An efficient characterization of a family of hyperbent functions with multiple trace terms

Jean-Pierre Flori, Sihem Mesnager

An efficient characterization of a family of hyperbent functions with multiple trace terms

Jean-Pierre Flori * Sihem Mesnager †

Wednesday 27th July, 2011

Abstract

Lisoněk recently reformulated the characterization of Charpin and Gong of a large class of hyperbent functions in terms of cardinalities of hyperelliptic curves. In this paper, we show that such a reformulation can be naturally extended to a distinct family of functions proposed by Mesnager. Doing so, a polynomial time and space test is obtained to test the hyperbentness of functions in this family. Finally we show how this reformulation can be transformed to obtain a more efficient test.

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 [32] 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 [37] in 2001, the so-called hyperbent functions. In fact, the first definition of hyperbent functions was based on a property of the extended Hadamard transform of Boolean functions introduced by Golomb and Gong [13]. 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 hyperbent functions and many related problems remain open. In particular, it seems difficult to define precisely an infinite class of hyperbent functions, as indicated by the number of open problems proposed by Charpin and Gong [5].

Some explicit constructions of hyperbent functions on $\mathbb{F}_{2^n}$ have been proposed in the literature. Monomial hyperbent functions are famous bent functions due to Dillon [7]. The list of currently known hyperbent functions is given in Table 1. In [5], Charpin and Gong have characterized by

*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

means of Dickson polynomials a large class of hyperbent functions, which includes the well-known monomial functions with the Dillon exponent as a particular case. Afterwards Mesnager [30] has characterized by means of Dickson polynomials another class of hyperbent functions, distinct from that of Charpin and Gong.

Very recently, Lisoněk [27] has reformulated the Charpin-Gong hyperbentness criterion in terms of the number of rational points on certain hyperelliptic curves. Using this criterion, the hyperbentness 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 [21], and Katz and Livné [17]. Following the works of Lachaud et al., and Lisoněk, the purpose of this paper is to establish an efficient new hyperbentness criterion for the class proposed by Mesnager.

It 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 hyperbent functions. We then recall the Charpin-Gong criterion and deduce the Lisoněk reformulation. Finally we show that such an approach naturally extends to the class of functions described by Mesnager and propose a slightly different reformulation leading to a faster test.

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 a an element of $\mathbb{F}_{2^m}$ used to define (hyper, semi)-bent Boolean functions with $n = 2m$ inputs.

2.1 Boolean functions in polynomial form

Let n be a positive integer. 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:

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

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:

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

called its polynomial form, where Γ_n is the set of integers obtained by choosing one element in each cyclotomic coset modulo $2^n - 1$, 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 $\epsilon = \mathrm{wt}(f)$ modulo 2. Recall that, given an integer e, $0 \le e \le 2^n - 1$, having the binary expansion: $e = \sum_{i=0}^{n-1} e_i 2^i$, $e_i \in \{0, 1\}$, the 2-weight of e, denoted by $w_2(e)$, is the Hamming weight of the binary vector $(e_0, e_1, \cdots, e_{n-1})$.

2.2 Walsh-Hadamard transform, bent and hyperbent 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:

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

Bent functions are functions with maximum non-linearity. They only exist for even number of inputs and can be defined as follows.

Definition 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 $\omega \in \mathbb{F}_{2^n}$.*

Hyperbent functions have even stronger properties than bent functions. More precisely, hyperbent functions can be defined as follows.

Definition 2. *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be hyperbent if the function $x \mapsto f(x^i)$ is bent for every integer i co-prime with $2^n - 1$.*

2.3 Binary exponential sums

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

Definition 3. *The binary Kloosterman sums on $\mathbb{F}_{2^m}$ are:*

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

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

Definition 4. *The cubic sums on $\mathbb{F}_{2^m}$ are:*

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

2.4 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 [25] 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 Elliptic and hyperelliptic curves

In this section we give basic definitions for elliptic and hyperelliptic curves as well as results about point counting on such curves over finite fields of characteristic 2. When we speak of cardinality of such curves and note $\#E(\mathbb{F}_{2^m})$, we mean the number of points on it with coordinates in the given finite field $\mathbb{F}_{2^m}$. We omit the reference to the finite field if the context is clear. The main fact about such curves we will use in the next section is that there exist algorithms to compute their cardinalities in polynomial time and space in m.

Classical treatment of the theory of elliptic curves can be found for example in [33, 15, 4, 36, 18]. A more cryptographic oriented point of view, and especially special treatment for even characteristic, can be found for example in [19, 20, 8, 3, 6, 10] An elliptic curve can be defined as follows.

Definition 5. *An elliptic curve E is a smooth projective algebraic curve of genus one with a rational point O_E.*

In more down-to-earth terms, such a curve can be described by a Weierstrass equation of the form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ ,$$

giving its affine part. There is an additional point at infinity O_E which can be seen as the only non-affine solution to the homogenized equation.

There are many different algorithms to compute the cardinality of elliptic curves. The main result we need has been given by Harley [14]. A complete description of many existing algorithms can be found in Vercauteren's thesis [35] or in [34, 24].

Theorem 6 ([14])**.** *Let E be an elliptic curve defined over $\mathbb{F}_{2^m}$. There exist an algorithm to compute the cardinality of E in $O(n^2(\log n)^2 \log\log n)$ time and $O(n^2)$ space.*

The theory of hyperelliptic curve, with a cryptographic point of view, can be found for example in [16, 20, 28, 11, 6, 10]. We can define rather generally an hyperelliptic curve as follows.

Definition 7. *An hyperelliptic curve H is a smooth projective algebraic curve which is a degree 2 covering of the projective line.*

This definition includes the elliptic curves, but it is sometimes understood that an hyperelliptic curve should be of genus $g \geq 2$.

A description of the different types of hyperelliptic curves in even characteristic can be found in [2]. For the cryptographic point of view, the curves are often chosen to be imaginary hyperelliptic curves. This is also the kind of curves we will encounter. Such an hyperelliptic curve of genus g can be described by an affine part given by the following equation:

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

where $h(x)$ is of degree $\leq g$ and $f(x)$ is monic of degree $2g + 1$.

The main result about point counting of hyperelliptic curves we use is given by Vercauteren [35].

Theorem 8. *Let H be an hyperelliptic curve of genus g defined over $\mathbb{F}_{2^m}$. There exist 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 stronger result is also given for hyperelliptic curves of a special form.

Definition 9. *An Artin-Schreier curve is an hyperelliptic curve whose affine part is given by an equation of the form:*

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

where $0 \geq n \geq g$ *and* $f(x)$ *is monic of degree* $2g + 1$.

Theorem 10. *Let* H *be an Artin-Schreier curve of genus* g *defined over* $\mathbb{F}_{2^m}$. *There exist an algorithm to compute the cardinality of* H *in*

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

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

3 Constructions of hyperbent functions

From now on, let $n = 2m$ be an even integer.

3.1 Hyperbent functions in polynomial form: state of the art

The list of currently known hyperbent functions is given in Table 1.

Class of functions	Conditions on the coefficients	References
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$; $\gcd(r, 2^m+1) = 1$	$K_m(a) = 0$	[7, 22, 23, 5]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$; m odd, $\gcd(r, 2^m+1) = 1$	$K_m(a) = 4$	[31]
$\mathrm{Tr}_1^n\left(a\zeta^i x^{3(2^m-1)}\right) + \mathrm{Tr}_1^2\left(\beta^j x^{\frac{2^n-1}{3}}\right)$; 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 of unity, $(i,j) \in \{0,1,2\}^2$, $a \in \mathbb{F}_{2^m}^*$	$K_m(a) = 4$ and $\mathrm{Tr}_1^m\left(a^{1/3}\right) = 0$	[29]
$\mathrm{Tr}_1^n\left(a\zeta^i x^{3(2^m-1)}\right) + \mathrm{Tr}_1^2\left(\beta^j x^{\frac{2^n-1}{3}}\right)$; 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 of unity $i \in \{1,2\}$, $j \in \{0,1,2\}$, $a \in \mathbb{F}_{2^m}^*$	$K_m(a) + C_m(a,a) = 4$ and $\mathrm{Tr}_1^m\left(a^{1/3}\right) = 1$	[29]
$\sum_{i=1}^{2^{m-1}-1} \mathrm{Tr}_1^n\left(ax^{i(2^m-1)}\right)$	$a \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2$	[12].
$\sum_{i=1}^{2^{m-2}-1} \mathrm{Tr}_1^n\left(ax^{i(2^m-1)}\right)$; m odd	$a^{(2^m-4)^{-1}} \in \{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m(x) = 0\}$	[12]

Table 1: Families of hyperbent functions

Moreover, Charpin and Gong [5] gave a characterization of hyperbentness 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 11 ([5])**.** *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_r} *be the function defined on* $\mathbb{F}_{2^n}$ *by* $f_{a_r}(x) = \sum_{r \in R} \mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right)$, $a_r \in \mathbb{F}_{2^m}$, *where* $R \subseteq S$. *Let* g_{a_r} *be the Boolean function defined on* $\mathbb{F}_{2^m}$ *by* $g_{a_r}(x) = \sum_{r \in R} \mathrm{Tr}_1^m(a_r D_r(x))$. *Then* f_{a_r} *is hyperbent if and only if*

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

Finally, Mesnager [30] gave a characterization of hyperbentness for another large class of hyperbent functions defined on $\mathbb{F}_{2^n}$ with multiple trace terms and which do not belong to the family considered by Charpin and Gong in [5]. There was a typo in the theorem given in [30] corrected here.

Theorem 12 ([30]). *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 $f_{a_r,b}$ be the function defined on $\mathbb{F}_{2^n}$ by* (1)

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

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

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

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

3.2 Reformulation in terms of cardinality of curves

The characterizations of hyperbentness given by Charpin and Gong (Theorem 11) as well as Mesnager (Theorem 12) can be naturally reformulated in terms of cardinality of curves.

The ideas in this approach go back to the works of Lachaud and Wolfmann [21], and Katz and Livné [17]. We recall a simple proof of their result here, because its generalizations can be proved in a very similar manner.

Theorem 13 ([21, 17]). *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

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

and

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

Using the additive version of Hilbert's Theorem 90, we get

$$\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}+ax\right)\right) = -2^m+1+2\#\{x\in\mathbb{F}_{2^m}^* \mid \exists t\in\mathbb{F}_{2^m} t^2+t=x^{-1}+ax\}$$
$$= -2^m+1+2\#\{x\in\mathbb{F}_{2^m}^* \mid \exists t\in\mathbb{F}_{2^m} t^2+xt=x+ax^3\} \ .$$

We recognize the number of points of E_a minus the only point with x-coordinate $x=0$ and the only point at infinity.

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

□

Hence the necessary and sufficient condition for hyperbentness of the monomial functions with the Dillon exponent given in Table 1 can be reformulated as follows.

Proposition 14. *The notations are as in Theorem 13. Moreover let r be an integer such that $\gcd(r,2^m+1)=1$ and f_a be the Boolean function with n inputs $f_a(x)=\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$. Then f_a is hyperbent if and only if*

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

The class of functions described by Mesnager in [31] can also be given such a treatment.

Proposition 15. *The notations are as in Theorem 13. 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 hyperbent if and only if*

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

The theory of elliptic curves is rich and was subsequently used in different papers to efficiently find specific values of Kloosterman sums [26, 1, 9], and so to build hyperbent functions. In particular, Theorem 6 shows that computing their cardinalities is polynomial time and space in m and so is testing the hyperbentness of such a Boolean function.

Very recently, Lisoněk [27] generalized this reformulation to the Charpin-Gong criterion (Theorem 11) for hyperbentness of Boolean function with multiple trace terms. His idea is that both terms of the equality can be reformulated in terms of cardinalities of hyperelliptic curves as in Theorem 13. We give detailed proofs of theses results because it is not completely available in [27] and we will use similar results to reformulate the Mesnager condition.

Proposition 16. *Let $f:\mathbb{F}_{2^m}\to\mathbb{F}_{2^m}$ be a function such that $f(0)=0$, $g=\mathrm{Tr}_1^m(f)$ and G_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by*

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

Then

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

Proof. Indeed

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

□

Proposition 17. *Let $f:\mathbb{F}_{2^m}\to\mathbb{F}_{2^m}$, $g=\mathrm{Tr}_1^m(f)$ and H_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by*

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

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. Indeed

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

□

We can now easily deduce the reformulation of the Charpin-Gong criterion.

Theorem 18 ([27])**.** *The notations are as in Theorem 11. Moreover, let H_{a_r} and G_{a_r} be the (affine) curves defined over $\mathbb{F}_{2^m}$ by*

$$\begin{aligned}H_{a_r}&: y^2+xy=x+x^2\sum_{r\in R}a_rD_r(x)\ ,\\ G_{a_r}&: y^2+y=\sum_{r\in R}a_rD_r(x)\ .\end{aligned}$$

Then f_{a_r} is hyperbent if and only if

$$\#H_{a_r}-\#G_{a_r}=-1\ .$$

Proof. According to Proposition 17, the left term becomes

$$\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right)+g_{a_r}(x)\right) = -2^m + \#H_{a_r} \ ;$$

and according to Proposition 16, the right term becomes

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

□

The smooth projective models of the curves H_{a_r} and G_{a_r} are hyperelliptic. Moreover they are Artin-Schreier curves. As for elliptic curves, Theorem 10 says that there exist an efficient algorithms to compute the cardinality of such curves. Thus Lisoněk obtained an efficient test for hyperbentness of Boolean functions in the class described by Charpin and Gong. Indeed, if we fix a subset of indices R and denote by r_{max} the maximal index (which we can suppose to be odd), the polynomial defining H_{a_r} (respectively G_{a_r}) is 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 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_r} and G_{a_r}).

We now show that a similar reformulation can be applied to the criterion of Mesnager for Boolean functions with multiple trace terms.

Theorem 19. *The notations are as in Theorem 12. Moreover, let H_{a_r} and G_{a_r} be the (affine) curves defined over $\mathbb{F}_{2^m}$ by*

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

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

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

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

$$\#H^3_{a_r} - \#G^3_{a_r} = 3 \ .$$

If $b=1$, then $f_{a_r,1}$ is hyperbent if and only if

$$\left(\#G^3_{a_r} - \#H^3_{a_r}\right) - \frac{3}{2}\left(\#G_{a_r} - \#H_{a_r}\right) = \frac{3}{2} \ .$$

Proof. If b is a primitive root of unity, according to Proposition 17 the left term of the criterion is

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

and according to Proposition 16 the right term is

$$2^m - 2\,\mathrm{wt}(g_{a_r} \circ D_3) + 3 = -2^m + 3 + \#G^3_{a_r} \ ,$$

so that the condition becomes

$$\#H^3_{a_r} - \#G^3_{a_r} = 3 \ .$$

Using the other formulation given in condition 2b of Theorem 12, we could directly get from Propositions 17 and 16

$$\begin{aligned}\sum_{x\in\mathbb{F}^*_{2^m},\mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_{a_r} \circ D_3(x)\right) &= \frac{1}{2}\left(\sum_{x\in\mathbb{F}^*_{2^m}} \chi\left(g_{a_r} \circ D_3(x)\right) - \sum_{x\in\mathbb{F}^*_{2^m}} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_{a_r} \circ D_3(x)\right)\right) \\ &= \frac{1}{2}\left(\left(-2^m - 1 + \#G^3_{a_r}\right) - \left(-2^m + \#H^3_{a_r}\right)\right) \\ &= \frac{1}{2}\left(\#G^3_{a_r} - \#H^3_{a_r} - 1\right) \ .\end{aligned}$$

If $b = 1$, in condition 3 of Theorem 12, using the previous calculations, the left term is

$$2\sum_{x\in\mathbb{F}^*_{2^m},\mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_{a_r} \circ D_3(x)\right) = \#G^3_{a_r} - \#H^3_{a_r} - 1 \ ;$$

and the right term is

$$\begin{aligned}2 + 3\sum_{x\in\mathbb{F}^*_{2^m},\mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_{a_r}(x)\right) &= 2 + \frac{3}{2}\left(\#G_{a_r} - \#H_{a_r} - 1\right) \\ &= \frac{1}{2} + \frac{3}{2}\left(\#G_{a_r} - \#H_{a_r}\right) \ .\end{aligned}$$

□

Here all the curves are also Artin-Schreier curves. So for a fixed subset of indices R, we also get a test polynomial 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 involved to define them. Denoting by r_{max} the maximal index as above, the genus of $H^3_{a_r}$ (respectively $G^3_{a_r}$) is $(3r_{max}+1)/2$ (respectively $(3r_{max}-1)/2$), so approximately three times that of H_{a_r} (respectively G_{a_r}). Therefore the associated test is 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 $(r_{max}-1)/2$. Hence we propose another reformulation of the Mesnager criterion involving less computations.

Theorem 20. *The notations are as in Theorem 19. If b is a primitive element of $\mathbb{F}_4$, then $f_{a_r,b}$ is hyperbent if and only if*

$$\#G^3_{a_r} - \frac{1}{2}\left(\#G_{a_r} + \#H_{a_r}\right) = -\frac{3}{2} \ .$$

If $b = 1$, then $f_{a_r,1}$ is hyperbent if and only if

$$2\#G^3_{a_r} - \frac{5}{2}\#G_{a_r} + \frac{1}{2}\#H_{a_r} = \frac{3}{2} \ .$$

Proof. We use the fact that m is odd, so that the function $x \mapsto D_3(x) = x^3 + x$ is a permutation of the set $\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m\left(x^{-1}\right) = 0\}$, and similar arguments as previously.

If b primitive, then

$$\begin{aligned}
\sum_{x \in \mathbb{F}_{2^m}^* | \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_{a_r} \circ D_3(x)\right) &= \sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(g_{a_r} \circ D_3(x)\right) - \sum_{x \in \mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=0} \chi\left(g_{a_r} \circ D_3(x)\right) \\
&= \sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(g_{a_r} \circ D_3(x)\right) - \sum_{x \in \mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=0} \chi\left(g_{a_r}(x)\right) \\
&= \sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(g_{a_r} \circ D_3(x)\right) \\
&\quad - \frac{1}{2}\left(\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(g_{a_r}(x)\right) + \sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_{a_r}(x)\right)\right) \\
&= \left(-2^m - 2 + \#G_{a_r}^3\right) - \frac{1}{2}\left(\left(-2^m - 2 + \#G_{a_r}\right) + \left(-2^m - 1 + \#H_{a_r}\right)\right) \\
&= -\frac{1}{2} + \#G_{a_r}^3 - \frac{1}{2}\left(\#G_{a_r} + \#H_{a_r}\right) \quad .
\end{aligned}$$

If $b = 1$, then

$$2 \sum_{x \in \mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_{a_r} \circ D_3(x)\right) = -1 + 2\#G_{a_r}^3 - \left(\#G_{a_r} + \#H_{a_r}\right) \quad .$$

□

Here 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 $(r_{max} - 1)/2$.

References

[1] Omran Ahmadi and Robert Granger. An efficient deterministic test for Kloosterman sum zeros. *CoRR*, abs/1104.3882, 2011.

[2] Enge Andreas. How to distinguish hyperelliptic curves in even characteristic. In *Public-Key Cryptography and Computational Number Theory*, de Gruyter Proceedings in Mathematics, pages 49–58. DE GRUYTER, July 2011. 0.

[3] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.

[4] J. W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

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

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

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

[8] Andreas Enge. *Elliptic Curves and Their Applications to Cryptography: An Introduction*. Springer, 1st edition, August 1999.

[9] Jean-Pierre Flori, Sihem Mesnager, and Gérard Cohen. The value 4 of binary kloosterman sums. Cryptology ePrint Archive, Report 2011/364, 2011. `http://eprint.iacr.org/`.

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

[11] P. Gaudry. Hyperelliptic curves and the HCDLP. In *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 133–150. Cambridge Univ. Press, Cambridge, 2005.

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

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

[14] Robert Harley. Asymptotically optimal p-adic point-counting. Email to NMBRTHRY list, December 2002. `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0212&L=nmbrthry&T=0&P=1343`.

[15] Dale Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[16] Michael Jacobson, Jr., Alfred Menezes, and Andreas Stein. Hyperelliptic curves and cryptography. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 255–282. Amer. Math. Soc., Providence, RI, 2004.

[17] 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.

[18] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[19] Neal Koblitz. Constructing elliptic curve cryptosystems in characteristic 2. In Alfred Menezes and Scott A. Vanstone, editors, *CRYPTO*, volume 537 of *Lecture Notes in Computer Science*, pages 156–167. Springer, 1990.

[20] Neal Koblitz. *Algebraic aspects of cryptography*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998. With an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato.

[21] 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.

[22] 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.

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

[24] Reynald Lercier, David Lubicz, and Frederik Vercauteren. Point counting on elliptic and hyperelliptic curves. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 407–453. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[25] 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.

[26] Petr Lisonek. On the connection between Kloosterman sums and elliptic curves. In Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, editors, *SETA*, volume 5203 of *Lecture Notes in Computer Science*, pages 182–187. Springer, 2008.

[27] Petr Lisoněk. Hyperbent functions and hyperelliptic curves. Talk given at Arithmetic, Geometry, Cryptography and Coding Theory (AGCT-13), slides available at `http://iml.univ-mrs.fr/~ritzenth/AGCT/talks/lisonek.pdf`, to appear in IEEE Transactions on Information Theory, March 2011.

[28] Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato. An elementary introduction to hyperelliptic curves. In *Algebraic aspects of cryptography*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998.

[29] 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.

[30] 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.

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

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

[33] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[34] F. Vercauteren. Advances in point counting. In *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 103–132. Cambridge Univ. Press, Cambridge, 2005.

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

[36] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.

[37] 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.