Remark 3.23,

$$\begin{aligned}\Lambda(a,b) = \chi\left(\mathrm{Tr}_1^4(b)\right)\overline{S}_0(a) \\ + \left(\chi\left(\mathrm{Tr}_1^4(b\xi)\right) + \chi\left(\mathrm{Tr}_1^4\left(b\xi^{-1}\right)\right)\right)\overline{S}_1(a) \\ + \left(\chi\left(\mathrm{Tr}_1^4\left(b\xi^2\right)\right) + \chi\left(\mathrm{Tr}_1^4\left(b\xi^{-2}\right)\right)\right)\overline{S}_2(a) \ .\end{aligned}$$

Introduce $\gamma = \xi + \xi^{-1} \in \mathbb{F}_4$. Then

$$\begin{aligned}\Lambda(a,b) = \chi\left(\mathrm{Tr}_1^4(b)\right)\overline{S}_0(a) \\ + \chi\left(\mathrm{Tr}_1^4(b\xi)\right)\left(1 + \chi\left(\mathrm{Tr}_1^4(b\gamma)\right)\right)\overline{S}_1(a) \\ + \chi\left(\mathrm{Tr}_1^4\left(b\xi^2\right)\right)\left(1 + \chi\left(\mathrm{Tr}_1^4\left(b\gamma^2\right)\right)\right)\overline{S}_2(a) \ .\end{aligned}$$

Next, recall that ξ is a 5-th root of unity , so that $\sum_{i=0}^{4}\xi^i = 0$. In particular, $\gamma + \gamma^2 = 1$ and

$$\mathrm{Tr}_1^4(b\gamma) + \mathrm{Tr}_1^4\left(b\gamma^2\right) = \mathrm{Tr}_1^4(b) \ .$$

We now explicitely compute the traces $\mathrm{Tr}_1^4\left(b\xi^i\right)$. The finite field $\mathbb{F}_{16}$ is represented as $\mathbb{F}_2[x]/(C_4(x))$ where $C_4(x) = x^4 + x + 1$ is the 4-th Conway polynomial. We denote the class of x modulo $C_4(x)$ by β; this is a primitive element of $\mathbb{F}_{16}$. Let $\xi = \beta^3$ be a 5-th root of unity. The traces $\mathrm{Tr}_1^4\left(b\xi^i\right)$ are given in Table 1. The expression of $\Lambda(a,\beta^j)$ as a sum of the partial exponential sums $\overline{S}_i$, together with the minimal polynomial m_j of β^j, are given in Table 2.

Moreover, if the coefficients a_r lie in $\mathbb{F}_{2^l}$, where $l = m/2$, then $l \equiv 1 \pmod 2$ and $2^l \equiv \pm 2 \pmod 5$ and Lemma 3.22 tells that either $\overline{S}_1(a) = \overline{S}_2(a)$ or $\overline{S}_1(a) = \overline{S}_3(a)$. But $\overline{S}_2(a) = \overline{S}_3(a)$, so that one always has

$$\overline{S}_1(a) = \overline{S}_2(a) \ .$$

j	$\Lambda(a,\beta^j)$	m_j
0	$\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_2$	$x+1$
1	$\overline{S}_0$	x^4+x+1
2	$\overline{S}_0$	x^4+x+1
3	$-\overline{S}_0 - 2\overline{S}_2$	$x^4+x^3+x^2+x+1$
4	$\overline{S}_0$	x^4+x+1
5	$\overline{S}_0 + 2\overline{S}_1 - 2\overline{S}_2$	x^2+x+1
6	$-\overline{S}_0 - 2\overline{S}_1$	$x^4+x^3+x^2+x+1$
7	$-\overline{S}_0 + 2\overline{S}_1$	x^4+x^3+1

j	$\Lambda(a,\beta^j)$	m_j
8	$\overline{S}_0$	x^4+x+1
9	$-\overline{S}_0 - 2\overline{S}_1$	$x^4+x^3+x^2+x+1$
10	$\overline{S}_0 - 2\overline{S}_1 + 2\overline{S}_2$	x^2+x+1
11	$-\overline{S}_0 + 2\overline{S}_2$	x^4+x^3+1
12	$-\overline{S}_0 - 2\overline{S}_2$	$x^4+x^3+x^2+x+1$
13	$-\overline{S}_0 + 2\overline{S}_1$	x^4+x^3+1
14	$-\overline{S}_0 + 2\overline{S}_2$	x^4+x^3+1

Table 2: $\Lambda(a,\beta^j)$ for $\tau = 5$

Finally applying Lemma 3.20 for $l = 1$ and $l = 5$ gives the following theorem which summarizes the above discussion.

Theorem 5.4 ([20]). *Let $\tau = 5$ and $m \equiv 2 \pmod 4$.*

1. *If $b = 1$, then $5\Lambda(f_{a,1}) = 4T_1(g_a \circ D_5) - 10T_1(g_a) - 3$.*
2. *If b is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 0$, then $5\Lambda(f_{a,b}) = 2T_1(g_a \circ D_5) + 1$.*
3. *Suppose moreover that $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$.*
   (a) *If b is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 1$, then $5\Lambda(f_{a,b}) = -3T_1(g_a \circ D_5) + 5T_1(g_a) + 1$.*
   (b) *If b is a primitive 5-th root of unity, then $5\Lambda(f_{a,b}) = -T_1(g_a \circ D_5) - 5T_1(g_a) - 3$.*
   (c) *If b is a primitive 3-rd root of unity, then $5\Lambda(f_{a,b}) = 2T_1(g_a \circ D_5) + 1$.*

5.2.3 The case $\tau = 7$

For $\tau = 7$, 1 and -1 do not lie in the same cyclotomic coset modulo 7, hence the next suitable value for τ is $\tau = 9$.

5.2.4 The case $\tau = 9$

In the case $\tau = 9$, $t = 6$ and $m \equiv 3 \pmod 6$. In particular, $t < 2m$ as soon as $m \neq 3$. Furthermore, if $f_{a,b}$ is hyper-bent, then its dual is f_{a,b^8}.

According to Remark 3.23,

$$\begin{aligned}\Lambda(a,b) = {} & \chi\left(\mathrm{Tr}_1^6(b)\right)\overline{S}_0(a) \\ & + \left(\chi\left(\mathrm{Tr}_1^6(b\xi)\right) + \chi\left(\mathrm{Tr}_1^6(b\xi^8)\right)\right)\overline{S}_1(a) + \left(\chi\left(\mathrm{Tr}_1^6(b\xi^2)\right) + \chi\left(\mathrm{Tr}_1^6(b\xi^7)\right)\right)\overline{S}_2(a) \\ & + \left(\chi\left(\mathrm{Tr}_1^6(b\xi^3)\right) + \chi\left(\mathrm{Tr}_1^6(b\xi^6)\right)\right)\overline{S}_3(a) + \left(\chi\left(\mathrm{Tr}_1^6(b\xi^4)\right) + \chi\left(\mathrm{Tr}_1^6(b\xi^5)\right)\right)\overline{S}_4(a) \ .\end{aligned}$$

Introduce $\gamma = \xi^8 + \xi \in \mathbb{F}_8$. Note that

$$\begin{aligned}\gamma^2 &= \xi^2 + \xi^7 \ , \\ \gamma^3 &= \xi + \xi^3 + \xi^6 + \xi^8 \ , \\ \gamma^4 &= \xi^4 + \xi^5 \ , \\ \gamma^5 &= \xi^3 + \xi^4 + \xi^5 + \xi^6 \ , \\ \gamma^6 &= \xi^2 + \xi^3 + \xi^6 + \xi^7 \ .\end{aligned}$$

Thus

$$\begin{aligned}\Lambda(a,b) = \chi\left(\mathrm{Tr}_1^6(b)\right)\overline{S}_0(a) \\ + \chi\left(\mathrm{Tr}_1^6(b\xi)\right)\left(1+\chi\left(\mathrm{Tr}_1^6(b\gamma)\right)\right)\overline{S}_1(a) + \chi\left(\mathrm{Tr}_1^6\left(b\xi^2\right)\right)\left(1+\chi\left(\mathrm{Tr}_1^6\left(b\gamma^2\right)\right)\right)\overline{S}_2(a) \\ + \chi\left(\mathrm{Tr}_1^6\left(b\xi^3\right)\right)\left(1+\chi\left(\mathrm{Tr}_1^6\left(b(\gamma^3+\gamma)\right)\right)\right)\overline{S}_3(a) + \chi\left(\mathrm{Tr}_1^6\left(b\xi^4\right)\right)\left(1+\chi\left(\mathrm{Tr}_1^6\left(b\gamma^4\right)\right)\right)\overline{S}_4(a) \ .\end{aligned}$$

Next, recall that $\sum_{i=0}^{8}\xi^i = 0$. Hence, $\gamma^2+\gamma^3+\gamma^4 = 1$ and

$$\mathrm{Tr}_1^6(b\gamma) + \mathrm{Tr}_1^6\left(b\gamma^2\right) + \mathrm{Tr}_1^6\left(b(\gamma+\gamma^3)\right) + \mathrm{Tr}_1^6\left(b\gamma^4\right) = \mathrm{Tr}_1^6(b) \ .$$

We now explicitely compute the traces $\mathrm{Tr}_1^6\left(b\xi^i\right)$. The finite field $\mathbb{F}_{64}$ is represented as $\mathbb{F}_2[x]/(C_6(x))$ where $C_6(x) = x^6+x^4+x^3+x+1$ is the 6-th Conway polynomial. We denote the class of x modulo $C_6(x)$ by β; this is a primitive element of $\mathbb{F}_{64}$. Let $\xi = \beta^7$ be a 9-th root of unity. The traces $\mathrm{Tr}_1^6\left(\beta^j\xi^i\right)$ are given in Table 3. The expression of $\Lambda(a,\beta^j)$ as a sum of the partial exponential sums $\overline{S}_i$, together with the minimal polynomial m_j of β^j, are given in Tables 4 and 5.

Moreover, if the coefficients a_r lie in $\mathbb{F}_{2^l}$, where $l = m/3$, then 2^l is -1, 2 or -4 modulo 9 when l is respectively 0, 1 and 2 modulo 3. In the last two cases, Lemma 3.22 tells that

$$\overline{S}_1(a) = \overline{S}_2(a) = \overline{S}_4(a) \ .$$

The corresponding expressions for $\Lambda(a,b)$, obtained after applying Lemma 3.20 for $l=1$, $l=3$ and $l=9$, are given in Table 6, where m_b is the minimal polynomial of b.

Finally, the following theorem summarizes the above discussion.

Theorem 5.5. *Let $\tau = 9$ and $m \equiv 3 \pmod 6$.*

1. *If $b=1$, then $9\Lambda(a,1) = 18T_1(g_a) - 12T_1(g_a\circ D_3) + 4T_1(g_a\circ D_9)) + 5$.*
2. *If b is a primitive 3-rd root of unity, then $9\Lambda(f_{a,b}) = 18T_1(g_a) - 6T_1(g_a\circ D_3) - 2T_1(g_a\circ D_9) + 5$.*
3. *Suppose moreover that $a_r \in \mathbb{F}_{2^{\frac{m}{3}}}$ and $\frac{m}{3} \not\equiv 0 \pmod 3$.*
   (a) *If the minimal polynomial of b is x^3+x+1, then $9\Lambda(a,b) = -6T_1(g_a) + 8T_1(g_a\circ D_3) + 1$.*
   (b) *If the minimal polynomial of b is x^3+x^2+1, then $9\Lambda(a,b) = -6T_1(g_a) - 4T_1(g_a\circ D_3) + 4T_1(g_a\circ D_9) - 3$.*
   (c) *If the minimal polynomial of b is x^6+x^3+1, then $9\Lambda(a,b) = 6T_1(g_a) + 4T_1(g_a\circ D_3) + 5$.*
   (d) *If the minimal polynomial of b is $x^6+x^4+x^2+x+1$, then $9\Lambda(a,b) = -6T_1(g_a) + 8T_1(g_a\circ D_3) + 1$.*
   (e) *If the minimal polynomial of b is $x^6+x^5+x^4+x^2+1$, then $9\Lambda(a,b) = -6T_1(g_a) + 2T_1(g_a\circ D_3) - 2T_1(g_a\circ D_9) - 3$.*
   (f) *If the minimal polynomial of b is x^6+x+1, then $9\Lambda(a,b) = -6T_1(g_a) - 4T_1(g_a\circ D_3) + 4T_1(g_a\circ D_9) - 3$.*
   (g) *If the minimal polynomial of b is x^6+x^5+1, then $9\Lambda(a,b) = 6T_1(g_a) - 2T_1(g_a\circ D_3) - 2T_1(g_a\circ D_9) + 1$.*
   (h) *If the minimal polynomial of b is $x^6+x^4+x^3+x+1$, then $9\Lambda(a,b) = 6T_1(g_a) - 8T_1(g_a\circ D_3) + 4T_1(g_a\circ D_9) + 1$.*
   (i) *If the minimal polynomial of b is $x^6+x^5+x^2+x+1$, then $9\Lambda(a,b) = 6T_1(g_a) - 2T_1(g_a\circ D_3) - 2T_1(g_a\circ D_9) + 1$.*

$j\backslash i$	0	1	2	3	4	5	6	7	8
0	0	0	0	1	0	0	1	0	0
1	0	0	0	1	1	0	1	1	0
2	0	0	0	1	0	1	1	0	1
3	1	0	0	1	1	1	0	1	1
4	0	1	0	1	0	0	1	1	0
5	0	1	1	1	1	0	1	0	1
6	1	1	0	0	0	1	1	1	1
7	0	0	1	0	0	1	0	0	0
8	0	0	1	1	0	1	1	0	0
9	0	0	1	0	1	1	0	1	0
10	0	0	1	1	1	0	1	1	1
11	1	0	1	0	0	1	1	0	0
12	1	1	1	1	0	1	0	1	0
13	1	0	0	0	1	1	1	1	1
14	0	1	0	0	1	0	0	0	0
15	0	1	1	0	1	1	0	0	0
16	0	1	0	1	1	0	1	0	0
17	0	1	1	1	0	1	1	1	0
18	0	1	0	0	1	1	0	0	1
19	1	1	1	0	1	0	1	0	1
20	0	0	0	1	1	1	1	1	1
21	1	0	0	1	0	0	0	0	0
22	1	1	0	1	1	0	0	0	0
23	1	0	1	1	0	1	0	0	0
24	1	1	1	0	1	1	1	0	0
25	1	0	0	1	1	0	0	1	0
26	1	1	0	1	0	1	0	1	1
27	0	0	1	1	1	1	1	1	0
28	0	0	1	0	0	0	0	0	1
29	1	0	1	1	0	0	0	0	1
30	0	1	1	0	1	0	0	0	1
31	1	1	0	1	1	1	0	0	1

$j\backslash i$	0	1	2	3	4	5	6	7	8
32	0	0	1	1	0	0	1	0	1
33	1	0	1	0	1	0	1	1	1
34	0	1	1	1	1	1	1	0	0
35	0	1	0	0	0	0	0	1	0
36	0	1	1	0	0	0	0	1	1
37	1	1	0	1	0	0	0	1	0
38	1	0	1	1	1	0	0	1	1
39	0	1	1	0	0	1	0	1	0
40	0	1	0	1	0	1	1	1	1
41	1	1	1	1	1	1	0	0	0
42	1	0	0	0	0	0	1	0	0
43	1	1	0	0	0	0	1	1	0
44	1	0	1	0	0	0	1	0	1
45	0	1	1	1	0	0	1	1	1
46	1	1	0	0	1	0	1	0	0
47	1	0	1	0	1	1	1	1	0
48	1	1	1	1	1	0	0	0	1
49	0	0	0	0	0	1	0	0	1
50	1	0	0	0	0	1	1	0	1
51	0	1	0	0	0	1	0	1	1
52	1	1	1	0	0	1	1	1	0
53	1	0	0	1	0	1	0	0	1
54	0	1	0	1	1	1	1	0	1
55	1	1	1	1	0	0	0	1	1
56	0	0	0	0	1	0	0	1	0
57	0	0	0	0	1	1	0	1	1
58	1	0	0	0	1	0	1	1	0
59	1	1	0	0	1	1	1	0	1
60	0	0	1	0	1	0	0	1	1
61	1	0	1	1	1	1	0	1	0
62	1	1	1	0	0	0	1	1	1

Table 3: Traces for $\tau = 9$

j	$\Lambda(a,\beta^j)$	m_j
0	$\overline{S}_0+2\overline{S}_1+2\overline{S}_2-2\overline{S}_3+2\overline{S}_4$	$x+1$
1	$\overline{S}_0+2\overline{S}_1-2\overline{S}_3$	$x^6+x^4+x^3+x+1$
2	$\overline{S}_0+2\overline{S}_2-2\overline{S}_3$	$x^6+x^4+x^3+x+1$
3	$-\overline{S}_0-2\overline{S}_4$	$x^6+x^5+x^4+x^2+1$
4	$\overline{S}_0-2\overline{S}_3+2\overline{S}_4$	$x^6+x^4+x^3+x+1$
5	$\overline{S}_0-2\overline{S}_1-2\overline{S}_3$	x^6+x+1
6	$-\overline{S}_0-2\overline{S}_1$	$x^6+x^5+x^4+x^2+1$
7	$\overline{S}_0+2\overline{S}_1+2\overline{S}_3$	x^6+x^3+1
8	$\overline{S}_0+2\overline{S}_1-2\overline{S}_3$	$x^6+x^4+x^3+x+1$
9	$\overline{S}_0+2\overline{S}_1-2\overline{S}_2+2\overline{S}_3-2\overline{S}_4$	x^3+x+1
10	$\overline{S}_0-2\overline{S}_2-2\overline{S}_3$	x^6+x+1
11	$-\overline{S}_0+2\overline{S}_1$	$x^6+x^5+x^2+x+1$
12	$-\overline{S}_0-2\overline{S}_2$	$x^6+x^5+x^4+x^2+1$
13	$-\overline{S}_0-2\overline{S}_4$	$x^6+x^5+x^4+x+1$
14	$\overline{S}_0+2\overline{S}_2+2\overline{S}_3$	x^6+x^3+1
15	$\overline{S}_0+2\overline{S}_3-2\overline{S}_4$	$x^6+x^4+x^2+x+1$
16	$\overline{S}_0+2\overline{S}_2-2\overline{S}_3$	$x^6+x^4+x^3+x+1$
17	$\overline{S}_0-2\overline{S}_2-2\overline{S}_3$	x^6+x+1
18	$\overline{S}_0-2\overline{S}_1+2\overline{S}_2+2\overline{S}_3-2\overline{S}_4$	x^3+x+1
19	$-\overline{S}_0-2\overline{S}_1$	$x^6+x^5+x^4+x+1$
20	$\overline{S}_0-2\overline{S}_3-2\overline{S}_4$	x^6+x+1
21	$-\overline{S}_0+2\overline{S}_1+2\overline{S}_2+2\overline{S}_4$	x^2+x+1
22	$-\overline{S}_0+2\overline{S}_2$	$x^6+x^5+x^2+x+1$
23	$-\overline{S}_0+2\overline{S}_1$	x^6+x^5+1
24	$-\overline{S}_0-2\overline{S}_4$	$x^6+x^5+x^4+x^2+1$
25	$-\overline{S}_0+2\overline{S}_1$	$x^6+x^5+x^2+x+1$
26	$-\overline{S}_0-2\overline{S}_1$	$x^6+x^5+x^4+x+1$
27	$\overline{S}_0+2\overline{S}_1-2\overline{S}_2-2\overline{S}_3-2\overline{S}_4$	x^3+x^2+1
28	$\overline{S}_0+2\overline{S}_3+2\overline{S}_4$	x^6+x^3+1
29	$-\overline{S}_0+2\overline{S}_4$	x^6+x^5+1
30	$\overline{S}_0-2\overline{S}_1+2\overline{S}_3$	$x^6+x^4+x^2+x+1$
31	$-\overline{S}_0-2\overline{S}_1+2\overline{S}_2-2\overline{S}_4$	$x^6+x^5+x^3+x^2+1$

Table 4: $\Lambda(a,\beta^j)$ for $\tau=9$ — Part I

j	$\Lambda(a,\beta^j)$	m_j
32	$\overline{S}_0 - 2\overline{S}_3 + 2\overline{S}_4$	$x^6+x^4+x^3+x+1$
33	$-\overline{S}_0 - 2\overline{S}_2$	$x^6+x^5+x^4+x^2+1$
34	$\overline{S}_0 - 2\overline{S}_3 - 2\overline{S}_4$	x^6+x+1
35	$\overline{S}_0 + 2\overline{S}_3 + 2\overline{S}_4$	x^6+x^3+1
36	$\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_2 + 2\overline{S}_3 + 2\overline{S}_4$	x^3+x+1
37	$-\overline{S}_0 + 2\overline{S}_4$	$x^6+x^5+x^2+x+1$
38	$-\overline{S}_0 - 2\overline{S}_2$	$x^6+x^5+x^4+x+1$
39	$\overline{S}_0 - 2\overline{S}_2 + 2\overline{S}_3$	$x^6+x^4+x^2+x+1$
40	$\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_3$	x^6+x+1
41	$-\overline{S}_0 - 2\overline{S}_4$	$x^6+x^5+x^4+x+1$
42	$-\overline{S}_0 + 2\overline{S}_1 + 2\overline{S}_2 + 2\overline{S}_4$	x^2+x+1
43	$-\overline{S}_0 + 2\overline{S}_4$	x^6+x^5+1
44	$-\overline{S}_0 + 2\overline{S}_4$	$x^6+x^5+x^2+x+1$
45	$\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_2 - 2\overline{S}_3 + 2\overline{S}_4$	x^3+x^2+1
46	$-\overline{S}_0 + 2\overline{S}_2$	x^6+x^5+1
47	$-\overline{S}_0 + 2\overline{S}_1 - 2\overline{S}_2 - 2\overline{S}_4$	$x^6+x^5+x^3+x^2+1$
48	$-\overline{S}_0 - 2\overline{S}_1$	$x^6+x^5+x^4+x^2+1$
49	$\overline{S}_0 + 2\overline{S}_2 + 2\overline{S}_3$	x^6+x^3+1
50	$-\overline{S}_0 + 2\overline{S}_2$	$x^6+x^5+x^2+x+1$
51	$\overline{S}_0 - 2\overline{S}_1 + 2\overline{S}_3$	$x^6+x^4+x^2+x+1$
52	$-\overline{S}_0 - 2\overline{S}_2$	$x^6+x^5+x^4+x+1$
53	$-\overline{S}_0 + 2\overline{S}_2$	x^6+x^5+1
54	$\overline{S}_0 - 2\overline{S}_1 + 2\overline{S}_2 - 2\overline{S}_3 - 2\overline{S}_4$	x^3+x^2+1
55	$-\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_2 + 2\overline{S}_4$	$x^6+x^5+x^3+x^2+1$
56	$\overline{S}_0 + 2\overline{S}_1 + 2\overline{S}_3$	x^6+x^3+1
57	$\overline{S}_0 + 2\overline{S}_3 - 2\overline{S}_4$	$x^6+x^4+x^2+x+1$
58	$-\overline{S}_0 + 2\overline{S}_1$	x^6+x^5+1
59	$-\overline{S}_0 - 2\overline{S}_1 + 2\overline{S}_2 - 2\overline{S}_4$	$x^6+x^5+x^3+x^2+1$
60	$\overline{S}_0 - 2\overline{S}_2 + 2\overline{S}_3$	$x^6+x^4+x^2+x+1$
61	$-\overline{S}_0 + 2\overline{S}_1 - 2\overline{S}_2 - 2\overline{S}_4$	$x^6+x^5+x^3+x^2+1$
62	$-\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_2 + 2\overline{S}_4$	$x^6+x^5+x^3+x^2+1$

Table 5: $\Lambda(a,\beta^j)$ for $\tau = 9$ — Part II

m_b	$9\Lambda(a,b)$	$o(b)$
$x+1$	$18T_1(g_a) - 12T_1(g_a \circ D_3) + 4T_1(g_a \circ D_9) + 5$	1
x^2+x+1	$18T_1(g_a) - 6T_1(g_a \circ D_3) - 2T_1(g_a \circ D_9) + 5$	3
x^3+x+1	$-6T_1(g_a) + 8T_1(g_a \circ D_3) + 1$	7
x^3+x^2+1	$-6T_1(g_a) - 4T_1(g_a \circ D_3) + 4T_1(g_a \circ D_9) - 3$	7
x^6+x^3+1	$6T_1(g_a) + 4T_1(g_a \circ D_3) + 5$	9
$x^6+x^4+x^2+x+1$	$-6T_1(g_a) + 8T_1(g_a \circ D_3) + 1$	21
$x^6+x^5+x^4+x^2+1$	$-6T_1(g_a) + 2T_1(g_a \circ D_3) - 2T_1(g_a \circ D_9) - 3$	21
x^6+x+1	$-6T_1(g_a) - 4T_1(g_a \circ D_3) + 4T_1(g_a \circ D_9) - 3$	63
x^6+x^5+1	$6T_1(g_a) - 2T_1(g_a \circ D_3) - 2T_1(g_a \circ D_9) + 1$	63
$x^6+x^4+x^3+x+1$	$6T_1(g_a) - 8T_1(g_a \circ D_3) + 4T_1(g_a \circ D_9) + 1$	63
$x^6+x^5+x^2+x+1$	$6T_1(g_a) - 2T_1(g_a \circ D_3) - 2T_1(g_a \circ D_9) + 1$	63
$x^6+x^5+x^4+x+1$	$-6T_1(g_a) + 2T_1(g_a \circ D_3) - 2T_1(g_a \circ D_9) - 3$	63
$x^6+x^5+x^3+x^2+1$	$-6T_1(g_a) + 2T_1(g_a \circ D_3) - 2T_1(g_a \circ D_9) - 3$	63

Table 6: $\Lambda(a,\beta^j)$ for $\tau = 9$ — Subfield case

(j) If the minimal polynomial of b is $x^6+x^5+x^4+x+1$, then $9\Lambda(a,b) = -6T_1(g_a) + 2T_1(g_a \circ D_3) - 2T_1(g_a \circ D_9) - 3$.

(k) If the minimal polynomial of b is $x^6+x^5+x^3+x^2+1$, then $9\Lambda(a,b) = -6T_1(g_a) + 2T_1(g_a \circ D_3) - 2T_1(g_a \circ D_9) - 3$.

5.2.5 The case $\tau = 11$

To conclude this subsection, we give a few results for $\tau = 11$, the next suitable value for τ. In this case, $t = 10$ and $m \equiv 5 \pmod{10}$. In particular, $t < 2m$ as soon as $m \neq 5$. Furthermore, if $f_{a,b}$ is hyper-bent, then its dual is $f_{a,b^{3}2}$. Listing all possible characterizations would not be of high interest, hence we chose to only present results valid when the coefficients a_r are not restricted to a strict subfield of $\mathbb{F}_{2^m}$.

The finite field $\mathbb{F}_{1024}$ is represented as $\mathbb{F}_2[x]/(C_{10}(x))$ where $C_{10}(x) = x^{10}+x^6+x^5+x^3+x^2+x+1$ is the 10-th Conway polynomial. We denote the class of x modulo $C_{10}(x)$ by β; this is a primitive element of $\mathbb{F}_{1024}$. The characterizations valid for $a_r \in \mathbb{F}_{2^m}$ are summarized in the following theorem.

Theorem 5.6. *Let $\tau = 11$ and $m \equiv 5 \pmod{10}$.*

1. *If $b = 1$, then* $11\Lambda(a,1) = 4T_1(g_a \circ D_{11}) - 22T_1(g_a) - 9$.
2. *If b is a 3-rd root of unity, a 341-th root of unity with minimal polynomial $x^{10}+x^9+x^8+x^3+x^2+x+1$, or a primitive element with minimal polynomial $x^{10}+x^9+x^8+x^4+x^3+x^2+1$ or $x^{10}+x^9+x^8+x^6+x^5+x+1$, then* $11\Lambda(a,b) = -2T_1(g_a \circ D_{11}) - 1$.

6 Conclusion

In this note, we have extended previous characterizations of hyper-bentness by Charpin and Gong, Mesnager, and Wang et al., to much wider classes of Boolean functions, giving as well more insight on the tools and restrictions involved in these approaches. A challenging question is to prove that the families of Boolean function considered in this note actually contain hyper-bent functions. Such results are quite rare and usually involve highbrow results, e.g. results from

algebraic curves theory. The case of monomial functions with the Dillon exponent is a much celebrated theorem of Lachaud and Wolfmann [12, Theorem 3.4]. The case of binomial functions with the Dillon exponent and an additional trace term over $\mathbb{F}_4$ has been treated by Mesnager [15], that of binomial functions with the Dillon exponent and an additional trace term over $\mathbb{F}_{16}$ has been treated by Wang et al. [19, 18].

References

[1] Claude Carlet and Philippe Gaborit. Hyper-bent functions and cyclic codes. *J. Comb. Theory, Ser. A*, 113(3):466–482, 2006.

[2] Pascale Charpin and Guang Gong. Hyperbent functions, Kloosterman sums, and Dickson polynomials. *IEEE Transactions on Information Theory*, 54(9):4230–4238, 2008.

[3] Wun Seng Chou, Javier Gomez-Calderon, and Gary L. Mullen. Value sets of Dickson polynomials over finite fields. *J. Number Theory*, 30(3):334–344, 1988.

[4] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[5] J. F. Dillon and Hans Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields and Their Applications*, 10(3):342–389, 2004.

[6] John Francis Dillon. *Elementary Hadamard Difference Sets*. ProQuest LLC, Ann Arbor, MI, 1974. Thesis (Ph.D.)–University of Maryland, College Park.

[7] François G. Dorais and Dominic W. Klyve. A Wieferich prime search up to 6.7×10^{15}. *Journal of Integer Sequences*, 14(9), 2011. Available online at `http://www.cs.uwaterloo.ca/journals/JIS/`.

[8] Guang Gong and Solomon W. Golomb. Transform domain analysis of DES. *IEEE Transactions on Information Theory*, 45(6):2065–2073, 1999.

[9] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford Ser. (2)*, 37(145):27–38, 1986.

[10] Christopher Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.

[11] The OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. `http://oeis.org`.

[12] Gilles Lachaud and Jacques Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. *IEEE Transactions on Information Theory*, 36(3):686Ð692, 1990.

[13] R. Lidl, G. L. Mullen, and G. Turnwald. *Dickson polynomials*, volume 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, Harlow, 1993.

[14] Sihem Mesnager. Hyper-bent Boolean functions with multiple trace terms. In M. Anwar Hasan and Tor Helleseth, editors, *WAIFI*, volume 6087 of *Lecture Notes in Computer Science*, pages 97–113. Springer, 2010.

[15] Sihem Mesnager. A new class of bent and hyper-bent Boolean functions in polynomial forms. *Des. Codes Cryptography*, 59(1-3):265–279, 2011.

[16] Hwasin Park, Joongsoo Park, and Daeyeoul Kim. A criterion on primitive roots modulo p. *J. KSIAM*, 4(1):29–38, 2000.

[17] O. S. Rothaus. On "bent" functions. *J. Comb. Theory, Ser. A*, 20(3):300–305, 1976.

[18] Baocheng Wang, Chunming Tang, Yanfeng Qi, and Yixian Yang. A generalization of the class of hyper-bent Boolean functions in binomial forms. Cryptology ePrint Archive, Report 2011/698, 2011. `http://eprint.iacr.org/`.

[19] Baocheng Wang, Chunming Tang, Yanfeng Qi, Yixian Yang, and Maozhi Xu. A new class of hyper-bent Boolean functions in binomial forms. *CoRR*, abs/1112.0062, 2011.

[20] Baocheng Wang, Chunming Tang, Yanfeng Qi, Yixian Yang, and Maozhi Xu. A new class of hyper-bent Boolean functions with multiple trace terms. Cryptology ePrint Archive, Report 2011/600, 2011. `http://eprint.iacr.org/`.

[21] Amr M. Youssef and Guang Gong. Hyper-bent functions. In Birgit Pfitzmann, editor, *EUROCRYPT*, volume 2045 of *Lecture Notes in Computer Science*, pages 406–419. Springer, 2001.