On CCZ-equivalence and its use in secondary constructions of bent functions

Lilya Budaghyan* and Claude Carlet†

Abstract

We prove that, for bent vectorial functions, CCZ-equivalence coincides with EA-equivalence. However, we show that CCZ-equivalence can be used for constructing bent functions which are new up to CCZ-equivalence. Using this approach we construct classes of nonquadratic bent Boolean and bent vectorial functions.

Keywords: Affine equivalence, Almost perfect nonlinear, Bent function, Boolean function, CCZ-equivalence, Nonlinearity.

1 Introduction

The notion of CCZ-equivalence of vectorial functions, introduced in [4] (the name was in fact introduced later in [1]), is a fecund notion which has led to new APN and AB functions. It seems to be the proper notion of equivalence for vectorial functions used as S-boxes in cryptosystems. Two vectorial functions F and F' from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ (that is, two (n,m)-functions) are called CCZ-equivalent if their graphs $G_F = \{(x, F(x));\, x \in \mathbb{F}_2^n\}$ and $G_{F'} = \{(x, F'(x));\, x \in \mathbb{F}_2^n\}$ are affine equivalent, that is, if there exists an affine permutation $\mathcal{L}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ such that $\mathcal{L}(G_F) = G_{F'}$. If F is an almost perfect nonlinear (APN) function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, that is, if any derivative $D_aF(x) = F(x) + F(x+a)$, $a \neq 0$, of F is 2-to-1 (which implies that F contributes an optimal resistance to the differential attack of the cipher in which it is used as an S-box), then F' is APN too. If F is almost bent (AB), that

*Department of Informatics, University of Bergen, PB 7803, 5020 Bergen, NORWAY; e-mail: Lilya.Budaghyan@ii.uib.no

†Universities of Paris 8 and Paris 13; CNRS, UMR 7539 LAGA; Address: University of Paris 8, Department of Mathematics, 2 rue de la liberté, 93526 Saint-Denis cedex 02, France; e-mail: claude.carlet@inria.fr

is, if its nonlinearity equals $2^{n-1} - 2^{\frac{n-1}{2}}$ (which implies that F contributes an optimal resistance of the cipher to the linear attack), then F' is also AB.

Recall that F and F' are called EA-equivalent if there exist affine automorphisms $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $L' : \mathbb{F}_2^m \to \mathbb{F}_2^m$ and an affine function $L'' : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that $F' = L' \circ F \circ L + L''$. EA-equivalence is a particular case of CCZ-equivalence [4]. Besides, every permutation is CCZ-equivalent to its inverse. As shown in [1], CCZ-equivalence is still more general.

The notion of CCZ-equivalence can be straightforwardly generalized to functions over finite fields of odd characteristic p. It has been proved in [2, 6] that, when applied to perfect nonlinear (also called planar) functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p^n$, that is, functions whose derivatives $D_aF(x) = F(x) - F(x+a)$, $a \neq 0$, are bijective, it is the same as EA-equivalence. A natural question is to ask whether this property is true for perfect nonlinear functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, that is, functions (also called bent) whose derivatives $D_aF(x) = F(x) + F(x+a)$, $a \neq 0$, are balanced (i.e. uniformly distributed over $\mathbb{F}_2^m$; these functions exist only for n even and $m \leq n/2$, see [8]). We prove in Section 2 that CCZ-equivalence coincides with EA-equivalence when applied to bent functions.

The result of Section 2 is merely a negative result since it means that all bent vectorial functions obtained by CCZ-equivalence from known bent functions are EA-equivalent to the original functions. However, CCZ-equivalence can be applied to a non-bent vectorial function F (from $\mathbb{F}_{2^n}$ to itself) of a low algebraic degree with bent components $\mathrm{tr}_n(bF(x))$ for some $b \in \mathbb{F}_{2^n}^*$, and obtain a vectorial function F' of a higher algebraic degree which hopefully has bent components $\mathrm{tr}_n(b'F'(x))$ for some $b' \in \mathbb{F}_{2^n}^*$ (which, according to the result of Section 2, cannot be CCZ-equivalent to the bent components of F unless they are EA-equivalent to them). We give in Sections 3 and 4 examples of vectorial functions from $\mathbb{F}_2^n$ to itself leading this way to new bent Boolean and bent vectorial functions. The significance of this approach is, for instance, that there are many quadratic non-bent vectorial functions with bent components and applying CCZ-equivalence to them, we can increase the algebraic degree and obtain nonquadratic bent functions which are CCZ-inequivalent to quadratic ones.

2 CCZ-equivalence and bent vectorial functions

If we identify $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ then a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is uniquely represented as a univariate polynomial over $\mathbb{F}_{2^m}$ of degree smaller than 2^n

$$F(x) = \sum_{i=0}^{2^m-1} c_i x^i, \quad c_i \in \mathbb{F}_{2^n}.$$

If m is a divisor of n then a function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ can be viewed as a function from $\mathbb{F}_{2^n}$ to itself and, therefore, it admits a univariate polynomial representation. More precisely, if $\mathrm{tr}_n(x)$ denotes the trace function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$, and $\mathrm{tr}_{n/m}(x)$ denotes the trace function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$, that is,

$$\begin{aligned}\mathrm{tr}_n(x) &= x + x^2 + x^4 + \ldots + x^{2^{n-1}}, \\ \mathrm{tr}_{n/m}(x) &= x + x^{2^m} + x^{2^{2m}} + \ldots + x^{2^{(n/m-1)m}},\end{aligned}$$

then F can be represented in the form $\mathrm{tr}_{n/m}(\sum_{i=0}^{2^n-1} c_i x^i)$ (and in the form $\mathrm{tr}_n(\sum_{i=0}^{2^n-1} c_i x^i)$ for $m = 1$). Indeed, there exists a function G from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ (for example $G(x) = aF(x)$, where $a \in \mathbb{F}_{2^n}$ and $\mathrm{tr}_{n/m}(a) = 1$) such that F equals $\mathrm{tr}_{n/m}(G(x))$.

For any integer k, $0 \le k \le 2^n - 1$, the number $w_2(k)$ of nonzero coefficients k_s, $0 \le k_s \le 1$, in the binary expansion $\sum_{s=0}^{n-1} 2^s k_s$ of k is called the 2-weight of k. The algebraic degree of a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is equal to the maximum 2-weight of the exponents i of the polynomial $F(x)$ such that $c_i \neq 0$, that is

$$d^\circ(F) = \max_{\substack{0 \le i \le 2^n-1 \\ c_i \neq 0}} w_2(i).$$

A Boolean function f of $\mathbb{F}_{2^n}$ is bent if and only if

$$\lambda_f(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{tr}_n(ux)} = \pm 2^{\frac{n}{2}}, \qquad \forall u \in \mathbb{F}_{2^n}.$$

A vectorial function $F: \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is bent if and only if for any $v \in \mathbb{F}_{2^m}^*$ its component function $\mathrm{tr}_m(vF(x))$ is bent, that is,

$$\lambda_F(u, v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_m(vF(x)) + \mathrm{tr}_n(ux)} = \pm 2^{\frac{n}{2}}, \qquad \forall u \in \mathbb{F}_{2^n}, \forall v \in \mathbb{F}_{2^m}^*.$$

The set of the absolute values of $\lambda_F(u, v)$ for $u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^m}^*$, is called the extended Walsh spectrum of F. Note that, though CCZ-equivalence preserves the extended Walsh spectrum of a function [1], this does not imply that if a function F has some bent components then any function CCZ-equivalent to F necessarily has any bent components.

If two functions are CCZ-equivalent and one of them is bent then the second is bent too. Below we show that, for bent vectorial functions, CCZ-equivalence coincides with EA-equivalence.

Theorem 1 *Let F be a bent function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. Then any function CCZ-equivalent to F is EA-equivalent to it.*

Proof. Let F' be CCZ-equivalent to F and $\mathcal{L}(x,y) = \big(L_1(x,y), L_2(x,y)\big)$ be an affine permutation of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ which maps the graph of F to the graph of F' and where $L_1 : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2^n$, $L_2 : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2^m$. Then $L_1(x, F(x))$ is a permutation (see e.g. [3]). We can write $L_1(x,y) = L'(x) + L''(y)$. For any element v of $\mathbb{F}_2^n$ we have

$$v \cdot L_1(x, F(x)) = v \cdot L'(x) + v \cdot L''(F(x)),$$

where "$\cdot$" is the inner product in $\mathbb{F}_2^n$ (which we can take as $x \cdot y = \mathrm{tr}_n(xy)$). The function $v \cdot L'(x)$ is an affine function. Since $L_1(x, F(x))$ is a permutation, any function $v \cdot L_1(x, F(x))$ is balanced (recall that this property is a necessary and sufficient condition, see e.g. [3]) and, hence, cannot be bent. Then, the adjoint operator L''' of L'' (satisfying $v \cdot L''(F(x)) = L'''(v) \cdot F(x)$) is the null function since if $L'''(v) \neq 0$ then $L'''(v) \cdot F(x)$ is bent. This means that L'' is null, that is, L_1 depends only on x, which corresponds to EA-equivalence by Proposition 3 of [1]. □

Since the algebraic degree is preserved by EA-equivalence then Theorem 1 implies that if two bent functions have different algebraic degrees then they are CCZ-inequivalent.

3 New bent Boolean functions obtained through CCZ-equivalence of non-bent vectorial functions

In this section, we show with two examples of infinite classes of functions that, despite the result of the previous section, CCZ-equivalence can be used for constructing new bent Boolean functions, by applying it to non-bent vectorial functions which admit bent components.

Let i be a positive integer. For n even, let us define:

$$\begin{aligned} F &: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \\ F(x) &= x^{2^i+1} + (x^{2^i} + x + 1)\,\mathrm{tr}_n(x^{2^i+1}), \end{aligned} \tag{1}$$

and for n divisible by 6:

$$G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$$

$$G(x) = \Big(x + \mathrm{tr}_{n/3}\big(x^{2(2^i+1)} + x^{4(2^i+1)}\big) + \mathrm{tr}_n(x)\,\mathrm{tr}_{n/3}\big(x^{2^i+1} + x^{2^{2i}(2^i+1)}\big)\Big)^{2^i+1}. \tag{2}$$

Functions F and G were constructed in [1] by applying CCZ-equivalence to $F'(x) = x^{2^i+1}$. When $\gcd(i,n) = 1$ these functions are APN, the function F has algebraic degree 3 (for $n \geq 4$), and the function G has algebraic degree 4 (however, the components of F and G may have lower algebraic degrees). Since algebraic degrees of non-affine functions are preserved by EA-equivalence then F and G are EA-inequivalent to F'. We know (see e.g. [3]) that if $n/\gcd(n,i)$ is even and $b \in \mathbb{F}_{2^n}$ is the (2^i+1)-th power of no element of $\mathbb{F}_{2^n}$ then the Boolean function $\mathrm{tr}_n(bF'(x))$ is bent. In general, if a vectorial function H has some bent components, it does not yet imply that a function CCZ-equivalent to H has necessarily bent components. Below we show that the two classes (1) and (2) above have bent nonquadratic components which are CCZ-inequivalent to the components of F' by Theorem 1.

3.1 The first class

We begin with the bent components of function (1).

Theorem 2 *Let $n \geq 6$ be an even integer and i be a positive integer not divisible by $n/2$ such that $n/\gcd(i,n)$ is even. If $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^i}$ is such that neither b nor $b+1$ are the (2^i+1)-th powers of elements of $\mathbb{F}_{2^n}$, and the function F is given by (1) then the Boolean function $f_b(x) = \mathrm{tr}_n(bF(x))$ is bent and has algebraic degree 3.*

Proof. By Theorem 2 of [1], which proves that the function F is CCZ-equivalent to $F'(x) = x^{2^i+1}$, the graph of F' is mapped to the graph of F by the linear involution:

$$\mathcal{L}(x,y) = \big(L_1(x,y), L_2(x,y)\big) = (x + \mathrm{tr}_n(y), y).$$

It is shown in the proof of Proposition 2 of [1] (and straightforward to check) that for any $a, b \in \mathbb{F}_{2^n}$:

$$\lambda_{F'}(a,b) = \lambda_F(\mathcal{L}^{-1*}(a,b)),$$

where $\mathcal{L}^{-1*}$ is the adjoint operator of $\mathcal{L}^{-1}$, that is, for any $(x,y), (x',y') \in \mathbb{F}_{2^n}^2$:

$$(x,y) \cdot \mathcal{L}^{-1*}(x',y') = \mathcal{L}^{-1}(x,y) \cdot (x',y'),$$

where $(x,y) \cdot (x',y') = \mathrm{tr}_n(xx') + \mathrm{tr}_n(yy')$.

The adjoint operator of $\mathcal{L}^{-1} = \mathcal{L}$ is

$$\mathcal{L}^*(x,y) = \big(L_1^*(x,y), L_2^*(x,y)\big) = (x, y + \mathrm{tr}_n(x)).$$

Indeed,

$$\begin{aligned}\mathcal{L}(x,y)\cdot(x',y') &= \operatorname{tr}_n\big((x+\operatorname{tr}_n(y))x'\big)+\operatorname{tr}_n(yy')\\ &= \operatorname{tr}_n(xx')+\operatorname{tr}_n(y)\operatorname{tr}_n(x')+\operatorname{tr}_n(yy')\\ &= \operatorname{tr}_n(xx')+\operatorname{tr}_n\big(y(y'+\operatorname{tr}_n(x'))\big)\\ &= (x,y)\cdot\mathcal{L}^*(x',y').\end{aligned}$$

Then to prove that $\operatorname{tr}_n(bF'(x))$ is bent for some $b\neq 0$, we need to determine the Walsh coefficients $\lambda_{F'}(a,b)$ for any a. According to what is recalled above, we have:

$$\lambda_{F'}(a,b)=\lambda_F(a,b+\operatorname{tr}_n(a)).$$

We know that $\lambda_F(a,b+\operatorname{tr}_n(a))=\pm 2^{n/2}$ if and only if $b+\operatorname{tr}_n(a)$ is not the (2^i+1)-th power of an element of $\mathbb{F}_{2^n}$ (see e.g. [7]) then $\operatorname{tr}_n(bF'(x))$ is bent if and only if neither b nor $b+1$ is the (2^i+1)-th power of an element of $\mathbb{F}_{2^n}$.

We denote $c=b^{2^{n-i}}+b$. If $b\notin\mathbb{F}_{2^i}$ then $c\neq 0$. For i not divisible by $n/2$ all items in $\operatorname{tr}_n(x^{2^i+1})=\sum_{j=0}^{n-1}x^{2^{i+j}+2^j}$ are pairwise different. Indeed, if for some $0\le j,k<n$, $k\neq j$, we have $2^{i+j}+2^j=2^{i+k}+2^k \mod (2^n-1)$ or, equivalently, $i+j=k \mod n$ and $i+k=j \mod n$ then obviously i is divisible by $n/2$.
We get

$$\begin{aligned}f_b(x) &= \operatorname{tr}_n(bx^{2^i+1})+\operatorname{tr}_n\big(b(x^{2^i}+x+1)\big)\operatorname{tr}_n(x^{2^i+1})\\ &= \operatorname{tr}_n(bx^{2^i+1})+\operatorname{tr}_n(b)\operatorname{tr}_n(x^{2^i+1})+\operatorname{tr}_n\big((b^{2^{n-i}}+b)x\big)\operatorname{tr}_n(x^{2^i+1})\\ &= Q(x)+\operatorname{tr}_n(cx)\operatorname{tr}_n(x^{2^i+1}),\end{aligned}$$

where Q is quadratic. Let us denote $A_j=\{j-i,j,j+i,j+2i\}$. Then, since $\sum_{0\le j<n}c^{j+2i}x^{2^j+2^{j+i}+2^{j+2i}}=\sum_{0\le j<n}c^{j+i}x^{2^{j-i}+2^j+2^{j+i}}$, we have

$$\begin{aligned}\operatorname{tr}_n(cx)\operatorname{tr}_n(x^{2^i+1}) &= \Big(\sum_{0\le k<n}c^{2^k}x^{2^k}\Big)\Big(\sum_{0\le j<n}x^{2^j+2^{j+i}}\Big)\\ &= \sum_{0\le j<n}c^{2^j}x^{2^{j+1}+2^{j+i}}+\sum_{0\le j<n}c^{2^{j+i}}x^{2^j+2^{j+i+1}}\\ &\quad+\sum_{0\le j<n}(c^{2^{j-i}}+c^{2^{j+i}})x^{2^{j-i}+2^j+2^{j+i}}\\ &\quad+\sum_{\substack{0\le j,k<n\\ k\notin A_j}}c^{2^k}x^{2^k+2^j+2^{j+i}}.\end{aligned}$$

For $n > 4$ all exponents $2^k + 2^j + 2^{j+i}$ in the sum

$$\sum_{\substack{0 \le j,k < n \\ k \notin A_j}} c^{2^k} x^{2^k + 2^j + 2^{j+i}}$$

are pairwise different, have 2-weight 3 and they obviously differ from the exponents in the first three sums above. Hence, the items with these exponents do not vanish and, therefore, f_b has algebraic degree 3. □

3.2 The existence of elements b satisfying the conditions of Theorem 2 and the type of the corresponding bent components

We first show that elements $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^i}$ such that neither b nor $b+1$ are the $(2^i + 1)$-th powers of elements of $\mathbb{F}_{2^n}$ always exist. We subsequently point out explicit values of such elements, under some conditions.

Proposition 1 *Let $n \ge 6$ be an even integer and i be a positive integer not divisible by $n/2$ such that $n/\gcd(i,n)$ is even. There exist at least $\frac{1}{3}(2^n - 1) - 2^{n/2} > 0$ elements b satisfying the conditions of Theorem 2.*

Proof. Since $n/\gcd(i,n)$ is even, we have $\gcd(2i,n) = 2\gcd(i,n)$ and we deduce that $\gcd(2^n - 1, 2^{2i} - 1) = 2^{\gcd(2i,n)} - 1 = (2^{\gcd(i,n)} + 1)(2^{\gcd(i,n)} - 1) = (2^{\gcd(i,n)} + 1)\gcd(2^n - 1, 2^i - 1)$. This implies $\gcd(2^n - 1, 2^i + 1) \ge 2^{\gcd(i,n)} + 1 \ge 3$ (note that this bound is tight since if $\gcd(i,n) = 1$ then $\gcd(2^n - 1, 2^i + 1) = 3$). Then the size of the set E of all $(2^i + 1)$-th powers of elements of $\mathbb{F}_{2^n}^*$ is at most $(2^n - 1)/3$ and this implies that $(F_{2^n} \cap F_{2^i}) \cup E \cup (1 + E)$ has size at most $2^{n/2} + 2(2^n - 1)/3 < 2^n - 1$ (since $n > 2$). This completes the proof. □

Proposition 2 *Let $n \ge 6$ be an even integer, i be a positive integer not divisible by $n/2$, and s be a divisor of i such that i/s is odd and n is divisible by $2s$ but not by $2s(2^s + 1)$. If $b \in \mathbb{F}_{2^{2s}} \setminus \mathbb{F}_{2^s}$ and the function F is given by (1) then the Boolean function $f_b(x) = \mathrm{tr}_n(bF(x))$ is bent and has algebraic degree 3.*

Proof. Obviously, $b \notin \mathbb{F}_{2^i}$. Since i/s is odd then

$$2^i + 1 = 2^s + 1 + (2^{2s} - 1)(2^s + 2^{3s} + 2^{5s} + .. + 2^{s(i/s-2)}) \tag{3}$$

is divisible by $2^s + 1$.

Since n is divisible by $2s$ then $2^n - 1$ is divisible by $2^{2s} - 1$ and therefore divisible by $2^s + 1$. Moreover, $2^n - 1$ is divisible by $(2^s + 1)^2$ if and only if n

is divisible by $2s(2^s+1)$. Indeed, if n is divisible by $2s(2^s+1)$, then 2^n-1 is divisible by $2^{2s(2^s+1)}-1$, and therefore by $2^{s(2^s+1)}+1$. Using (3) we get

$$\begin{aligned}
2^{s(2^s+1)}+1 &= 2^s+1+(2^{2s}-1)(2^s+2^{3s}+..+2^{s(2^s+1-2)}) \\
&= (2^s+1)\big(1+(2^s-1)(2^s+2^{3s}+..+2^{s(2^s+1-2)})\big) \\
&= (2^s+1)\big(1+(2^s+1)(2^s+2^{3s}+..+2^{s(2^s+1-2)}) \\
&\quad -2(2^s+2^{3s}+..+2^{s(2^s+1-2)})\big) \\
&= (2^s+1)\Big(1+(2^s+1)(2^s+2^{3s}+..+2^{s(2^s+1-2)}) \\
&\quad +2^s-2\big((2^s+1)+(2^{3s}+1)+...+(2^{s(2^s+1-2)}+1)\big)\Big) \\
&= (2^s+1)\Big((2^s+1)\big(1+2^s+2^{3s}+...+2^{s(2^s+1-2)}\big) \\
&\quad -2\big((2^s+1)+(2^{3s}+1)+...+(2^{s(2^s+1-2)}+1)\big)\Big)
\end{aligned}$$

which is divisible by $(2^s+1)^2$ since for any l odd $2^{sl}+1$ is divisible by 2^s+1 as it is observed above. If $n=2s(k(2^s+1)+t)$ for some k and $1\le t\le 2^s$, then $2^n-1=2^{2st}\,(2^{2sk(2^s+1)}-1)+(2^{2st}-1)$. As it is shown above $2^{2sk(2^s+1)}-1$ is divisible by $(2^s+1)^2$. For t odd

$$\begin{aligned}
2^{st}+1 &= 2^s+1+(2^{2s}-1)(2^s+2^{3s}+..+2^{s(t-2)}) \\
&= (2^s+1)\Big(1+(2^s+1)\big(2^s+2^{3s}+...+2^{s(t-2)}\big) \\
&\quad +(t-1)-2\big((2^s+1)+(2^{3s}+1)+...+(2^{s(t-2)}+1)\big)\Big) \\
&= (2^s+1)^2T+t(2^s+1)
\end{aligned}$$

for some T, and therefore $2^{2st}-1$ is divisible by 2^s+1 but not by $(2^s+1)^2$ since $2^{st}-1$ is not divisible by 2^s+1. For t even $2^{st}-1=(2^{2s}-1)(1+2^{2s}+...+2^{s(t-2)})$ is divisible by 2^s+1 but not by $(2^s+1)^2$ since $1+2^{2s}+...+2^{s(t-2)} = t/2+(2^{2s}-1)+(2^{4s}-1)+...+(2^{s(t-2)}-1)$. Hence $2^{2st}-1$ is not divisible by $(2^s+1)^2$ since $2^{st}+1$ is not divisible by 2^s+1.

Since 2^n-1 is not divisible by $(2^s+1)^2$ then any element which is not the (2^s+1)-th power of an element in $\mathbb{F}_{2^{2s}}$ is not the (2^s+1)-th power of an element in $\mathbb{F}_{2^n}$ either, and we can apply Theorem 2 to finish the proof. □

An n-variable Boolean bent function belongs to the Maiorana-McFarland class if, writing its input in the form (x,y), with $x,y\in\mathbb{F}_2^{n/2}$, the corresponding output equals $x\cdot\pi(x)+g(x)$, where π is a permutation of $\mathbb{F}_2^{n/2}$ and g is a Boolean function over $\mathbb{F}_2^{n/2}$. The completed class of Maiorana-McFarland's functions is the set of those functions which are EA-equivalent to Maiorana-McFarland functions. These bent functions are characterized by the fact that there exists an $n/2$-dimensional vector space such that the second order derivatives

$$D_aD_cf(x) = f(x) + f(x+a) + f(x+c) + f(x+a+c)$$

of the function in directions a and c belonging to this vector space all vanish [5]. Almost all bent functions found in trace representation (listed e.g. in [3]) are in the completed Maiorana-McFarland class. It is interesting to see whether this is also the case of the bent functions of Theorem 2. We checked with a computer that it is the case for $n = 6$. Below we prove that this is also true for the functions f_b of Theorem 2 when $b \in \mathbb{F}_{2^{n/2}}$.

Proposition 3 *The bent functions f_b of Theorem 2 belong to the completed Maiorana-McFarland class when $b \in \mathbb{F}_{2^{n/2}}$. In particular, all the functions of Proposition 2 are in the completed Maiorana-McFarland class when n is divisible by $4s$.*

Proof. To check whether f_b is in the Maiorana-McFarland class, we need to see whether there exists an $n/2$-dimensional vector space such that the second order derivatives

$$D_aD_cf_b(x) = f_b(x) + f_b(x+a) + f_b(x+c) + f_b(x+a+c)$$

vanish when a and c belong to this vector space. We have

$$f_b(x) = \mathrm{tr}_n(bx^{2^i+1}) + \mathrm{tr}_n(b(x^{2^i} + x + 1))\,\mathrm{tr}_n(x^{2^i+1}),$$

$$\begin{aligned}
D_af_b(x) &= \mathrm{tr}_n(bx^{2^i+1}) + \mathrm{tr}_n(bx^{2^i+1} + bax^{2^i} + ba^{2^i}x + ba^{2^i+1}) \\
&\quad + \mathrm{tr}_n(b(x^{2^i} + x + 1))\,\mathrm{tr}_n(x^{2^i+1})) \\
&\quad + \mathrm{tr}_n(b(x^{2^i} + x + 1 + a^{2^i} + a))\,\mathrm{tr}_n(x^{2^i+1} + ax^{2^i} + a^{2^i}x + a^{2^i+1})) \\
&= \mathrm{tr}_n(bax^{2^i} + ba^{2^i}x + ba^{2^i+1}) + \mathrm{tr}_n(b(a^{2^i} + a))\,\mathrm{tr}_n(x^{2^i+1})) \\
&\quad + \mathrm{tr}_n(b(x^{2^i} + x + 1))\,\mathrm{tr}_n(ax^{2^i} + a^{2^i}x + a^{2^i+1})) \\
&\quad + \mathrm{tr}_n(b(a^{2^i} + a))\,\mathrm{tr}_n(ax^{2^i} + a^{2^i}x + a^{2^i+1})),
\end{aligned}$$

$$\begin{aligned}
D_aD_cf_b(x) &= \mathrm{tr}_n(bac^{2^i} + ba^{2^i}c) + \mathrm{tr}_n(b(a^{2^i} + a))\,\mathrm{tr}_n(cx^{2^i} + c^{2^i}x + c^{2^i+1})) \\
&\quad + \mathrm{tr}_n(b(c^{2^i} + c))\,\mathrm{tr}_n(ax^{2^i} + a^{2^i}x + a^{2^i+1})) \\
&\quad + \mathrm{tr}_n(b(x^{2^i} + x + 1))\,\mathrm{tr}_n(ac^{2^i} + a^{2^i}c)) \\
&\quad + \mathrm{tr}_n(b(c^{2^i} + c))\,\mathrm{tr}_n(ac^{2^i} + a^{2^i}c)) \\
&\quad + \mathrm{tr}_n(b(a^{2^i} + a))\,\mathrm{tr}_n(ac^{2^i} + a^{2^i}c)) \\
&= \mathrm{tr}_n(\lambda x) + \epsilon,
\end{aligned}$$

where

$$\begin{aligned}
\lambda &= (c^{2^{n-i}} + c^{2^i}) \operatorname{tr}_n(b(a^{2^i} + a)) + (a^{2^{n-i}} + a^{2^i}) \operatorname{tr}_n(b(c^{2^i} + c)) \\
&\quad +(b^{2^{n-i}} + b) \operatorname{tr}_n(ac^{2^i} + a^{2^i} c)), \\
\epsilon &= \operatorname{tr}_n(bac^{2^i} + ba^{2^i} c) + \operatorname{tr}_n(b(a^{2^i} + a)) \operatorname{tr}_n(c^{2^i+1}) \\
&\quad + \operatorname{tr}_n(b(c^{2^i} + c)) \operatorname{tr}_n(a^{2^i+1}) + \operatorname{tr}_n(b) \operatorname{tr}_n(ac^{2^i} + a^{2^i} c) \\
&\quad + \operatorname{tr}_n(b(c^{2^i} + c)) \operatorname{tr}_n(ac^{2^i} + a^{2^i} c) + \operatorname{tr}_n(b(a^{2^i} + a)) \operatorname{tr}_n(ac^{2^i} + a^{2^i} c).
\end{aligned}$$

The function $D_a D_c f_b$ is null if and only if $\epsilon = \lambda = 0$. Then the $n/2$-dimensional vector space can be taken equal to $\mathbb{F}_{2^{n/2}}$. Indeed, if $a, b, c \in \mathbb{F}_{2^{n/2}}$, then λ and ϵ are null since the trace of any element of $\mathbb{F}_{2^{n/2}}$ is null. If, in conditions of Proposition 2, n is divisible by $4s$ then $b \in \mathbb{F}_{2^{2s}} \subset \mathbb{F}_{2^{n/2}}$. □

3.3 The second class

We study now the bent components of function (2).

Theorem 3 *Let n be a positive integer divisible by 6 and let i be a positive integer not divisible by $n/2$ such that $n/\gcd(i,n)$ is even. Let $b \in \mathbb{F}_{2^n}$ be such that, for any $d \in \mathbb{F}_8$, the element $b + d + d^2$ is not the $(2^i + 1)$-th power of an element of $\mathbb{F}_{2^n}$ and let G be given by (2). Then the Boolean function $g_b(x) = \operatorname{tr}_n(b\, G(x))$ is bent. If, in addition, i is divisible by 3 and $b \notin \mathbb{F}_{2^i}$ then g_b has algebraic degree 3. If i is not divisible by 3 then g_b has algebraic degree at least 3, and it is exactly 4 if $n \geq 12$, and either $b \notin \mathbb{F}_8$ or $\operatorname{tr}_3(b) \neq 0$.*

Proof. By Theorem 3 of [1], which proves that the function G is CCZ-equivalent to $F'(x) = x^{2^i+1}$, the graph of F' is mapped to the graph of G by the linear involution

$$\mathcal{L}(x, y) = (x + \operatorname{tr}_{n/3}(y^2 + y^4), y).$$

We have

$$\mathcal{L}^*(x, y) = (x, y + \operatorname{tr}_{n/3}(x^2 + x^4)).$$

Indeed, we have

$$\operatorname{tr}_n\left(\operatorname{tr}_{n/3}(y^2 + y^4)x'\right) = \operatorname{tr}_n\left(\sum_{\substack{0 \leq j \leq n-1/ \\ \frac{n}{3} \nmid j}} x' y^{2^j}\right) =$$

$$\mathrm{tr}_n \left(\sum_{\substack{0 \le j \le n-1/ \\ \frac{n}{3} \not| j}} x'^{2^{n-j}} y \right) = \mathrm{tr}_n \left(\sum_{\substack{0 \le j \le n-1/ \\ \frac{n}{3} \not| j}} x'^{2^j} y \right) = \mathrm{tr}_n \left(\mathrm{tr}_{n/3}(x'^2 + x'^4) y \right).$$

Since $\mathcal{L}$ and $\mathcal{L}^*$ are involutions, we have

$$\lambda_G(a, b) = \lambda_{F'}(a, b + \mathrm{tr}_{n/3}(a^2 + a^4)).$$

Thus, $\mathrm{tr}_n(b\,G(x))$ is bent if and only if $b + \mathrm{tr}_{n/3}(a^2 + a^4)$ is not the $(2^i + 1)$-th power of an element of $\mathbb{F}_{2^n}$ for any a. This proves the first part of Theorem 3.

For i divisible by 3 we have:

$$\begin{aligned} G(x) &= [x + \mathrm{tr}_{n/3} \left(x^{2(2^i+1)} + x^{4(2^i+1)} \right)]^{2^i+1} \\ &= x^{2^i+1} + \mathrm{tr}_{n/3} \left(x^{2^i+1} + x^{4(2^i+1)} \right) + (x + x^{2^i}) \, \mathrm{tr}_{n/3} \left(x^{2(2^i+1)} + x^{4(2^i+1)} \right). \end{aligned}$$

Since $tr_{n/3}(x^{2i2^i+1}) = tr_{n/3}(x^{2^i+1})$. Clearly, $c = b + b^{2^{n-i}} \neq 0$ because $b \notin \mathbb{F}_{2^i}$. For some quadratic function Q we have:

$$\begin{aligned} g_b(x) &= Q(x) + \mathrm{tr}_n \left(b(x + x^{2^i}) \, \mathrm{tr}_{n/3} \left(x^{2(2^i+1)} + x^{4(2^i+1)} \right) \right) \\ &= Q(x) + \mathrm{tr}_3 \left(\mathrm{tr}_{n/3} \left(cx \right) \mathrm{tr}_{n/3} \left(x^{2(2^i+1)} + x^{4(2^i+1)} \right) \right) \end{aligned}$$

and it is not difficult to see that for i not divisible by $n/2$ the cubic terms of g_b do not vanish.

Let i be not divisible by 3. For simplicity we consider only the case $i = 1$. It is not difficult to see that for $T(x) = \mathrm{tr}_{n/3}(x^3)$ we have

$$G(x) = C(x) + \mathrm{tr}_3 \left(T(x)^3 \right) + \mathrm{tr}_n(x) \Big(x \big(T(x) + T(x)^2 \big) + x^2 \big(T(x) + T(x)^4 \big) \Big).$$

where C is a cubic function

$$C(x) = x^3 + T(x) + \mathrm{tr}_n(x) \big(T(x) + T(x)^4 \big) + x \big(T(x) + T(x)^4 \big) + x^2 \big(T(x)^2 + T(x)^4 \big).$$

Hence,

$$\begin{aligned}
g_b(x) &= \operatorname{tr}_n(bC(x)) + \operatorname{tr}_n(b)\operatorname{tr}_3\left(T(x)^3\right) \\
&\quad + \operatorname{tr}_n(x)\operatorname{tr}_3\left(T(x)\operatorname{tr}_{n/3}(bx + bx^2 + (b^2+b^4)x^4)\right) \\
&= \operatorname{tr}_n(bC(x)) + \operatorname{tr}_n(b)\Big(\sum_{0\le j,t<n/3} x^{2^{3j+1}+2^{3j}+2^{3t+2}+2^{3t+1}} \\
&\quad + \sum_{0\le j,t<n/3} x^{2^{3j+3}+2^{3j+2}+2^{3t+1}+2^{3t}} \\
&\quad + \sum_{0\le j,t<n/3} x^{2^{3j+3}+2^{3j+2}+2^{3t+2}+2^{3t+1}}\Big) \\
&\quad + \sum_{\substack{0\le j,k<n\\0\le t<n/3}} u_k x^{2^j+2^k+2^{3t}+2^{3t+1}} \\
&\quad + \sum_{\substack{0\le j,k<n\\0\le t<n/3}} v_k x^{2^j+2^k+2^{3t+1}+2^{3t+2}} \\
&\quad + \sum_{\substack{0\le j,k<n\\0\le t<n/3}} w_k x^{2^j+2^k+2^{3t+2}+2^{3t+3}}
\end{aligned}$$

where for $0 \le k < n$

$$u_k = \begin{cases} b^{2^k} & \text{if } k = 0 \mod 3 \\ b^{2^{k-1}} & \text{if } k = 1 \mod 3 \\ (b^2+b^4)^{2^{k-2}} & \text{if } k = 2 \mod 3, \end{cases}$$

$$v_k = \begin{cases} b^{2^k} & \text{if } k = 1 \mod 3 \\ b^{2^{k-1}} & \text{if } k = 2 \mod 3 \\ (b^2+b^4)^{2^{k-2}} & \text{if } k = 0 \mod 3, \end{cases}$$

$$w_k = \begin{cases} b^{2^k} & \text{if } k = 2 \mod 3 \\ b^{2^{k-1}} & \text{if } k = 0 \mod 3 \\ (b^2+b^4)^{2^{k-2}} & \text{if } k = 1 \mod 3. \end{cases}$$

Assume $n \ge 12$. Then the exponent $2^6 + 2^9 + 2^0 + 2^1$ has 2-weight 4 and, obviously, we have items with this exponent only with coefficients u_6 and u_9. Then $u_6 + u_9 = b^{2^6} + b^{2^9} = (b + b^8)^{2^6} \ne 0$ when $b \notin \mathbb{F}_{2^3}$. Hence, in the univariate polynomial representation of g_b the item $x^{2^6+2^9+2^0+2^1}$ has a non-zero coefficient and, therefore, g_b has algebraic degree 4 for $b \notin \mathbb{F}_{2^3}$.
If $b \in \mathbb{F}_{2^3}$ then $\operatorname{tr}_n(b) = 0$. If $\operatorname{tr}_3(b) \ne 0$ then we have items with the exponent $2^6 + 2^8 + 2^0 + 2^1$ only with coefficients u_6 and u_8 and $u_6 + u_8 =$

$b^{2^6} + (b^2 + b^4)^{2^6} = \mathrm{tr}_3(b) \neq 0$. Hence, again g_b has algebraic degree 4 when $b \in \mathbb{F}_{2^3}$ and $\mathrm{tr}_3(b) \neq 0$.

Let $n \geq 6$. It is not difficult to see that when $b \in \mathbb{F}_{2^3}$ and $\mathrm{tr}_3(b) = 0$ then all items with exponents of 2-weight 4 vanish. Then

$$\begin{aligned} g_b(x) &= \mathrm{tr}_n(bC(x)) \\ &= \mathrm{tr}_n\left(b(x^3 + T(x))\right) + \mathrm{tr}_3\left(T(x)\,\mathrm{tr}_{n/3}(bx + b^2x^2 + b^2x^4 + b^4x^8)\right) \\ &= \mathrm{tr}_n\left(b(x^3 + T(x))\right) + \sum_{\substack{0 \leq k < n \\ 0 \leq t < n/3}} b^2 x^{2^k + 2^{3t} + 2^{3t+1}} \\ &\quad + \sum_{\substack{0 \leq k < n \\ 0 \leq t < n/3}} b^4 x^{2^k + 2^{3t+1} + 2^{3t+2}} + \sum_{\substack{0 \leq k < n \\ 0 \leq t < n/3}} b x^{2^k + 2^{3t+2} + 2^{3t+3}} \end{aligned}$$

and in g_b the only item with the exponent $2^0 + 2^1 + 2^3$ has the coefficient b^2. Hence g_b has algebraic degree 3 when $b \in \mathbb{F}_{2^3}^*$ and $\mathrm{tr}_3(b) = 0$. □

3.4 The existence of elements b satisfying the conditions of Theorem 3

Proposition 4 *Let n be a positive even integer divisible by 6 and i be a positive integer not divisible by $n/2$ such that $n/\gcd(i,n)$ is even and $\gcd(i,n) \neq 1$. There exist at least $\frac{1}{5}(2^n - 1) - 2^{n/2} > 0$ elements b satisfying the conditions of Theorem* 3.

Proof. As in the proof of Proposition 1, we have $\gcd(2^n - 1, 2^i + 1) \geq 2^{\gcd(i,n)} + 1$. This implies $\gcd(2^n - 1, 2^i + 1) \geq 5$. Since the number of $d + d^2$ equals 4 and the size of the set E' of all $(2^i + 1)$-th powers of elements of $\mathbb{F}_{2^n}^*$ is at most $(2^n - 1)/5$, this implies that $(F_{2^n} \cap F_{2^i}) \cup E' \cup (1 + E')$ has size at most $2^{n/2} + 4(2^n - 1)/5 < 2^n - 1$. This completes the proof. □

Proposition 5 *Let i, n, s be positive integers such that i is not divisible by $n/2$, $\gcd(i, 6s) = 3s$, n is divisible by $6s$ but not by $6s(2^{3s} + 1)$. If $b \in \mathbb{F}_{2^{6s}} \setminus \mathbb{F}_{2^{3s}}$ and the function G is given by* (2) *then the Boolean function $g_b(x) = \mathrm{tr}_n(bG(x))$ is bent and cubic.*

Proof. Since n is divisible by $6s$ but not by $6s(2^{3s} + 1)$) and $i/(3s)$ is odd then $2^i + 1$ is divisible by $2^{3s} + 1$, and $2^n - 1$ is divisible by $2^{3s} + 1$ but not by $(2^{3s} + 1)^2$ (see the proof of Proposition 2). Then for any $b \in \mathbb{F}_{2^{6s}} \setminus \mathbb{F}_{2^{3s}}$ and any $d \in \mathbb{F}_8$ obviously $b + d + d^2$ is not the $(2^{3s} + 1)$-th power of an element of $\mathbb{F}_{2^n}$ (and therefore it is not the $(2^i + 1)$-th power). Indeed, since

$2^{6s}-1 = (2^{3s}-1)(2^{3s}+1)$ then $b \in \mathbb{F}_{2^{6s}}$ is the $(2^{3s}+1)$-th power of an element of $\mathbb{F}_{2^{6s}}$ if and only if $b \in \mathbb{F}_{2^{3s}}$. Since $2^n - 1$ is not divisible by $(2^{3s}+1)^2$ then, $b \in \mathbb{F}_{2^{6s}}$ is $(2^{3s}+1)$-th power of an element of $\mathbb{F}_{2^n}$ if and only if b is $(2^{3s}+1)$-th power of an element of $\mathbb{F}_{2^{6s}}$. More precisely, if $b \in \mathbb{F}_{2^{6s}}$ then for some primitive element α of $\mathbb{F}_{2^n}$ and some k we have $b = \alpha^{k(2^n-1)/(2^{6s}-1)}$. Since $(2^n-1)/(2^{6s}-1)$ is not divisible by $2^{3s}+1$ then b is the $(2^{3s}+1)$-th power of an element of $\mathbb{F}_{2^n}$ if and only if k is divisible by $2^{3s}+1$, that is, if and only if b is the $(2^{3s}+1)$-th power of an element of $\mathbb{F}_{2^{6s}}$, and that is, if and only if $b \in \mathbb{F}_{2^{3s}}$. For $b \in \mathbb{F}_{2^{6s}} \setminus \mathbb{F}_{2^{3s}}$ and any $d \in \mathbb{F}_8$ obviously $b+d+d^2 \in \mathbb{F}_{2^{6s}} \setminus \mathbb{F}_{2^{3s}}$.

Clearly, $b \notin \mathbb{F}_{2^i}$ because i/s is odd. By Theorem 3 the function g_b is bent and cubic. □

Proposition 6 *Let i, n, s be positive integers such that $n \geq 12$, $\gcd(i, 6s) = s$, $\gcd(s, 3) = 1$, and n is divisible by $6s$ but not by $6s(2^s+1)$, and the function G be given by (2). If $b \in \mathbb{F}_{2^{6s}} \setminus \mathbb{F}_{2^{3s}}$ is such that for any $d \in \mathbb{F}_8$ the element $b+d+d^2$ is not the (2^s+1)-th power of an element of $\mathbb{F}_{2^{6s}}$ then the function $g_b(x) = \mathrm{tr}_n(bG(x))$ is bent and has algebraic degree 4.*

Proof. Since i/s is odd then $\gcd(2^i+1, 2^s+1) = 2^s+1$. As shown in the proof of Proposition 2 if t is not divisible by 2^s+1 then $2^{2st}-1$ is divisible by 2^s+1 but not by $(2^s+1)^2$. Hence, for $s \neq 1$ the number $2^{6s}-1$ is divisible by 2^s+1 but not by $(2^s+1)^2$.

If $s \neq 1$ then n is divisible by $2s$ but not by $2s(2^s+1)$. Then, as shown in the proof of Proposition 2, 2^n-1 is divisible by 2^s+1 but not by $(2^s+1)^2$. Therefore, if for some $b \in \mathbb{F}_{2^{6s}} \setminus \mathbb{F}_{2^{3s}}$ all elements $b+d+d^2$ are not the (2^s+1)-th power of an element of $\mathbb{F}_{2^{6s}}$ for any $d \in \mathbb{F}_8$, then they are not (2^s+1)-th power of an element of $\mathbb{F}_{2^n}$ (and therefore they are not the (2^i+1)-th power of an element of $\mathbb{F}_{2^n}$). For example, for $s = 2$ there are 1736 such elements b, and for $s = 4$ there are 13172960 such elements in $\mathbb{F}_{2^{24}} \setminus \mathbb{F}_{2^{12}}$.

If $s = 1$ then n is divisible by 6 but not by 9. For t even and any j we have $2^{jt}-1 = (2^{2j}-1)(t/2 + (2^{2j}-1) + ... + (2^{j(t-2)}-1))$. Therefore, taking $j = 3$ and $t = n/3$ (which is even and not divisible by 3) 2^n-1 is divisible by 27 only if $t/2$ is divisible by 3, which is not the case. Hence, if for $b \in \mathbb{F}_{2^6} \setminus \mathbb{F}_{2^3}$ all elements $b+d+d^2$ are not cubes in $\mathbb{F}_{2^6}$ for any $d \in \mathbb{F}_8$, then they are not cubes in $\mathbb{F}_{2^n}$ (and therefore they are not the (2^i+1)-th power of an element of $\mathbb{F}_{2^n}$). These elements b are zeros of one of the polynomials x^6+x+1 and $x^6+x^4+x^3+x+1$.

Hence, in these cases g_b is bent and has algebraic degree 4 by Theorem 3. □

Since F' is quadratic and since EA-equivalence preserves the algebraic degree then according to Theorem 1, the bent nonquadratic components of F and G are CCZ-inequivalent to the components of F'.

Proposition 7 *The functions f_b and g_b of Theorems* 2 *and* 3 *(and Propositions* 2, 5 *and* 6*) are CCZ-inequivalent to any component of* $F'(x) = x^{2^i+1}$.

The existence or non-existence of APN permutations over $\mathbb{F}_{2^n}$ when n is even is an open problem. For the case of quadratic APN functions this problem was solved negatively in [9]. Hence for n even the APN function $F'(x) = x^{2^i+1}$, $\gcd(i, n) = 1$, is EA-inequivalent to any permutation. However, it is potentially possible that F' is CCZ-equivalent to a nonquadratic APN permutation. From this point of view the following facts are interesting.

Corollary 1 *Let n and i be positive integers and* $\gcd(i, n) = 1$. *If* $\gcd(n, 6) = 2$ *then the APN function F given by* (1) *is EA-inequivalent to any permutation over* $\mathbb{F}_{2^n}$. *If* $\gcd(n, 18) = 6$ *then the APN function G given by* (2) *is EA-inequivalent to any permutation over* $\mathbb{F}_{2^n}$.

Proof. By Theorem 2 of [1] the function F is APN and it has bent components by Proposition 2. By Theorem 3 of [1] the function G is APN and it has bent components by Proposition 6. Therefore, F and G are not EA-equivalent to any permutation. □

4 New bent vectorial functions

Let F be a function from $\mathbb{F}_{2^n}$ to itself, n be divisible by m, and $b \in \mathbb{F}_{2^n}^*$. We know from [8] that an (n, m)-function $\mathrm{tr}_{n/m}(bF(x))$ is bent if and only if for any $v \in \mathbb{F}_{2^m}^*$ the Boolean function $\mathrm{tr}_n(bvF(x))$ is bent. Hence we can obtain vectorial bent functions from Theorem 2.

Theorem 4 *Let $n \geq 6$ be an even integer divisible by m, i be a positive integer not divisible by $n/2$ such that $n/\gcd(i, n)$ is even. If $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^i}$ is such that for any $v \in \mathbb{F}_{2^m}^*$ neither bv nor $bv + 1$ are the $(2^i + 1)$-th powers of elements of $\mathbb{F}_{2^n}$, and the function F is given by* (1) *then the function* $\mathrm{tr}_{n/m}(bF(x))$ *is bent and has algebraic degree* 3.

In particular we obtain the following vectorial bent functions from Proposition 2.

Corollary 2 *Let $n \geq 6$ be an even integer, i be a positive integer not divisible by $n/2$ and s a divisor of i such that i/s is odd and n is divisible by $2s$ but not by $2s(2^s + 1)$. If $b \in \mathbb{F}_{2^{2s}} \setminus \mathbb{F}_{2^s}$ and the function F is given by* (1) *then the function $f(x) = \mathrm{tr}_{n/s}(bF(x))$ is bent and has algebraic degree* 3.

Proof. Since $b \in \mathbb{F}_{2^{2s}} \setminus \mathbb{F}_{2^s}$ then $bv \in \mathbb{F}_{2^{2s}} \setminus \mathbb{F}_{2^s}$ for any $v \in \mathbb{F}_{2^s}^*$. Hence by Proposition 2 the functions $\mathrm{tr}_n(bvF(x))$ are bent for all $v \in \mathbb{F}_{2^s}^*$, and, therefore, $\mathrm{tr}_{n/s}(bF(x))$ is bent. □

Theorem 3, and in particular Propositions 5 and 6, also give new bent vectorial functions.

Theorem 5 *Let i, m, n be positive integers such that n is divisible by $6m$, and i is not divisible by $n/2$ and $n/\gcd(i,n)$ is even. Let $b \in \mathbb{F}_{2^n}$ be such that, for any $d \in \mathbb{F}_8$ and any $v \in \mathbb{F}_{2^m}^*$, $bv + d + d^2$ is not the (2^i+1)-th power of an element of $\mathbb{F}_{2^n}$. If the function G is given by (2) then the Boolean function $\mathrm{tr}_{n/m}(b\,G(x))$ is bent.*

Corollary 3 *Let i, n, s be positive integers such that i is not divisible by $n/2$, $\gcd(i, 6s) = 3s$, n is divisible by $6s$ but not by $6s(2^{3s}+1)$, $b \in \mathbb{F}_{2^{6s}} \setminus \mathbb{F}_{2^{3s}}$ and the function G be given by (2). Then the function $g_b(x) = \mathrm{tr}_{n/s}(bG(x))$ is bent and cubic.*

Corollary 4 *Let i, n, s be positive integers such that $n \geq 12$, $\gcd(i, 6s) = s$, $\gcd(s, 3) = 1$, n is divisible by $6s$ but not by $6s(2^s+1)$, and the function G be given by (2). If $b \in \mathbb{F}_{2^{6s}} \setminus \mathbb{F}_{2^{3s}}$ is such that for any $d \in \mathbb{F}_8$ and any $v \in \mathbb{F}_{2^{3s}}^*$ the element $bv + d + d^2$ is not the (2^s+1)-th power in $\mathbb{F}_{2^{6s}}$ then the function $g_b(x) = \mathrm{tr}_{n/3s}(bG(x))$ is bent and has algebraic degree 4.*

Since $F'(x) = x^{2^i+1}$ is quadratic and since EA-equivalence preserves the algebraic degree then according to Theorem 1, the bent functions of Theorems 4 and 5, and Corollaries 2–4 in particular, are CCZ-inequivalent to $\mathrm{tr}_{n/m}(vF'(x))$ for any $v \in \mathbb{F}_{2^n}$ and any divisor m of n.

Proposition 8 *The bent functions f_b and g_b of Theorems 4 and 5 (and Corollaries 2, 3 and 4) are CCZ-inequivalent to $\mathrm{tr}_{n/m}(vF'(x))$ for any $v \in \mathbb{F}_{2^n}$ and any divisor m of n.*

Acknowledgments

We would like to thank Gregor Leander for useful discussions. The research of the first author was supported by Norwegian Research Council.

References

[1] L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Functions. *IEEE Trans. Inform. Theory*, vol. 52, no. 3, pp. 1141-1152, March 2006.

[2] L. Budaghyan and T. Helleseth. New perfect nonlinear multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime p. *Proceedings of SETA 2008*, Lecture Notes in Computer Science 5203, pp. 401-414, 2008.

[3] C. Carlet. Vectorial Boolean Functions for Cryptography. Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, in press.

[4] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2), pp. 125-156, 1998.

[5] J. F. Dillon. *Elementary Hadamard Difference sets*. Ph. D. Thesis, Univ. of Maryland, 1974.

[6] G. Kyureghyan and A. Pott. Some theormes on planar mappings. *Proceedings of WAIFI 2008*, Lecture Notes in Computer Science 5130, pp. 115-122, 2008.

[7] G. Leander. Monomial bent functions. *Proceedings of the Workshop on Coding and Cryptography* 2005, Bergen, pp. 462-470, 2005. And *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 738-743, 2006.

[8] K. Nyberg. Perfect non-linear S-boxes. *Proceedings of EUROCRYPT' 91, Lecture Notes in Computer Science* 547, pp. 378-386, 1992.

[9] K. Nyberg. S-boxes and Round Functions with Controllable Linearity and Differential Uniformity. *Proceedings of Fast Software Encryption 1994, Lecture Notes in Computer Science* 1008, pp. 111-130, 1995.