An efficient characterization of a family of hyper-bent functions with multiple trace terms

Jean-Pierre Flori * Sihem Mesnager †

Sunday 8th January, 2012

Abstract

Lisoněk recently reformulated the characterization of Charpin and Gong of a large class of hyper-bent functions in terms of cardinalities of hyperelliptic curves following previous ideas of Lachaud and Wolfmann, and Katz and Livné. In this paper, we present a generic approach of such ideas and show that it applies naturally to a distinct family of functions proposed by Mesnager. Doing so, a polynomial time and space test for the hyper-bentness of functions in this family is obtained. We then show how this reformulation can be transformed to obtain a more efficient test leading to a substantial practical gain. We finally elaborate on an open problem about hyperelliptic curves related to a family of Boolean functions studied by charpin and Gong.

Keywords. Boolean functions, Walsh-Hadamard transform, Maximum nonlinearity, Hyper-bent functions, Hyperelliptic curves, Dickson polynomials.

1 Introduction

Boolean functions form an important component of various practical cryptographic algorithms. They can for example be viewed as components of S-boxes and are used in different types of cryptographic applications such as block ciphers, stream ciphers and in coding theory. One basic criterion for their design is nonlinearity. The significance of this aspect has again been demonstrated by the recent development of linear cryptanalysis by Matsui and others. Bent functions are Boolean functions achieving the highest possible nonlinearity. In view of the Parseval equation this definition implies that such functions only exist for an even number of variables.

Bent functions were introduced by Rothaus [23] in 1976. They turned out to be rather complicated combinatorial objects. A concrete description of all bent functions is elusive. The class of bent functions contains a subclass of functions, introduced by Youssef and Gong [25] in 2001, the so-called hyper-bent functions. In fact, the first definition of hyper-bent functions was based on a property of the extended Hadamard transform of Boolean functions introduced by Golomb and Gong [12]. Golomb and Gong proposed that S-boxes should not be approximated by a bijective monomial, providing a new criterion for S-box design. The classification of hyper-bent functions and many related problems remain open. In particular, it seems difficult to define

*Institut Télécom, Télécom ParisTech, UMR 7539, CNRS LTCI, 46 rue Barrault, F-75634 Paris Cedex 13, France. flori@enst.fr

†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

precisely an infinite class of hyper-bent functions, as indicated by the number of open problems proposed by Charpin and Gong [4].

Some explicit constructions of hyper-bent functions on $\mathbb{F}_{2^n}$ have been proposed in the literature. Monomial hyper-bent functions are famous bent functions due to Dillon [8]. The list of currently known hyper-bent functions is given in Table 1. Charpin and Gong [4] have characterized by means of Dickson polynomials a large class of hyper-bent functions, which includes the well-known monomial functions with the Dillon exponent as a particular case. Afterward Mesnager [21] has characterized by means of Dickson polynomials another class of hyper-bent functions, distinct from that of Charpin and Gong.

Very recently, Lisoněk [19] has reformulated the Charpin-Gong hyper-bentness criterion in terms of the number of rational points on certain hyperelliptic curves. Using this criterion, the hyper-bentness of a given function can be tested in both polynomial time and space in n. The ideas in its approach go back to the works of Lachaud and Wolfmann [14], and Katz and Livné [13]. In this paper, we present a generic formulation of such results leading us to easily deduce the previous results of Lachaud and Wolfmann, Katz and Livné, or Lisoněk, as well as giving an efficient version of the more recent hyper-bentness criterion proposed by Mesnager for a different class of Boolean functions in polynomial form. We subsequently propose a slightly different version leading to practical speed-ups in the test for hyper-bentness and so in the generation of hyper-bent functions.

This paper is organized as follows. In Section 2, we recall definitions for Boolean functions, binary exponential sums, Dickson polynomials and hyperelliptic curves. In Section 3, we recall the known classes of hyper-bent functions. We then present the general framework to express several exponential sums in terms of cardinalities of hyperelliptic curves and deduce the different reformulations mentioned above.

2 Notation and preliminaries

For any set S, $S^* = S \setminus \{0\}$ and $\#S$ denotes the cardinality of S. Unless stated otherwise, m will be a positive integer greater than 3 and the Boolean functions we study will have $n = 2m$ inputs.

2.1 Boolean functions in polynomial form

A Boolean function f on $\mathbb{F}_{2^n}$ is an $\mathbb{F}_2$-valued function on the Galois field $\mathbb{F}_{2^n}$ of order 2^n. The *weight* of f, denoted by $\mathrm{wt}(f)$, is the *Hamming weight* of the image vector of f, that is, the cardinality of its support $\{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.

For any positive integer k, and r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$ is denoted by $\mathrm{Tr}_r^k(\cdot)$. It can be defined as

$$\mathrm{Tr}_r^k(x) = \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}} \ .$$

In particular, we denote the *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ by $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

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

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

valid for all $x \in \mathbb{F}_{2^n}$ and called its polynomial form. In the above expression:

- Γ_n is the set of integers obtained by choosing one element in each cyclotomic coset modulo $2^n - 1$ (including the trivial coset containing 0 and only 0), the most usual choice being the smallest element in each cyclotomic coset, called the coset leader,
- $o(j)$ is the size of the cyclotomic coset containing j,
- and $\epsilon = \mathrm{wt}(f) \pmod 2$.

The *algebraic degree* of f is then equal to the maximum 2-weight (or Hamming weight) of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$.

2.2 Walsh-Hadamard transform, bent and hyper-bent functions

Let f be a Boolean function on $\mathbb{F}_{2^n}$. Its *"sign" function* is the integer-valued function $\chi(f) = (-1)^f$. 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. They only exist for n even and can be defined as follows.

Definition 2.1. *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) 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 $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be hyper-bent if its extended Walsh-Hadamard transform only takes the values $\pm 2^{\frac{n}{2}}$.*

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

2.3 Binary exponential sums

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

Definition 2.3 (Binary Kloosterman sums)**.** *The binary Kloosterman sums on $\mathbb{F}_{2^m}$ are:*

$$K_m(a) = 1 + \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_1^m\left(ax + \frac{1}{x}\right)}, \quad a \in \mathbb{F}_{2^m} \ .$$

It is an elementary fact that $K_m(a) = K_m(a^2)$.
The cubic sums are defined as follows.

Definition 2.4 (Cubic sums)**.** *The cubic sums on $\mathbb{F}_{2^m}$ are:*

$$C_m(a, b) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m\left(ax^3 + bx\right)}, \quad a, b \in \mathbb{F}_{2^m} \ .$$

We also define the following classical character sum on the set of (2^m+1)-th roots of unity.

Definition 2.5. *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*

$$\Lambda(f) = \sum_{u \in U} \chi\left(f(u)\right) \ .$$

2.4 Binary Dickson polynomials

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

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

Moreover, the family of Dickson polynomials $D_r(X)$ can also be defined by the following recurrence relation:

$$D_{i+2}(X) = X D_{i+1}(X) + D_i(X) \ ,$$

with initial values

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

The reader can refer to the monograph of Lidl, Mullen and Turnwald [18] for many useful properties and applications of Dickson polynomials. We give the list of the first six Dickson polynomials:

$$D_0(X) = 0, \ D_1(X) = X, \ D_2(X) = X^2 \ ,$$
$$D_3(X) = X + X^3, \ D_4(X) = X^4, \ D_5(X) = X + X^3 + X^5 \ .$$

2.5 Hyperelliptic curves

In this section we give basic definitions and results for hyperelliptic curves with a special emphasis on point counting on such curves over finite fields of even characteristic.

For a general overview of the theory of such curves, with a cryptographic point of view, the reader is referred to the textbooks of Cohen et al. [5] or that of Galbraith [10]. Hyperelliptic curves can be defined abstractly as follows.

Definition 2.6. *A hyperelliptic curve H is a smooth projective algebraic curve which is a degree 2 covering of the projective line.*

This definition includes elliptic curves, i.e. curves of genus 1, but it is sometimes understood that a hyperelliptic curve should be of genus $g \geq 2$, this is mainly a matter of taste.

Hyperelliptic curve can also be defined in a much more down-to-earth manner by giving an equation describing their affine part. In even characteristic, normal forms for such equations have been completely described by Enge [9]. For cryptographic applications however, the curves are often chosen to be *imaginary* hyperelliptic curves. This is also the only kind of curves we will encounter in this paper. For such curves, the equation describing the affine part of the curve can be chosen to be of the following form:

$$H : y^2 + h(x)y = f(x) \ ,$$

where $h(x)$ is of a polynomial of degree $\leq g$, the genus of the curve, and $f(x)$ is a monic polynomial of degree $2g+1$. Furthermore, imaginary hyperelliptic curves have always exactly

one point at infinity. Beware that the point at infinity on the projective curve associated with the homogenization of the above equation is singular as soon as $g \geq 2$. Hence, the hyperelliptic curve, which is smooth, is not the projective curve associated with the homogenized equation, but by a desingularization thereof. It is a fact that the obtained smooth curve has also exactly one point at infinity and that its affine part is described by the same equation as the original singular projective curve. Anyhow, we will be mostly interested in the affine parts of such curves so that the distinction between the singular and nonsingular models is not that important.

The cardinality of such a curve H over the finite field $\mathbb{F}_{2^m}$ is understood as its numbers of points with coordinates in the finite field $\mathbb{F}_{2^m}$, which are also called $\mathbb{F}_{2^m}$*-rational points*. It is denoted by $\#H(\mathbb{F}_{2^m})$. The reference to the finite field is usually omitted when the context makes it clear. A very important result is that there exist algorithms to compute that cardinality in polynomial time and space in m. Such a result has been given by Denef and Vercauteren [6, 7, 24] and is stated below.

Theorem 2.7. *Let H be an imaginary hyperelliptic curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the cardinality of H in*

$$O(g^3m^3(g^2 + \log^2 m \log\log m) \log gm \log\log gm)$$

bit operations and $O(g^4m^3)$ memory.

A slightly stronger result is true for hyperelliptic curves of a special form: the Artin-Schreier curves.

Definition 2.8. *An Artin-Schreier curve is an imaginary hyperelliptic curve whose affine part is given by an equation of the form:*

$$H : y^2 + x^k y = f(x),$$

where g is the genus of the curve, $0 \leq k \leq g$ and $f(x)$ is monic of degree $2g + 1$.

Theorem 2.9. *Let H be an Artin-Schreier curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the cardinality of H in*

$$O(g^3m^3(g^2 + \log^2 m \log\log m) \log gm \log\log gm)$$

bit operations and $O(g^3m^3)$ memory.

A quasi-quadratic algorithm was also described by Lercier and Lubicz [17].

Theorem 2.10. *Let H be a hyperelliptic curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the cardinality of H in*

$$O(2^{4g+o(1)}g^3m^{2+o(1)})$$

bit operations and $O(2^{3g+o(1)}m^2)$ memory.

Nevertheless, it should be remarked that the time and space complexities of this last algorithm are exponential in the genus of the curve.

Class of functions	Conditions on the coefficients	References
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$	$K_m(a)=0$	[8, 15, 16, 4]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)+\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$; m odd	$K_m(a)=4$	[22]
$\mathrm{Tr}_1^n\left(a\zeta^i x^{3(2^m-1)}\right)+\mathrm{Tr}_1^2\left(\beta^j x^{\frac{2^n-1}{3}}\right)$; m odd and $m\not\equiv 3 \pmod 6$, β is a primitive element of $\mathbb{F}_4$, ζ is a generator of the cyclic group U of (2^m+1)-th roots of unity, $(i,j)\in\{0,1,2\}^2$	$K_m(a)=4$ and $\mathrm{Tr}_1^m\left(a^{1/3}\right)=0$	[20]
$\mathrm{Tr}_1^n\left(a\zeta^i x^{3(2^m-1)}\right)+\mathrm{Tr}_1^2\left(\beta^j x^{\frac{2^n-1}{3}}\right)$; m odd and $m\not\equiv 3 \pmod 6$, β is a primitive element of $\mathbb{F}_4$, ζ is a generator of the cyclic group U of (2^m+1)-th roots of unity, $i\in\{1,2\}$, $j\in\{0,1,2\}$	$K_m(a)+C_m(a,a)=4$ and $\mathrm{Tr}_1^m\left(a^{1/3}\right)=1$	[20]
$\sum_{i=1}^{2^{m-1}-1}\mathrm{Tr}_1^n\left(ax^{i(2^m-1)}\right)$	$a\notin\mathbb{F}_2$	[11].
$\sum_{i=1}^{2^{m-2}-1}\mathrm{Tr}_1^n\left(ax^{i(2^m-1)}\right)$; m odd	$\mathrm{Tr}_1^m\left(a^{(2^m-4)^{-1}}\right)=0$	[11]

Table 1: Families of hyper-bent functions

3 Constructions of hyper-bent functions

3.1 Hyper-bent functions in polynomial form: state of the art

The list of currently known hyper-bent functions is given in Table 1 where $n=2m$ is an even integer, r is an integer co-prime with 2^m+1, and $a\in\mathbb{F}_{2^m}^*$ and $b\in\mathbb{F}_4^*$ are non-zero finite field elements.

Moreover, Charpin and Gong [4] gave a characterization of hyper-bentness for a large class of Boolean functions defined on $\mathbb{F}_{2^n}$, which includes the well-known monomial functions with the Dillon exponent as a special case.

Theorem 3.1 (Charpin-Gong criterion [4, Theorem 7]). *Let $n=2m$. Let S be a set of representatives of the cyclotomic classes modulo 2^m+1 whose cosets have full size n. Let f_a be the function defined on $\mathbb{F}_{2^n}$ by $f_a(x)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right)$, where $R\subseteq S$ and $a_r\in\mathbb{F}_{2^m}$. Let g_a be the Boolean function defined on $\mathbb{F}_{2^m}$ by $g_a(x)=\sum_{r\in R}\mathrm{Tr}_1^m\left(a_r D_r(x)\right)$. Then f_a is hyper-bent if and only if*

$$\sum_{x\in\mathbb{F}_{2^m}^*}\chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right)+g_a(x)\right)=2^m-2\,\mathrm{wt}(g_a)-1\ .$$

More recently, Mesnager [21][1] gave a similar characterization of hyper-bentness for another large class of hyper-bent functions with multiple trace terms which do not belong to the family considered by Charpin and Gong [4].

Theorem 3.2 (Mesnager criterion [21, Theorems 13 and 15]). *Let $n=2m$ with m odd and S be a set of representatives of the cyclotomic classes modulo 2^n-1 whose cosets have full size n. Let $b\in\mathbb{F}_4^*$. Let $f_{a,b}$ be the function defined on $\mathbb{F}_{2^n}$ by*

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

where $R\subseteq S$ and all the coefficients a_r are in $\mathbb{F}_{2^m}$. Let g_a be the related function defined on $\mathbb{F}_{2^m}$ by $g_a(x)=\sum_{r\in R}\mathrm{Tr}_1^m\left(a_r D_r(x)\right)$, where $D_r(x)$ is the Dickson polynomial of degree r. Then:

[1] There was a typo in the theorem given in the original article [21] where the last term in the right hand side of Condition 2c reads 4 instead of 3. This is an unfortunate consequence of the fact that the summation set used in the statement of that condition within the theorem is $\mathbb{F}_{2^m}^*$, whereas it is $\mathbb{F}_{2^m}$ within the proof of the theorem.

1. *$f_{a,b}$ is hyper-bent if and only if $f_{a,b}$ is bent.*
2. *If b is a primitive element of $\mathbb{F}_4$, then the three following assertions are equivalent:*
   (a) *$f_{a,b}$ is hyper-bent;*
   (b) $\displaystyle\sum_{x\in\mathbb{F}_{2^m}^*,\ \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a(D_3(x))\right) = -2$;
   (c) $\displaystyle\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_a(D_3(x))\right) = 2^m - 2\,\mathrm{wt}(g_a \circ D_3) + 3$.
3. *$f_{a,1}$ is hyper-bent if and only if*

$$2 \sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a(D_3(x))\right) - 3 \sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a(x)\right) = 2 \ .$$

3.2 Reformulation in terms of cardinalities of hyperelliptic curves

The characterizations of hyper-bentness given by Charpin and Gong (Theorem 3.1) and Mesnager (Theorem 3.2) can be naturally reformulated in terms of cardinalities of hyperelliptic curves. These ideas go back to the works of Lachaud and Wolfmann [14], and Katz and Livné [13], and the reformulation of Kloosterman sums using elliptic curves.

We begin this section by giving two propositions relating exponential sums with cardinalities of hyperelliptic curves.

Proposition 3.3. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function such that $f(0) = 0$, $g = \mathrm{Tr}_1^m(f)$ be its composition with the absolute trace and G_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by*

$$G_f : y^2 + y = f(x) \ .$$

Then

$$\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g(x)\right) = -2^m - 1 + \#G_f \ .$$

Proof. The first step of the proof is to express $\chi(g(c))$ as $1 - 2g(x)$ where $g(x)$ is now understood to be integer-valued:

$$\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g(x)\right) = \sum_{x\in\mathbb{F}_{2^m}^*} \left(1 - 2g(x)\right) \ .$$

The sum can then be split according to the value of $g(x)$ yielding the equality

$$\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g(x)\right) = 2^m - 1 - 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid g(x) = 1\right\} \ .$$

We supposed that $g(0) = 0$, so we can include zero in the summation set in the right hand side of the previous equality and deduce

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g(x)\right) &= 2^m - 1 - 2\#\left\{x \in \mathbb{F}_{2^m} \mid g(x) = 1\right\} \\ &= 2^m - 1 - 2\left(2^m - \#\left\{x \in \mathbb{F}_{2^m} \mid g(x) = 0\right\}\right) \\ &= -2^m - 1 + 2\#\left\{x \in \mathbb{F}_{2^m} \mid g(x) = 0\right\} \ .\end{aligned}$$

The additive version of Hilbert's Theorem 90 characterizes elements of trace zero as those which can be written as $t + t^2$ so that we get the equivalent formulation

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(g(x)\right) = -2^m - 1 + 2\#\left\{x \in \mathbb{F}_{2^m} \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + t = f(x)\right\} \ .$$

The last term of the right hand side of the above equality is nothing but the number of $\mathbb{F}_{2^m}$-rational (affine) points of G_f, whence

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(g(x)\right) = -2^m - 1 + \#G_f \ ,$$

which concludes the proof of the proposition. □

Proposition 3.4. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function, $g = \mathrm{Tr}_1^m(f)$ be its composition with the absolute trace and H_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by*

$$H_f : y^2 + xy = x + x^2 f(x) \ ,$$

Then

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g(x)\right) = -2^m + \#H_f \ .$$

Proof. The proof is quite similar as that of Proposition 3.3. It begins with the same sequence of equalities:

$$\begin{aligned}
\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g(x)\right) &= \sum_{x \in \mathbb{F}_{2^m}^*} \left(1 - 2(\mathrm{Tr}_1^m\left(x^{-1}\right) + g(x))\right) \\
&= 2^m - 1 - 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m\left(x^{-1}\right) + g(x) = 1\right\} \\
&= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m\left(x^{-1}\right) + g(x) = 0\right\} \\
&= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + t = x^{-1} + f(x)\right\} \ .
\end{aligned}$$

The additional step is then to substitute t by t/x before clearing denominators, which is legal since x is non-zero, before finishing the proof using the same arguments.

$$\begin{aligned}
\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g(x)\right) &= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ (t/x)^2 + (t/x) = x^{-1} + f(x)\right\} \\
&= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + xt = x + x^2 f(x)\right\} \\
&= -2^m + 1 + \#H_f - \#\left\{P \in H_f \mid x = 0\right\} \\
&= -2^m + \#H_f \ .
\end{aligned}$$

□

The sets of elements whose inverse have a given absolute trace are important objects to study.

Definition 3.5. *Let $i \in \mathbb{F}_2$. Then $\mathcal{T}_i$ denotes the set*

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

We will frequently use the following easy lemma which involves such sets and that we state without proof.

Lemma 3.6. *Let $g : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function. Then*

$$\sum_{x \in T_i} \chi\left(g(x)\right) = \frac{1}{2}\left(\sum_{x \in \mathbb{F}_{2^m}} \chi\left(g(x)\right) + (-1)^i \sum_{x \in \mathbb{F}_{2^m}} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g(x)\right)\right) \ .$$

Combined with Propositions 3.3 and 3.4, it gives an expression of the sums on $\mathcal{T}_i$ using cardinalities of hyperelliptic curves.

Corollary 3.7. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function such that $f(0) = 0$, $g = \mathrm{Tr}_1^m(f)$ be its composition with the absolute trace. Let G_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by*

$$G_f : y^2 + y = f(x) \ ,$$

and H_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by

$$H_f : y^2 + xy = x + x^2 f(x) \ ,$$

Then

$$\sum_{x \in \mathcal{T}_i} \chi\left(g(x)\right) = \frac{1}{2}\left((-2^m + \#G_f) + (-1)^i(-2^m + 1 + \#H_f)\right) \ .$$

The original result of Lachaud and Wolfmann, and Katz and Livné, is a direct consequence of the above propositions.

Theorem 3.8 ([14, 13])**.** *Let $m \geq 3$ be any positive integer, $a \in \mathbb{F}_{2^m}^*$ and E_a the (projective) elliptic curve defined over $\mathbb{F}_{2^m}$ whose affine part is given by the equation*

$$E_a : y^2 + xy = x^3 + a \ .$$

Then

$$\#E_a = 2^m + K_m(a) \ .$$

Proof. Indeed, the Kloosterman sum is defined as

$$K_m(a) = 1 + \sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) \ ,$$

so applying Proposition 3.4, we get

$$K_m(a) = 1 - 2^m + \#H_a \ ,$$

where H_a is the affine curve defined by

$$H_a : y^2 + xy = ax^3 + a \ .$$

The corresponding projective curve is nonsingular and not only has the same j-invariant as E_a, but is even isomorphic to E_a over $\mathbb{F}_{2^m}$. Hence, both curves have the same number of $\mathbb{F}_{2^m}$-rational (projective) points. Taking into account the only point at infinity on both curves, we deduce the equality of the theorem:

$$K_m(a) = -2^m + \#E_a \ .$$

□

This result has been used to reformulate the necessary and sufficient condition for hyper-bentness of the monomial functions with the Dillon exponent given in Table 1 as follows.

Proposition 3.9. *The notation is as in Theorem 3.8. Moreover let r be an integer such that $\gcd(r, 2^m+1) = 1$ and f_a be the Boolean function $f_a(x) = \mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$. Then f_a is hyper-bent if and only if*

$$\#E_a = 2^m \ .$$

The same remark applies to the class of binomial functions described by Mesnager [22].

Proposition 3.10. *The notation is as in Theorem 3.8. Moreover, suppose that m is odd and let r be an integer such that $\gcd(r, 2^m + 1) = 1$, $b \in \mathbb{F}_4^*$ and $f_{a,b}$ be the Boolean function $f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$. Then $f_{a,b}$ is hyper-bent[2] if and only if*

$$\#E_a = 2^m + 4 \ .$$

In particular, such results imply that testing the hyper-bentness of these monomial and binomial functions is polynomial time and space in m.

In fact, much more can be deduced from Propositions 3.3 and 3.4. Lisoněk [19, Theorem 2] used similar ideas to reformulate the Charpin-Gong criterion (Theorem 3.1). Using similar arguments as those given in Propositions 3.3 and 3.4, he could indeed express both sides of the criterion in terms of cardinalities of hyperelliptic curves. He went further and also expressed every value of the extended Walsh-Hadamard transform of the Boolean function of the Charpin-Gong family with such terms [19, Theorem 3].

Such an approach is valid in a more general setting as we show below. To this end, the first step is to express the character sum of Definition 2.5 in terms of exponential sums on all $\mathbb{F}_{2^m}$ and Dickson polynomials. These sums can then be transformed using Propositions 3.3 and 3.4.

Proposition 3.11. *The notation is as in Theorem 3.2 except that we allow b to be equal to zero. In that specific case, we do not suppose m to be odd. Let β be a primitive element of $\mathbb{F}_4$. Moreover, let G_a and H_a be the (affine) curves defined over $\mathbb{F}_{2^m}$ by*

$$G_a : y^2 + y = \sum_{r \in R} a_r D_r(x) \ ,$$
$$H_a : y^2 + xy = x + x^2 \sum_{r \in R} a_r D_r(x) \ ;$$

and let G_a^3 and H_a^3 be the (affine) curves defined over $\mathbb{F}_{2^m}$ by

$$G_a^3 : y^2 + y = \sum_{r \in R} a_r D_r(D_3(x)) \ ,$$
$$H_a^3 : y^2 + xy = x + x^2 \sum_{r \in R} a_r D_r(D_3(x)) \ .$$

Then

1. $\Lambda(f_{a,0}) = \#G_a - \#H_a$;
2. $\Lambda(f_{a,1}) = \dfrac{2}{3}\left(\#G_a^3 - \#H_a^3\right) - (\#G_a - \#H_a)$;

[2] In the original paper of Mesnager [22] it is first shown that the theorem is valid to characterize the bentness of $f_{a,b}$ and then that $f_{a,b}$ is bent if and only if it is hyper-bent.

3. $\Lambda(f_{a,\beta}) = \Lambda(f_{a,\beta^2}) = -\frac{1}{3}\left(\#G_a^3 - \#H_a^3\right)$.

Proof. The case $b = 0$ can be treated using the following equality established by Charpin and Gong [4, Proof of Theorem 7]:

$$\#\left\{u \in U \mid f_{a,0}(u) = 1\right\} = 2\#\left\{x \in \mathcal{T}_1 \mid g_a(x) = 1\right\} \quad .$$

Alternatively, one can directly use the more general lemma proved by Mesnager [21, Lemma 12] which states in particular that

$$\Lambda(f_{a,0}) = 1 + 2\sum_{x \in \mathcal{T}_1} \chi\left(g_a(x)\right) \quad .$$

According to Corollary 3.7, the quantity $\Lambda(f_{a,0})$ can then be expressed as

$$\begin{aligned}\Lambda(f_{a,0}) &= 1 + (-2^m + \#G_a) - (-2^m + 1 + \#H_a) \\ &= \#G_a - \#H_a \quad .\end{aligned}$$

The case $b = 1$ is treated using an equality mentioned by Mesnager [21, Proof of Theorem 15]:

$$\Lambda(f_{a,1}) = -\frac{1}{3} + \frac{4}{3}\sum_{x \in \mathcal{T}_1} \chi\left(g_a(D_3(x))\right) - 2\sum_{x \in \mathcal{T}_1} \chi\left(g_a(x)\right) \quad .$$

Corollary 3.7 is then used to obtain the equality

$$\begin{aligned}\Lambda(f_{a,1}) &= -\frac{1}{3} + \frac{2}{3}\left((-2^m + \#G_a^3) - (-2^m + 1 + \#H_a^3)\right) \\ &\qquad - \left((-2^m + \#G_a) - (-2^m + 1 + \#H_a)\right) \\ &= -\frac{1}{3} + \frac{2}{3}\left(\#G_a^3 - \#H_a^3 - 1\right) - (\#G_a - \#H_a - 1) \\ &= \frac{2}{3}\left(\#G_a^3 - \#H_a^3\right) - (\#G_a - \#H_a) \quad .\end{aligned}$$

The case $b = \beta$ uses another equality mentioned by Mesnager [21, Proof of Theorem 13]:

$$\Lambda(f_{a,\beta}) = -\frac{1}{3}\left(1 + 2\sum_{x \in \mathcal{T}_1} \chi\left(g_a(D_3(x))\right)\right) \quad .$$

Applying Corollary 3.7 yields

$$\begin{aligned}\Lambda(f_{a,\beta}) &= -\frac{1}{3}\left(1 + \left((-2^m + \#G_a^3) - (-2^m + 1 + \#H_a^3)\right)\right) \\ &= -\frac{1}{3}\left(\#G_a^3 - \#H_a^3\right) \quad .\end{aligned}$$

□

In the following, we express the extended Walsh-Hadamard transform of $f_{a,b}$ in function of $\Lambda(f_{a,b})$.

Proposition 3.12. *The notation is as in Proposition 3.11. Then*

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

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

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

Proof. We denote by U the set of (2^m+1)-th roots of unity in $\mathbb{F}_{2^n}$. 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 $f_{a,b}$ at (ω, k) can consequently be expressed as

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

But

$$\begin{aligned}f_{a,b}(yu) &= \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r (yu)^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(b(yu)^{\frac{2^n-1}{3}}\right) \\ &= \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r y^{r(2^m-1)} u^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(by^{(2^m-1)\frac{2^m+1}{3}} u^{\frac{2^n-1}{3}}\right) \\ &= \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r u^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bu^{\frac{2^n-1}{3}}\right) \\ &= f_{a,b}(u) \ ,\end{aligned}$$

so that

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

If $\omega = 0$, then $\widehat{\chi_f}(\omega,k) = 1 + \Lambda(f_{a,b})\left(-1+2^m\right)$ as desired. If $\omega \neq 0$, then one uses the transitivity of the trace: $\mathrm{Tr}_1^n(x) = \mathrm{Tr}_1^m\left(\mathrm{Tr}_m^n(x)\right) = \mathrm{Tr}_1^m\left(x + x^{2^m}\right)$, and the fact that k is coprime with 2^m+1 to deduce that the sum over $\mathbb{F}_{2^m}$ is non-zero if and only if $u^{2k} = \omega^{2^m-1}$ and get the final equality

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

□

In particular, the above functions are hyper-bent if and only if $\Lambda(f_{a,b}) = 1$.

The reformulation of the Charpin-Gong criterion by Lisoněk is a direct consequence of Propositions 3.11 and 3.12.

Corollary 3.13 (Reformulation of the Charpin-Gong criterion [19, Theorem 2])**.** *The notation is as in Proposition 3.11. Then $f_{a,0}$ is hyper-bent if and only if*

$$\#G_a - \#H_a = 1 \ .$$

Let us now fix a subset of indices $R \subseteq S$ and denote by r_{max} the maximal index. We can suppose r_{max} to be odd and will do so for two reasons:

1. it ensures that the smooth projective models of the curves H_a and G_a are imaginary hyperelliptic curves and such curves are way easier to manipulate than more general hyperelliptic curves;

2. for efficiency reasons r_{max} should be as small as possible, so the natural choice for the the indices in a cyclotomic coset will be the coset leaders which are odd integers.

In fact, the curves H_a and G_a are even Artin-Schreier curves. Theorem 2.9 states that there exist efficient algorithms to compute the cardinality of such curves. Thus, Lisoněk obtained an efficient test for hyper-bentness of Boolean functions in the class described by Charpin and Gong. The polynomial defining H_a (respectively G_a) is indeed of degree $r_{max}+2$ (respectively r_{max}), so the curve is of genus $(r_{max}+1)/2$ (respectively $(r_{max}-1)/2$). The complexity for testing the hyper-bentness of a Boolean function in this family is then dominated by the computation of the cardinality of a curve of genus $(r_{max}+1)/2$, which is polynomial in m for a fixed r_{max} (and so fixed genera for the curves H_a and G_a).

Applying directly a similar approach to the criterion of Mesnager yields a less pleasant reformulation.

Corollary 3.14 (Reformulation of the Mesnager criterion)**.** *The notation is as in Proposition 3.11.*
If $b = 1$, then $f_{a,1}$ is hyper-bent if and only if

$$2\left(\#G_a^3 - \#H_a^3\right) - 3\left(\#G_a - \#H_a\right) = 3 \ .$$

If b is a primitive element of $\mathbb{F}_4$, then $f_{a,b}$ is hyper-bent if and only if

$$\#G_a^3 - \#H_a^3 = -3 \ .$$

All the curves are once again Artin-Schreier curves. So, for a fixed subset of indices $R \subseteq S$, we also get a test with polynomial time and space in m. However, the complexity of the point counting algorithms also depends on the genera of the curves, and so on the degrees of the polynomials defining them. Denoting by r_{max} the maximal index as above, the genus of H_a^3 (respectively G_a^3) is $(3r_{max}+1)/2$ (respectively $(3r_{max}-1)/2$), so approximately three times that of H_a (respectively G_a). Therefore, the associated test will be much slower than for Boolean functions of the family of Charpin and Gong for a given subset R: we have to compute the cardinalities of two curves of genera $(3r_{max}+1)/2$ and $(3r_{max}-1)/2$ if b is primitive, or four curves of genera $(3r_{max}+1)/2$, $(3r_{max}-1)/2$, $(r_{max}+1)/2$ and $(r_{max}-1)/2$ if $b = 1$, instead of two curves of genera $(r_{max}+1)/2$ and $(r_{max}-1)/2$.

Fortunately, it is possible to use a similar approach to obtain a more efficient reformulation using the fact that, if m is odd, then the function $x \mapsto D_3(x) = x^3 + x$ is a permutation of the set $\mathcal{T}_0$ [3].

Proposition 3.15. *The notation is as in Proposition 3.11.*
Then

1. $\Lambda(f_{a,1}) = \dfrac{4}{3}\#G_a^3 - \dfrac{5}{3}\#G_a + \dfrac{1}{3}\#H_a$;

2. $\Lambda(f_{a,\beta}) = \Lambda(f_{a,\beta^2}) = -\dfrac{2}{3}\#G_a^3 + \dfrac{1}{3}\left(\#G_a + \#H_a\right)$.

Proof. The idea of the proof is to use the permutation $x \mapsto D_3(x) = x^3 + x$ before applying Corollary 3.7.

If $b = 1$, then we get

$$\begin{aligned}\Lambda(f_{a,1}) &= -\frac{1}{3} + \frac{4}{3}\sum_{x\in\mathcal{T}_1}\chi\left(g_a(D_3(x))\right) - 2\sum_{x\in\mathcal{T}_1}\chi\left(g_a(x)\right)\\ &= -\frac{1}{3} + \frac{4}{3}\left(\sum_{x\in\mathbb{F}_{2^m}}\chi\left(g_a(D_3(x))\right) - \sum_{x\in\mathcal{T}_0}\chi\left(g_a(D_3(x))\right)\right) - 2\sum_{x\in\mathcal{T}_1}\chi\left(g_a(x)\right)\\ &= -\frac{1}{3} + \frac{4}{3}\left(\sum_{x\in\mathbb{F}_{2^m}}\chi\left(g_a(D_3(x))\right) - \sum_{x\in\mathcal{T}_0}\chi\left(g_a(x)\right)\right) - 2\sum_{x\in\mathcal{T}_1}\chi\left(g_a(x)\right) \ ,\end{aligned}$$

so that Proposition 3.3 and Corollary 3.7 yield

$$\begin{aligned}\Lambda(f_{a,1}) &= -\frac{1}{3} + \frac{4}{3}\left(-2^m + \#G_a^3\right) - \frac{2}{3}\left((-2^m + \#G_a) + (-2^m + 1 + \#H_a)\right)\\ &\qquad - \left((-2^m + \#G_a) - (-2^m + 1 + \#H_a)\right)\\ &= \frac{4}{3}\#G_a^3 - \frac{5}{3}\#G_a + \frac{1}{3}\#H_a \ .\end{aligned}$$

For the case $b = \beta$, we get

$$\begin{aligned}\Lambda(f_{a,\beta}) &= -\frac{1}{3}\left(1 + 2\sum_{x\in\mathcal{T}_1}\chi\left(g_a(D_3(x))\right)\right)\\ &= -\frac{1}{3}\left(1 + 2\left(\sum_{x\in\mathbb{F}_{2^m}}\chi\left(g_a(D_3(x))\right) - \sum_{x\in\mathcal{T}_0}\chi\left(g_a(D_3(x))\right)\right)\right)\\ &= -\frac{1}{3}\left(1 + 2\left(\sum_{x\in\mathbb{F}_{2^m}}\chi\left(g_a(D_3(x))\right) - \sum_{x\in\mathcal{T}_0}\chi\left(g_a(x)\right)\right)\right) \ .\end{aligned}$$

Proposition 3.3 and Corollary 3.7 then give

$$\begin{aligned}\Lambda(f_{a,\beta}) &= -\frac{1}{3}\left(1 + 2(-2^m\#G_a^3) - \left((-2^m + \#G_a) + (-2^m + 1 + \#H_a)\right)\right)\\ &= -\frac{1}{3}\left(2\#G_a^3 - \#G_a - \#H_a\right) \ .\end{aligned}$$

□

The previous proposition trivially implies the following new reformulation.

Corollary 3.16 (Reformulation of the Mesnager criterion)**.** *The notation is as in Proposition 3.11.*
If $b = 1$, then $f_{a,1}$ is hyper-bent if and only if

$$4\#G_a^3 - 5\#G_a + \#H_a = 3 \ .$$

If b is a primitive element of $\mathbb{F}_4$, then $f_{a,b}$ is hyper-bent if and only if

$$2\#G_a^3 - (\#G_a + \#H_a) = -3 \ .$$

Thus, we discarded the computation of the cardinality of the curve of genus $(3r_{max} + 1)/2$ and we have to compute the cardinalities of three curves of genera $(3r_{max} - 1)/2$, $(r_{max} + 1)/2$ and $(r_{max} - 1)/2$. Nonetheless, the overall complexity is the same as before.

m	$\#G_a$	$\#H_a$	$\#G_a^3$	$\#H_a^3$	m	$\#G_a$	$\#H_a$	$\#G_a^3$	$\#H_a^3$
21	0.017	0.488	6.857	13.894	41	0.018	1.868	40.877	108.704
23	0.016	0.576	8.736	16.021	43	0.018	2.575	47.010	128.340
25	0.017	0.653	10.587	20.287	45	0.019	4.986	62.107	176.841
27	0.016	0.912	13.684	25.704	47	0.019	5.663	84.905	210.458
29	0.017	0.869	14.843	27.667	49	0.019	6.532	94.532	234.329
31	0.016	1.026	17.766	34.532	51	0.019	7.982	125.468	242.358
33	0.017	1.166	31.258	59.000	53	0.019	7.676	133.737	249.522
35	0.018	1.317	26.809	57.998	55	0.019	8.437	116.552	275.870
37	0.018	1.562	33.321	79.949	57	0.020	9.504	127.507	305.787
39	0.019	1.893	46.768	99.544	59	0.020	9.881	162.632	360.508
					61	0.020	11.767	182.481	395.841

Table 2: Meantimes needed to compute the number of points on G_a, H_a, G_a^3 and H_a^3

3.3 Experimental results

In the previous section, we have shown how to obtain a more efficient reformulation of the Charpin-Gong and Mesnager criteria in terms of cardinalities of hyperelliptic curves. Even though the overall complexity is not changed between the different reformulations we presented, the practical gain is non-negligible. To illustrate this fact, we performed several simulations with Magma v2.17-13 [1]. The computations were performed on an Intel Core2 Quad CPU Q6600 cadenced at 2.40 GHz. The set R of indices used was $R = \{1, 3\}$ and one hundred of couples of coefficients (a_1, a_3) were randomly generated in $\mathbb{F}_{2^m}^*$. The meantimes needed to compute the number of points on the curves G_a, H_a, G_a^3 and H_a^3 for odd integers m between 21 and 61 are presented in Table 2. A random search on such pairs showed that the Boolean functions associated with the following coefficients are hyper-bent (the finite field $\mathbb{F}_{2^m}$ is represented as $\mathbb{F}_2[x]$ quotiented by the ideal generated by the m-th binary Conway polynomial):

- for $b = 0$, the pair

$$\begin{aligned} a_1 &= x^{34} + x^{31} + x^{29} + x^{27} + x^{26} + x^{24} + x^{23} + x^{21} + x^{20} + x^{18} + x^{17} + x^{16} \\ &\quad + x^{15} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 \ , \\ a_3 &= x^{32} + x^{29} + x^{27} + x^{25} + x^{24} + x^{23} + x^{21} + x^{20} + x^{18} + x^{16} + x^{12} + x^8 \\ &\quad + x^4 + x \ , \end{aligned}$$

  in $\mathbb{F}_{2^{35}}$ represented as $\mathbb{F}_2[x]/\left(x^{35} + x^{11} + x^{10} + x^7 + x^5 + x^2 + 1\right)$;

- for $b = 1$, the pair

$$\begin{aligned} a_1 &= x^{27} + x^{26} + x^{25} + x^{24} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} \\ &\quad + x^{14} + x^{13} + x^{11} + x^7 + x^5 + x^4 + x^2 + 1 \ , \\ a_3 &= x^{30} + x^{29} + x^{27} + x^{26} + x^{22} + x^{20} + x^{17} + x^{16} + x^{15} + x^{12} + x^{10} + x^4 \\ &\quad + x^3 + x^2 \ , \end{aligned}$$

  in $\mathbb{F}_{2^{33}}$ represented as $\mathbb{F}_2[x]/\left(x^{33} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^3 + 1\right)$;

- for $b = \beta$ a primitive element of $\mathbb{F}_4$, the pair

$$\begin{aligned} a_1 &= x^{32} + x^{31} + x^{29} + x^{27} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{18} + x^{17} + x^{15} \\ &\quad + x^{11} + x^{10} + x^9 + x^3 + x^2 + x \ , \\ a_2 &= x^{32} + x^{29} + x^{28} + x^{27} + x^{26} + x^{24} + x^{22} + x^{18} + x^{17} + x^{13} + x^{10} + x^8 \\ &\quad + x^7 + x^6 + x^5 + x^4 \ , \end{aligned}$$

in $\mathbb{F}_{2^{33}}$ represented as $\mathbb{F}_2[x]/\left(x^{33} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^3 + 1\right)$.

3.4 Application to a family of Charpin and Gong

To conclude this paper, we show how Corollary 3.13 applies to a family of binomial functions studied by Charpin and Gong [4, Proposition 3], and what problem is implied in the language of hyperelliptic curves.

Charpin and Gong applied their criterion to a family of binomial functions and obtained the following result.

Proposition 3.17 (Family of binomial functions of Charpin and Gong [4, Proposition 3])**.** *Let m be an odd integer and $n = 2m$. Let $a \in \mathbb{F}_{2^m}^*$ and $f_a : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be the Boolean function defined as*

$$f_a(x) = \mathrm{Tr}_1^n\left(a(x^{2^m-1} + x^{3(2^m-1)}\right) \ .$$

Then:

1. *If $m = 3$, then f_a is hyperbent if and only if $a \neq 1$.*
2. *If $m > 3$ and $\mathrm{Tr}_1^m(a) = 1$, then f_a is not hyperbent.*

We now suppose that m is an odd integer greater than 3 and that $a \in \mathbb{F}_{2^m}^*$. Recall that Corollary 3.13 implies that f_a is hyperbent if and only if $\#G_a - \#H_a = 1$ where the affine curves G_a and H_a are defined as

$$\begin{aligned} G_a &: y^2 + y = ax^3 \ , \\ H_a &: y^2 + xy = ax^5 + x \ . \end{aligned}$$

The projective model of G_a is non-singular and so is an elliptic curve, but much more can be easily deduced about its number of points. Indeed, m is odd so that the function $x \mapsto ax^3$ induces a permutation of $\mathbb{F}_{2^m}^*$, and consequently of $\mathbb{F}_{2^m}$. Therefore, the number of points of the (affine) curve G_a is exactly

$$\#G_a = 2^m \ .$$

The criterion for hyperbentness of f_a is thus reduced to the following equality involving the number of point of the (affine) curve H_a:

$$\#H_a = 2^m - 1 \ ;$$

or equivalently that the associated projective curve has exactly 2^m points.

Hence, the open problem of the non-emptyness of the family of binomial functions of Charpin and Gong [4, Open Problem 5] is equivalent to the following open problem.

Open problem 3.18. *Does there exist a projective hyperelliptic curve $H_a : y^2 + xy = ax^5 + x$ where $a \in \mathbb{F}_{2^m}$ with exactly 2^m $\mathbb{F}_{2^m}$-rational points for an infinite number of odd integers $m \geq 3$?*

m	Conway polynomial	Exponent
3	x^3+x+1	1
5	x^5+x^2+1	19
7	x^7+x+1	120
9	x^9+x^4+1	271
11	$x^{11}+x^2+1$	34
13	$x^{13}+x^4+x^3+x+1$	7908
15	$x^{15}+x^5+x^4+x^2+1$	28112
17	$x^{17}+x^3+1$	7111
19	$x^{19}+x^5+x^2+x+1$	104525
21	$x^{21}+x^6+x^5+x^2+1$	946692
23	$x^{23}+x^5+1$	2867172
25	$x^{25}+x^8+x^6+x^2+1$	3149617
27	$x^{27}+x^{12}+x^{10}+x^9+x^7+x^5+x^3+x^2+1$	48219351
29	$x^{29}+x^2+1$	527863282
31	$x^{31}+x^3+1$	1868652941
33	$x^{33}+x^{13}+x^{12}+x^{11}+x^{10}+x^8+x^6+x^3+1$	7284997393
35	$x^{35}+x^{11}+x^{10}+x^7+x^5+x^2+1$	22923167491
37	$x^{37}+x^5+x^4+x^3+x^2+x+1$	73386028483
39	$x^{39}+x^{15}+x^{12}+x^{11}+x^{10}+x^9+x^7+x^6+x^5+x^2+1$	418407929890
41	$x^{41}+x^3+1$	1756526869868

Table 3: Exponents e addressing the open problem for m odd up to 41

Numerical evidence supports the validity of this question: Table 3 gives values of a defined over $\mathbb{F}_{2^m}$ addressing it for m odd up to 41. In Table 3, the field $\mathbb{F}_{2^m}$ with $m \geq 3$ odd is represented as the quotient of $\mathbb{F}_2[x]$ by the Conway polynomial of degree m and a is given by an exponent e such that $a = x^e$. It should be noted that similar evidence has been found for the case where m is even. However, this fact is not relevant for the study of the family of binomial functions of Charpin and Gong, but shows that the reformulation of the original problem in terms of hyperelliptic curves is not restricted to the case where m is odd.

4 Conclusion

The link between the zero (resp. the value four) of Kloosterman sums and the Dillon (resp. Dillon-like) monomial (resp. binomial) hyper-bent functions has been recently generalized by Charpin and Gong and by Mesnager to a link between some exponential sums involving Dickson polynomials and some hyper-bent functions with multiple trace terms. In this paper, exponential sums in generic form have been related with cardinalities of hyperelliptic curves. This generic approach allows us to recover the known results in this context and to characterize efficiently the property of hyper-bentess of a new family of hyper-bent functions (in the line of the recent results of Lisonek on this topic)

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and

number theory (London, 1993).

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

[3] P. Charpin, T. Helleseth, and V. Zinoviev. Divisibility properties of kloosterman sums over finite fields of characteristic two. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 2608 –2612, july 2008.

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

[5] H. Cohen, G. Frey, and R. Avanzi. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete mathematics and its applications. Chapman & Hall/CRC, 2006.

[6] Jan Denef and Frederik Vercauteren. An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2. In Claus Fieker and David R. Kohel, editors, *ANTS*, volume 2369 of *Lecture Notes in Computer Science*, pages 308–323. Springer, 2002.

[7] Jan Denef and Frederik Vercauteren. An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2. *J. Cryptology*, 19(1):1–25, 2006.

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

[9] Andreas Enge. How to distinguish hyperelliptic curves in even characteristic. In *Public-key cryptography and computational number theory (Warsaw, 2000)*, pages 49–58. de Gruyter, Berlin, 2001.

[10] Steven Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2011. `http://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html`.

[11] Faruk Gologlu. *Almost Bent and Almost Perfect Nonlinear Functions, Exponential Sums, Geometries and Sequences*. PhD thesis, University of Magdeburg, 2009.

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

[13] Nicholas Katz and Ron Livné. Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 309(11):723–726, 1989.

[14] Gilles Lachaud and Jacques Wolfmann. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 305(20):881–883, 1987.

[15] 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.

[16] N. G. Leander. Monomial bent functions. *IEEE Transactions on Information Theory*, 52(2):738–743, 2006.

[17] Reynald Lercier and David Lubicz. A quasi quadratic time algorithm for hyperelliptic curve point counting. *Ramanujan J.*, 12(3):399–423, 2006.

[18] 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.

[19] P. Lisonek. An efficient characterization of a family of hyperbent functions. *Information Theory, IEEE Transactions on*, 57(9):6010 –6014, sept. 2011.

[20] Sihem Mesnager. A new family of hyper-bent Boolean functions in polynomial form. In Matthew G. Parker, editor, *IMA Int. Conf.*, volume 5921 of *Lecture Notes in Computer Science*, pages 402–417. Springer, 2009.

[21] 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.

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

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

[24] Frederik Vercauteren. *Computing zeta functions of curves over finite fields*. PhD thesis, Katholieke Universiteit Leuven, 2003.

[25] 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.