J. Math. Cryptol. **7** (2013), 43–68
DOI 10.1515/jmc-2012-0013

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

Jean-Pierre Flori and Sihem Mesnager

Communicated by Rainer Steinwandt

Abstract. The connection between exponential sums and algebraic varieties has been known for at least six decades. Recently, Lisoněk exploited it to reformulate the Charpin–Gong characterization of a large class of hyper-bent functions in terms of numbers of points on hyperelliptic curves. As a consequence, he obtained a polynomial time and space algorithm for certain subclasses of functions in the Charpin–Gong family. In this paper, we settle a more general framework, together with detailed proofs, for such an approach 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 as well. Nonetheless, a straightforward application of such results does not provide a satisfactory criterion for explicit generation of functions in the Mesnager family. To address this issue, we show how 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.

2010 Mathematics Subject Classification. 94C10, 14H52.

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 [26] 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 [11]. 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 precisely an infinite class of hyper-bent functions, as indicated by the number of open problems proposed by Charpin and Gong [2].

Some explicit constructions of hyper-bent functions have been proposed in the literature. Monomial hyper-bent functions are famous bent functions due to Dillon [7]. Charpin and Gong [2] characterized by means of exponential sums and 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] characterized another class of hyper-bent functions, distinct from that of Charpin and Gong.

Connecting exponential sums and a number of points on algebraic varieties is folklore. Such ideas go back, at least, to the work of Weil [25] where the Riemann hypothesis is used to bound the values of Kloosterman sums. Later, Lachaud and Wolfmann [17] and Katz and Livné [15] exploited the theory of elliptic curves to study the distribution of Kloosterman sums. Very recently, Lisoněk [20] followed this approach to reformulate the Charpin–Gong hyper-bentness criterion in terms of hyperelliptic curves. The algorithmic theory of such curves shows that this reformulation gives rise to a test in both polynomial time and space when restricted to certain subclasses of functions.

In this paper, we present a more generic formulation of the connection between Boolean functions, exponential sums and hyperelliptic curves. This leads us to easily deduce the previous results of Lisoněk, as well as giving an efficient version of the more recent hyper-bentness criterion proposed by Mesnager. We subsequently propose a slightly different reformulation leading to practical speed-ups.

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 characterizations of Charpin and Gong, and Mesnager for hyper-bent functions with multiple trace terms. We then present the general framework to express several exponential sums in terms of the number of points on hyperelliptic curves and deduce the different reformulations mentioned above[1]. We conclude by providing a complexity analysis of the reformu-

[1] The authors have used these results to study and efficiently characterize hyper-bentness of another family of Boolean functions [8].

lated tests, together with experimental data, showing that they are not only asymptotically faster, but that they also provide practical improvements to the generation of hyper-bent functions.

2 Notation and preliminaries

For any set S, we define $S^* = S \setminus \{0\}$ and denote by $\#S$ the cardinality of S. Unless stated otherwise, $m \geq 1$ will be a positive integer and the Boolean function of interest will usually have $n = 2m$ inputs. When working over $\mathbb{F}_{2^m}$, we make the abuse of notation $1/0 = 0^{2^m-2} = 0$.

2.1 Boolean functions in polynomial form

A Boolean function f on $\mathbb{F}_{2^n}$ can be considered as an $\mathbb{F}_2$-valued function on the Galois field $\mathbb{F}_{2^n}$ of order 2^n. The trace from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$ where k divides n is denoted by Tr_k^n. Every Boolean function has a unique trace expansion of the form

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

called its polynomial form, where

- 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,
- $a_j \in \mathbb{F}_{2^{o(j)}}$, and
- $\epsilon = \mathrm{wt}(f) \pmod 2$.

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

We denote by $\chi : x \in \mathbb{F}_2 \mapsto (-1)^x \in \{-1, 1\}$ the additive character of $\mathbb{F}_2$. The *Walsh–Hadamard transform* of f is the discrete Fourier transform of $\chi_f = \chi \circ f$, 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

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

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

Hyper-bent functions have even stronger properties and 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 $\pm 2^{\frac{n}{2}}$.

2.3 Binary exponential sums

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

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

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

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

Definition 2.4. 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

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

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

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

Binary Dickson polynomials $D_r(X)$ 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 is referred to the monograph of Lidl, Mullen and Turnwald [19] for many useful properties and applications of Dickson polynomials. The first six binary Dickson polynomials are

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

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 textbook of Cohen et al. [4] or that of Galbraith [10].

For our purposes, it is enough to consider *imaginary* hyperelliptic curves. Imaginary hyperelliptic curves are smooth projective curves whose affine part can be described by an equation of the form

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

where $h(x)$ is a polynomial of degree at most g, the genus of the curve, and $f(x)$ is a monic polynomial of degree $2g + 1$. They have exactly one point at infinity. Curves for which $h(x) = x^k$, where $0 \leq k \leq g$, are called Artin–Schreier curves. The case $g = 1$ corresponds to elliptic curves.

The number of points on a hyperelliptic 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 this number of points in polynomial time and space in m. Such a result was given by Denef and Vercauteren who extended a previous result of Kedlaya [16] in odd characteristic.

Theorem 2.5 ([24, Theorem 4.4.1] and [6]). *Let H be an imaginary hyperelliptic curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the number of points on H in*

$$O(g^{5+\epsilon} m^{3+\epsilon})$$

bit operations and $O(g^4 m^3)$ memory, where $\epsilon \in \mathbb{R}_+^*$ is any strictly positive real number.

A slightly stronger result is true for Artin–Schreier curves.

Theorem 2.6 ([24, Theorem 4.3.1] and [5]). *Let H be an Artin–Schreier curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the number of points on H in*

$$O\left(g^{5+\epsilon}m^{3+\epsilon}\right)$$

bit operations and $O(g^3m^3)$ memory, where $\epsilon \in \mathbb{R}_+^*$ is any strictly positive real number.

Better complexities were recently obtained through the use of complex methods involving deformation theory. For example, Hubrechts obtained the following result.

Theorem 2.7 ([14, Theorem 2]). *Let H be an hyperelliptic curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the number of points on H in*

$$O\left(g^{7.376}m^2 + g^{3.376}m^{2.667}\right)$$

bit operations and $O(g^5m^2 + g^3m^{2.5})$ memory.

In fact such algorithms are even more interesting when one wants to compute the number of points on several curves within the same family.

To conclude, let us mention the existence of a quasi-quadratic algorithm described by Lercier and Lubicz [18].

Theorem 2.8. *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*

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

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 and so it is of practical interest for curves of relatively small genera only.

3 Constructions of hyper-bent functions

3.1 Characterization involving exponential sums

Charpin and Gong [2] 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 [2, 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*[2] *on $\mathbb{F}_{2^n}$ by*

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

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

$$g_a(x) = \sum_{r \in R} \mathrm{Tr}_1^m(a_r D_r(x)).$$

Then f_a is hyper-bent if and only if

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

More recently, Mesnager [21] gave a similar characterization[3] 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.

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 $2^m + 1$ whose cosets have full size n. Let $f_{a,b}$ be the function defined on $\mathbb{F}_{2^n}$ by*

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

where $R \subseteq S$, all the coefficients a_r are in $\mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_4^*$. Let g_a be the related function defined on $\mathbb{F}_{2^m}$ by

$$g_a(x) = \sum_{r \in R} \mathrm{Tr}_1^m(a_r D_r(x)),$$

where $D_r(x)$ is the Dickson polynomial of degree r. Then:

[2] Although the definition of f_a depends on the family $\{a_r\}_{r \in R}$, we use the subscript a for conciseness.

[3] There was a typo in the theorem given in the original article [21] where the last term in the right-hand side of condition (i) (c) 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.

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

(c) $$\sum_{x\in\mathbb{F}_{2^m}^*} \chi\big(\mathrm{Tr}_1^m(1/x) + g_a(D_3(x))\big) = 2^m - 2\,\mathrm{wt}(g_a \circ D_3) + 3.$$

(ii) *$f_{a,1}$ is hyper-bent if and only if*

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

3.2 Reformulation in terms of hyperelliptic curves

Reformulating exponential sums in terms of number of points on algebraic varieties is a classical approach. Lachaud and Wolfmann [17] as well as Katz and Livné [15] used such a connection to describe Kloosterman sums in terms of elliptic curves and devise their distribution. Lisoněk [20] recently applied similar ideas to express the exponential sums involved in the Charpin–Gong criterion in terms of hyperelliptic curves. In this subsection, we present a more general framework for such an approach. As a consequence, a reformulation of the Mesnager criterion is deduced.

We start by giving two propositions relating exponential sums with cardinalities of hyperelliptic curve, thus generalizing the ad hoc form used by Lisoněk [20], which will be of interest later on.

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

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

Then

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

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

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

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

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

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

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

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

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

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

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

which concludes the proof of the proposition. □

Proposition 3.4. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function, $g = \mathrm{Tr}_1^m(f)$, 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

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

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

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

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.

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

□

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

Definition 3.5. Let $i\in\mathbb{F}_2$ and $\mathcal{T}_i$ denote the set

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

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*[4]

$$\sum_{x\in\mathcal{T}_i}\chi(g(x)) = \frac{1}{2}\Big(\sum_{x\in\mathbb{F}_{2^m}}\chi(g(x)) + (-1)^i\sum_{x\in\mathbb{F}_{2^m}}\chi\big(\mathrm{Tr}_1^m(1/x)+g(x)\big)\Big).$$

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 $f(0)=0$, and $g=\mathrm{Tr}_1^m(f)$. 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

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

Then

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

[4] Recall that we consider that $1/0=0$, so that $0\in\mathcal{T}_0$ and $\mathrm{Tr}_1^m(1/0)=0$.

The following well-known observation is a direct consequence of the above propositions.

Proposition 3.8 ([15, 17]). *Let $m \geq 1$ 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, let $b = a^{1/2} \in \mathbb{F}_{2^m}$ and recall that $K_m(a) = K_m(b)$. The Kloosterman sum $K_m(b)$ is defined as

$$K_m(b) = 1 + \sum_{x \in \mathbb{F}_{2^m}^*} \chi\big(\mathrm{Tr}_1^m(1/x + bx)\big),$$

so applying Proposition 3.4, we get

$$K_m(b) = 1 - 2^m + \#H_b,$$

where H_b is the affine curve defined by

$$H_b : y^2 + xy = bx^3 + x.$$

Over $\mathbb{F}_{2^m}$, this curve is isomorphic to $E_a : y^2 + xy = x^3 + a$. Hence, both curves have the same number of $\mathbb{F}_{2^m}$-rational points. Taking into account the only point at infinity on both curves, which is already included in $\#E_a$, but not in $\#H_a$, we deduce the equality of the proposition:

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

This result has been used by several authors to reformulate the necessary and sufficient condition for hyper-bentness of the monomial functions with the Dillon exponent as follows.

Proposition 3.9. *The notation is as in Proposition* 3.8. *Moreover let r be an integer such that* $\gcd(r, 2^m + 1) = 1$ *and f_a be the Boolean function*

$$f_a(x) = \mathrm{Tr}_1^n\big(ax^{r(2^m-1)}\big).$$

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 ([9]). *The notation is as in Proposition* 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[5] *if and only if*

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

In particular, these reformulations imply that testing the hyper-bentness of these monomial and binomial functions is polynomial time and space in m. Not only are the corresponding tests asymptotically fast, but the existence of specific algorithms for point counting on elliptic curves makes them very practical tests.

To continue with the general case of hyperelliptic curves, much more can be deduced from Propositions 3.3 and 3.4. First, Lisoněk [20, Theorem 2] used such ideas in the specific case of the Charpin–Gong criterion. He could indeed express both sides of the criterion in terms of cardinalities of hyperelliptic curves. In fact, he went further and also expressed every value of the extended Walsh–Hadamard transform with such terms [20, Theorem 3].

Such an approach is valid in a more general setting as we show below. The following proposition shows that the expression of the extended Walsh–Hadamard transform of $f_{a,b}$ as a function of $\Lambda(f_{a,b})$ given by Lisoněk in the Charpin–Gong case, i.e., when $b = 0$, can be extended to the Mesnager family, i.e., when $b \in \mathbb{F}_4^*$.

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. Then*

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

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

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

[5] 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.

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

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

But

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

so that

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

If $\omega = 0$, then $\widehat{\chi_{f_{a,b}}}(\omega,k) = 1 + \Lambda(f_{a,b})(-1+2^m)$ as desired. If $\omega \neq 0$, then one uses the transitivity of the trace: $\mathrm{Tr}_1^n(x) = \mathrm{Tr}_1^m(\mathrm{Tr}_m^n(x)) = \mathrm{Tr}_1^m(x + x^{2^m})$, which yields

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

As k is co-prime with $2^m - 1$, the map $y \mapsto y^k$ is a permutation of $\mathbb{F}_{2^m}$ and the sum over $\mathbb{F}_{2^m}$ is non-zero if and only if $u^{2k} = \omega^{2^m-1}$. As 2 and k are co-prime with $2^m + 1$, this equation has a unique solution $u \in U$, the cyclic group of $(2^m + 1)$-th roots of unity in $\mathbb{F}_{2^n}$, and we get the final equality

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

In particular, the above functions are hyper-bent if and only if $\Lambda(f_{a,b}) = 1$. These sums can then be transformed using Propositions 3.3 and 3.4.

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

(i) $\Lambda(f_{a,0}) = \#G_a - \#H_a$;

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

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

Proof. The case $b = 0$ can be treated using the following equality established by Charpin and Gong [2, proof of Theorem 7]:

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

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

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

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

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

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

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

Corollary 3.7 is then used to obtain the equality

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

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

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

Applying Corollary 3.7 yields

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

□

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

Corollary 3.13 (Reformulation of the Charpin–Gong criterion [20, Theorem 2]). *The notation is as in Proposition* 3.12. *Then* $f_{a,0}$ *is hyper-bent if and only if*

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

As a consequence of this corollary, Lisoněk obtained a polynomial time and space test for hyper-bentness of Boolean functions in the Charpin–Gong family. Let $r_{\max}$ the maximal index in R, which can be supposed to be odd, and will be for two reasons:

(i) it ensures that the curves H_a and G_a are imaginary hyperelliptic curves;

(ii) as will be discussed below, $r_{\max}$ should be as small as possible for efficiency reasons, so the natural choice for the indices in a cyclotomic coset will be the coset leaders which are odd integers.

In fact, the curves G_a and H_a are even Artin–Schreier curves. Theorems 2.6 and 2.7 state that there exist efficient algorithms to compute the cardinality of such curves as long as $r_{\max}$ is supposed to be relatively small. 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 $(r_{\max}+1)/2$. Then, applying Theorem 2.7 gives the following time and space complexities in m and $r_{\max}$.

Theorem 3.14. *The notation is as in Theorem* 3.1. *Let moreover $r_{\max}$ be the maximal index in R. Then the hyper-bentness of f_a can be checked in*

$$O\big(r_{\max}^{7.376}m^2 + r_{\max}^{3.376}m^{2.667}\big)$$

bit operations and $O(r_{\max}^5 m^2 + r_{\max}^3 m^{2.5})$ memory.

Therefore, if R is supposed to be fixed, then so are $r_{\max}$ and the genera of the curves G_a and H_a, and the complexities of Theorem 3.14 are indeed polynomial in m as stated by Lisoněk [20, Theorem 5]. Asymptotically, this is much better than a straightforward application of Theorem 3.1 where the exponential sums on $\mathbb{F}_{2^m}$ are naively computed one term at a time. Indeed, for each of the 2^{m-1} terms of the partial exponential sums over $\mathcal{T}_1$, one has to compute the function $g_a(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x))$. The time complexity of this computation is dominated by the cost of a constant number of multiplications in $\mathbb{F}_{2^m}$. Therefore, the total time complexity is $O(2^m m^{1+\epsilon})$ and the space complexity is $O(m)$, where $\epsilon \in \mathbb{R}_+^*$ is any strictly positive real number. Testing hyper-bentness through a naive computation of $\Lambda(f_a)$ yields similar complexity, although the arithmetic takes place in $\mathbb{F}_{2^n}$ rather than $\mathbb{F}_{2^m}$.

It should be remarked that if no restriction is cast upon R, then the maximal index $r_{\max}$ will obviously depend on m and will in fact grow, at least, as $2^m/m$. It is indeed sufficient to note that this is true when m is prime. Then, each non-trivial cyclotomic coset has indeed size dividing $n = 2m$. It has size 2 if and only if $3r \equiv 0 \pmod{2^m+1}$ for $0 \le r \le 2^m$, i.e., $3r = 2^m+1$ or $3r = 2(2^m+1)$. Hence, there are exactly one such class when $3 \mid 2^m+1$, that is when m is odd, and no such class otherwise. The size of the other cosets is then $2m$, so that the largest coset leader, which is odd, is at least $(2^m-2)/m$.

Consequently, the time and space complexities of Theorem 3.14 will become exponential, whereas the time complexities of the naive approaches will become $O(2^m m^{2+\epsilon})$ (now dominated by the computation of an exponentation with an arbitrary large exponent), where $\epsilon \in \mathbb{R}_+^*$ is any strictly positive real number, and their space complexities will not change.

Nonetheless, fixing a set R, i.e., only looking for Boolean functions with a given polynomial form within a large family, is customary in cryptographic applications. Moreover, experimental data provided by Lisoněk [20, Table 1] and in Section 3.3 show that such reformulations also have a practical impact, so that the above approach seems meaningful.

We now proceed with the Mesnager family. Unfortunately, applying directly similar ideas gives a reformulation where curves of higher genera appear.

Corollary 3.15 (Reformulation of the Mesnager criterion). *The notation is as in Proposition* 3.12.

If $b = 1$, then $f_{a,1}$ is hyper-bent if and only if

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

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

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

Let $r_{\max}$ be the maximal odd index in R. The two additional curves G_a^3 and H_a^3 are Artin–Schreier curves as well. The genus of H_a^3 (respectively G_a^3) is $(3r_{\max} + 1)/2$ (respectively $(3r_{\max} - 1)/2$). Therefore, 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 $(r_{\max} - 1)/2$. The time and space complexities needed to compute these numbers of points are asymptotically the same as that of Lisoněk for functions in the Charpin–Gong family.

Theorem 3.16. *The notation is as in Theorem* 3.2. *Let moreover $r_{\max}$ be the maximal index in R. Then the hyper-bentness of $f_{a,b}$ can be checked in*

$$O\left(r_{\max}^{7.376} m^2 + r_{\max}^{3.376} m^{2.667}\right)$$

bit operations and $O(r_{\max}^5 m^2 + r_{\max}^3 m^{2.5})$ memory.

In particular, if R is supposed to be fixed, so that $r_{\max}$ is, we also get a test with polynomial time and space in m. Nonetheless, the discrepancy in the genera of the curves involved has a strong influence on the running time. Testing hyper-bentness

of functions in the Mesnager family using the above result is much slower than testing hyper-bentness of functions in the Charpin–Gong family for a given subset R and maximal index $r_{\max}$. Experimental evidence supporting this affirmation is given in Section 3.3.

To partially address this issue, we now propose another reformulation of the Mesnager criterion 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 $\mathcal{T}_0$ (see [3]).

Proposition 3.17. *The notation is as in Proposition* 3.12*. Then*

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

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

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

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

so that Proposition 3.3 and Corollary 3.7, together with the facts that $g_a(0) = 0$ and $0 \in \mathcal{T}_0$, yield

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

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

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

$$= -\frac{1}{3}\Big(1 + 2\Big(\sum_{x\in\mathbb{F}_{2^m}} \chi(g_a(D_3(x))) - \sum_{x\in\mathcal{T}_0} \chi(g_a(x))\Big)\Big).$$

Proposition 3.3 and Corollary 3.7 then give

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

□

The previous proposition trivially implies the following reformulation.

Corollary 3.18 (Reformulation of the Mesnager criterion). *The notation is as in Proposition* 3.12.

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 $(r_{\max} - 1)/2$. Even though the complexities of the associated test are the same as before, that is

$$O\big(r_{\max}^{7.376}m^2 + r_{\max}^{3.376}m^{2.667}\big)$$

bit operations and $O(r_{\max}^5 m^2 + r_{\max}^3 m^{2.5})$ memory, we will show in the next subsection that the practical gain is non-negligible.

3.3 Experimental results

In the previous subsection, we have shown how the Mesnager criterion can be reformulated in terms of cardinalities of hyperelliptic curves; we now study the practical impact of such reformulations.

To begin with, even though the overall complexity is not changed between the two reformulations we presented, the practical difference 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

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

Table 1. Meantimes needed to compute the number of points on G_a, H_a, G_a^3 and H_a^3.

(in seconds) 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 59 are presented in Table 1. These data show that using the second reformulation is roughly twice as fast as using the first one. It also confirms that testing a function in the Mesnager family using such a reformulation is much slower than testing a function in the Charpin–Gong family.

Table 2 shows how the second reformulation compares with a straightforward application of more classical characterizations involving exponential sums where the given sums are computed one term at a time. The column Λ indicates the meantimes (in seconds) needed to check the hyper-bentness of a function $f_{a,b}$ in the Mesnager family by computing naively the exponential sum $\Lambda(f_{a,1})$, the column $\mathcal{T}_i$ by computing naively the exponential sums on $\mathcal{T}_i$ of Theorem 3.2, and the column $\#H$ by using the second reformulation of the previous section, for $b = 1$ and ten random pairs (a_1, a_3) of coefficients in $\mathbb{F}_{2^m}$ for m from 1 to 29, and only one couple (a_1, a_3) for m from 31 to 59.

Two remarks should be made about the data exposed in Table 2. First, it should be noted that Magma actually uses a *naive* point counting based on exponential sums for m up to 20 where it switches to the Denef–Vercauteren algorithm mentioned in Theorem 2.5. Nonetheless, the fact that a naive point counting algorithm has an exponential time complexity and the experimental data provided in Table 2 show that using such an algorithm for m greater than 20 would not be beneficial. Second, it is clear that the reformulations in terms of hyperelliptic curves are of practical interest, for relatively small values of m, and for values of m of cryptographic interest.

m	Λ	$\mathcal{T}_i$	$\#H$	m	Λ	$\mathcal{T}_i$	$\#H$
1	0.000	0.000	0.000	31	23213.840	29521.440	18.460
3	0.000	0.000	0.000	33	109889.470	119733.320	29.030
5	0.000	0.000	0.000	35	445344.020	490439.190	25.750
7	0.001	0.001	0.000	37	–	–	33.631
9	0.003	0.003	0.002	39	–	–	46.898
11	0.019	0.011	0.004	41	–	–	40.585
13	0.073	0.042	0.018	43	–	–	46.713
15	0.301	0.166	0.076	45	–	–	63.693
17	1.165	0.658	0.300	47	–	–	86.434
19	4.571	2.693	1.277	49	–	–	95.525
21	20.863	24.376	6.893	51	–	–	127.055
23	76.744	99.918	8.769	53	–	–	133.471
25	330.874	410.432	10.642	55	–	–	116.726
27	1371.403	1716.147	13.914	57	–	–	127.596
29	5472.347	6794.873	14.799	59	–	–	161.185

Table 2. Meantimes needed to test the hyper-bentness of $f_{a,1}$.

As a final piece of experimental evidence, the second reformulation made it possible to find hyper-bent functions of cryptographic size in the Mesnager family, even though the tests are much slower than the corresponding ones for functions in the Charpin–Gong family. A random search on pairs (a_1, a_3) as above indeed showed that the Boolean functions associated with the following coefficients[6] 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 [12, 13]):

For $b = 0$, the pair

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

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

[6] Recall that the coefficient a_1 and a_3 are defined over $\mathbb{F}_{2^m}$, but that the corresponding Boolean functions have $n = 2m$ inputs.

For $b = 1$, the pair

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

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

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

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

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

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 [2, 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 3.19 (Family of binomial functions of Charpin and Gong [2, 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*

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

Then:

(i) *If $m = 3$, then f_a is hyper-bent if and only if $a \neq 1$.*

(ii) *If $m > 3$ and $\mathrm{Tr}_1^m(a) = 1$, then f_a is not hyper-bent.*

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 hyper-bent if and only if $\#G_a - \#H_a = 1$

where the affine curves G_a and H_a are defined as

$$G_a : y^2 + y = ax^3,$$
$$H_a : y^2 + xy = ax^5 + x.$$

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 hyper-bentness of f_a is thus reduced to the following equality involving the number of points 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-emptiness of the family of binomial functions of Charpin and Gong [2, Open Problem 5] is equivalent to the following open problem.

Open Problem 3.20. 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 $m \geq 3$?

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 ideal generated by the Conway polynomial [12,13] 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

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.

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 number of points on hyperelliptic curves. This generic approach allows us to recover known results and to characterize efficiently the property of hyper-bentness of a new family of hyper-bent functions (in the line of the recent results of Lisoněk on this topic).

Bibliography

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[2] P. Charpin and G. Gong, Hyperbent functions, Kloosterman sums, and Dickson polynomials, *IEEE Trans. Inform. Theory* **54** (2008), 4230–4238.

[3] P. Charpin, T. Helleseth and V. Zinoviev, Divisibility properties of Kloosterman sums over finite fields of characteristic two, in: *IEEE International Symposium on Information Theory* (ISIT 2008), 2608–2612.

[4] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren (eds.), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, 2006.

[5] J. Denef and F. Vercauteren, An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2, in: *ANTS*, Lecture Notes in Comput. Sci. 2369, Springer (2002), 308–323.

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

[7] J. F. Dillon, *Elementary Hadamard difference sets*, Ph.D. thesis, University of Maryland, College Park, ProQuest LLC, Ann Arbor 1974.

[8] J.-P. Flori and S. Mesnager, Dickson polynomials, hyperelliptic curves and hyperbent functions, in: *SETA*, Lecture Notes in Comput. Sci. 7280, Springer (2012), 40–52.

[9] J.-P. Flori, S. Mesnager and G. Cohen, Binary Kloosterman sums with value 4, in: *IMA Int. Conf.*, Lecture Notes in Comput. Sci. 7089, Springer (2011), 61–78.

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

[11] G. Gong and S. W. Golomb, Transform domain analysis of DES, *IEEE Trans. Inform. Theory* **45** (1999), 2065–2073.

[12] L. S. Heath and N. A. Loehr, New algorithms for generating Conway polynomials over finite fields, in: *Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms* (Baltimore 1999), ACM, New York (1999), 429–437.

[13] L. S. Heath and N. A. Loehr, New algorithms for generating Conway polynomials over finite fields, *J. Symbolic Comput.* **38** (2004), 1003–1024.

[14] H. Hubrechts, Point counting in families of hyperelliptic curves in characteristic 2, *LMS J. Comput. Math.* **10** (2007), 207–234.

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

[16] K. S. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, *J. Ramanujan Math. Soc.* **16** (2001), 323–338.

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

[18] R. Lercier and D. Lubicz, A quasi quadratic time algorithm for hyperelliptic curve point counting, *Ramanujan J.* **12** (2006), 399–423.

[19] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson Polynomials*, Pitman Monogr. Surv. Pure Appl. Math. 65, Longman Scientific & Technical, Harlow, 1993.

[20] P. Lisoněk, An efficient characterization of a family of hyperbent functions, *IEEE Trans. Inform. Theory* **57** (2011), 6010–6014.

[21] S. Mesnager, Hyper-bent boolean functions with multiple trace terms, in: *WAIFI*, Lecture Notes in Comput. Sci. 6087, Springer (2010), 97–113.

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

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

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

[25] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. U.S.A.* **34** (1948), 204–207.

[26] A. M. Youssef and G. Gong, Hyper-bent functions, in: *EUROCRYPT*, Lecture Notes in Comput. Sci. 2045, Springer (2001), 406–419.

Received October 13, 2012; revised December 24, 2012; accepted May 22, 2013.

Author information

Jean-Pierre Flori, Institut Télécom, Télécom ParisTech, UMR 7539, CNRS LTCI,
46 rue Barrault, 75634 Paris Cedex 13, France.
E-mail: `flori@enst.fr`

Sihem Mesnager, 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.
E-mail: `smesnager@univ-paris8.fr`