Vectorial quadratic bent functions as a product of two linearized polynomials

A Pott, E Pasalic, A Muratovic-Ribic, S Bajric

Vectorial quadratic bent functions as a product of two linearized polynomials

A. Pott[1], E. Pasalic[2], A. Muratović-Ribić[3], and S. Bajrić[4]

[1] University Otto-von-Guericke, Faculty of Mathematics, Magdeburg, Germany
alexander.pott@ovgu.de
[2] University of Primorska, FAMNIT and IAM, Koper, Slovenia
enes.pasalic6@gmail.com
[3] University of Sarajevo, Department of Mathematics, Zmaja od Bosne 33-35, 71000 Sarajevo, Bosnia and Herzegovina
amela@pmf.unsa.ba
[4] University of Primorska, FAMNIT, Koper, Slovenia
samed.bajric@upr.si

Abstract. To identify and specify trace bent functions of the form $Tr_1^n(P(x))$, where $P(x) \in GF(2^n)[x]$, has been an important research topic lately. We show that an infinite class of quadratic vectorial bent functions can be specified in the univariate polynomial form as $F(x) = Tr_k^n(\alpha x^{2^i}(x + x^{2^k}))$, where $n = 2k$, $i = 0, \ldots, n-1$, and $\alpha \notin GF(2^k)$. Most notably, apart from the cases $i \in \{0, k\}$ for which the polynomial $x^{2^i}(x+x^{2^k})$ is affinely equivalent to the monomial x^{2^k+1}, for the remaining indices i the function $x^{2^i}(x+x^{2^k})$ seems to be affinely inequivalent to x^{2^k+1}, as confirmed by computer simulations for small n. It is well-known that $Tr_1^n(\alpha x^{2^k+1})$ is Boolean bent for exactly $2^{2k} - 2^k$ values (this is at the same time the maximum cardinality possible) of $\alpha \in GF(2^n)$ and the same is true for our class of quadratic bent functions of the form $Tr_1^n(\alpha x^{2^i}(x + x^{2^k}))$, though for $i > 0$ the associated functions $F : GF(2^n) \to GF(2^n)$ are in general CCZ inequivalent and also have different differential distributions.

Keywords : Cryptography, Boolean functions, Bent functions, Vectorial bent functions, Trace functions, CCZ inequivalence.

1 Introduction

Bent functions are extremal combinatorial objects with several areas of application, such as coding theory, maximum length sequences, cryptography, the theory of difference sets to name a few. The term bent Boolean function was introduced by Rothaus [26], where also two classes of bent functions were considered. Among other equivalent characterizations of bent functions, the one that is most often used is a characterization of bent functions as a class of Boolean functions having so-called flat Walsh-Hadamard spectrum. It means that for any bent function over $GF(2)^n$, its Hamming distance to any affine function in n variables is constant including the distance to the all-zero function (or all-one function).

Monomial Boolean trace bent functions of the form $Tr_1^n(ax^d)$ have been considered in several works [7, 15, 4, 11, 12], and to the best of our knowledge the functions in these references are the only known classes of monomial trace bent functions (up to affine equivalence), see also Section 4. On the other hand, binomial (or generally multiple) trace bent

functions are harder to analyze and only a few (absolute trace)[1] classes of these functions have been exhibited [13, 6, 28, 5, 20, 21]. The result of Dobbertin and Leander [13] related to so-called linear Niho exponents was later generalized in [16], where the existence of bent functions with multiple trace terms consisting of 2^r Niho exponents were confirmed.

The bent property of Boolean functions can be easily extended to vectorial mappings $F : GF(2^n) \to GF(2^m)$ by requesting that all nonzero linear combinations of the coordinate functions of F are also bent, i.e., $Tr_1^m(\lambda F(x))$ is bent for all $\lambda \in GF(2^m)^*$, $x \in GF(2^n)$. The construction of such *vectorial bent functions* have been initially considered by Nyberg in [24]. It was shown in [24] that vectorial bent functions can only exist for $m \leq n/2$, and can be constructed coordinate-wise using some known classes of bent functions. The same problem has also been treated in [27] and more recently in [14]. Instead, the bent property of functions $f : GF(2^n) \to GF(2^m)$ for $GF(2^m) \subset GF(2^n)$ may also be established directly as it was done recently in [23] for the trace functions of the form $F(x) = Tr_k^n(\sum_{i=0}^{2^k} a_i x^{i(2^k-1)})$, where $n = 2k$ and $a_i \in GF(2^n)$.

In this article, we consider binomial trace functions of the form $F(x) = Tr_k^n(\alpha x^{2^i}(x + x^{2^{n/2}}))$, where $n = 2k$, $i = 0, \ldots, n-1$, and α is a primitive element of $GF(2^n)$. It is shown that F is vectorial bent for any even $n \geq 4$. Thus, a new generic class of vectorial bent functions is deduced and most notably this class has the property of having the maximum cardinality of those α for which $f_\alpha(x) = Tr_1^n(\alpha x^{2^i}(x + x^{2^{n/2}}))$ is Boolean bent. More precisely, we show that f_α is a bent function for any $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, thus the cardinality being $2^n - 2^{n/2}$ which can be shown to be maximal. This interesting property is not shared by many classes of known bent functions. For the known classes of monomial bent functions of the form $f(x) = Tr_1^n(\alpha x^d)$ (for some suitable choices of the exponent d) it turns out that the maximum cardinality of α's for which f is bent is only achieved for $d = 2^k + 1$. Moreover, we show that the function $Tr_k^n(\alpha x^{2^i}(x^{2^j} + (x^{2^j})^{2^k}))$ is also vectorial bent, for any even $n = 2k$.

Nevertheless, the corresponding functions over finite fields, namely $x^{2^i}(x + x^{2^{n/2}})$ and x^{2^k+1} are not CZZ equivalent unless $i = 0$ or $i = k$. Furthermore, the two polynomials also have different differential distributions but however it does not imply that the associated vectorial bent mappings are necessarily EA-inequivalent. Notice that for bent functions CCZ equivalence is identical to EA-equivalence. The problem of establishing the EA-(non)equivalence of the two classes is left open.

The rest of the article is organized as follows. Some basic definitions are given in Section 2. In Section 3, we show that the function $F(x) = Tr_k^n(\alpha x^{2^i}(x + x^{2^{n/2}}))$ is vectorial bent, for any even $n = 2k$. Furthermore, some interesting facts regarding the maximum cardinality of the corresponding Boolean bent mappings are provided. Some simulation results concerning the distribution of differentials of our class and their comparison to x^{2^k+1} are given in Section 4. A few concluding remarks are found in Section 5.

[1] Here the absolute trace is used to distinguish the functions of the type $Tr_1^n(\sum_{i=1}^r \lambda_i x^{d_i})$ from the functions that use different trace such as the function defined by $Tr_1^n(\lambda x^{d_1}) + Tr_1^2(\beta x^{d_2})$ as considered in [19].

2 Preliminaries

Let $\mathbb{F}_{2^n}$ denote the finite Galois field $GF(2^n)$ consisting of 2^n elements. The group of units of $\mathbb{F}_{2^n}$, denoted by $\mathbb{F}_{2^n}^*$, is a cyclic group consisting of 2^n-1 elements. An element $\alpha \in \mathbb{F}_{2^n}$ is said to be a primitive element if it is a generator of the multiplicative group $\mathbb{F}_{2^n}^*$. Once the basis of the field is fixed, say $\{\gamma_0, \ldots, \gamma_{n-1}\}$ so that $\alpha = \alpha_0\gamma_0 + \ldots + \alpha_{n-1}\gamma_{n-1}$, where $\gamma_i \in \mathbb{F}_{2^n}$ and $\alpha_i \in \mathbb{F}_2$, there is a natural isomorphism between $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$ given by

$$\alpha_0\gamma_0 + \ldots + \alpha_{n-1}\gamma_{n-1} \in \mathbb{F}_{2^n} \longmapsto (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{F}_2^n.$$

Any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, or alternatively from $\mathbb{F}_2^n \to \mathbb{F}_2$, is said to be a *Boolean function* on n variables. The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$.

The *trace function* $Tr_m^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, a mapping to a subfield $\mathbb{F}_{2^m} \subset \mathbb{F}_{2^n}$, when $m \mid n$, is defined as

$$Tr_m^n(x) = x + x^{2^m} + x^{2^{2m}} + \ldots + x^{2^{(n/m-1)m}}, \text{ for all } x \in \mathbb{F}_{2^n}. \tag{1}$$

The absolute trace $Tr_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$, then maps to the prime field.

The *Walsh–Hadamard transform* of a Boolean function $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_{2^n}$ is defined by

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\lambda x)}. \tag{2}$$

The multiset

$$\{W_f(\lambda) : \lambda \in \mathbb{F}_{2^n}\} \tag{3}$$

is said to be the *Walsh–Hadamard spectrum* of the Boolean function f. For any even positive integer $n = 2k$, there exist Boolean functions with a flat Walsh–Hadamard spectrum. A function $f \in \mathcal{B}_n$ is called *bent* if and only if $|W_f(\lambda)| = 2^k$ for all $\lambda \in \mathbb{F}_{2^n}$.

The nonlinearity of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and hereby the resistance to linear cryptanalysis of Matsui [18] is measured through *extended Walsh-Hadamard transform* defined as,

$$W_F(\sigma, \gamma) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(\gamma F(x))+Tr_1^n(\sigma x)}, \ \sigma \in \mathbb{F}_{2^n}, \gamma \in \mathbb{F}_{2^m}^*. \tag{4}$$

Here, $\gamma \in \mathbb{F}_{2^m}^*$ selects nonzero linear combinations of the coordinate functions of F, where F is represented as $F(x) = (f_1(x), \ldots, f_m(x))$, for $f_i : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Using this representation, F is a *vectorial bent function* of dimension $m \leq n/2, n$ is even, if and only if $a_1f_1(x) + \ldots + a_mf_m(x)$ is a bent function for any choice of $a_i \in \mathbb{F}_2$, where not all of the a_is are zero. Equivalently, F is a vectorial bent function if and only if $|W_F(\sigma, \gamma)| = 2^{n/2}$, for any $\gamma \in \mathbb{F}_{2^m}^*$ and any $\sigma \in \mathbb{F}_{2^n}$.

3 Vectorial bentness through adjoint operators

In this section we derive our main results related to the vectorial bentness of $F(x) = Tr_k^n(\alpha x^{2^i}(x + x^{2^k}))$ and to the maximum possible cardinality of those α so that $f_\alpha(x) = Tr_1^n(\alpha G(x))$ is Boolean bent for an arbitrary polynomial $G(x) \in \mathbb{F}_{2^n}[x]$. To establish the upper bound on the cardinality of αs for which $f_\alpha(x)$ is bent we utilize an old result due to Bose and Burton [2].

Theorem 1 *[2] Let $\mathbb{F}_q$ be the finite field of order $q = p^r$ and $\mathbb{PG}(n, \mathbb{F}_q)$ the projective space of dimension n over $\mathbb{F}_q$. A set S of points in $\mathbb{PG}(n, \mathbb{F}_q)$ that meet all $(n-k)$-dimensional subspaces of $\mathbb{PG}(n, \mathbb{F}_q)$ has at least $\frac{q^{k+1}-1}{q-1}$ points with equality if and only if S is a subspace of dimension k.*

Translating this into affine language (and setting $q = 2$ to deal with the Boolean case), we obtain two important corollaries.

Corollary 1 *A set S of elements in $\mathbb{F}_2^n \setminus \{0\}$ meeting all $(n+1-k)$-dimensional subspaces of $\mathbb{F}_2^n$ has at least $2^k - 1$ elements with equality if and only if $S \cup \{0\}$ is a k-dimensional subspace of $\mathbb{F}_2^n$.*

The correspondence to bent functions is as follows.

Corollary 2 *Let $n = 2k$, and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be arbitrary. Define*

$$S := \{\alpha \in \mathbb{F}_{2^n} : x \mapsto Tr_1^n(\alpha F(x)) \quad \text{is not bent}\}.$$

Then, $|S| \geq 2^k$ with equality if and only if S is a linear subspace of dimension k.

Proof. If $|S| < 2^k$, then there are at most $2^k - 2$ non-zero elements α for which $Tr_1^n(\alpha F(x))$ is not bent. Due to Corollary 1, this set cannot meet all subspaces of dimension $n+1-k = k+1$, hence there must be at least one subspace T of dimension $k+1$ disjoint from $S \setminus \{0\}$. This shows that there is a $(k+1)$-dimensional subspace

$$T \subseteq \{\alpha : Tr_1^n(\alpha F(x)) \quad \text{is bent}\} \cup \{0\},$$

that is, there is a vectorial bent function from $\mathbb{F}_2^{2k}$ to $\mathbb{F}_2^{k+1}$, which is impossible due to the Nyberg bound. □

We now proceed with our main results regarding the vectorial bentness of $F(x) = Tr_k^n(\alpha x^{2^i}(x + x^{2^k}))$. Let $V = \mathbb{F}_2^{2k}$ be the vector space over $\mathbb{F}_2$ of dimension $2k = n$. The result below uses a well-known fact that a Boolean function $f : V \to \mathbb{F}_2$ is bent if and only if $x \mapsto f(x) + f(x + a)$ is balanced for all nonzero $a \in V$.

Proposition 1 *Let $V = \mathbb{F}_2^{2k}$ and let $\langle , \rangle$ be a non-degenerate symmetric bilinear form on V. If $\mathcal{L} : V \to V$ is linear, we denote the adjoint operator by $\mathcal{L}^*$, i.e., $\langle x, \mathcal{L}(y)\rangle = \langle \mathcal{L}^*(x), y\rangle$ for all $x, y \in V$. The function $f : V \to \mathbb{F}_2$, defined by $x \mapsto \langle x, \mathcal{L}(x)\rangle$, is bent if and only if $\mathcal{L} + \mathcal{L}^*$ is invertible.*

Proof. We have

$$\begin{aligned} f(x+a) + f(x) &= \langle x + a, \mathcal{L}(x + a)\rangle + \langle x, \mathcal{L}(x)\rangle \\ &= \langle a, \mathcal{L}(a)\rangle + \langle x, \mathcal{L}(a)\rangle + \langle a, \mathcal{L}(x)\rangle \\ &= \langle a, \mathcal{L}(a)\rangle + \langle x, \mathcal{L}(a)\rangle + \langle \mathcal{L}^*(a), x\rangle \\ &= \langle a, \mathcal{L}(a)\rangle + \langle x, \mathcal{L}(a) + \mathcal{L}^*(a)\rangle. \end{aligned}$$

This function is balanced if and only if $\mathcal{L}(a) + \mathcal{L}^*(a) \neq 0$ for all nonzero $a \in V$, hence f is bent if and only if $\mathcal{L} + \mathcal{L}^*$ is invertible. □

Remark 1 *Let $V = \mathbb{F}_2^n$ and $\langle , \rangle$ be the standard inner product. If $\mathcal{L} : V \to V$ such that $\mathcal{L}(x) = Ax$, where A is a binary matrix of size $n \times n$, then $\mathcal{L}^* : V \to V$ is defined by $\mathcal{L}^*(x) = A^T x$. Hence, $x \mapsto x^T Ax$ is bent if and only if $A + A^T$ is regular (of full rank).*

Remark 1 is well known and it is essentially equivalent to Proposition 1. However, Proposition 1 is a more elegant (since it is coordinate-free) statement. It has the advantage that it can be used, no matter how the inner product is defined. For instance, in the multivariate case the inner product is usually defined using the classical form $\sum x_i y_i$, or, in the univariate world, using the trace bilinear version $Tr_1^n(xy)$. We believe that one should try to formulate theorems coordinate-free as long as it is possible.

Proposition 2 *Let $V = \mathbb{F}_{2^n}$ and $\langle x, y \rangle = Tr_1^n(xy)$ be the trace bilinear form. If $\mathcal{L} : V \to V$ is defined by $\mathcal{L}(x) = \alpha x^{2^i}$, $\alpha \in V$ and for $i = 0, \ldots, n-1$, then $\mathcal{L}^*(x) = \alpha^{2^{n-i}} x^{2^{n-i}}$.*

Proof. Note that

$$\langle x, \mathcal{L}(y) \rangle = Tr_1^n(x\mathcal{L}(y)) = Tr_1^n(x\alpha y^{2^i}) = Tr_1^n(x^{2^{n-i}} \alpha^{2^{n-i}} y) = \langle \mathcal{L}^*(x), y \rangle ,$$

for all $x, y \in V$, which then implies the result. ∎

We are now going to prove the main theorem of this article.

Theorem 2 *Let $V = \mathbb{F}_{2^n}$, $n = 2k$ and i be an positive integer. Then, the mapping f_α defined by*

$$f_\alpha(x) = Tr_1^n(\alpha x^{2^i}(x + x^{2^k}))$$

is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$.

Proof. We have

$$\begin{aligned} f_\alpha(x) &= Tr_1^n(\alpha x^{2^i}(x + x^{2^k})) \\ &= Tr_1^n(x\alpha x^{2^i}) + Tr_1^n(x^{2^i} \alpha x^{2^k}) \\ &= Tr_1^n(x\alpha x^{2^i}) + Tr_1^n(x\alpha^{2^k} x^{2^{i+k}}) \\ &= Tr_1^n(x\mathcal{L}(x)), \end{aligned}$$

where $\mathcal{L}(x) = \alpha x^{2^i} + \alpha^{2^k} x^{2^{i+k}}$. The adjoint operator $\mathcal{L}^*$ is

$$\begin{aligned} \mathcal{L}^*(x) &= \alpha^{2^{n-i}} x^{2^{n-i}} + (\alpha^{2^k})^{2^{n-(i+k)}} x^{2^{n-(i+k)}} \\ &= \alpha^{2^{2k-i}} x^{2^{2k-i}} + \alpha^{2^{2k-i}} x^{2^{k-i}}. \end{aligned}$$

Then it follows,

$$\begin{aligned} \mathcal{L}(x) + \mathcal{L}^*(x) &= \alpha x^{2^i} + \alpha^{2^k} x^{2^{i+k}} + \alpha^{2^{2k-i}} x^{2^{2k-i}} + \alpha^{2^{2k-i}} x^{2^{k-i}} \\ &= (\alpha x^{2^i}) + (\alpha x^{2^i})^{2^k} + \alpha^{2^{2k-i}} (x^{2^{k-i}} + (x^{2^{k-i}})^{2^k}). \end{aligned}$$

Note that $y + y^{2^k} \in \mathbb{F}_{2^k}$ iff $y \in \mathbb{F}_{2^{2k}}$, hence we have $\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \in \mathbb{F}_{2^k}$ as well as $x^{2^{k-i}} + (x^{2^{k-i}})^{2^k} \in \mathbb{F}_{2^k}$. In order to show that $\mathcal{L}(x) + \mathcal{L}^*(x)$ is invertible, we need to show that $\mathcal{L}(x) + \mathcal{L}^*(x) = 0$ if and only if $x = 0$. If $\alpha \notin \mathbb{F}_{2^k}$, then $\mathcal{L}(x) + \mathcal{L}^*(x) = 0$ is possible only if $\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} = 0$ and $x^{2^{k-i}} + (x^{2^{k-i}})^{2^k} = 0$. Otherwise, 0 would be the sum of an element in $\mathbb{F}_{2^k}$ and an element not in $\mathbb{F}_{2^k}$ (the element $\alpha^{2^{2k-i}}(x^{2^{k-i}} + (x^{2^{k-i}})^{2^k})$) which is impossible. Since $y + y^{2^k} = 0$ iff $y \in \mathbb{F}_{2^k}$, we obtain that both x as well as αx^{2^i} have to belong to $\mathbb{F}_{2^k}$, which is possible only if $x = 0$ since $\alpha \notin \mathbb{F}_{2^k}$. This shows the bentness of f_α for $\alpha \notin \mathbb{F}_{2^k}$.
Now assume that $\alpha \in \mathbb{F}_{2^k}$ and f_α is bent. This is impossible due to Corollary 2 since in that case we would have $|S| < 2^k$ (using the notation of Corollary 2). □

The next result shows that the above property of being Boolean bent for any $\alpha \notin \mathbb{F}_{2^k}$ implies that the corresponding vectorial mapping is bent.

Proposition 3 *Let $f_\alpha(x) = Tr_1^n(\alpha G(x))$, $n = 2k$, be a Boolean bent function for any $\alpha \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$, where $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Then, $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$, defined as $F(x) = Tr_k^n(\alpha G(x))$ is a vectorial bent function for any $\alpha \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$.*

Proof. For $\gamma \in \mathbb{F}_{2^k}{}^*$ and $\sigma \in \mathbb{F}_{2^n}$, we consider the extended Walsh spectra,

$$\begin{aligned} W_F(\sigma,\gamma) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^k(\gamma F(x))+Tr_1^n(\sigma x)} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^k(\gamma Tr_k^n(\alpha G(x)))+Tr_1^n(\sigma x)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^k(Tr_k^n(\gamma\alpha G(x)))+Tr_1^n(\sigma x)} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f_{\gamma\alpha}(x)+Tr_1^n(\sigma x)} = \pm 2^{n/2}, \end{aligned}$$

by assumption on f_α, since for any $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$ we have $\gamma\alpha \notin \mathbb{F}_{2^k}$.

Example 1 *Consider the Boolean function $Tr_1^n(\alpha x^4(x + x^{2^k}))$, $n = 2k$, which can be verified to be bent for any $\alpha \notin \mathbb{F}_{2^k}$. Thus, $F(x) = Tr_k^n(\alpha x^4(x + x^{2^k}))$ is a vectorial bent function.*

3.1 Generalization of the approach

In what follows, we show that the function $Tr_k^n(\alpha x^{2^i}(x^{2^j} + (x^{2^j})^{2^k}))$ is vectorial bent, for any even $n = 2k$. Before proving the main result of this section we first give some preparatory results.

Proposition 4 *Assume that $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a bent function. Then the function $g(x) = f(x^{2^i})$ is bent.*

Proof. Note that mapping $y \to y^{2^i}$ is a permutation on $\mathbb{F}_{2^n}$. Also $Tr_1^n(y) = Tr_1^n(y^{2^i})$ for all $y \in \mathbb{F}_{2^n}$. Computing the Walsh-Hadamard transform we have

$$\begin{aligned} W_g(\sigma) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x^{2^i})+Tr_1^n(\sigma x)} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x^{2^i})+Tr_1^n(\sigma^{2^i} x^{2^i})} \\ &= \sum_{y\in\mathbb{F}_{2^n}} (-1)^{f(y)+Tr_1^n(\sigma^{2^i} y)} = W_f(\sigma^{2^i}) = \pm 2^k, \end{aligned}$$

for all $\sigma \in \mathbb{F}_{2^n}$. □

Proposition 5 *Assume that $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is a vectorial bent function. Then the function $G(x) = F(x^{2^i})$ is vectorial bent.*

Proof. Computing the extended Walsh-Hadamard transform we have

$$\begin{aligned} W_G(\sigma, \gamma) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(\gamma G(x)) + Tr_1^n(\sigma x)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(\gamma F(x^{2^i})) + Tr_1^n(\sigma^{2^i} x^{2^i})} \\ &= \sum_{y \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(\gamma F(y)) + Tr_1^n(\sigma^{2^i} y)} = W_F(\sigma^{2^i}, \gamma) = \pm 2^{n/2}. \end{aligned}$$

□

Corollary 3 *A function $f(x)$ is bent if and only if $f(x^{2^i})$ is a bent function. A function $F(x)$ is vectorial bent if and only if $F(x^{2^i})$ is a vectorial bent function.*

Remark 2 *Note that the opposite direction of the proof of the above corollary follows directly from the fact $x = (x^{2^i})^{2^{(n-i)}}$.*

The main results of this section are the following.

Theorem 3 *The function $g_\alpha(x) = Tr_1^n(\alpha x^{2^i}(x^{2^j} + (x^{2^j})^{2^k}))$ is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$.*

Proof. By Theorem 2 we know that $f_\alpha(x) = Tr_1^n(\alpha x^{2^t}(x + x^{2^k}))$ is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$, for any $t \in \mathbb{Z}$. By Corollary 3 $f_\alpha(x)$ is bent if and only if $g_\alpha(x) = f_\alpha(x^{2^j})$ is bent. Therefore, for $t = i - j$ we have

$$\begin{aligned} g_\alpha(x) &= f_\alpha(x^{2^j}) \\ &= Tr_1^n\left(\alpha (x^{2^j})^{2^t}(x^{2^j} + (x^{2^j})^{2^k})\right) = Tr_1^n\left(\alpha x^{2^{(j+t)}}(x^{2^j} + (x^{2^j})^{2^k})\right) \\ &= Tr_1^n\left(\alpha x^{2^i}(x^{2^j} + (x^{2^j})^{2^k})\right) \end{aligned}$$

is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$. □

Theorem 4 *The function $G_\alpha(x) = Tr_k^n\left(\alpha x^{2^i}(x^{2^j} + (x^{2^j})^{2^k})\right)$ is vectorial bent.*

Proof. The proof follows from Corollary 3 and Proposition 3. □

4 CCZ and EA (non)equivalence to some bent monomials

In the previous section we have established that $f_\alpha(x) = Tr_1^n(\alpha x^{2^i}(x^{2^j} + (x^{2^j})^{2^k}))$ is bent for any $\alpha \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$. In other words, $|S| = 2^k$ is of minimal cardinality (the set of those α for which f_α is bent is of maximal cardinality $2^{2k} - 2^k$ where S was defined in Corollary 2. This situation does not arise frequently for the known bent monomials. In the first place, certain bent monomials x^d such as those with Dillon's exponent of the form $d = r(2^k - 1)$ (where integer r is suitably chosen) may give rise to sporadic Boolean bent functions $Tr_1^n(\alpha x^{r(2^k+1)})$ for a few α but the function $Tr_k^n(\alpha x^{r(2^k+1)})$ cannot be vectorial bent, see [23]. The following list [22] of monomial functions $f(x) = Tr_1^n(\alpha x^d)$ are bent on $\mathbb{F}_{2^n}$, with $n = 2k$:

1. $d = 2^m + 1$ with $n/\gcd(m, n)$ being even and $\alpha \notin \{y^d : y \in \mathbb{F}_{2^n}\}$;
2. $d = r(2^k - 1)$ with $\gcd(r, 2^k + 1) = 1$ and $\alpha \in \mathbb{F}_{2^k}$ being -1 of the Kloosterman sum;
3. $d = 2^{2m} - 2^m + 1$ with $\gcd(m, n) = 1$ and $\alpha \notin \{y^3 : y \in \mathbb{F}_{2^n}\}$;
4. $d = (2^m + 1)^2$ with $n = 4m$ and m odd, $\alpha \in \omega\mathbb{F}_{2^m}$ with $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$;
5. $d = 2^{2m} + 2^m + 1$ with $n = 6m$ and $m > 1$, $\alpha \in \mathbb{F}_{2^{3m}}$ with $Tr_m^{3m}(\alpha) = 0$.

Remark that it has been check exhaustively that these are no other monomial bent functions for $n \leq 20$.

Then, apparently the maximum possible cardinality of α in the previously mentioned sense is only achieved by the first class for the special case when $m = k$. In this case the exponent $d = 2^k+1$ and it is easily verified that $|S| = 2^k$ as it is the case for our class. Since both corresponding polynomials, namely $x^{2^i}(x+x^{2^k})$ and x^{2^k+1} are quadratic it might be the case that our class is CCZ equivalent to the monomial x^{2^k+1}. This is indeed the case for $i = 0$ and $i = k$, whereas for $i \neq 0, k$ it has been established by MAGMA (for small values of n) that the functions are not CCZ equivalent, therefore it is not possible that our functions are, in general, CCZ equivalent to x^{2^k+1}. Nevertheless, it still does not imply that the vectorial bent mappings $Tr_k^n(\alpha x^{2^i}(x + x^{2^k}))$ and $Tr_k^n(\alpha x^{2^k+1})$ are inequivalent. This interesting question remains open for the time being.

5 Conclusions

An infinite class of quadratic vectorial bent functions of the form $F(x) = Tr_k^n(\alpha x^{2^i}(x + x^{2^{n/2}}))$, where $n = 2k$ and α is a primitive element of the field $GF(2^n)$, have been specified. It would be of interest to specify similar classes where instead of $x+x^{2^{n/2}}$ some other suitable linear mappings are used. This appears as an interesting challenge for future work on this topic along with the analysis of non-quadratic cases.

Acknowledgements : The authors thank Prof. Klaus Metsch (University of Giessen) for pointing out the connection to the Bose-Burton theorem.

References

1. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, vol. 4(1):3–72, 1991.
2. R. C. Bose, and R. C. Burton. A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes. *Journal of Combinatorial Theory*, vol. 1 :96–104, 1966.
3. L. Budaghyan and T. Helleseth. Planar functions and commutative semifields. *Tatra Mt. Math. Publ.*, 45:15–25, 2010.
4. A. Canteaut, P. Charpin, and G. Kyureghyan. A new class of monomial bent functions. *Finite Fields and Their Applications*, 14(1):221–241, 2008.
5. C. Carlet and P. Gaborit. Hyper–bent functions and cyclic codes. *Journal of Combinatorial Theory, Series A*, 113(3):466–482, 2006.
6. P. Charpin and G. Gong. Hyperbent functions, Kloosterman sums and Dickson polynomials. *IEEE Trans. on Inform. Theory*, IT–54(9):4230–4238, 2008.
7. P. Charpin and G. Kyureghyan. Cubic monomial bent functions: a subclass of $\mathcal{M}$. *SIAM Journal of Discrete Math.*, 22(2):650–665, 2008.
8. R. S. Coulter and M. Henderson. Commutative presemifileds and semifields. *Adv. Math.*, vol. 217:282–304, 2008.
9. R. S. Coulter and R. W. Matthews. Planar functions and planes of Lenz-Barlotti class ii. *Des. Codes Cryptogr.*, vol. 10:167–184, 1997.
10. P Dembowski and T. G. Ostrom. Planes of order n with collineation groups of order n^2. *Mathematische Zeitschrift*, 103:239–258, 1968.
11. J. Dillon and H. Dobbertin. New cyclic difference sets with singer parameters. *Finite Fields and Their Applications*, 10(3):342–389, 2004.
12. J. F. Dillon. Elementary Haddamard Difference Sets. Ph. D. thesis, University of Maryland, U.S.A., 1974.
13. H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit. Construction of bent functions via Niho power functions. *Journal of Combinatorial Theory, Series A*, 113(5):779–798, 2006.
14. K. Feng and J. Yang. Vectorial boolean functions with good cryptographic properties. *Int. J. Found. Comput. Sci.*, 22(6):1271–1282, 2011.
15. N. G. Leander. Monomial bent functions. *IEEE Trans. on Inform. Theory*, IT–52(2):738–743, 2006.
16. N. G. Leander and A. Kholosha. Bent functions with 2^r Niho exponents. *IEEE Trans. on Inform. Theory*, IT–52(12): 5529–5532, 2006.
17. R. Lidl and R. E. Niederreiter. *Finite fields*. Cambridge University Press, Second Edition, 1997.
18. M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology—EUROCRYPT'93*, LNCS 765, pp. 386–397. Springer–Verlag, 1993.
19. S. Mesnager. A new class of bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. *IEEE Trans. on Inform. Theory*, IT–57(9):5996–6009, 2011.
20. S. Mesnager, and J.-P. Flori. Hyperbent functions via Dillon–like exponents. *IEEE Trans. on Inform. Theory*, IT–59(5):3215–3232, 2013.
21. J.-P. Flori, and S. Mesnager. An efficient characterization of a family of hyper-bent functions with multiple trace terms. *Journal of Mathematical Cryptology*, 7(1):43–68, 2013.
22. G. L. Mullen, and D. Panario. Handbook of Finite Fields. Discrete Mathematics and Its Applications, CRC Press, 2013.
23. A. Muratović-Ribić, E. Pasalic, and S. Bajrić. Vectorial bent functions from multiple terms trace functions. *IEEE Trans. on Inform. Theory*, IT–60(2):1337–1347, 2014.
24. K. Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology—EUROCRYPT'91*, LNCS 547, pp. 378–385. Springer–Verlag, 1991.
25. K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in Cryptology—EUROCRYPT'93*, volume LNCS 765, pages 55–64. Springer-Verlag, 1993.

26. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3): 300–305, 1976.
27. J. Wu, Y. Wei, and X. Wang. An optimized method for multiple output bent functions. *Acta Electronica Sinica*, 33(3):521–523, 2005.
28. A. M. Youssef and G. Gong. Hyper-bent functions. In *Advances in Cryptology—EUROCRYPT 2001*, LNCS 2045, pp. 406–419. Springer–Verlag, 2001.