On existence (based on an arithmetical problem) and constructions of bent functions*

Sihem Mesnager[1], Gérard Cohen[2], and David Madore[2]

[1] Department of Mathematics, University of Paris VIII, University of Paris XIII, LAGA, UMR 7539, CNRS, and Télécom ParisTech, France
[2] Télécom ParisTech, UMR 5141, CNRS, France

Abstract. Bent functions are maximally nonlinear Boolean functions. They are wonderful creatures introduced by O. Rothaus in the 1960's and studied firstly by J. Dillon since 1974. Using some involutions over finite fields, we present new constructions of bent functions in the line of recent Mesnager's works. One of the constructions is based on an arithmetical problem. We discuss existence of such bent functions using Fermat hypersurface and Lang-Weil estimations.

Keywords: Boolean functions, bent functions, finite fields, arithmetic and geometric tools.

1 Introduction

Bent functions are maximally nonlinear Boolean functions with an even number of variables. They were introduced by Rothaus [35] in 1976 but already studied by Dillon [14] since 1974. For their own sake as interesting combinatorial objects, but also for their relations to coding theory (e.g. Reed-Muller codes, Kerdock codes), combinatorics (e.g. difference sets), design theory (any difference set can be used to construct a symmetric design), sequence theory, and applications in cryptography (design of stream ciphers and of S-boxes for block ciphers), they have attracted a lot of research for four decades. Yet, their classification is still elusive, therefore, not only their characterization, but also their generation are challenging problems. A non-exhaustive list of references dealing with constructions of binary bent Boolean functions is [17] [25],[14], [3], [4], [15],[22],[16], [37], [23], [11], [2], [10], [6], [30], [27], [28], [29], [8], [1], [34], [24], [31], [32]. Some open problems can be found in [7]. For a recent survey, see [9]. A book devoted especially to bent functions and containing a complete survey (including variations, generalizations and applications) is [33].

Bent functions occur in pairs. In fact, given a bent function one can define its dual which is again bent. Computing the dual of a given bent function is not an easy task in general. Recently, the first author has derived in [31] several new infinite classes of bent functions defined over the finite field $\mathbb{F}_{2^n}$ with their duals. All these families are obtained by selecting three pairwise distinct bent functions from general classes and satisfying some conditions. In [32], the first author extends the results of [31] and exhibits several new infinite families of bent functions, together with their duals. Some of them are obtained via new infinite families of permutations that the author provides with their compositional inverses. In [32] , secondary-like constructions of permutations leading to

* The paper was presented as an invited talk entitled " Bent functions and their connections to coding theory and cryptography " at the fifteenth International Conference on Cryptography and Coding, Oxford, United Kingdom (IMACC 2015) given by S. Mesnager.

several families of bent functions have also been introduced. The paper is in the line of [31] and [32]. Our objective is to provide more primary constructions of bent functions defined over the finite field $\mathbb{F}_{2^{2m}} \simeq \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ in bivariate representation in terms of the sum of the products of trace functions.

This paper is organized as follows. Formal definitions and necessary preliminaries are introduced in Section 2. In Section 3, we present an overview of the previous constructions of binary bent functions related to our work. Next, in the line of [31] and [32] based on special permutations, we investigate bent functions from involutions. We focus on monomial involutions and show how one can derive bent functions. A main result is given by Theorem 2. Finally, in Section 5, we study the existence of functions derived from Theorem 2. The problem of designing new primary bent functions turns out to be an arithmetical problem that we study by giving solutions using arithmetic and geometric tools.

2 Notation and Preliminaries

A Boolean function on the finite field $\mathbb{F}_{2^n}$ of order 2^n is a mapping from $\mathbb{F}_{2^n}$ to the prime field $\mathbb{F}_2$. It can be represented as a polynomial in one variable $x \in \mathbb{F}_{2^n}$ of the form $f(x) = \sum_{j=0}^{2^n-1} a_j x^j$ where the a_j's are elements of the field. Such a function f is Boolean if and only if a_0 and a_{2^n-1} belong to $\mathbb{F}_2$ and $a_{2j} = a_j^2$ for every $j \notin \{0, 2^n - 1\}$ (where $2j$ is taken modulo $2^n - 1$). This leads to a unique representation which we call the *polynomial form* (for more details, see e.g. [6]). First, recall that for any positive integers k, and r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$, denoted by Tr_r^k, is the mapping defined for every $x \in \mathbb{F}_{2^k}$ as:

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

In particular, we denote the *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ by $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. We make use of some known properties of the trace function such as $Tr_1^n(x) = Tr_1^n(x^2)$ and for every integer r dividing k, the mapping $x \mapsto Tr_r^k(x)$ is $\mathbb{F}_{2^k}$-linear.

The *bivariate representation* of Boolean functions makes sense only when n is an even integer. It plays an important role for defining bent functions and is defined as follows: we identify $\mathbb{F}_{2^n}$ (where $n = 2m$) with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ and consider then the input to f as an ordered pair (x, y) of elements of $\mathbb{F}_{2^m}$. There exists a unique bivariate polynomial

$$\sum_{0 \le i,j \le 2^m-1} a_{i,j} x^i y^j$$

over $\mathbb{F}_{2^m}$ such that f is the bivariate polynomial function over $\mathbb{F}_{2^m}$ associated to it. Then the algebraic degree of f equals $\max_{(i,j)\,|\,a_{i,j}\neq 0}(w_2(i) + w_2(j))$. The function f being Boolean, its bivariate representation can be written in the (non unique) form $f(x, y) = Tr_1^m(P(x, y))$ where $P(x, y)$ is some polynomial in two variables over $\mathbb{F}_{2^m}$. There exist other representations of Boolean functions not used in this paper (see e.g. [6]) in which we shall only consider functions in their bivariate representation.

If f is a Boolean function defined on $\mathbb{F}_{2^n}$, then the Walsh Hadamard transform of f is the discrete Fourier transform of the sign function $\chi_f := (-1)^f$ of f, whose value at $\omega \in \mathbb{F}_{2^n}$ is defined as follows:

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\omega x)}.$$

Bent functions can be defined in terms of the Walsh transform as follows.

Definition 1. *Let n be an even integer. A Boolean function f on $\mathbb{F}_{2^n}$ is said to be bent if its Walsh transform satisfies $\widehat{\chi_f}(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_{2^n}$.*

The automorphism group of the set of bent functions (i.e., the group of permutations π on $\mathbb{F}_{2^n}$ such that $f \circ \pi$ is bent for every bent function f) is the general affine group, that is, the group of linear automorphisms composed by translations. The corresponding notion of equivalence between functions is called *affine equivalence*. Also, if f is bent and ℓ is affine, then $f + \ell$ is bent. A class of bent functions is called a *complete class* if it is globally invariant under the action of the general affine group and under the addition of affine functions. The corresponding notion of equivalence is called *extended affine equivalence*, in brief, *EA-equivalence*.

Bent functions occur in pair. In fact, given a bent function f over $\mathbb{F}_{2^n}$, we define its *dual function*, denoted by $\widetilde{f}$, when considering the signs of the values of the Walsh transform $\widehat{\chi_f}(x)$ $(x \in \mathbb{F}_{2^n})$ of f. More precisely, $\widetilde{f}$ is defined by the equation:

$$(-1)^{\widetilde{f}(x)} 2^{\frac{n}{2}} = \widehat{\chi_f}(x). \tag{2.1}$$

Due to the involution law the Fourier transform is self-inverse. Thus the dual of a bent function is again bent , and $\widetilde{\widetilde{f}} = f$. A bent function is said to be self-dual if $\widetilde{f} = f$.

Let us recall a fundamental class of Boolean bent functions. Bent functions from the Maiorana-McFarland construction are defined over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by (2.2):

$$f(x, y) = Tr_1^m(\phi(y)x) + g(y), \quad (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \tag{2.2}$$

where m is some positive integer, ϕ is a function from $\mathbb{F}_{2^m}$ to itself and g stands for a Boolean function over $\mathbb{F}_{2^m}$. We have the following well-known result (e.g. see [6], [33]).

Proposition 1. *Let m be a positive integer. Let g be a Boolean function defined over $\mathbb{F}_{2^m}$. Define f over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by (2.2). Then f is bent if and only if ϕ is a permutation of $\mathbb{F}_{2^m}$. Furthermore, its dual function $\tilde{f}$ is*

$$\tilde{f}(x, y) = Tr_1^m(y\phi^{-1}(x)) + g(\phi^{-1}(x)) \tag{2.3}$$

where ϕ^{-1} denotes the inverse mapping of the permutation ϕ.

The class of bent functions given by (2.2) is the so-called Maiorana-McFarland class. It has been widely studied because its Walsh transform can be easily computed and its elements are completely characterized (e.g. see [6]).

3 Related previous constructions of bent functions

In [5] a secondary construction of bent functions is provided (building new bent functions from already defined ones). It is proved there that if f_1, f_2 and f_3 are bent, then if $\psi := f_1 + f_2 + f_3$ is bent and if $\tilde{\psi} = \tilde{f_1} + \tilde{f_2} + \tilde{f_3}$, then $g(x) = f_1(x)f_2(x) + f_1(x)f_3(x) + f_2(x)f_3(x)$ is bent, and $\tilde{g} = \tilde{f_1}\tilde{f_2} + \tilde{f_1}\tilde{f_3} + \tilde{f_2}\tilde{f_3}$. Next, the first author has completed this result by proving in [31] that the converse is also true. The combined result is stated in the following theorem.

Theorem 1. *([31]) Let n be an even integer. Let f_1, f_2 and f_3 be three pairwise distinct bent functions over $\mathbb{F}_{2^n}$ such that $\psi = f_1 + f_2 + f_3$ is bent . Let g be a Boolean function defined by*

$$g(x) = f_1(x)f_2(x) + f_1(x)f_3(x) + f_2(x)f_3(x). \tag{3.1}$$

Then g is bent if and only if $\tilde{\psi} + \tilde{f_1} + \tilde{f_2} + \tilde{f_3} = 0$. Furthermore, if g is bent, then its dual function $\tilde{g}$ is given by

$$\tilde{g}(x) = \tilde{f_1}(x)\tilde{f_2}(x) + \tilde{f_1}(x)\tilde{f_3}(x) + \tilde{f_2}(x)\tilde{f_3}(x),\ \forall x \in \mathbb{F}_{2^n}.$$

In [31] and [32], the first author has studied functions g of the shape (3.1) and derived several new primary constructions of bent functions.

To apply Theorem 1 to a 3-tuple of functions of the form (2.2) with $g = 0$, one has to choose appropriately the maps ϕ involved in their expressions. The following result is proven in ([31]).

Corollary 1. *Let m be a positive integer. Let ϕ_1, ϕ_2 and ϕ_3 be three permutations of $\mathbb{F}_{2^m}$. Then,*

$$g(x,y) = Tr_1^m(x\phi_1(y))Tr_1^m(x\phi_2(y)) + Tr_1^m(x\phi_1(y))Tr_1^m(x\phi_3(y)) + Tr_1^m(x\phi_2(y))Tr_1^m(x\phi_3(y))$$

is bent if and only if

1. *$\psi = \phi_1 + \phi_2 + \phi_3$ is a permutation,*
2. *$\psi^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$.*

Furthermore, its dual function $\tilde{g}$ is given by

$$\tilde{g}(x,y) = Tr_1^m(\phi_1^{-1}(x)y)Tr_1^m(\phi_2^{-1}(x)y) + Tr_1^m(\phi_1^{-1}(x)y)Tr_1^m(\phi_3^{-1}(x)y) + Tr_1^m(\phi_2^{-1}(x)y)Tr_1^m(\phi_3^{-1}(x)y).$$

Permutations satisfying $(\mathcal{A}_m)$ were introduced by the first author in [32].

Definition 2. *Let m be a positive integer. Three permutations ϕ_1, ϕ_2 and ϕ_3 of $\mathbb{F}_{2^m}$ are said to satisfy $(\mathcal{A}_m)$ if the following two conditions hold*

1. *Their sum $\psi = \phi_1 + \phi_2 + \phi_3$ is a permutation of $\mathbb{F}_{2^m}$.*
2. *$\psi^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$.*

Several new bent functions have been exhibited from monomial permutations (see [31]) and from more families of new permutations of $\mathbb{F}_{2^m}$ (see [32]). Firstly, we list below the constructions obtained by the first author in [31].

1. Bent functions obtained by selecting Niho bent functions :
   - $f(x) = Tr_1^m(\lambda x^{2^m+1}) + Tr_1^n(ax)Tr_1^n(bx)$; $x \in \mathbb{F}_{2^n}$, $n = 2m$, $\lambda \in \mathbb{F}_{2^m}^\star$ and $(a,b) \in \mathbb{F}_{2^n}^\star \times \mathbb{F}_{2^n}^\star$ such that $a \neq b$ and $Tr_1^n(\lambda^{-1}b^{2^m}a) = 0$.

     $$\tilde{f}(x) = Tr_1^m(\lambda^{-1}x^{2^m+1}) + \left(Tr_1^m(\lambda^{-1}a^{2^m+1}) + Tr_1^n(\lambda^{-1}a^{2^m}x)\right) \times \left(Tr_1^m(\lambda^{-1}b^{2^m+1}) + Tr_1^n(\lambda^{-1}b^{2^m}x)\right) + 1.$$

- $g(x) = Tr_1^m(x^{2^m+1}) + Tr_1^n\Big(\sum_{i=1}^{2^{r-1}-1} x^{(2^m-1)\frac{i}{2^r}+1}\Big) + Tr_1^n(\lambda x)Tr_1^n(\mu x)$; $x \in \mathbb{F}_{2^n}$, $n = 2m$, $(\lambda, \mu) \in \mathbb{F}_{2^m}^\star \times \mathbb{F}_{2^m}^\star$ $(\lambda \neq \mu)$.

  $\tilde{g}(x) = Tr_1^m\Big(\big(u(1+x+x^{2^m}) + u^{2^{n-r}} + x^{2^m}\big)(1+x+x^{2^m})^{\frac{1}{2^r-1}}\Big) \times Tr_1^m\Big((\lambda+\mu)(1+x+x^{2^m})^{\frac{1}{2^r-1}}\Big) + Tr_1^m\Big(\big(u(1+x+x^{2^m}) + u^{2^{n-r}} + x^{2^m} + \lambda\big)(1+x+x^{2^m})^{\frac{1}{2^r-1}}\Big)$
  $\times Tr_1^m\Big(\big(u(1+x+x^{2^m}) + u^{2^{n-r}} + x^{2^m} + \mu\big)(1+x+x^{2^m})^{\frac{1}{2^r-1}}\Big)$; where $u \in \mathbb{F}_{2^n}$ satisfying $u + u^{2^m} = 1$.

2. Bent functions obtained by selecting bent Boolean functions of Maiorana-McFarland's class :
   - $f(x,y) = Tr_1^m(a_1y^dx)Tr_1^m(a_2y^dx) + Tr_1^m(a_1y^dx)Tr_1^m(a_3y^dx) + Tr_1^m(a_2y^dx)Tr_1^m(a_3y^dx)$; where $(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, d is a positive integer which is not a power of 2 and $gcd(d, 2^m-1) = 1$, a_i's are pairwise distinct such that $b := a_1 + a_2 + a_3 \neq 0$ and $a_1^{-e} + a_2^{-e} + a_3^{-e} = b^{-e}$ where $e = d^{-1} \pmod{2^m-1}$.

     $\tilde{f}(x,y) = Tr_1^m(a_1^{-e}x^ey)Tr_1^m(a_2^{-e}x^ey) + Tr_1^m(a_1^{-e}x^ey)Tr_1^m(a_3^{-e}x^ey) + Tr_1^m(a_2^{-e}x^ey)Tr_1^m(a_3^{-e}x^ey)$.
   - $g(x,y) = Tr_1^m(a^{-11}x^{11}y)Tr_1^m(a^{-11}c^{-11}x^{11}y)$
     $Tr_1^m(a^{-11}x^{11}y)Tr_1^m(c^{11}a^{-11}x^{11}y) + Tr_1^m(a^{-11}c^{-11}x^{11}y)Tr_1^m(c^{11}a^{-11}x^{11}y)$; where $(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, $a \in \mathbb{F}_{2^n}^\star$ with $n = 2m$ is a multiple of 4 but not of 10, $c \in \mathbb{F}_{2^m}$ is such that $c^4 + c + 1 = 0$.

     $\tilde{g}(x,y) = Tr_1^m(ay^dx)Tr_1^m(acy^dx) + Tr_1^m(ay^dx)Tr_1^m\big(ac^{-1}y^dx\big) + Tr_1^m(acy^dx)Tr_1^m\big(ac^{-1}y^dx\big)$; with $d = 11^{-1} \pmod{2^n-1}$.
   - $h(x,y) = (Tr_1^m(a_1y^dx) + g_1(y))(Tr_1^m(a_2y^dx) + g_2(y)) + (Tr_1^m(a_1y^dx) + g_1(y))(Tr_1^m(a_3y^dx) + g_3(y)) + (Tr_1^m(a_2y^dx) + g_2(y))(Tr_1^m(a_3y^dx) + g_3(y))$; where $m = 2r$, $gcd(d, 2^m-1) = 1$, a_1, a_2 and a_3 are three pairwise distinct elements of $\mathbb{F}_{2^m}$ such that $b := a_1 + a_2 + a_3 \neq 0$ and $a_1^{-e} + a_2^{-e} + a_3^{-e} = b^{-e}$ and for $i \in \{1,2,3\}$, $g_i \in \mathcal{D}_m := \{g : \mathbb{F}_{2^m} \to \mathbb{F}_2 \mid g(ax) = g(x), \forall (a,x) \in \mathbb{F}_{2^r} \times \mathbb{F}_{2^m}\}$.

     $\tilde{h}(x,y) = (Tr_1^m(a_1^{-e}x^ey) + g_1(x^e))(Tr_1^m(a_2^{-e}x^ey) + g_2(x^e)) + (Tr_1^m(a_1^{-e}x^ey) + g_1(x^e))(Tr_1^m(a_3^{-e}x^ey) + g_3(x^e)) + (Tr_1^m(a_2^{-e}x^ey) + g_2(x^e))(Tr_1^m(a_3^{-e}x^ey) + g_3(x^e))$ where $e = d^{-1} \pmod{2^m-1}$.
3. Self-dual bent functions obtained by selecting functions from Maiorana-McFarland completed class[3] :
   - $g(x) = Tr_1^{4k}(a_1x^{2^k+1})Tr_1^{4k}(a_2x^{2^k+1}) + Tr_1^{4k}(a_1x^{2^k+1})Tr_1^{4k}(a_3x^{2^k+1}) + Tr_1^{4k}(a_2x^{2^k+1})Tr_1^{4k}(a_3x^{2^k+1})$; where $x \in \mathbb{F}_{2^{4k}}$, $k \geq 2$, a_1, a_2, a_3 be three pairwise distinct nonzero solutions in $\mathbb{F}_{2^{4k}}$ of the equation $\lambda^{2^{3k}} + \lambda = 1$ such that $a_1 + a_2 + a_3 \neq 0$.
4. Bent functions obtained by selecting functions from PS_{ap} :
   - $f(x,y) = Tr_1^m(a_1y^{2^m-2}x)Tr_1^m(a_2y^{2^m-2}x) + Tr_1^m(a_1y^{2^m-2}x)Tr_1^m(a_3y^{2^m-2}x)$
     $+ Tr_1^m(a_2y^{2^m-2}x)Tr_1^m(a_3y^{2^m-2}x)$; where $(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, the a_i's are pairwise distinct in $\mathbb{F}_{2^m}$ such that $a_1 + a_2 + a_3 \neq 0$.

     $\tilde{f}(x,y) = f(y,x)$.

[3] The Maiorana-McFarland completed class is the smallest class containing the class of Maiorana-McFarland which is globally invariant under the action of the general affine group and under the addition of affine functions.

5. Bent functions obtained by combining Niho bent functions and self-dual bent functions :
   - $f(x) = Tr_1^{2k}(x^{2^{2k}+1}) + Tr_1^{4k}(ax)Tr_1^{2k}(x^{2^{2k}+1}) + Tr_1^{4k}(ax)Tr_1^{4k}(\lambda_2(x+\beta)^{2^k+1}) + Tr_1^{4k}(ax)$; where $x \in \mathbb{F}_{2^{4k}}$ $(k \geq 2)$, $\lambda_2 \in \mathbb{F}_{2^{4k}}$ such that $\lambda_2 + \lambda_2^{2^{3k}} = 1$, $a \in \mathbb{F}_{2^{4k}}^{\star}$ is a solution of $a^{2^{2k}} + \lambda_2{}^{2^{-k}}a^{2^{-k}} + \lambda_2 a^{2^k} = 0$ and $\beta \in \mathbb{F}_{2^{4k}}$ such that $Tr_1^{4k}(\beta a) = Tr_1^{2k}(a^{2^{2k}+1}) + Tr_1^{4k}(\lambda_2 a^{2^k+1})$.

   $$\tilde{f}(x) = Tr_1^{2k}(x^{2^{2k}+1}) + \Big(Tr_1^{2k}(x^{2^{2k}+1}) + Tr_1^{4k}(\lambda_2 x^{2^k+1}) + Tr_1^{4k}(\beta x)\Big) \times \Big(Tr_1^{4k}(a^{2^k}x) + Tr_1^{2k}(a^{2^{2k}+1})\Big).$$

Secondly, we list below the infinite families of bent functions from new permutations and their duals provided by the first author in [32].

1. Let m be a positive integer. Let L be a linear permutation on $\mathbb{F}_{2^m}$. Let f be a Boolean function over $\mathbb{F}_{2^m}$ such that $\mathcal{L}_f^0 := \{\alpha \in \mathbb{F}_{2^m} \mid D_\alpha f = 0\}$ is of dimension at least two over $\mathbb{F}_2$. Let $(\alpha_1, \alpha_2, \alpha_3)$ be any 3-tuple of pairwise distinct elements of $\mathcal{L}_f^0$ such that $\alpha_1 + \alpha_2 + \alpha_3 \neq 0$. Then the Boolean function g defined in bivariate representation on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by $g(x,y) = Tr_1^m(xL(y)) + f(y)\Big(Tr_1^m(L(\alpha_1)x)Tr_1^m(L(\alpha_2)x)$
   $+ Tr_1^m(L(\alpha_1)x)Tr_1^m(L(\alpha_3)x) + Tr_1^m(L(\alpha_2)x)Tr_1^m(L(\alpha_3)x)\Big)$ is bent and its dual function $\tilde{g}$ is given by $\tilde{g}(x,y) = Tr_1^m(L^{-1}(x)y)$
   $+ f(L^{-1}(x))\Big(Tr_1^m(\alpha_1 y)Tr_1^m(\alpha_2 y) + Tr_1^m(\alpha_1 y)Tr_1^m(\alpha_3 y) + Tr_1^m(\alpha_2 y)Tr_1^m(\alpha_3 y)\Big)$.
2. Let $m = 2k$. Let $a \in \mathbb{F}_{2^k}$ and $b \in \mathbb{F}_{2^m}$ such that $b^{2^k+1} \neq a^2$. Set $\alpha = b^{2^k+1} + a^2$ and $\rho = a + b^{2^k}$. Let g_1, g_2 and g_3 be three Boolean functions over $\mathbb{F}_{2^k}$. Then the Boolean function h defined in bivariate representation on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

   $$\begin{aligned} h(x,y) = {} & Tr_1^m(axy + bxy^{2^k}) + Tr_1^m(xg_1(Tr_k^m(\rho y)))Tr_1^m(xg_2(Tr_k^m(\rho y))) \\ & + Tr_1^m(xg_1(Tr_k^m(\rho y)))Tr_1^m(xg_3(Tr_k^m(\rho y))) \\ & + Tr_1^m(xg_2(Tr_k^m(\rho y)))Tr_1^m(xg_3(Tr_k^m(\rho y))) \end{aligned}$$

   is bent and its dual function $\tilde{h}$ is given by

   $$\begin{aligned} \tilde{h}(x,y) = {} & Tr_1^m\Big(\alpha^{-1}(axy + bx^{2^k}y)\Big) \\ & + Tr_1^m\Big(\alpha^{-1}(a+b)yg_1\left(Tr_k^m(x)\right)\Big)Tr_1^m\Big(\alpha^{-1}(a+b)yg_2\left(Tr_k^m(x)\right)\Big) \\ & + Tr_1^m\Big(\alpha^{-1}(a+b)yg_1\left(Tr_k^m(x)\right)\Big)Tr_1^m\Big(\alpha^{-1}(a+b)yg_3\left(Tr_k^m(x)\right)\Big) \\ & + Tr_1^m\Big(\alpha^{-1}(a+b)yg_2\left(Tr_k^m(x)\right)\Big)Tr_1^m\Big(\alpha^{-1}(a+b)yg_3\left(Tr_k^m(x)\right)\Big). \end{aligned}$$

3. Let n be a multiple of m where m is a positive integer and $n \neq m$. Let ϕ_1, ϕ_2 and ϕ_3 be three permutations over $\mathbb{F}_{2^m}$ satisfying $(\mathcal{A}_m)$. Let (a_1, a_2, a_3) be a 3-tuple of $\mathbb{F}_{2^m}^{\star}$ such that $a_1 + a_2 + a_3 \neq 0$. Set

   $$\begin{aligned} g(x,y) = {} & Tr_1^n(x\phi_1(y))Tr_1^n(x\phi_2(y)) + Tr_1^n(x\phi_1(y))Tr_1^n(x\phi_3(y)) \\ & + Tr_1^n(x\phi_2(y))Tr_1^n(x\phi_3(y)) \end{aligned}$$

   if $(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ and

   $$\begin{aligned} g(x,y) = {} & Tr_1^n(a_1 xy^{2^n-2})Tr_1^n(a_2 xy^{2^n-2}) + Tr_1^n(a_1 xy^{2^n-2})Tr_1^n(a_3 xy^{2^n-2}) \\ & + Tr_1^n(a_2 xy^{2^n-2})Tr_1^n(a_3 xy^{2^n-2}) \end{aligned}$$

if $(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Then g is bent and its dual function $\tilde{g}$ is defined by

$$\begin{aligned}\tilde{g}(x,y) = &Tr_1^n(\phi_1^{-1}(x)y)Tr_1^n(\phi_2^{-1}(x)y) + Tr_1^n(\phi_1^{-1}(x)y)Tr_1^n(\phi_3^{-1}(x)y)\\ &+ Tr_1^n(\phi_2^{-1}(x)y)Tr_1^n(\phi_3^{-1}(x)y)\end{aligned}$$

if $(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^n}$ and

$$\begin{aligned}\tilde{g}(x,y) = &Tr_1^n(a_1x^{2^n-2}y)Tr_1^n(a_2x^{2^n-2}y) + Tr_1^n(a_1x^{2^n-2}y)Tr_1^n(a_3x^{2^n-2}y)\\ &+ Tr_1^n(a_2x^{2^n-2}y)Tr_1^n(a_3x^{2^n-2}y)\end{aligned}$$

if $(x,y) \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m} \times \mathbb{F}_{2^n}$.

4. Let n be a multiple of m where m is a positive integer and $n \neq m$. Let ϕ_1, ϕ_2 and ϕ_3 be three permutations over $\mathbb{F}_{2^m}$ satisfying $(\mathcal{A}_m)$. Let $a \in \mathbb{F}_{2^m}^\star$ and $c \in \mathbb{F}_{2^n}$ such that $c^4 + c + 1 = 0$. Let d be the inverse of 11 modulo $2^n - 1$. Set

$$\begin{aligned}g(x,y) = &Tr_1^n(x\phi_1(y))Tr_1^n(x\phi_2(y)) + Tr_1^n(x\phi_1(y))Tr_1^n(x\phi_3(y))\\ &+ Tr_1^n(x\phi_2(y))Tr_1^n(x\phi_3(y))\end{aligned}$$

if $(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ and

$$\begin{aligned}g(x,y) = &Tr_1^n(axy^d)Tr_1^n(acxy^d) + Tr_1^n(axy^d)Tr_1^n(ac^{-1}xy^d)\\ &+ Tr_1^n(acxy^d)Tr_1^n(ac^{-1}xy^d)\end{aligned}$$

if $(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Then g is bent and its dual function $\tilde{g}$ is defined by

$$\begin{aligned}\tilde{g}(x,y) = &Tr_1^n(\phi_1^{-1}(x)y)Tr_1^n(\phi_2^{-1}(x)y) + Tr_1^n(\phi_1^{-1}(x)y)Tr_1^n(\phi_3^{-1}(x)y)\\ &+ Tr_1^n(\phi_2^{-1}(x)y)Tr_1^n(\phi_3^{-1}(x)y)\end{aligned}$$

if $(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^n}$ and

$$\begin{aligned}\tilde{g}(x,y) = &Tr_1^n(a^{-11}x^{11}y)Tr_1^n(a^{-11}c^{-11}x^{11}y) + Tr_1^n(a^{-11}x^{11}y)Tr_1^n(a^{-11}c^{11}x^{11}y)\\ &+ Tr_1^n(a^{-11}c^{-11}x^{11}y)Tr_1^n(a^{-11}c^{11}x^{11}y)\end{aligned}$$

if $(x,y) \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m} \times \mathbb{F}_{2^n}$.

5. Let n be a multiple of m where m is a positive integer and $n \neq m$. Let ϕ_1, ϕ_2 and ϕ_3 be three permutations over $\mathbb{F}_{2^m}$ satisfying $(\mathcal{A}_m)$. Let $\alpha \in \mathbb{F}_{2^m}^\star$. Let d be a positive integer such that d and $2^n - 1$ are coprime. Denote by e the inverse of d modulo $2^n - 1$. Set

$$\begin{aligned}g(x,y) = &Tr_1^n(x\phi_1(y))Tr_1^n(x\phi_2(y)) + Tr_1^n(x\phi_1(y))Tr_1^n(x\phi_3(y))\\ &+ Tr_1^n(x\phi_2(y))Tr_1^n(x\phi_3(y))\end{aligned}$$

if $(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ and $g(x,y) = Tr_1^n(\alpha xy^d)$ if $(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Then g is bent and its dual function $\tilde{g}$ is defined by

$$\begin{aligned}\tilde{g}(x,y) = &Tr_1^n(\phi_1^{-1}(x)y)Tr_1^n(\phi_2^{-1}(x)y) + Tr_1^n(\phi_1^{-1}(x)y)Tr_1^n(\phi_3^{-1}(x)y)\\ &+ Tr_1^n(\phi_2^{-1}(x)y)Tr_1^n(\phi_3^{-1}(x)y)\end{aligned}$$

if $(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^n}$ and $\tilde{g}(x,y) = Tr_1^n(\alpha^{-e}x^ey)$ if $(x,y) \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m} \times \mathbb{F}_{2^n}$.

6. Let $n = 2m$ where m is a positive integer. Let ϕ_1, ϕ_2 and ϕ_3 be three permutations over $\mathbb{F}_{2^m}$ satisfying $(\mathcal{A}_m)$. Let d be a positive integer such that $d+1$ and 2^n-1 are coprime. Let $\lambda \in \mathbb{F}_{2^m}^\star$. Set

$$\begin{aligned} g(x,y) = &Tr_1^n(x\phi_1(y))Tr_1^n(x\phi_2(y)) + Tr_1^n(x\phi_1(y))Tr_1^n(x\phi_3(y)) \\ &+ Tr_1^n(x\phi_2(y))Tr_1^n(x\phi_3(y)) \end{aligned}$$

if $(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ and $g(x,y) = Tr_1^n\left(\lambda xy\left(Tr_m^n(y)\right)^d\right)$ if $(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Then g is bent and its dual function $\tilde{g}$ is defined by

$$\begin{aligned} \tilde{g}(x,y) = &Tr_1^n(\phi_1^{-1}(x)y)Tr_1^n(\phi_2^{-1}(x)y) + Tr_1^n(\phi_1^{-1}(x)y)Tr_1^n(\phi_3^{-1}(x)y) \\ &+ Tr_1^n(\phi_2^{-1}(x)y)Tr_1^n(\phi_3^{-1}(x)y) \end{aligned}$$

if $(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^n}$ and $\tilde{g}(x,y) = Tr_1^n\left(\lambda^{-\frac{1}{d+1}} x\left(Tr_m^n(x)\right)^{-\frac{d}{d+1}} y\right)$ if $(x,y) \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m} \times \mathbb{F}_{2^n}$.

4 More constructions of bent functions

In this section, we provide from classes of involutions more primary constructions of bent functions in the line of [31] and [32].

An *involution* is a special permutation, but the involution property includes the bijectivity as it appears in the classical definition.

Definition 3. *Let F be any function over $\mathbb{F}_{2^n}$. We say that F is an involution if $F \circ F(x) = x$, for all $x \in \mathbb{F}_{2^n}$.*

In a recent work, Charpin, Mesnager and Sarkar [12] have provided a mathematical study of these involutions. The authors have considered several classes of polynomials and characterized when they are involutions (especially monomials as well as linear involutions) and presented several constructions. New involutions from known ones have also been derived. The following result is an easy consequence of Theorem 1 showing that one can derive bent functions from involutions.

Corollary 2. *Let m be a positive integer. Let ϕ_1, ϕ_2 and ϕ_3 be three involutions of $\mathbb{F}_{2^m}$. Then,*

$$g(x,y) = Tr_1^m(x\phi_1(y))Tr_1^m(x\phi_2(y)) + Tr_1^m(x\phi_1(y))Tr_1^m(x\phi_3(y)) + Tr_1^m(x\phi_2(y))Tr_1^m(x\phi_3(y))$$

is bent if and only if $\psi = \phi_1 + \phi_2 + \phi_3$ is an involution.
Furthermore, its dual function $\tilde{g}$ is given by $\tilde{g}(x,y) = g(y,x)$.

Remark 1. Notice that this gives a very handy way to compute the dual (namely, transpose the two arguments), in stark contrast with the univariate case.

Using a monomial involution (see [12]), a first construction of a new family of bent functions is given by the following statement.

Theorem 2. *Let n be an integer. Let d be a positive integer such that $d^2 \equiv 1 \pmod{2^n-1}$. Let Φ_1, Φ_2 and Φ_3 be three mappings from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by $\Phi_i(x) = \lambda_i x^d$ for all $i \in \{1,2,3\}$, where the $\lambda_i \in \mathbb{F}_{2^n}^\star$ are pairwise distinct such that $\lambda_i^{d+1} = 1$ and ${\lambda_0}^{d+1} = 1$, where $\lambda_0 := \lambda_1 + \lambda_2 + \lambda_3$. Let g be the Boolean function defined over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ by*

$$g(x,y) = Tr_1^n(\Phi_1(y)x)Tr_1^n(\Phi_2(y)x) + Tr_1^n(\Phi_2(y)x)Tr_1^n(\Phi_3(y)x) + Tr_1^n(\Phi_1(y)x)Tr_1^n(\Phi_3(y)x). \quad (4.1)$$

Then the Boolean function g defined over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ by (4.1) is bent and its dual is given by $\tilde{g}(x,y) = g(y,x)$.

Proof. Set $f_i(x,y) := Tr_1^n(\Phi_i(y)x)$ for all $i \in \{1,2,3\}$. The function f_i belongs to Maiorana-McFarland's class. Moreover, $\Phi_i(y) = \lambda_i y^d$ is a polynomial over $\mathbb{F}_{2^m}$ which is an involution if and only if $\lambda_i^{d+1} = 1$ and $d^2 \equiv 1 \pmod{2^n - 1}$. Indeed, we have $\Phi_i(\Phi_i(y)) = \lambda_i^{d+1} y^{d^2}$, hence $\lambda_i^{d+1} y^{d^2} = y$ if and only if $\lambda_i^{d+1} \equiv 1$ and $y^{d^2} \equiv y \pmod{y^{2^n} + y}$, that is, $d^2 \equiv 1 \pmod{2^n - 1}$. Using the same arguments, $\sum_{i=1}^3 \Phi_i$ is an involution since we have $(\lambda_1 + \lambda_2 + \lambda_3)^{d+1} = 1$ by hypothesis. Now, since Φ_i (resp. $\sum_{i=1}^3 \Phi_i$) is in particular a permutation over $\mathbb{F}_{2^n}$, for every $i \in \{1,2,3\}$ the Boolean function f_i (resp. $\psi := \sum_{i=1}^3 f_i$) is bent whose dual function equals $\tilde{f}_i$ (resp. $\tilde{\psi}$) defined by $\tilde{f}_i(x,y) = Tr_1^n(y\Phi_i^{-1}(x)) = Tr_1^n(y\Phi_i(x))$, $\forall (x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ (resp. $\tilde{\psi}(x,y) = Tr_1^n(y(\Phi_1 + \Phi_2 + \Phi_3)^{-1}(x)) = Tr_1^n(y(\Phi_1 + \Phi_2 + \Phi_3)(x))$). Therefore, the condition of bentness given in Theorem 1 holds, which completes the proof.

Remark 2. Note that if we multiply λ_1, λ_2, λ_3 by a same non-zero constant a say, $\lambda_i = \frac{1}{a}\mu_i$ for all $i \in \{1,2,3\}$, then the functions g constructed via the λ_i and those h constructed via the μ_i are linked by the relation $h(x,y) = g(ax,y)$. Therefore the functions g and h are affinely equivalent.

The existence of bent functions given in Theorem 2 is a non-trivial arithmetical problem and is discussed in the next session.

Using similar arguments as previously, we derive in Proposition 2 and Proposition 3 more constructions of bent functions based on some involutions of $\mathbb{F}_{2^n}$ (see [12]) as application of Corollary 2.

Proposition 2. *Let $n = rk$ be an integer with $k > 1$ and $r > 1$. For $i \in \{1,2,3\}$, let γ_i be an element of $\mathbb{F}_{2^n}^\star$ such that $Tr_k^n(\gamma_i) = 0$ and Φ_i be a mapping defined over $\mathbb{F}_{2^n}$ by*

$$\Phi_i(x) = x + \gamma_i Tr_k^n(x).$$

Then the Boolean function g defined over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ by (4.1) is bent and its dual function is given by $\tilde{g}(x,y) = g(y,x)$.

Proposition 3. *Let $n = 2m$ be an even integer. Let h_1, h_2, h_3 be three linear mappings from $\mathbb{F}_{2^m}$ to itself. For $i \in \{1,2,3\}$, let Φ_i be a mapping from $\mathbb{F}_{2^n}$ to itself defined by*

$$\Phi_i(x) = h_i(Tr_m^n(x)) + x.$$

Then the Boolean function g defined over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ by (4.1) is bent and its dual function is given by $\tilde{g}(x,y) = g(y,x)$.

Remark 3. Set $\Phi_i'(x) = h_i(Tr_m^n(x)) + x^{2^m}$. Let g' be the Boolean function derived from (4.1) using the Φ_i''s. Then g' is bent and its dual is given by $\tilde{g'}(x,y) = g'(y,x)$. Clearly the functions g (given by the previous theorem) and g' are affinely equivalent.

5 Finding primary bent functions from Theorem 2

5.1 Discussion

We now turn to the question of finding values n, d and λ_i which can be used in Theorem 2 and further satisfying certain "non-obviousness" conditions to be laid out below. In other words, we are looking for n, d such that $d^2 \equiv 1 \pmod{2^n - 1}$ and $\lambda_i \in \mathbb{F}_{2^n}^\star$ such that $\lambda_i^{d+1} = 1$ with $\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = 0$ and perhaps some additional constraints such as $\lambda_i \neq \lambda_j$ for $i \neq j$. We further refine the problem by introducing the quantity $e := \operatorname{lcm}(d+1, N)/(d+1) = N/\gcd(d+1, N)$ where $N := 2^n - 1$; the significance of this quantity is that for λ_i to be a $(d+1)$-th root of unity in $\mathbb{F}_{2^n}$, a necessary and sufficient condition is that λ_i be a nonzero e-th power, say $\lambda_i = Z_i^e$ (because there are $\gcd(r, N)$ solutions to $rx = 0$ in $\mathbb{Z}/N\mathbb{Z}$, namely the multiples of $N/\gcd(r, N)$).

So, discussing on the value of e, we now have two problems: the *arithmetical problem*, namely, finding for which values of n, d we have $d^2 \equiv 1 \pmod{2^n - 1}$ with $N/\gcd(d+1, N) = e$; and the *algebraic problem*, namely, finding $Z_0, \ldots, Z_3$ nonzero such that $Z_0^e + Z_1^e + Z_2^e + Z_3^e = 0$ (and perhaps some additional constraints for non-obviousness).

In the sequel, we shall denote by $G(e) \leq \mathbb{F}_{2^n}^\star$ the cyclic group of e-th powers.

5.2 The arithmetical problem

Given an odd positive integer e, we ask upon what conditions we can find n, d such that $d^2 \equiv 1 \pmod{2^n - 1}$ with $N/\gcd(d+1, N) = e$ for $N := 2^n - 1$.

Let us temporarily forget about N being $2^n - 1$ (except that it is odd). Now if $N = p_1^{v_1} \cdots p_s^{v_s}$ where the p_i are distinct odd primes, finding d such that $d^2 \equiv 1 \pmod{N}$ amounts, by the Chinese remainder theorem, to choosing $\varepsilon_i \in \{\pm 1\}$, and taking $d \equiv \varepsilon_i \pmod{p_i^{v_i}}$ (thus, there are 2^s possible values of d with $d^2 \equiv 1 \pmod{N}$). Then clearly $N/\gcd(d+1, N)$ is the product of the $p_i^{v_i}$ where i ranges over those indices such that $\varepsilon_i = +1$. So if we fix e (a positive odd integer) and look for appropriate values of N, we find that there exists a d (necessarily unique) such that $d^2 \equiv 1 \pmod{N}$ and $N/\gcd(d+1, N) = e$ iff N is the product of e by a positive odd integer prime to it, in other words, N odd and $N \equiv te \pmod{e^2}$ where t is prime to e (and defined modulo e).

Now if we fix an odd positive integer e, and if we choose for t one of the $\varphi(e)$ invertible classes mod e (where φ is Euler's totient function), we are interested in those n such that $2^n \equiv 1 + te \pmod{e^2}$. Not much more can be said about this in general unless we know something about the multiplicative order of 2 mod e^2, but at least we can discuss the small values of e:

Proposition 4. – *For $e = 3$: there exists d such that $d^2 \equiv 1 \pmod{2^n - 1}$ with $N/\gcd(d+1, N) = e$ (again with $N := 2^n - 1$) iff $n \equiv 2$ or $n \equiv 4 \pmod 6$.*
– *For $e = 5$: there exists d such that $d^2 \equiv 1 \pmod{2^n - 1}$ with $N/\gcd(d+1, N) = e$ (again with $N := 2^n - 1$) iff n is congruent mod 20 to one of the following values: $4, 8, 12, 16$.*
– *For $e = 7$: there exists d such that $d^2 \equiv 1 \pmod{2^n - 1}$ with $N/\gcd(d+1, N) = e$ (again with $N := 2^n - 1$) iff n is congruent mod 21 to one of the following values: $3, 6, 9, 12, 15, 18$.*

Proof. In each case, we compute the order of 2 mod e^2, namely 6 for $e = 3$, resp. 20 for $e = 5$, and 21 for $e = 7$, and we then simply compute $2^n \bmod e^2$ for each value of n modulo this order, keeping those which are congruent to $1 + te$ for t prime to e.

5.3 The algebraic problem: generalities

We now turn to the "algebraic problem": given e a positive odd integer and n such that e divides $N := 2^n - 1$, we wish to find $Z_0, \ldots, Z_3$ nonzero such that $Z_0^e + Z_1^e + Z_2^e + Z_3^e = 0$.

The latter equation defines (in 3-dimensional projective space $\mathbb{P}^3_{\mathbb{F}_{2^n}}$) a smooth algebraic surface of a class known as *Fermat hypersurfaces*, which have been studied from the arithmetic and geometric points of view (see, e.g., [13, §2.14]). The equation has obvious solutions: if $\{i_0, i_1, i_2, i_3\} = \{0, 1, 2, 3\}$ is a labeling of the indices and ω, ω' two e-th roots of unity, then any solution to $\omega Z_{i_0} + Z_{i_1} = 0$ and $\omega' Z_{i_2} + Z_{i_3} = 0$ satisfies $Z_0^e + Z_1^e + Z_2^e + Z_3^e = 0$: these are known as the *standard lines* on the Fermat surface, corresponding to cases where two of the λ_i are equal. Solutions which do not lie on one of the lines are known as nonobvious solutions. We now comment on their existence and explicitly construct some.

5.4 Using the Lang-Weil estimates

Assume $e \geq 3$ (some odd integer) is arbitrary but fixed. We show that nonobvious solutions exist for n large enough, albeit in a nonconstructive way.

The polynomial $Z_0^e + Z_1^e + Z_2^e + Z_3^e$ is irreducible over the algebraic closure of $\mathbb{F}_2$. (Indeed, if it could be written as PQ with P, Q nonconstant, then all its partial derivatives would vanish where $P = Q = 0$, and nontrivial such points would exist because elementary dimension theory, e.g. [19, theorem I.7.2], guarantees that over an algebraically closed field, r homogeneous polynomials in $> r$ variables always have a nontrivial common zero. But on the other hand it is clear that the partial derivatives of $Z_0^e + Z_1^e + Z_2^e + Z_3^e$ never all vanish unless all the Z_i vanish. In geometric terms, what we are saying is that a smooth projective hypersurface is geometrically irreducible.)

Because of this, we can apply the Lang-Weil estimates [20, theorem 1], and conclude that the number of solutions to $Z_0^e + Z_1^e + Z_2^e + Z_3^e = 0$ (in projective 3-space, i.e., up to multiplication by a common constant) over $\mathbb{F}_{2^n}$ is $q^2 + O(q^{3/2})$ where $q := 2^n$ and the constant implied by $O(q^{3/2})$ is absolute. Even if we deduct the at most $O(q)$ points located on each of the curves $Z_i = 0$ and standard lines, we are still left with the same estimate for the number of solutions. This proves:

Proposition 5. *For any odd $e \geq 3$, there exists n_0 such that if $n \geq n_0$, there exist $Z_0, \ldots, Z_3 \in \mathbb{F}_{2^n}$ all nonzero and not located on the standard lines $(\omega Z_{i_0} + Z_{i_1} = 0) \wedge (\omega' Z_{i_2} + Z_{i_3} = 0)$, such that $Z_0^e + Z_1^e + Z_2^e + Z_3^e = 0$.*

In particular, if d is such that $d^2 \equiv 1 \pmod{2^n - 1}$ and $(2^n - 1)/\gcd(d + 1, 2^n - 1) = e$, and if we let $\lambda_i = Z_i^e$, Theorem 2 applies, and no two of the λ_i are equal.

5.5 A lower bound on the number of solutions

Denote by $N(s, e, g)$ the number of solutions of

$$x_1^e + \cdots x_s^e = g, x_i \in \mathbb{F}_{2^n}, g \in \mathbb{F}_{2^n}^\star.$$

By Theorem 5.22 in [21] (see also [38]), we have:

$$N(s, e, g) \geq 2^{n(s-1)} - (e-1)^s 2^{n(s-1)/2}.$$

In particular, in the cases of interest to us, namely $s = 2, 3, g \in G(e)$:

– $N(2,e,g) \geq 2^n - (e-1)^2 2^{n/2} > 0$, for $2^n > (e-1)^4$.
– $N(3,e,g) \geq 2^{2n} - (e-1)^3 2^n > 0$, for $2^n > (e-1)^3$.

Since we are interested only in nontrivial solutions, we should substract at most $2e$ from $N(2,e,g)$ and $3e^2 2^n$ from $N(3,e,g)$ respectively. Once we know there are solutions, there exist deterministic algorithms for finding them, running in polynomial time in terms of e and n (see Theorem A3 in [39]).

5.6 A semi-explicit construction

Proposition 6. *If $N > e(2e+1)$, there exist non trivial zero sums of 4 terms in $G(e)$.*

Proof. Consider all the $M := \binom{|G(e)|}{2}$ pairs $\{a,b\}$ of elements in $G(e)$. If $M > N$, two different pairs must have the same sum, providing a non-trivial 4-term 0-sum of elements of $G(e)$. This occurs as soon as $N > e(2e+1)$.

Remark 4. Let $c^i + a = c^j + b$ be such a sum; upon normalization, we get: $c + c^{j-i+1} + a' + b' = 0$. That is, we can fix freely one element (c) in the sum.

5.7 From three to four e-powers

Let $a + b + c = 0$ be a non-trivial zero sum of 3 elements of $G(e)$ (e-th powers). By cubing this equation, we get: $c^3 = a^3 + b^3 + ab(a+b) = a' + b' + abc$, i.e., a non-trivial zero sum of 4 elements in $G(e)$!

Remark 5. This generalizes to any characteristic $p \neq 3$, but since now we have: $-c^3 = a^3 + b^3 - 3abc$, we need -1 and 3 to be e-th powers (a sufficient condition being that e does not divide $(p-1)$, in which case all elements of F_p are e-th powers).

6 The case $e = 3$

We now specialise to the case $e = 3$ and delve further into the study of explicit solutions.

6.1 Explicit parametrization in the case $e = 3$

if $e = 3$, the equation $Z_0^3 + Z_1^3 + Z_2^3 + Z_3^3 = 0$ defines a smooth *cubic surface* (here, a diagonal one), and the 27 sets of simultaneous equations $\ell_{\omega,i_0,i_1|\omega',i_2,i_3} := (\omega Z_{i_0} + Z_{i_1} = 0) \wedge (\omega' Z_{i_2} + Z_{i_3} = 0)$ (with $\{i_0,i_1,i_2,i_3\} = \{0,1,2,3\}$ and ω, ω' any two cube roots of unity) define the 27 lines on that cubic surface. We refer to [19, V.§4] as well as [26, chap. IV] and the references therein for general background on cubic surfaces and their configuration of 27 lines.

Geometrically (i.e., over an algebraically closed field), a smooth cubic surface is isomorphic to the *blowup* of the projective plane in six points in general position: see [19, *loc. cit.*] or [18, p. 480 & 545]: in practice, this means that the points on the cubic surface correspond to points on the projective plane, except for the six exceptional points which must be replaced by their set of tangent directions (and correspond to six pairwise skew lines on the cubic surface); in particular, the cubic

surface is *rational*, meaning that its points can be (almost bijectively) parametrized by rational functions. The same analysis can be performed for a cubic surface over an arbitrary field provided we can find six pairwise skew lines which are (collectively) defined over the base field. This is the case for $Z_0^3 + Z_1^3 + Z_2^3 + Z_3^3 = 0$ over any field, as we can simultaneously "blow down" the two lines $\ell_{\omega_0,0,1|\omega_0,2,3}$, for ω_0 ranging over the two primitive cube roots of unity, and their image under cyclic permutations of (Z_1, Z_2, Z_3), all six of which are pairwise skew. Explicitly, in characteristic two, if we blow them down to the points $(1 : \omega_0 : 1)$ and corresponding cyclic permutation of the coordinates $(U : V : W)$, we get the parametrization:

$$\begin{aligned} Z_0 &= UV^2 + VW^2 + WU^2 \\ Z_1 &= U^2V + V^2W + W^2U + V^3 + W^3 \\ Z_2 &= U^2V + V^2W + W^2U + U^3 + W^3 \\ Z_3 &= U^2V + V^2W + W^2U + U^3 + V^3 \end{aligned}$$

satisfying $Z_0^3 + Z_1^3 + Z_2^3 + Z_3^3 = 0$, whose inverse is given (projectively, i.e., up to constants) by

$$\begin{aligned} U &= Z_0^2 + Z_1^2 + Z_1Z_2 + Z_2Z_3 + Z_3^2 \\ V &= Z_1^2 + Z_0Z_2 + Z_2^2 + Z_0Z_3 + Z_3^2 \\ W &= Z_0Z_1 + Z_0Z_2 + Z_1Z_2 + Z_0Z_3 + Z_1Z_3 + Z_2Z_3 + Z_3^2 \end{aligned}$$

(or any one obtained by cyclically permuting both Z_1, Z_2, Z_3 and U, V, W).

The gist of the above explanations is that, if over any field of characteristic two, we substitute *any* values U, V, W other than the six exceptional points $(1 : \omega_0 : 1)$, $(1 : 1 : \omega_0)$, $(\omega_0 : 1 : 1)$ in the first set of equations above, we obtain a solution to $Z_0^3 + Z_1^3 + Z_2^3 + Z_3^3 = 0$; if furthermore the point $(U : V : W)$ is not located on one of the fifteen plane lines through two of the exceptional points (e.g., $U = V$, $V = W$, $U = W$, etc.) or one of the six conics through five of them, the resulting (Z_0, Z_1, Z_2, Z_3) will not be on one of the lines of the cubic surface (i.e., it will be *nonobvious* in the terminology used above), and if $(U : V : W)$ is furthermore chosen outside of the plane cubics $UV^2 + VW^2 + WU^2 = 0$ etc. (given by the equations for the Z_i themselves), the point will have nonzero coordinates so we can use it in construction given in Theorem 2.

(The equations themselves can be checked without any appeal to the machinery of algebraic geometry: for example, using symetries, it is straightforward that, in characteristic two, $(UV^2 + VW^2 + WU^2)^3 + (U^2V + V^2W + W^2U + V^3 + W^3)^3 + (U^2V + V^2W + W^2U + U^3 + W^3)^3 + (U^2V + V^2W + W^2U + U^3 + V^3)^3 = 0$; and one can similarly check that substituting the first set of equations in the second recovers U, V, W up to a common factor, namely $U^4V + UV^4 + U^2V^2W + UVW^3 + W^5$.)

6.2 An explicit example

We present an explicit example with $n = 10$ and $d = 340$. To this end, we represent $\mathbb{F}_{2^{10}}$ modulo the minimal polynomial $m(x) := x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$. Let $\xi \in \mathbb{F}_{2^{10}}$ be the class of x mod $m(x)$. Then for example taking $U = 1$, $V = \xi$, $W = 1 + \xi$ in the equations above gives $Z_0 = \xi^3 + \xi^2 + 1$, $Z_1 = \xi^3 + \xi^2$, $Z_2 = \xi^2 + 1$ and $Z_3 = \xi$, whose cubes, viz., $\lambda_0 = \xi^9 + \xi^8 + \xi^7 + \xi^4 + \xi^3 + \xi^2 + 1$, $\lambda_1 = \xi^9 + \xi^8 + \xi^7 + \xi^6$, $\lambda_2 = \xi^6 + \xi^4 + \xi^2 + 1$ and $\lambda_3 = \xi^3$ all satisfy $\lambda_i^{341} = 1$ (and sum up to 0).

Acknowledgments. The first author thanks Jens Groth (Program Chair of the international conference IMACC 2015) and the committee members for their nice invitation to give an invited talk on bent functions and presenting the main results of this work.

References

1. Budaghyan, L., Carlet, C., Helleseth, T Kholosha, A., and Mesnager, S.: Further results on Niho bent functions. *IEEE Transactions on Information Theory*, 58(11), pages 6979-6985 (2012)
2. Canteaut, A ., Charpin, P., and Kyureghyan. G.: A new class of monomial bent functions. *Finite Fields and Their Applications*, 14(1), pages 221-241 (2008)
3. Carlet, C.: Two new classes of bent functions.: In *Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science 765*, pages 77-101 (1994)
4. Carlet, C.: A construction of bent function.: In *Proceedings of the Third International Conference on Finite Fields and Applications*, pages 47-58. Cambridge University Press (1996)
5. Carlet, C.: On bent and highly nonlinear balanced/resilient functions and their algebraic immunities. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer Berlin Heidelberg. 1-28 (2006)
6. Carlet, C.: Boolean functions for Cryptography and Error Correcting Codes. In Yves Crama and Peter L. Hammer, editors, Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge University Press. 257-397 (2010)
7. C. Carlet.: Open problems on binary bent functions. Proceeding of the conference *Open problems in mathematical and computational sciences*, Sept. 18-20, 2013, in Istanbul, Turkey, pp. 203-241, Springer (2014).
8. Carlet, C, Mesnager. S.: On Dillon's class H of bent functions, Niho bent functions and O-polynomials. *Journal of Combinatorial Theory, Series A*, 118(8), pages 2392-2410 (2011)
9. Carlet, C., and Mesnager, S.: Four decades of research on bent functions. Journal Designs, Codes and Cryptography (to appear)
10. Charpin, P., and Gong, G.: Hyperbent functions, Kloosterman sums and Dickson polynomials. In *ISIT 2008*, pages 1758-1762 (2008)
11. Charpin, P., and Kyureghyan, G.: Cubic monomial bent functions: A subclass of $\mathcal{M}$. *SIAM Journal on Discrete Mathematics*, 22(2), pages 650-665 (2008)
12. Charpin, P., Mesnager, S., and Sarkar, S.: On involutions of finite fields. In Proceedings of 2015 IEEE International Symposium on Information Theory, ISIT (2015)
13. O. Debarre.: *Higher-Dimensional Algebraic Geometry.* Springer, Universitext (2001)
14. J. Dillon.: *Elementary Hadamard difference sets.* PhD thesis, University of Maryland (1974)
15. Dillon, J., and Dobbertin, H.: New cyclic difference sets with Singer parameters. *Finite Fields and Their Applications*, 10(3), pages 342-389 (2004)
16. Dobbertin, H., and Leander, G., and Canteaut, A., and Carlet, C., and Felke, P., and Gaborit, P.: Construction of bent functions via Niho power functions. *Journal of Combinatorial Theory, Series A*, 113, pages 779-798 (2006)
17. Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. *IEEE Transactions on Information Theory*, 14(1), pages 154-156 (1968)
18. Griffiths, P., and Harris, J.: *Principles of Algebraic Geometry.* Wiley (1978)
19. Hartshorne, R.: *Algebraic Geometry.* Springer, GTM **52** (1977)
20. Lang, S., and Weil, A.: "Number of Points on Varieties in Finite Fields". *Amer. J. Math.* **76** 819-827 (1954)
21. Lidl, R., and Niederreiter, H.: *Finite Fields.* Encyclopedia Math. Appl. 20, Addison-Wesley (1983)
22. Leander, G.: Monomial bent functions. *IEEE Transactions on Information Theory*, 52(2), pages 738-743 (2006)
23. Leander, G., and Kholosha, A.: Bent functions with 2^r Niho exponents. *IEEE Transactions on Information Theory*, 52(12), pages 5529-5532 (2006)
24. Li, N., Helleseth, T., Tang, X., and Kholosha, A.: Several new classes of bent functions from Dillon exponents. *IEEE Transactions on Information Theory*, 59(3), pages 1818-1831 (2013)
25. McFarland, R. L.: A family of noncyclic difference sets. *Journal of Combinatorial Theory, Series A*, 15, pages 1-10 1(973)

26. Manin, Yu. l.: *Cubic Forms: Algebra, Geometry, Arithmetic*. North-Holland (1974)
27. Mesnager, S.: A new family of hyper-bent boolean functions in polynomial form. *Proceedings of Twelfth International Conference on Cryptography and Coding*, IMACC 2009, LNCS 5921, pages 402-417, Springer, Heidelberg (2009)
28. Mesnager, S.: Hyper-bent boolean functions with multiple trace terms. *Proceedings of International Workshop on the Arithmetic of Finite Fields*, WAIFI 2010, LNCS 6087, pages 97-113. Springer, Heidelberg (2010)
29. Mesnager, S.: 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), pages 5996-6009 (2011)
30. Mesnager, S.: A new class of bent and hyper-bent boolean functions in polynomial forms. *Designs, Codes and Cryptography*, 59(1-3), pages 265-279 (2011)
31. Mesnager, S.: Several new infinite families of bent functions and their duals. IEEE Trans. Inf. Theory. 60(7), 4397-4407 (2014)
32. Mesnager, S.: Further constructions of infinite families of bent functions from new permutations and their duals. Journal of Cryptography and Communications (CCDS), Springer (to appear)
33. Mesnager, S.: Bent functions: fundamentals and results. Springer 2015 (to appear)
34. Mesnager, S., and Flori, J. P.: Hyper-bent functions via Dillon-like exponents. *IEEE Transactions on Information Theory*, 59(5), pages 3215-3232, (2013)
35. Rothaus, O.S.: On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20:300–305 (1976).
36. Tao, T., and Vu, V.: *Additive Combinatorics*. Cambridge University Press (2006)
37. Yu, N.Y., and Gong, G.: Construction of quadratic bent functions in polynomial forms. *IEEE Transactions on Information Theory*, 52(7), pages 3291-3299, (2006)
38. Winterhof, A.: On Waring's problem in finite fields. *Acta Arithmetica LXXXVII.2*,171-177 (1998).
39. van de Woestijne, C. E.: *Deterministic equation solving over finite fields*. PhD Thesis, Math. Inst. Univ. Leiden (2006)