# Dickson polynomials, hyperelliptic curves and hyper-bent functions

Jean-Pierre Flori * Sihem Mesnager †

Friday 13th January, 2012

**Abstract**

In this paper, we study the action of Dickson polynomials on subsets of finite fields of even characteristic related to the trace of the inverse of an element and provide an alternate proof of a not so well-known result. Such properties are then applied to the study of a family of Boolean functions and a characterization of their hyper-bentness in terms of exponential sums recently proposed by Wang et al. Finally, we extend previous works of Lisoněk and Flori and Mesnager to reformulate this characterization in terms of the number of points on hyperelliptic curves and present some numerical results leading to an interesting problem.

## 1 Introduction

Hyper-bent functions were defined by Youssef and Gong [26] in 2001 and are both of theoretical and practical interest. In fact, they were initially proposed by Golomb and Gong [11] as a component of S-boxes to ensure the security of symmetric cryptosystems. But such functions are rare, and so interesting from a combinatorial point of view: they indeed have stronger properties than the well-known bent functions which were already studied by Dillon [8] and Rothaus [21] more than three decades ago and whose classification is still elusive. Therefore, not only their study, but also their generation are challenging problems.

Recently, Charpin and Gong [3] proposed a characterization of hyper-bentness for a family of Boolean functions in polynomial form through exponential sums. Mesnager [17, 18] and Wang et al. [25] extended this to a couple of other families of Boolean functions with additional trace terms.

A fundamental object in these works are Dickson polynomials [14]. A good understanding of their properties, and in particular of those involving the subsets of finite fields composed of elements whose inverses have have a given trace, is therefore crucial. An important result which can be found in the work of Dobbertin et al. [9, Lemma 18] deals with these sets. Although it is qualified as well-known, a subtle fact emphasized in the remark following this lemma does not seem to be; it is often reproved in an elementary way in very specific cases, even by highbrow researchers. An alternate and general proof of this fact, together with other useful facts relating Dickson polynomials and exponential sums, are the core of Section 2.

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

†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

Section 3 is then devoted to a finer study of the family of Boolean functions introduced by Wang et al. [25]. We provide additional results about this family, including useful expressions for their extended Walsh-Hadamard transforms, their algebraic degrees and their duals. In Section 4, we extend reformulations in terms of hyperelliptic curves of the aforementioned hyper-bentness characterizations, previously proposed by Lisoněk [16] and Flori and Mesnager [10], to the characterization proposed by Wang et al. and show how profit can be taken from the properties of Dickson polynomials presented in Section 2. To conclude, we provide numerical results about a specific subclass of the Wang et al. family and propose an interesting theoretical question in Section 5.

Throughout this paper, $m \geq 0$ is a positive integer and $n = 2m$. The base field for our work will be $\mathbb{F}_{2^m}$, but our final motivation is the study of Boolean functions defined over $\mathbb{F}_{2^n}$. While working over finite fields, we use the shorthand notation $1/0 = 0$.

# 2 Dickson polynomials and the trace of inverse

Dickson polynomials can be defined explicitely as follows[1].

**Definition 2.1** (Dickson polynomials [14, Definition 2.1], [15, Equation 7.6])**.** *The Dickson polynomials are defined as* $D_0(x) = 0$ *and*

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

*for* $r \geq 1$.

Alternative definitions are possible through the recurrence relation they verify, such as [14, Lemma 2.3]

$$D_{r+2}(x) = xD_{r+1}(x) + D_r(x) \ ,$$

and [14, Exercice 2.2.(i)]

$$D_{r+4}(x) = x^2 D_{r+2}(x) + D_r(x) \ .$$

The first six Dickson polynomials are

$$D_0(x) = 0, \ D_1(x) = x, \ D_2(x) = x^2 \ ,$$

$$D_3(x) = x^3 + x, \ D_4(x) = x^4, \ D_5(x) = x^5 + x^3 + x \ .$$

A well-known result by Chou, Gomez-Calderon and Mullen [5] describes the cardinality of the preimage of an arbitraty element.

**Theorem 2.2** ([5, Theorem 9'], [14, Theorem 3.26'])**.** *Let* $\mathbb{F}_{2^m}$ *be the finite field with* $2^m$ *elements and* $1 \leq r \leq 2^n - 1$ *be an integer. Let*

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

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

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

[1] These are actually binary Dickson polynomials of the first kind associated with 1.

As a corollary, they obtain the cardinalities of the value sets of Dickson polynomials [5, Theorems 10 and 10'], [14, Theorems 3.27 and 3.30], and in particular a proof of the characterizations of Dickson polynomials as permutation polynomials [5, Corollary 11], [14, Corollary 3.28].

The proof heavily relies on the study of the map

$$\begin{aligned} \mathbb{F}_{2^n} &\to \mathbb{F}_{2^m} \\ x &\mapsto x + x^{-1} \end{aligned}$$

and Waring's formula [14, Theorem 1.1], [15, Theorem 1.76] which ensures that [14, Equation 2.2], [15, Equation 7.8]

$$D_r(x + x^{-1}) = x^r + x^{-r} \ .$$

Dillon and Dobbertin [7, pp 355–356] remarked that a more careful analysis shows that Dickson polynomials leave the sets of elements whose inverses have a given absolute trace fixed[2].

**Lemma 2.3** ([7, pp 355–356])**.** *Let $r \geq 0$ be an integer and $x \in \mathbb{F}_{2^m}$. Then*

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

We denote the above sets as follows.

**Definition 2.4.** *We denote by $\mathcal{T}_i$ for $i \in \mathbb{F}_2$ the set*

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

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

**Corollary 2.5.** *Let $1 \leq r \leq 2^n - 1$ be an integer. Then the map $x \mapsto D_r(x)$ induces a permutation of*

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

This property was recently used and reproved in a elementary way by Charpin, Helleseth and Zinoviev [4, Proof of Lemma 14] for $D_3$ as well as Wang et al. [24, Proof of Proposition 5] for the case $D_5$, who remarked that

$$\frac{1}{D_3(x)} = \frac{1}{x} + \frac{1}{x+1} + \frac{1}{x^2+1}, \ \frac{1}{D_5(x)} = \frac{1}{x} + \frac{x}{x^2+x+1} + \frac{x}{x^4+x^2+1} \ .$$

A much more general fact is actually true as we now demonstrate. To this end auxiliary polynomials are needed[3].

[2] A weaker statement is also proved by Ranto [20, Lemma 4] who assumes that $k = \gcd(r, 2^m - 1) = 1$.

[3] These polynomials may be seen as an even characteristic equivalent of to another variation of Dickson polynomials defined by Schur [22], [14, Theorem 2.20]. Let $a$ be an element in a commutative ring and define $D_r^*(x, a)$ as

$$D_0^*(x, a) = 1, \ D_1^*(x, a) = x$$

for $r = 0, \ 1$, and by the recurrence relation

$$D_r^*(x, a) = 2xD_{r-1}^*(x, a) - aD_{r-2}^*(x, a)$$

for $r \geq 2$. They satisfy the relation [14, Exercice 2.3.(i)]

$$a^r(a - x^2) = aD_r^*(x, a)^2 - 2xD_r^*(x, a)D_{r+1}^*(x, a) + D_{r+1}^*(x, a)^2 \ .$$

**Definition 2.6.** *Let $r \geq 0$ be an integer. Define $f_r$ as*

$$D_r(x) = \begin{cases} xf_r(x)^2 & \text{if } r \text{ is odd} \ , \\ x^2 f_r(x)^2 & \text{if } r \text{ is even} \ . \end{cases}$$

The following relation between $D_r$ and $f_r$ is then verified.

**Lemma 2.7.** *Let $r \geq 0$ be an integer. Then*

$$x + D_r(x) + x^2 f_r(x) f_{r+1}(x) + D_{r+1}(x) = 0 \ .$$

*Proof.* We equivalently show that

$$x^2 + D_r(x)^2 + x^4 f_r(x)^2 f_{r+1}(x)^2 + D_{r+1}(x)^2 = 0 \ ,$$

which can be rewritten as

$$x^2 + D_r(x)^2 + xD_r(x)D_{r+1}(x) + D_{r+1}(x)^2 = 0 \ .$$

For $r = 0$, this is trivially verified. For $r \geq 1$, write down $D_{r+1}(x)$ as $D_{r+1}(x) = xD_r(x) + D_{r-1}(x)$ and the result follows by induction. □

As a corollary we get a general expression for $\frac{1}{D_r(x)}$ involving $f_r(x)$.

**Corollary 2.8.** *Let $r \geq 1$ be an integer. Then*

$$\begin{aligned} \frac{1}{D_r(x)} &= \frac{1}{x} + \frac{f_{r-1}(x)}{f_r(x)} + \frac{f_{r-1}(x)^2}{f_r(x)^2} \ , \\ &= \frac{1}{x} + \frac{f_{r+1}(x)}{f_r(x)} + \frac{f_{r+1}(x)^2}{f_r(x)^2} \ . \end{aligned}$$

*Proof.* Since $D_{2r}(x) = D_r(x)$, we can suppose that $r$ is odd without loss of generality. Then

$$\begin{aligned} \frac{1}{D_r(x)} &= \frac{1}{xf_r(x)^2} = \frac{x}{x^2 f_r(x)^2} \\ &= \frac{D_r(x) + x^2 f_r(x) f_{r+1}(x) + D_{r+1}(x)}{x^2 f_r(x)^2} \\ &= \frac{xf_r(x)^2 + x^2 f_r(x) f_{r+1}(x) + x^2 f_{r+1}(x)^2}{x^2 f_r(x)^2} \\ &= \frac{1}{x} + \frac{f_{r+1}(x)}{f_r(x)} + \frac{f_{r+1}(x)^2}{f_r(x)^2} \ ; \end{aligned}$$

the other equality being deduced in a similar way. □

Lemma 2.3 directly follows from Corollary 2.8.

We define the corresponding exponential sums as follows. Recall that for a Boolean function $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$, its *"sign" function* is the integer-valued function $\chi(f) = \chi_f = (-1)^f$, i.e. $f$ composed with the additive character of $\mathbb{F}_2$.

**Definition 2.9.** *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function. We denote by $K_i^r(f)$ the exponential sum on $\mathcal{T}_i$ for $i \in \mathbb{F}_2$ for $f \circ D_r$, that is*

$$K_i^r(f) = \sum_{x \in \mathcal{T}_i} \chi_{f \circ D_r}(x) \ .$$

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

**Lemma 2.10.** *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function. Then*

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

And we finally record the following corollary.

**Corollary 2.11.** *Let $1 \le r \le 2^n - 1$ be an integer and $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function. Suppose moreover that $k = \gcd(r, 2^m - 1) = 1$. Then*

$$\begin{aligned} K_0^r(f) &= K_0(f) \ , \\ K_1^r(f) &= \sum_{x\in\mathbb{F}_{2^m}} \chi_{f\circ D_r}(x) - K_0(f) \ . \end{aligned}$$

# 3 Some properties of the Wang et al. family

Let $f$ be a Boolean function on $\mathbb{F}_{2^n}$. The *Walsh-Hadamard transform* of $f$ is the discrete Fourier transform of $\chi_f$, 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 3.1.** *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be bent if $\widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}$ for all $\omega \in \mathbb{F}_{2^n}$.*

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

**Definition 3.2.** *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 $\pm 2^{\frac{n}{2}}$.*

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].

A useful tool to study hyper-bentness is the following exponential sum.

**Definition 3.3.** *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*

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

Recently, Wang et al. [25] extended ideas of Charpin-Gong [3] and Mesnager [19, 17, 18] to a new family of Boolean functions.

**Definition 3.4** (Wang et al. family [25])**.** *Suppose that* $m \equiv 2 \pmod 4$ *and let* $E$ *be a set of representatives of the cyclotomic classes modulo* $2^n - 1$ *of full size* $n$*. For a subset* $R \subseteq E$*, let* $a_r$ *be non-zero elements in* $\mathbb{F}_{2^m}^*$ *for* $r \in R$ *and* $b$ *be an element in* $\mathbb{F}_{16}^*$[4]*. The function* $f_{a,b}$ *is then defined as*

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

The divisibility condition on $m$ essentially entails that $2^m \equiv -1 \pmod 5$. A first consequence of this equality is that all functions in this family have the same algebraic degree.

**Proposition 3.5.** *The algebraic degree of the function* $f_{a,b}$ *is equal to* $m$*.*

*Proof.* The exponent $2^m - 1$ has 2-weight $m$ since $2^m - 1 = 1 + 2 + 2^2 + \cdots + 2^{m-1}$. Moreover, $m \equiv 2 \pmod 4$ so that $n = 2m$ can be expressed as $n = 8l + 4$. Then

$$\begin{aligned} \frac{2^n - 1}{5} &= \frac{16^{2l+1} - 1}{5} = 3 \times \frac{16^{2l+1} - 1}{15} \\ &= 3 \times \sum_{i=0}^{2m} 16^i = \sum_{i=0}^{2l} 2^{4i} + \sum_{i=0}^{2l} 2^{4i+1} \quad . \end{aligned}$$

Therefore, the 2-weight of $\frac{2^n-1}{5}$ is $4l + 2 = \frac{n}{2} = m$ as well.

Both Boolean functions $x \mapsto \sum_{r \in R} \mathrm{Tr}_1^n \left( a_r x^{r(2^m-1)} \right)$ and $x \mapsto \mathrm{Tr}_1^4 \left( b x^{\frac{2^n-1}{5}} \right)$ are thus of algebraic degree $m$. Since they are separate parts in the trace representation of $f_{a,b}$, the algebraic degree of $f_{a,b}$ is equal to $m$ as well. □

The divisibility condition on $m$ also implies that $f_{a,b}(xy) = f_{a,b}(y)$ for any $x$ in the subfield $\mathbb{F}_{2^m}$. The extended Walsh-Hadamard spectrum of $f_{a,b}$ can then be expressed with $\Lambda(f_{a,b})$ in a classical manner [16, Theorem 3], [10, Proposition 3.12], thus extending the result of Wang et al. [25, Proposition 3.1].

**Proposition 3.6.** *The notation is as in Definition 3.4. 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,*

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

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

The dual of $f_{a,b}$ can then be explicitely computed when $f_{a,b}$ is hyper-bent.

**Proposition 3.7.** *If* $f_{a,b}$ *is hyper-bent, then its dual is* $f_{a,b^4}$*, i.e. we have*

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_{f_{a,b}}}(\omega) = 2^m \chi_{f_{a,b^4}}(\omega).$$

*Proof.* Let $u \in U$ be the unique element such that $u^{1-2^m} = u^2 = \omega^{2^m-1}$, that is $u = \omega^{(2^m-1)/2}$. Then $f_{a,b}(u) = f_{a,b}(\omega^{-1})$.

Moreover, since $m \equiv 2 \pmod 4$, 15 divides $2^m - 4$. Hence, $b^{2^m} = b^4$ and it follows that $f_{a,b}(\omega^{-1}) = f_{a,b^4}(\omega)$. □

[4]Setting $b = 0$ gives back the original family of Charpin and Gong [3], and in this case it is not necessary to suppose $m \equiv 2 \pmod 4$.

Extending the approach of Mesnager [19, 17, 18], Wang et al. [25] deduced the following expressions for $\Lambda(f_{a,b})$.

**Theorem 3.8** ([25]). *The notation is as in Definition 3.4. Denote moreover by $g_a$ the Boolean function on $\mathbb{F}_{2^m}$ defined by $g_a(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x))$.*

1. *If $b = 1$, then $5\Lambda(f_{a,1}) = 4K_1^5(g_a) - 10K_1(g_a) - 3$.*
2. *If $b$ is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 0$, then $5\Lambda(f_{a,b}) = 2K_1^5(g_a) + 1$.*
3. *If moreover $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$, then*
   (a) *if $b$ is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 1$, then $5\Lambda(f_{a,b}) = -3K_1^5(g_a) + 5K_1(g_a) + 1$;*
   (b) *if $b$ is a primitive 5-th root of unity, then $5\Lambda(f_{a,b}) = -K_1^5(g_a) - 5K_1(g_a) - 3$;*
   (c) *if $b$ is a primitive 3-rd root of unity, then $5\Lambda(f_{a,b}) = 2K_1(g_a) + 1$.*

# 4 Hyperelliptic curves and an efficient reformulation

The previous characterizations for hyper-bentness can be reformulated in terms of number of points on hyperelliptic curves. The main ideas in this approach stem in the works of Lachaud and Wolfmann [13], as well as Katz and Livné [12], back in the eighties, and were extended quite recently by Lisoněk [16] and Flori and Mesnager [10]. As we show below, such an approach is interesting both from practical and theoretical point of views. On the one hand, efficient point counting algorithms for hyperelliptic curves lead to a polynomial time and space test for the hyper-bentness of functions in the Wang et al. family. On the other hand, theoretical results about the number of points on hyperelliptic curves can be used to study the hyper-bentness of families of Boolean functions, and conversely interesting problems about hyperelliptic curves arise from this study.

We now state the fundamental connection between Boolean functions, exponential sums and hyperelliptic curves.

**Proposition 4.1** ([10, Propositions 3.3 and 3.4]). *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function such that $f(0) = 0$ and $g$ be the corresponding Boolean function $g = \mathrm{Tr}_1^m(f)$. 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*

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

*Then*

$$\sum_{x\in\mathbb{F}_{2^m}} \chi_g(x) = \#G_f - 2^m \ ,$$

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

As we did for exponential sums, we superscript the curves $G_f$ and $H_f$ by $r$ to mean that the corresponding functions $f$ and $g$ are composed with $D_r$.

Proposition 4.1 gives the following reformulation of Lemma 2.10 in terms of curves.

**Corollary 4.2.** *The notation is as in Proposition 4.1. Then*

$$K_i(g) = \frac{1}{2}\left((\#G_f - 2^m) + (-1)^i(\#H_f - 2^m + 1)\right) \quad .$$

When applied to Corollary 2.11, we get the following interesting result about curves.

**Corollary 4.3.** *The notation is as in Proposition 4.1. Let moreover $1 \leq r \leq 2^n - 1$ be an integer such that $k = \gcd(r, 2^m - 1) = 1$. Then*

$$\#H_f^r + \#G_f^r = \#H_f + \#G_f \quad .$$

Applying Corollary 4.2 to Theorem 3.8 leads to the following reformulation.

**Theorem 4.4.** *The notation is as in Theorem 3.8 and Proposition 4.1.*

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

Applying Corollary 4.3 then yields a more practical reformulation for explicit generation of hyper-bent functions.

**Theorem 4.5.** *The notation is as in Theorem 4.4.*

1. *If $b = 1$, then $5\Lambda(f_{a,1}) = 4\#G_a^5 - 7\#G_a + 3\#H_a$.*
2. *If $b$ is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 0$, then $5\Lambda(f_{a,b}) = 2\#G_a^5 - \#G_a - \#H_a$.*
3. *If moreover $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$, then*
   (a) *if $b$ is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 1$, then $5\Lambda(f_{a,b}) = -3\#G_a^5 + 4\#G_a - \#H_a$;*
   (b) *if $b$ is a primitive 5-th root of unity, then $5\Lambda(f_{a,b}) = -\#G_a^5 - 2\#G_a + 3\#H_a$;*
   (c) *if $b$ is a primitive 3-rd root of unity, then $5\Lambda(f_{a,b}) = 2\#G_a^5 - \#G_a - \#H_a$.*

Now recall that the zeta function of a (smooth projective) curve $C$ defined over $\mathbb{F}_q$ is

$$Z(C/\mathbb{F}_q; t) = \exp\left(\sum_{i=1}^{\infty} \frac{\#C(\mathbb{F}_{q^i})}{i} t^i\right) \quad .$$

Weil has conjectured and proved that, for a curve of genus $g$, the zeta function $Z(C/\mathbb{F}_q; t)$ can be written as a rational function

$$Z(C/\mathbb{F}_q; t) = \frac{t^{2g}\chi(1/t)}{(1-t)(1-qt)} \quad ,$$

| $m$ | $\#G_a$ | $\#H_a$ | $\#G_a^5$ | $\#H_a^5$ | $m$ | $\#G_a$ | $\#H_a$ | $\#G_a^5$ | $\#H_a^5$ |
|---|---|---|---|---|---|---|---|---|---|
| 6 | 0.000 | 0.001 | 0.000 | 0.000 | 30 | 0.024 | 1.165 | 132.982 | 197.473 |
| 10 | 0.001 | 0.001 | 0.000 | 0.000 | 34 | 0.035 | 1.376 | 338.97 | 570.014 |
| 14 | 0.010 | 0.012 | 0.020 | 0.019 | 38 | 0.080 | 1.520 | 394.670 | 627.62 |
| 18 | 0.244 | 0.217 | 0.309 | 0.318 | 42 | 0.050 | 2.390 | 491.030 | 958.810 |
| 22 | 0.019 | 0.634 | 52.533 | 81.334 | 46 | 0.037 | 5.069 | 742.901 | 1111.722 |
| 26 | 0.021 | 0.850 | 82.884 | 1.735 | 50 | 0.042 | 7.814 | 1022.621 | 1428.279 |

Table 1: Meantimes needed to compute the number of points on $G_a$, $H_a$, $G_a^5$ and $H_a^5$

where $\chi(t)$ is the characteristic polynomial of the Frobenius endomorphism of the Jacobian of $C$ and that

$$\chi(t) = a_g t^g + \sum_{i=0}^{g-1} a_i (t^{2g-i} + q^{g-i} t^i) \ .$$

In particular, the knowledge of $\chi(t)$ and its factorization over the complex numbers entails that of $\#C(\mathbb{F}_{q^i})$ for all $i \geq 1$. In particular, one has

$$\begin{aligned} \#C(\mathbb{F}_q) &= q + 1 + a_1 \ , \\ \#C(\mathbb{F}_{q^2}) &= q^2 + 1 + 2a_2 - a_1^2 \ . \end{aligned}$$

Furthermore, the curves we defined are in fact *Artin-Schreier* curves, which are a special kind of imaginary hyperelliptic curves in even characteristic, and Denef and Vercauteren [6, 23] have shown that it is possible to efficiently compute their zeta functions.

**Theorem 4.6** ([23, Theorem 4.3.1])**.** *Let $C$ be an Artin-Schreier curve of genus $g$ defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the zeta function of $C$ 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.*

We can therefore compute the number of points of such curves in polynomial time and space in the size of the base field. It should also be remarked that the time and space complexities of the above algorithm are also polynomial in the genus of the curve.

If we fix a set $R \subset E$ of indices and suppose that the maximum index $r_{max} \in R$ is odd, then the genera of the curves $H_a^5$, $G_a^5$, $H_a$ and $G_a$ are respectively $\frac{5r_{max}+1}{2}$, $\frac{5r_{max}-1}{2}$, $\frac{r_{max}+1}{2}$ and $\frac{r_{max}-1}{2}$. Therefore, even though the overall time and space complexities in $m$ of the point counting algorithm will not change, discarding the computation of the zeta function of the curve $H_a^5$ by using the reformulation of Theorem 4.4, rather than that of Theorem 4.5, will have a practical impact.

To illustrate this fact, we performed several simulations with Magma v2.18-2 [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 ten 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 $G_a$, $H_a$, $G_a^5$ and $H_a^3$ for integers $m \equiv 2 \pmod 4$ between 6 and 50 are presented in Table 1. It should be noted that Magma [1] actually uses a naive point counting algorithm for $m \leq 20$ and only switches to the Vercauteren-Kedlaya algorithm for higher values. Nonetheless, the time needed for the naive method growing exponentially, it quickly becomes far less efficient than the Vercauteren-Kedlaya one, even for curves of high genera such as $G_a^5$ and $H_a^5$.

# 5 A family of trinomial functions

We now investigate the case where $R = \{1, 3\}$ and $a_1 = a_3 = a$ and $b$ is a primitive element of $\mathbb{F}_4$ of trace zero. In this case, the functions of the Wang et al. family are of the form

$$f_{a,b} = \mathrm{Tr}_1^n \left( a(x^{3(2^m-1)} + x^{(2^m-1)}) \right) + \mathrm{Tr}_1^4 \left( b^{\frac{2^n-1}{5}} \right) \ ,$$

and the associated condition for hyper-bentness is

$$K_1^5(g_a) = 2 \ ,$$

or equivalently

$$2\#G_a^5 - \#G_a - \#H_a = 5 \ .$$

For small values of $m$, numerical investigation pointed out that the associated value $\nu_a$ defined as

$$\nu_a = \frac{K_1^5(g_a) - 2}{10} + (-1)^{\frac{m-2}{4}} = \frac{2\#G_a^5 - \#G_a - \#H_a - 5}{20} + (-1)^{\frac{m-2}{4}}$$

takes even integer values with absolute value bounded by a given constant. For $m \in \{6, 10, 14, 18\}$, the constants were respectively 2, 12, 80 and 314. In particular, it is never equal to $(-1)^{\frac{m-2}{4}}$ and the associated family of Boolean functions contains no hyper-bent functions. Proving the above fact is therefore both of practical and theoretical interest.

# 6 Conclusion

In this paper, we have presented some classical but no so well-known facts about Dickson polynomials and exponential sums, and provided an alternate proof of an important fact involving their action on sets of elements whose inverses have a given trace. We put a particular emphasis on exposing this connection, and the connection between exponential sums and hyperelliptic curves, in a setting as general as possible, in order to make them suitable for use in the study of new families of Boolean functions. As a first step for this approach, we subsequently applied these results to the study of the hyper-bentness of a family of Boolean functions recently introduced by Wang et al., thus refining their results and extending previous approaches of Lisoněk and Flori and Mesnager. Finally, we provided experimental evidence that reformulations in terms of hyperelliptic curves is crucial for the explicit generation of hyper-bent functions and proposed an interesting theoretical question related to a family of trinomial functions.

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

[4] Pascale Charpin, Tor Helleseth, and Victor Zinoviev. Divisibility properties of classical binary Kloosterman sums. *Discrete Mathematics*, 309(12):3975–3984, 2009.

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

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

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

[9] Hans Dobbertin, Patrick Felke, Tor Helleseth, and Petri Rosendahl. Niho type cross-correlation functions via dickson polynomials and kloosterman sums. *IEEE Transactions on Information Theory*, 52(2):613–627, 2006.

[10] Jean-Pierre Flori and Sihem Mesnager. An efficient characterization of a family of hyperbent functions with multiple trace terms. Cryptology ePrint Archive, Report 2011/373, 2011. `http://eprint.iacr.org/`.

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

[12] 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.

[13] 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.

[14] 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.

[15] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

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

[17] 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.

[18] Sihem Mesnager. Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. *IEEE Transactions on Information Theory*, 57(9):5996–6009, 2011.

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

[20] Kalle Ranto. On algebraic decoding of the Z4-linear Goethals-like codes. *IEEE Transactions on Information Theory*, 46(6):2193–2197, 2000.

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

[22] Issai Schur. *Gesammelte Abhandlungen. Band III.* Springer-Verlag, Berlin, 1973. Herausgegeben von Alfred Brauer und Hans Rohrbach.

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

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

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

[26] 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.