Des. Codes Cryptogr.
DOI 10.1007/s10623-010-9466-9

CCZ-equivalence of bent vectorial functions and related constructions

Lilya Budaghyan · Claude Carlet

Received: 10 February 2009 / Revised: 17 April 2009 / Accepted: 1 August 2010

Abstract We observe that the CCZ-equivalence of bent vectorial functions over $\mathbf{F}_2^n$ (n even) reduces to their EA-equivalence. Then we show that in spite of this fact, CCZ-equivalence can be used for constructing bent functions which are new up to EA-equivalence and therefore to CCZ-equivalence: applying CCZ-equivalence to a non-bent vectorial function F which has some bent components, we get a function F' which also has some bent components and whose bent components are CCZ-inequivalent to the components of the original function F. 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

Mathematics Subject Classification (2000) 06E30 · 11T71

1 Introduction

The notion (recalled below) of CCZ-equivalence of vectorial functions, introduced in [13] (and which corresponds to graph equivalence, but the term of CCZ-equivalence, introduced in [8], is now widely used in the literature), is a fecund notion which has led to new APN and AB functions, up to EA-equivalence. It seems to be the proper notion of equivalence for vectorial functions used as S-boxes in cryptosystems (see more in [4]). Two vectorial

The research of the first author was supported by Norwegian Research Council.

L. Budaghyan (✉)
Department of Informatics, University of Bergen, PB 7803, 5020 Bergen, Norway
e-mail: Lilya.Budaghyan@ii.uib.no

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

Published online: 06 January 2011

functions F and F' from $\mathbf{F}_2^n$ to $\mathbf{F}_2^m$ (that is, two (n, m)-functions) are called CCZ-equivalent if their graphs $G_F = \{(x, F(x));\ x \in \mathbf{F}_2^n\}$ and $G_{F'} = \{(x, F'(x));\ x \in \mathbf{F}_2^n\}$ are affine equivalent, that is, if there exists an affine permutation $\mathcal{L}$ of $\mathbf{F}_2^n \times \mathbf{F}_2^m$ such that $\mathcal{L}(G_F) = G_{F'}$. If F is an almost perfect nonlinear (APN) function from $\mathbf{F}_2^n$ to $\mathbf{F}_2^n$, that is, if any derivative of F:

$$D_a F(x) = F(x + a) - F(x), \qquad a \in \mathbf{F}_2^n \backslash \{0\}$$

(i.e. $D_a F(x) = F(x + a) + F(x)$ since we are in characteristic 2) is 2-to-1 (which implies that F contributes to an optimal resistance to the differential attack [1] on the cipher in which it is used as an S-box), then F' is APN too. If F is almost bent (AB), that is, if its nonlinearity equals $2^{n-1} - 2^{\frac{n-1}{2}}$ (which implies that F contributes to an optimal resistance of the cipher to the linear attack [18]), then F' is also AB. F and F' are called EA-equivalent (extended affine equivalent) if there exist affine automorphisms $L : \mathbf{F}_2^n \to \mathbf{F}_2^n$ and $L' : \mathbf{F}_2^m \to \mathbf{F}_2^m$ and an affine function $L'' : \mathbf{F}_2^n \to \mathbf{F}_2^m$ such that $F' = L' \circ F \circ L + L''$. EA-equivalence is a particular case of CCZ-equivalence [13]. Besides, every permutation is CCZ-equivalent to its inverse. As shown in [8], CCZ-equivalence is more general than the conjunction of the EA-equivalence of functions and the inversion of permutations.

The relation between CCZ-equivalence and EA-equivalence for (n, m)-functions in general has been studied in [4]. It is proven that for Boolean functions (that is, for $m = 1$), CCZ-equivalence coincides with EA-equivalence, and, on the contrary, for (n, m)-functions, CCZ-equivalence is strictly more general than EA-equivalence when $n \geq 5$ and m is greater or equal to the smallest positive divisor of n different from 1.

The principle of CCZ-equivalence can be straightforwardly generalized to functions over finite fields of any odd characteristic p. It has been proved in [5,15] that, when applied to perfect nonlinear (also called planar) functions from $\mathbf{F}_p^n$ to $\mathbf{F}_p^n$, that is, functions whose derivatives $D_a F(x)$, $a \neq 0$, are bijective, it is the same as EA-equivalence. A natural question is to ask whether this property is true for perfect nonlinear functions (also called bent) from $\mathbf{F}_2^n$ to $\mathbf{F}_2^m$, that is, functions whose derivatives $D_a F(x)$, $a \neq 0$, are balanced (i.e. have outputs uniformly distributed over $\mathbf{F}_2^m$; these functions exist only for n even and $m \leq n/2$, see [19]). We prove in Sect. 3 that for any positive integers n and m, CCZ-equivalence coincides with EA-equivalence when applied to bent (n, m)-functions.

The fact that CCZ-equivalence of bent functions is the same as their EA-equivalence means that all bent vectorial functions obtained by CCZ-equivalence from known bent functions are EA-equivalent to the original functions. However, we will show that CCZ-equivalence can be applied to a non-bent vectorial function F, for instance from $\mathbf{F}_{2^n}$ to itself, with bent components $\mathrm{tr}_n(bF(x))$ for some $b \in \mathbf{F}_{2^n}^*$ (where $\mathrm{tr}_n(x)$ denotes the trace function $\mathrm{tr}_n(x) = x + x^2 + x^4 + \cdots + x^{2^{n-1}}$ from $\mathbf{F}_{2^n}$ into $\mathbf{F}_2$), and obtain a vectorial function F' which can hopefully have bent components $\mathrm{tr}_n(b'F'(x))$ for some $b' \in \mathbf{F}_{2^n}^*$, of algebraic degrees strictly greater than the degree of F. According to the result of Sect. 3, these bent components of F' cannot be CCZ-equivalent to the bent components of F. We give in Sects. 4 and 5 examples F and G of vectorial functions from $\mathbf{F}_{2^n}$ to itself leading this way to new families of bent Boolean and bent vectorial functions. The first one F is defined for any n even and the second one G is defined for any n divisible by 6. These functions were constructed in [8] by applying CCZ-equivalence to the so-called Gold function $F'(x) = x^{2^i+1}$. 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 (but the components of F and G can have lower algebraic degrees [8]). The functions F and G are EA-inequivalent to F', and it is known that if $n/\gcd(n, i)$ is even then for certain elements $b \in \mathbf{F}_{2^n}$ the Boolean functions

$\mathrm{tr}_n(bF'(x))$ are bent. In general, if a vectorial function H has some bent components, this does not yet imply that a function CCZ-equivalent to H has necessarily bent components. First we prove that the functions F and G have bent nonquadratic components (which are CCZ-inequivalent to the components of F') and then we show that this also leads to new families of vectorial bent functions (with a number of output bits smaller than half the number of input bits, though). These bent functions are new in a sense that we shall precise below.

Note that there are only a few families of bent functions given in trace representation known so far. The significance of the introduced approach is partly 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, and hopefully new.

2 Preliminaries

In all the paper, n and m are positive integers. An (n, m)-function F has a unique representation as a polynomial on n variables with coefficients in $\mathbf{F}_2^m$

$$F(x_1, \ldots, x_n) = \sum_{u \in \mathbf{F}_2^n} c(u) \left(\prod_{i=1}^{n} x_i^{u_i} \right).$$

This representation is called the algebraic normal form of F and its degree $d^\circ(F)$ the algebraic degree of the function F. Obviously, F is affine if and only if $d^\circ(F) \leq 1$. We say that F is quadratic if $d^\circ(F) = 2$, and we call F a cubic function if $d^\circ(F) = 3$. The algebraic degree of a function is invariant under EA-equivalence (if the function is not affine) but it is not preserved by CCZ-equivalence.

A Boolean function f on $\mathbf{F}_2^n$ is bent if and only if

$$\lambda_f(u) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+u\cdot x} = \pm 2^{\frac{n}{2}}, \quad \forall u \in \mathbf{F}_2^n,$$

where "$\cdot$" is any inner product in $\mathbf{F}_2^n$ (this notion does not depend on the choice of the inner product and is equivalent to saying that f lies at maximal Hamming distance to affine functions). An (n, m)-function F is bent if and only if, for any $v \in \mathbf{F}_2^m \setminus \{0\}$, its component function $v \cdot F(x)$ is bent, where "$\cdot$" is any inner product in $\mathbf{F}_2^m$, that is,

$$\lambda_F(u, v) = \sum_{x \in \mathbf{F}_2^n} (-1)^{v\cdot F(x)+u\cdot x} = \pm 2^{\frac{n}{2}}, \quad \forall u \in \mathbf{F}_2^n, \forall v \in \mathbf{F}_2^m \setminus \{0\}.$$

This is equivalent to saying that all derivatives $D_a F(x) = F(x) + F(x + a)$, $a \neq 0$, of F are balanced (i.e., as already recalled, have uniformly distributed output).

The set of the absolute values of $\lambda_F(u, v)$ for $u \in \mathbf{F}_2^n$, $v \in \mathbf{F}_2^m \setminus \{0\}$, is called the extended Walsh spectrum of F. Note that, though CCZ-equivalence preserves the extended Walsh spectrum of a function [8], this does not imply that if a function F has some bent components then any function CCZ-equivalent to F necessarily has any bent component.

If we identify $\mathbf{F}_2^n$ with the finite field $\mathbf{F}_{2^n}$ then an (n, n)-function F is uniquely represented as a univariate polynomial over $\mathbf{F}_{2^n}$ of degree smaller than 2^n

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

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

$$\mathrm{tr}_n^m(x) = x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{(n/m-1)m}},$$

then F can be represented in the form $\mathrm{tr}_n^m(\sum_{i=0}^{2^n-1} c_i x^i)$ (and, for $m = 1$, in the form $\mathrm{tr}_n(\sum_{i=0}^{2^n-1} c_i x^i)$). Indeed, there exists a function G from $\mathbf{F}_{2^n}$ to $\mathbf{F}_{2^n}$ (for example $G(x) = aF(x)$, where $a \in \mathbf{F}_{2^n}$ 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 an (n, n)-function F is equal to the maximum 2-weight of the exponents i of the polynomial $F(x)$ such that $c_i \neq 0$:

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

An inner product in $\mathbf{F}_{2^n}$ is $u \cdot x = \mathrm{tr}_n(ux)$. Hence, a Boolean function f on $\mathbf{F}_{2^n}$ is bent if and only if

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

In this framework, an (n, m)-function F is bent if and only if, for any $v \in \mathbf{F}_{2^m}^*$, its component function $\mathrm{tr}_m(vF(x))$ is bent, that is,

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

3 CCZ-equivalence of bent vectorial functions reduces to their EA-equivalence

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

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

Proof Let F' be CCZ-equivalent to F and $\mathcal{L}(x, y) = (L_1(x, y), L_2(x, y))$, (with $L_1 : \mathbf{F}_2^n \times \mathbf{F}_2^m \to \mathbf{F}_2^n$, $L_2 : \mathbf{F}_2^n \times \mathbf{F}_2^m \to \mathbf{F}_2^m$) be an affine permutation of $\mathbf{F}_2^n \times \mathbf{F}_2^m$ which maps the graph of F to the graph of F'. Then $L_1(x, F(x))$ is a permutation (see e.g. [9]), and for some affine functions $L' : \mathbf{F}_2^n \to \mathbf{F}_2^n$ and $L'' : \mathbf{F}_2^m \to \mathbf{F}_2^n$ we can write $L_1(x, y) = L'(x) + L''(y)$.

For any element v of $\mathbf{F}_2^n$ 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 $\mathbf{F}_2^n$ (if $\mathbf{F}_2^n$ is identified with $\mathbf{F}_{2^n}$, we can take $u \cdot v = \mathrm{tr}_n(uv)$ for any $u, v \in \mathbf{F}_{2^n}$). Since $L_1(x, F(x))$ is a permutation, then any function $v \cdot L_1(x, F(x))$ is balanced (recall that this property is a necessary and sufficient condition) and, hence, cannot be bent. Therefore, $v \cdot L''(F(x))$ cannot be bent either because $v \cdot L'(x)$ is an affine function. 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 [8]. □

Remark 1 Let p be any odd prime, n and m any positive integers. Recall that, like in the binary case, a function F from $\mathbf{F}_p^n$ to $\mathbf{F}_p^m$ is called perfect nonlinear or bent if for all $a \in \mathbf{F}_p^n \backslash \{0\}$ its derivatives $D_a F(x)$ are balanced (see [12] for a survey of these functions). It is proven in [5,15] that for perfect nonlinear functions CCZ-equivalence coincides with EA-equivalence when $n = m$. However, it can be easily seen from the proof of Theorem 1 that CCZ-equivalence coincides with EA-equivalence for bent functions from $\mathbf{F}_p^n$ to $\mathbf{F}_p^m$ for any odd prime p and any positive integers n and m. The proof of Proposition 1 of [5] works for this general case as well.

Since the algebraic degree is preserved by EA-equivalence then Theorem 1 gives a very simple criterion for distinguishing inequivalent bent functions.

Corollary 1 *Let n and m be any positive integers. If two bent (n, m)-functions have different algebraic degrees then they are CCZ-inequivalent.*

4 Obtaining new bent Boolean functions through the CCZ-equivalence of non-bent vectorial functions

We show now 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. We give two examples illustrating this fact.

Let i be a positive integer. Let us define for n even the (n, n)-function:

$$F(x) = x^{2^i+1} + (x^{2^i} + x + 1)\mathrm{tr}_n(x^{2^i+1}), \tag{1}$$

and for n divisible by 6 the (n, n)-function:

$$G(x) = \left(x + \mathrm{tr}_n^3\left(x^{2(2^i+1)} + x^{4(2^i+1)}\right) + \mathrm{tr}_n(x)\mathrm{tr}_n^3\left(x^{2^i+1} + x^{2^{2i}(2^i+1)}\right)\right)^{2^i+1}. \tag{2}$$

The functions F and G were constructed in [8] by applying CCZ-equivalence to the Gold function $F'(x) = x^{2^i+1}$. 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, some components of F and G have lower algebraic degrees) [8]. Since the 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. [16,17]) that if $n/\gcd(n, i)$ is even and $b \in \mathbf{F}_{2^n}$ is not the $(2^i + 1)$-th power of an element of $\mathbf{F}_{2^n}$, then the Boolean function $\mathrm{tr}_n(bF'(x))$ is bent. In general, if a vectorial function H has some bent components, this 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 Corollary 1.

4.1 The infinite class of the functions F

Let us determine the bent cubic 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. Let the function F be given by (1), and $b \in \mathbf{F}_{2^n} \backslash \mathbf{F}_{2^i}$. Then the Boolean function $f_b(x) = tr_n(bF(x))$ has algebraic degree 3, and it is bent if and only if neither b nor $b + 1$ are the $(2^i + 1)$-th powers of elements of $\mathbf{F}_{2^n}$.*

Proof Firstly we prove that for $n/\gcd(i,n)$ even and $b \in \mathbf{F}_{2^n}$ the function f_b is bent if and only if neither b nor $b+1$ is the (2^i+1)-th power of an element of $\mathbf{F}_{2^n}$.

By Theorem 2 of [8], 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

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

It is shown in the proof of Proposition 2 of [8] (and straightforward to check) that for any $a, b \in \mathbf{F}_{2^n}$

$$\lambda_{F'}(a,b) = \lambda_F(\mathcal{L}^{-1*}(a,b)), \tag{3}$$

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

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

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

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

$$\mathcal{L}^*(x,y) = \left(L_1^*(x,y), L_2^*(x,y)\right) = (x, y + \mathrm{tr}_n(x)). \tag{4}$$

Indeed,

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

According to (3) and (4)

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

or, equivalently,

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

When $n/\gcd(i,n)$ is even, it is known that $\lambda_{F'}(a, b+\mathrm{tr}_n(a)) = \pm 2^{n/2}$ if and only if $b+\mathrm{tr}_n(a)$ is not the (2^i+1)-th power of an element of $\mathbf{F}_{2^n}$ (see e.g. [16,17]). Hence, f_b is bent if and only if neither b nor $b+1$ is the (2^i+1)-th power of an element of $\mathbf{F}_{2^n}$.

Now we prove that for $n \geq 6$ and i not divisible by $n/2$ and $b \notin \mathbf{F}_{2^i}$ the function f_b has algebraic degree 3.

Note that $c = b^{2^{n-i}} + b \neq 0$ since $b \notin \mathbf{F}_{2^i}$, and

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

where Q is quadratic. To prove that f_b is cubic we need to show that there are cubic terms in $\mathrm{tr}_n(cx)\mathrm{tr}_n(x^{2^i+1})$ which do not vanish.

All items in $\mathrm{tr}_n(x^{2^i+1}) = \sum_{j=0}^{n-1} x^{2^{i+j}+2^j}$ are pairwise different since i is not divisible by $n/2$. Indeed, if for some $0 \leq j, k < n$, $k \neq j$, we have $2^{i+j}+2^j = 2^{i+k}+2^k \bmod (2^n-1)$ or, equivalently, $i+j = k \bmod n$ and $i+k = j \bmod n$ then obviously i is divisible by $n/2$.

Let us denote $A_j = \{j-i, j, j+i, j+2i\}$. Then, since

$$\sum_{0\le j<n} c^{2^{j+2i}} x^{2^j+2^{j+i}+2^{j+2i}} = \sum_{0\le j<n} c^{2^{j+i}} x^{2^{j-i}+2^j+2^{j+i}},$$

we have

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

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. □

Since F' is quadratic, then according to Corollary 1, the bent nonquadratic components of F are CCZ-inequivalent to the components of F'.

Corollary 2 *The functions f_b of Theorem 2 are CCZ-inequivalent to any component of $F'(x) = x^{2^i+1}$.*

Remark 2 Knowing the number of EA-inequivalent bent components of a given function W we cannot predict how many bent components can have the function W' which is CCZ-equivalent to W. For instance, x^3 has only one bent component up to EA-equivalence while for small values of n we can check that F has at least 2 bent components up to EA-equivalence. Another interesting example is Dillon–Wolfe function [14], it is CCZ-equivalent to a function with bent components but it itself has no bent component at all. □

4.2 The existence of elements b satisfying the conditions of Theorem 2

We first show that there always exist elements b satisfying the conditions of Theorem 2. This result is only an existence result. We shall need a more effective one, for building new bent vectorial functions. So, we subsequently point out explicit values of such elements b, 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 more than $\frac{1}{3}(2^n-1)-2^{n/2}>0$ elements $b\in \mathbf{F}_{2^n}\setminus\mathbf{F}_{2^i}$ such that neither b nor $b+1$ are the (2^i+1)-th powers of elements of $\mathbf{F}_{2^n}$.*

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 $\gcd(2^n-1, 2^i+1) \geq 2^{\gcd(i,n)}+1 \geq 3$ (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 $\mathbf{F}^*_{2^n}$ is at most $(2^n-1)/3$ and this implies that $(\mathbf{F}_{2^n} \cap \mathbf{F}_{2^i}) \cup E \cup (1+E)$ has size at most $2^{n/2} + 2(2^n-1)/3 < 2^n - 1$ (since $n > 2$). This completes the proof. □

In the proposition below, we describe some cases where elements b satisfying the conditions of Theorem 2 can be very easily chosen.

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

Proof We are going to show that under the assumption of this proposition the conditions of Theorem 2 are satisfied. Since n is divisible by $2s$ and i/s is odd then $n/\gcd(i,n)$ is even. We have $b \notin \mathbf{F}_{2^i}$ because $b \in \mathbf{F}_{2^{2s}} \backslash \mathbf{F}_{2^s}$ and i/s is odd. Besides, obviously, $b+1 \in \mathbf{F}_{2^{2s}} \backslash \mathbf{F}_{2^s}$. Hence, we need only to prove that any element b in $\mathbf{F}_{2^{2s}} \backslash \mathbf{F}_{2^s}$ is not the (2^i+1)-th power of an element of $\mathbf{F}_{2^n}$.

Note that if the element b is not the (2^s+1)-th power of an element of $\mathbf{F}_{2^n}$ then it is not the (2^i+1)-th power of an element of $\mathbf{F}_{2^n}$. Indeed, for any positive integer u and any positive odd integer v the number $2^{uv}+1$ is divisible by 2^u+1 since

$$2^{uv} + 1 = 2^u + 1 + (2^{2u} - 1)(2^u + 2^{3u} + 2^{5u} + \cdots + 2^{u(v-2)}), \tag{5}$$

and, therefore, recalling that i/s is odd, 2^s+1 is a divisor of 2^i+1.

Since $b \in \mathbf{F}_{2^{2s}} \backslash \mathbf{F}_{2^s}$ then there exists a primitive element α of $\mathbf{F}^*_{2^n}$, and a positive integer k not divisible by 2^s+1, such that $b = \alpha^{k(2^n-1)/(2^{2s}-1)}$. Obviously, b is the (2^s+1)-th power of an element of $\mathbf{F}_{2^n}$ if and only if k is divisible by $r = (2^s+1)/\gcd\left(2^s+1, (2^n-1)/(2^{2s}-1)\right)$. Hence, if we can prove that $r = 2^s+1$, that is, 2^n-1 is not divisible by $(2^s+1)q$ for any divisor $q \neq 1$ of 2^s+1, then b is not the (2^s+1)-th power of an element of $\mathbf{F}_{2^n}$ (and, therefore, is not the (2^i+1)-th power of an element of $\mathbf{F}_{2^n}$), and by Theorem 2 the function f_b is bent and has algebraic degree 3.

Let $q \neq 1$ be any divisor of 2^s+1 and n be divisible by $2s$. Below we prove that 2^n-1 is divisible by $(2^s+1)q$ if and only if n is divisible by $2sq$.

If n is divisible by $2sq$ then 2^n-1 is divisible by $2^{2sq}-1$ and, therefore, by $2^{sq}+1$. Since q is odd (being a divisor of 2^s+1) then using (5) we get

$$\begin{aligned}
2^{sq} + 1 &= (2^s+1)\left(1 + (2^s-1)(2^s + 2^{3s} + \cdots + 2^{s(q-2)})\right) \\
&= (2^s+1)\Big(1 + (2^s+1)(2^s + 2^{3s} + \cdots + 2^{s(q-2)}) \\
&\quad -2(2^s + 2^{3s} + \cdots + 2^{s(q-2)})\Big) \\
&= (2^s+1)\Big(1 + (2^s+1)(2^s + 2^{3s} + \cdots + 2^{s(q-2)}) \\
&\quad +(q-1) - 2\left((2^s+1) + (2^{3s}+1) + \cdots + (2^{s(q-2)}+1)\right)\Big) \\
&= (2^s+1)^2\left(2^s + 2^{3s} + \cdots + 2^{s(q-2)}\right) + (2^s+1)q \\
&\quad -2(2^s+1)\left((2^s+1) + (2^{3s}+1) + \cdots + (2^{s(q-2)}+1)\right)
\end{aligned} \tag{6}$$

which is divisible by $(2^s+1)q$ because q is a divisor of 2^s+1 and because for any odd positive integer v the number $2^{sv}+1$ is divisible by 2^s+1 as it is observed above. Hence, $2^{sq}+1$, and therefore also 2^n-1, are divisible by $(2^s+1)q$.

Let now n be divisible by $2s$ but not by $2sq$. Then there exist positive integers w and t such that $1 \leq t < q$ and $n = 2s(wq+t)$. Then

$$2^n - 1 = 2^{2st}\,(2^{2swq}-1) + (2^{2st}-1). \tag{7}$$

As it is shown above $2^{2swq}-1$ is divisible by $(2^s+1)q$ because the number $2swq$ is divisible by $2sq$. Therefore, because of (7), the number 2^n-1 is divisible by $(2^s+1)q$ if and only if $2^{2st}-1$ is divisible by $(2^s+1)q$. But $2^{2st}-1$ is not divisible by $(2^s+1)q$ as we show below by considering separately the cases t odd and t even.
For t odd, using equality (6) and remembering that for any positive odd integer v the number $2^{sv}+1$ is divisible by 2^s+1, we get

$$\begin{aligned}2^{st}+1 &= (2^s+1)^2\left(2^s+2^{3s}+\cdots+2^{s(t-2)}\right)+(2^s+1)t\\ &\quad -2(2^s+1)\left((2^s+1)+(2^{3s}+1)+\cdots+(2^{s(t-2)}+1)\right)\\ &= (2^s+1)^2T+(2^s+1)t\end{aligned}$$

for some integer T. Hence, $2^{st}+1$ is divisible by 2^s+1 but not by $(2^s+1)q$, and, since $2^{st}-1$ is not divisible by q (otherwise the odd integer q would be a divisor of $2^{st}+1$ and $2^{st}-1$ which is obviously impossible), then the number $2^{2st}-1$ is also divisible by 2^s+1 but not by $(2^s+1)q$.
For t even

$$\begin{aligned}2^{st}-1 &= (2^{2s}-1)(1+2^{2s}+\cdots+2^{s(t-2)})\\ &= (2^{2s}-1)\left(t/2+(2^{2s}-1)+(2^{4s}-1)+\cdots+(2^{s(t-2)}-1)\right)\\ &= (2^{2s}-1)t/2+(2^s+1)^2R\end{aligned}$$

for some integer R. Hence, $2^{st}-1$ is divisible by 2^s+1 but not by $(2^s+1)q$. The odd integer $q \neq 1$ is a divisor of 2^s+1, and therefore it is a divisor of $2^{st}-1$. Then, obviously, it is not a divisor of $2^{st}+1 = (2^{st}-1)+2$. Thus, $2^{2st}-1$ cannot be divisible by $(2^s+1)q$.
Hence, for both t odd and t even the number $2^{2st}-1$ is not divisible by $(2^s+1)q$, and, therefore, 2^n-1 is not divisible by $(2^s+1)q$. □

4.3 The relation of the functions of Theorem 2 to the Maiorana-McFarland class of bent functions

An n-variable Boolean bent function belongs to the Maiorana-McFarland (MM) class if, writing its input in the form (x, y), with $x, y \in \mathbf{F}_2^{n/2}$, the corresponding output equals $x \cdot \pi(y) + g(y)$, where π is a permutation of $\mathbf{F}_2^{n/2}$ and g is a Boolean function over $\mathbf{F}_2^{n/2}$. 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 [14]. Many bent functions found in trace representation (listed e.g. in [10]) 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. However, it is in general difficult to determine what is the exact intersection between a given infinite class of bent functions and the completed Maiorana-McFarland class. Below we prove a partial result: the functions f_b of Theorem 2 belong to the completed Maiorana-McFarland class when b belongs to $\mathbf{F}_{2^{n/2}}$.

Proposition 3 *The bent functions f_b of Theorem 2 belong to the completed Maiorana-McFarland class when $b \in \mathbf{F}_{2^{n/2}}$. 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

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

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

where

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

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

Remark 3 For $n \geq 8$ the functions f_b are not in class $PSap$, up to EA-equivalence, because the degree of $PSap$ functions is always $n/2$.

4.4 The infinite class of the functions G

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 $b \in \mathbf{F}_{2^n}$ and let G be given by (2). Then the Boolean function $g_b(x) = tr_n(b\,G(x))$ is bent if and only if, for any $d \in \mathbf{F}_8$, the element $b + d + d^2$ is not the (2^i+1)-th power of an element of $\mathbf{F}_{2^n}$. If, in addition, i is divisible by 3 and $b \notin \mathbf{F}_{2^i}$ 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 $b \notin \mathbf{F}_8$ or $tr_3(b) \neq 0$.*

Proof First we are going to prove that for $n/\gcd(i,n)$ even, the function g_b is bent if and only if the element b of $\mathbf{F}_{2^n}$ is such that for any $d \in \mathbf{F}_8$, the element $b + d + d^2$ is not the (2^i+1)-th power of an element of $\mathbf{F}_{2^n}$. By Theorem 3 of [8], 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

$$\mathcal{L}(x,y) = (x + \mathrm{tr}_n^3(y^2 + y^4), y).$$

For the adjoint operator $\mathcal{L}^*$ of $\mathcal{L}^*$ we have

$$\mathcal{L}^*(x,y) = (x, y + \mathrm{tr}_n^3(x^2 + x^4))$$

because

$$\begin{aligned}
\mathrm{tr}_n\left(\mathrm{tr}_n^3(y^2+y^4)x'\right) &= \mathrm{tr}_n\left(\sum_{\substack{0\leq j\leq n-1\\ \frac{n}{3}\nmid j}} x' y^{2^j}\right)\\
&= \mathrm{tr}_n\left(\sum_{\substack{0\leq j\leq n-1\\ \frac{n}{3}\nmid j}} x'^{2^{n-j}} y\right)\\
&= \mathrm{tr}_n\left(\sum_{\substack{0\leq j\leq n-1\\ \frac{n}{3}\nmid j}} x'^{2^j} y\right)\\
&= \mathrm{tr}_n\left(\mathrm{tr}_n^3(x'^2+x'^4)y\right).
\end{aligned}$$

Since $\mathcal{L}$ and $\mathcal{L}^*$ are involutions and since $\lambda_G(a,b) = \lambda_{F'}(\mathcal{L}^{-1*}(a,b))$, then we get

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

Thus, g_b 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 $\mathbf{F}_{2^n}$ for any a. This proves the first part of Theorem 3.

We prove below that the function g_b has algebraic degree 3 when i is divisible by 3 but not by $n/2$ and $b \notin \mathbf{F}_{2^i}$.
Since $\mathrm{tr}_n^3(x^{2^{2i}(2^i+1)}) = \mathrm{tr}_n^3(x^{2^i+1})$ for i divisible by 3 then

$$\begin{aligned} G(x) &= \left(x + \mathrm{tr}_n^3\left(x^{2(2^i+1)} + x^{4(2^i+1)}\right)\right)^{2^i+1} \\ &= x^{2^i+1} + \mathrm{tr}_n^3\left(x^{2^i+1} + x^{4(2^i+1)}\right) + (x + x^{2^i})\mathrm{tr}_n^3\left(x^{2(2^i+1)} + x^{4(2^i+1)}\right). \end{aligned}$$

Clearly, $c = b + b^{2^{n-i}} \neq 0$ because $b \notin \mathbf{F}_{2^i}$, and, since i is not divisible by $n/2$ then all terms in $\mathrm{tr}_n^3\left(x^{2(2^i+1)} + x^{4(2^i+1)}\right)$ are pairwise different. For some quadratic function Q, we have

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

and it is not difficult to see that the cubic terms of g_b do not vanish. Indeed,

$$\begin{aligned} &\mathrm{tr}_3\left(\mathrm{tr}_n^3\,(cx)\,\mathrm{tr}_n^3\left(x^{2(2^i+1)} + x^{4(2^i+1)}\right)\right) \\ &= \sum_{j,k=0}^{n/3-3} c^{2^{3k}} x^{2^{3k}+2^{3j+1}+2^{3j+i+1}} + \sum_{j,k=0}^{n/3-3} c^{2^{3k}} x^{2^{3k}+2^{3j+2}+2^{3j+i+2}} \\ &\quad + \sum_{j,k=0}^{n/3-3} c^{2^{3k+1}} x^{2^{3k+1}+2^{3j+2}+2^{3j+i+2}} + \sum_{j,k=0}^{n/3-3} c^{2^{3k+1}} x^{2^{3k+1}+2^{3j+3}+2^{3j+i+3}} \\ &\quad + \sum_{j,k=0}^{n/3-3} c^{2^{3k+2}} x^{2^{3k+2}+2^{3j+3}+2^{3j+i+3}} + \sum_{j,k=0}^{n/3-3} c^{2^{3k+2}} x^{2^{3k+2}+2^{3j+4}+2^{3j+i+4}}. \end{aligned}$$

The item with the exponent $1 + 2^1 + 2^{i+1}$ of x appears only in the first sum above and, obviously, it does not vanish there. As i is divisible by 3 but not by $n/2$ then this exponent has 2-weight 3.

Let now i be not divisible by 3. We are going to prove that in this case the function g_b has algebraic degree at least 3, and it is exactly 4 if $n \geq 12$, and either $b \notin \mathbf{F}_8$ or $\mathrm{tr}_3(b) \neq 0$. For $n = 6$ it is checked with a computer that g_b has algebraic degree at least 3 for any $b \in \mathbf{F}_{2^6}^*$. Let $n \geq 12$. For simplicity we consider only the case $i = 1$. Denoting $T(x) = \mathrm{tr}_n^3(x^3)$ we get

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

where

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

is a cubic function. Hence,

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

where for $0 \le k < n$

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

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

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

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 $u_6 + u_9 = b^{2^6} + b^{2^9} = (b + b^8)^{2^6} \neq 0$ when $b \notin \mathbf{F}_{2^3}$. 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 $b \notin \mathbf{F}_{2^3}$.

If $b \in \mathbf{F}_{2^3}$ then $\mathrm{tr}_n(b) = 0$. If $\mathrm{tr}_3(b) \neq 0$ 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 $b \in \mathbf{F}_{2^3}$ and $\mathrm{tr}_3(b) \neq 0$.

Let $b \in \mathbf{F}_{2^3}$ and $\mathrm{tr}_3(b) = 0$. Then all items with exponents of 2-weight 4 vanish and

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

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 $b \in \mathbf{F}_{2^3}^*$ and $\mathrm{tr}_3(b) = 0$. □

Since F' is quadratic then, according to Corollary 1, the bent nonquadratic components of G are CCZ-inequivalent to the components of F'.

Corollary 3 *The functions g_b of Theorem 3 are CCZ-inequivalent to any component of $F'(x) = x^{2^i+1}$.*

Remark 4 We checked with a computer that for $n = 6$ there are cubic bent components of G which are EA-inequivalent to any component of F. This implies that in general cubic bent components of G are EA-inequivalent to cubic bent components of F.

4.5 The existence of elements b satisfying the conditions of Theorem 3 and relation to MM class

We prove in Proposition 4 the existence of elements b satisfying the conditions of Theorem 3 for $\gcd(i, n) \neq 1$. The existence of such elements for the case $\gcd(i, n) = 1$ when $\gcd(9, n) \neq 9$ will be shown in Proposition 6.

Proposition 4 *Let n be a positive even integer divisible by 6 and i 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 $b \in \mathbf{F}_{2^n} \backslash \mathbf{F}_{2^i}$ such that, for any $d \in \mathbf{F}_8$, the element $b + d + d^2$ is not the $(2^i + 1)$-th power of an element of $\mathbf{F}_{2^n}$.*

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 $\mathbf{F}_{2^n}^*$ is at most $(2^n - 1)/5$, this implies that $\left(\mathbf{F}_{2^n} \cap \mathbf{F}_{2^i}\right) \cup \left(\bigcup_{d \in \mathbf{F}_8} (d + d^2 + E')\right)$ has size at most $2^{n/2} + 4(2^n - 1)/5 < 2^n - 1$. This completes the proof. □

Here again, we shall need a more effective result, in order to build a bent vectorial function deduced from G. Next proposition describes cases for i divisible by 3 where elements b satisfying the conditions of Theorem 3 can be very easily chosen.

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

Proof We are going to show that, under these assumptions, the conditions of Theorem 3 are satisfied. Note that since $\gcd(i, 6s) = 3s$ then $\frac{i}{3s}$ is odd, and since $b \in \mathbf{F}_{2^{6s}} \backslash \mathbf{F}_{2^{3s}}$ then $b \notin \mathbf{F}_{2^i}$. Besides, $n/\gcd(i, n)$ is even because $\gcd(i, 6s) = 3s$ and $\gcd(n, 6s) = 6s$.

According to (5) the number $2^i + 1$ is divisible by $2^{3s} + 1$ because $\frac{i}{3s}$ is odd. Therefore if b is not the $(2^{3s} + 1)$-th power of an element of $\mathbf{F}_{2^n}$ then it is not the $(2^i + 1)$-th power of an element of $\mathbf{F}_{2^n}$. Besides, since $b \in \mathbf{F}_{2^{6s}} \backslash \mathbf{F}_{2^{3s}}$ then for any $d \in \mathbf{F}_8$ we have $b + d + d^2 \in \mathbf{F}_{2^{6s}} \backslash \mathbf{F}_{2^{3s}}$. Hence, it is enough to prove that any element b in $\mathbf{F}_{2^{6s}} \backslash \mathbf{F}_{2^{3s}}$ is not the $(2^{3s} + 1)$-th power of an element of $\mathbf{F}_{2^n}$.

Since $b \in \mathbf{F}_{2^{6s}} \backslash \mathbf{F}_{2^{3s}}$ then there exists a primitive element α of $\mathbf{F}_{2^n}$, and a positive integer k not divisible by $2^{3s} + 1$, such that $b = \alpha^{k(2^n-1)/(2^{6s}-1)}$. Obviously, b is the $(2^{3s} + 1)$-th power of an element of $\mathbf{F}_{2^n}$ if and only if k is divisible by $r = (2^{3s} + 1)/\gcd\left(2^{3s} + 1, (2^n - 1)/(2^{6s} - 1)\right)$. But since $\gcd(n, 6s(2^{3s} + 1)) = 6s$ then $r = 2^{3s} + 1$ (see the proof of Proposition 2). Hence, b cannot be the $(2^{3s} + 1)$-th power of an element of $\mathbf{F}_{2^n}$. □

For i not divisible by 3 we obtain a slightly more complex description of some elements b satisfying the conditions of Theorem 3.

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

Proof We have that i/s is odd and $n/\gcd(i, n)$ is even because $\gcd(i, 2s) = s$ and $\gcd(n, 6s(2^{3s} + 1)) = 6s$. Then $2^i + 1$ is divisible by $2^s + 1$ due to (5). Therefore if b is not the $(2^s + 1)$-th power of an element of $\mathbf{F}_{2^n}$ then it is not the $(2^i + 1)$-th power of an element of $\mathbf{F}_{2^n}$. Besides, since $b \in \mathbf{F}_{2^{6s}}$ then for any $d \in \mathbf{F}_8$ we have $b + d + d^2 \in \mathbf{F}_{2^{6s}}$. Hence we need only to prove that any element $b \in \mathbf{F}_{2^{6s}}$, which is not the $(2^s + 1)$-th power of an element of $\mathbf{F}_{2^{6s}}$, is not the $(2^s + 1)$-th power of an element of $\mathbf{F}_{2^n}$.

Since $b \in \mathbf{F}_{2^{6s}}$ then there exists a primitive element α of $\mathbf{F}_{2^n}$ and a positive integer k such that $b = \alpha^{k(2^n-1)/(2^{6s}-1)}$. Since $\gcd(n, 6s(2^{3s} + 1)) = 6s$ then, as shown in the proof of Proposition 2, we have $\gcd\left(2^{3s} + 1, (2^n - 1)/(2^{6s} - 1)\right) = 1$, and therefore $\gcd\left(2^s + 1, (2^n - 1)/(2^{6s} - 1)\right) = 1$ because $2^s + 1$ is a divisor of $2^{3s} + 1$. Hence b is the $(2^s + 1)$-th power of an element of $\mathbf{F}_{2^n}$ if and only if k is divisible by $2^s + 1$, that is, if and only if b is the $(2^s + 1)$-th power of an element of $\mathbf{F}_{2^{6s}}$. □

For small values of s it is easy to count the exact numbers of elements $b \in \mathbf{F}_{2^{6s}}$ which satisfy the condition of Proposition 6. For instance, for $s = 2$ there are 1736 such elements b, and for $s = 4$ there are 13172960 such elements. For $s = 1$ there are 12 such elements and these elements b are zeros of one of the polynomials $x^6 + x + 1$ and $x^6 + x^4 + x^3 + x + 1$. Hence, if in addition to conditions of Theorem 3 we have $\gcd(i, n) = 1$ and $\gcd(9, n) = 3$ then Proposition 6 ensures the existence of elements satisfying the conditions of this theorem.

Thanks to computer investigations, we know that some of the constructed bent functions g_b (Theorem 3) are neither in MM class nor in PS class:

Proposition 7 *For $n = 12$ and $i = 1$, α a primitive element of $\mathbf{F}_{2^n}$ (determined by MAGMA), the function $tr_n(\alpha^{19}G(x))$ is a bent function of algebraic degree 4 which is neither in MM class nor in PS class, up to EA-equivalence (that is, up to CCZ-equivalence).*

This shows by an example that having a vectorial function F with bent components all of which are in the MM class, we can construct a function F' CCZ-equivalent to F but which has some non-MM bent components.

Remark 5 For $n \geq 10$ the functions g_b are not in class $PSap$, up to EA- equivalence, because the degree of $PSap$ functions is always $n/2$.

4.6 Further constructions?

Applying CCZ-equivalence to the quadratic APN function $x^3 + \mathrm{tr}_n(x^9)$, it is possible to construct classes of nonquadratic APN mappings with some bent components. The same affine transformations $\mathcal{L}$ as those which gave respectively F and G from Gold functions, when they are applied to the graph of $x^3 + \mathrm{tr}_n(x^9)$ (which is CCZ-inequivalent to Gold), give graphs of functions as well, and some of the components of the resulting CCZ-equivalent APN functions are bent.

Proposition 8 ([7]) *Let n be an even positive integer, $H : \mathbf{F}_{2^n} \to \mathbf{F}_{2^n}$, $H(x) = x^3 + tr_n(x^9)$, then the following functions are CCZ-equivalent to H*

1) *the function with algebraic degree* 3

$$x^3 + tr_n(x^9) + (x^2 + x + 1)tr_n(x^3);$$

2) *for n divisible by* 6 *the function with algebraic degree* 4

$$\left(x + tr_n^3(x^6 + x^{12}) + tr_n(x)tr_n^3(x^3 + x^{12})\right)^3$$
$$+ tr_n\left(\left(x + tr_n^3(x^6 + x^{12}) + tr_n(x)tr_n^3(x^3 + x^{12})\right)^9\right).$$

The bent components of the functions of Proposition 8 have the same algebraic degrees as those of F, resp. G. We could check by a computer that for small values of n the bent components of those functions are equivalent to bent components of F and G, respectively. We do not know if in general the resulting APN functions have bent components inequivalent to those of F and G and it seems difficult to see this mathematically.

Remark 6 Little is known on CCZ-equivalence, which is still not well understood. Since [8] appeared, constructing more infinite classes of functions CCZ-equivalent to Gold (or to other APN functions such as Kasami, which are the other known case of vectorial functions with bent components) and EA-inequivalent to them and to their inverses is an open problem. Nobody knows whether CCZ-equivalence excluding EA-equivalence is rare or not. Note that, as proved in [6], if (L_1, L_2) and (L_1, L_2') are linear permutations and $F_1 = L_1(x, F(x))$ is a permutation as well, then the functions obtained by CCZ-equivalence from F by using (L_1, L_2) and (L_1, L_2') are EA-equivalent; so finding new EA-inequivalent functions by using CCZ-equivalence needs to find new permutations F_1, which is the difficult task. Even finding such permutations for certain values of n may be hard, not to mention finding infinite families. For instance, applying CCZ-equivalence to the trinomial APN function over $\mathbf{F}_{2^6}$ from a family of [2], Dillon et al. constructed an APN permutation over $\mathbf{F}_{2^6}$, by this disproving the conjecture on non-existence of APN permutations over $\mathbf{F}_{2^{2n}}$ [3]. This difficult result is very important for future applications. However, it seems quite difficult to generalize it to a family.

For $n = 12$ we give below another example illustrating the application of CCZ-equivalence in constructions of bent functions.

Example 1 Let α be a primitive element of $\mathbf{F}_{2^{12}}$ and $P : \mathbf{F}_{2^{12}} \to \mathbf{F}_{2^{12}}$, $P(x) = \alpha x^3 + \alpha^{256}x^{528} + \alpha^{257}x^{514}$. The function P is EA-equivalent to the trinomial APN function from [2]. Let

$$L_1 = \mathrm{tr}_{12}^3(y) + \alpha\mathrm{tr}_{12}^3(\alpha^4 x) + \alpha^2\mathrm{tr}_{12}^3(\alpha^{16}x) + \alpha^4\mathrm{tr}_{12}^3(\alpha^{64}x),$$
$$L_2 = \mathrm{tr}_{12}^3(x) + \alpha\mathrm{tr}_{12}^3(\alpha^4 y) + \alpha^2\mathrm{tr}_{12}^3(\alpha^{16}y) + \alpha^4\mathrm{tr}_{12}^3(\alpha^{64}y).$$

Then the linear function (L_1, L_2) is a permutation of $\mathbf{F}_{2^{12}}^2$ and the function $P_1(x) = L_1(x, P(x))$ is a permutation of $\mathbf{F}_{2^{12}}$. Therefore, the function $P' = P_2 \circ P_1^{-1}$, where $P_2(x) = L_2(x, P(x))$, is CCZ-equivalent to P. The function $\mathrm{tr}_{12}(\alpha^9 P(x))$ is bent and has algebraic degree 5, it is EA-inequivalent to any function from MM classes (as checked with a computer). Obviously, it is EA-inequivalent to any bent component of F, F', G, P or any PSap function because of the algebraic degree.

4.7 Non-existence of APN permutations EA-equivalent to functions F and G

Finding APN permutations over $\mathbf{F}_{2^n}$ when n is even is a hard problem. Non-existence of such quadratic functions was proven in [20]. Hence the APN function $F'(x) = x^{2^i+1}$,

$\gcd(i, n) = 1$, n even, is EA-inequivalent to any permutation. However, it is potentially possible that F' is CCZ-equivalent to a nonquadratic APN permutation. For instance, the only known example of an APN permutation for n even is constructed in [3] by applying CCZ-equivalence to a quadratic APN function over $\mathbf{F}_{2^6}$. From this point of view the following facts are interesting.

Corollary 4 *Let n and i be positive integers and $\gcd(i, n) = 1$. If n is even then the APN function F given by (1) is EA-inequivalent to any permutation over $\mathbf{F}_{2^n}$. If $\gcd(n, 18) = 6$ then the APN function G given by (2) is EA-inequivalent to any permutation over $\mathbf{F}_{2^n}$.*

Proof The function F has bent components by Proposition 1, and G has bent components by Proposition 6. Therefore, F and G are not EA-equivalent to any permutation. □

5 New classes of bent vectorial functions in trace representation

Let F be a function from $\mathbf{F}_{2^n}$ to itself and $b \in \mathbf{F}_{2^n}^*$. We know from [19] that, for n divisible by m, the (n, m)-function $\mathrm{tr}_n^m(bF(x))$ is bent if and only if, for any $v \in \mathbf{F}_{2^m}^*$, 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 and i a positive integer not divisible by $n/2$ and such that $n/\gcd(i, n)$ is even. If $b \in \mathbf{F}_{2^n} \backslash \mathbf{F}_{2^i}$ is such that for any $v \in \mathbf{F}_{2^m}^*$, neither bv nor $bv + 1$ are the $(2^i + 1)$-th powers of elements of $\mathbf{F}_{2^n}$, and the function F is given by (1) then the function $f_b(x) = tr_n^m(bF(x))$ is bent and has algebraic degree 3.*

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

Corollary 5 *Let $n \geq 6$ be an even integer, i a positive integer not divisible by $n/2$ and s a divisor of i such that i/s is odd and $\gcd(n, 2s(2^s + 1)) = 2s$. If $b \in \mathbf{F}_{2^{2s}} \backslash \mathbf{F}_{2^s}$ and the function F is given by (1), then the function $f_b(x) = tr_n^s(bF(x))$ is bent and has algebraic degree 3.*

Proof Since $b \in \mathbf{F}_{2^{2s}} \backslash \mathbf{F}_{2^s}$ then $bv \in \mathbf{F}_{2^{2s}} \backslash \mathbf{F}_{2^s}$ for any $v \in \mathbf{F}_{2^s}^*$. Hence by Proposition 2 the functions $\mathrm{tr}_n(bvF(x))$ are bent and cubic for all $v \in \mathbf{F}_{2^s}^*$, and, therefore, $\mathrm{tr}_n^s(bF(x))$ is bent and has algebraic degree 3. □

Theorem 3 also leads to new bent vectorial functions.

Theorem 5 *Let n be a positive integer divisible by 6, $m > 1$ a divisor of n, and i a positive integer not divisible by $n/2$ such that $n/\gcd(i, n)$ is even. Let $b \in \mathbf{F}_{2^n}$ be such that, for any $d \in \mathbf{F}_8$ and any $v \in \mathbf{F}_{2^m}^*$, $bv + d + d^2$ is not the $(2^i + 1)$-th power of an element of $\mathbf{F}_{2^n}$. If the function G is given by (2) then the Boolean function $g_b(x) = tr_n^m(b\,G(x))$ is bent. If, in addition, i is divisible by 3, and $bv \notin \mathbf{F}_{2^i}$ for some $v \in \mathbf{F}_{2^m}^*$ 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 for some $v \in \mathbf{F}_{2^m}^*$ either $bv \notin \mathbf{F}_8$ or $tr_3(bv) \neq 0$.*

Proposition 5 allows us to describe some particular cases of bent vectorial functions of Theorem 5 for i divisible by 3.

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

Proof Since $b \in \mathbf{F}_{2^{6s}} \backslash \mathbf{F}_{2^{3s}}$ then $bv \in \mathbf{F}_{2^{6s}} \backslash \mathbf{F}_{2^{3s}}$ for any $v \in \mathbf{F}^*_{2^{3s}}$. Hence by Proposition 5 the functions $\mathrm{tr}_n(bvF(x))$ are bent and cubic for all $v \in \mathbf{F}^*_{2^{3s}}$, and, therefore, $\mathrm{tr}^{3s}_n(bF(x))$ is bent and cubic. □

Next corollary follows from Proposition 6 and refers to the case where i is not divisible by 3.

Corollary 7 *Let i, n, s be positive integers such that $n \geq 12$, $\gcd(i, 2s) = s$, $\gcd(i, 3) = 1$, and $\gcd(n, 6s(2^{3s} + 1)) = 6s$. If the function G is given by (2) and $b \in \mathbf{F}_{2^{6s}}$ is such that for any $d \in \mathbf{F}_8$ and any $v \in \mathbf{F}^*_{2^{3s}}$ the element $bv + d + d^2$ is not the $(2^s + 1)$-th power in $\mathbf{F}_{2^{6s}}$ then the function $g_b(x) = tr^{3s}_n(bG(x))$ is bent and has algebraic degree 4.*

Since $F'(x) = x^{2^i+1}$ is quadratic, then according to Corollary 1:

Corollary 8 *The bent functions f_b and g_b of Theorems 4 and 5 (and Corollaries 5, 6 and 7, in particular) are CCZ-inequivalent to $tr^m_n(vF'(x))$ for any $v \in \mathbf{F}_{2^n}$ and any divisor m of n.*

Remark 7 To our knowledge there are only three known infinite classes of vectorial bent functions expressed in trace representation $\mathrm{tr}^m_n(F(x))$: the function $\mathrm{tr}^m_n(x^{2^{n/2}+1})$ (which is a Maiorana McFarland function), the function $\mathrm{tr}^m_n(wx^d)$ where n is congruent to 2 mod 4, $d = 2^i + 1$ is a Gold exponent (with $(i, n) = 1$) and w is not a cube, and the function $\mathrm{tr}^m_n(wx^d)$ where n is congruent to 2 mod 4, $d = 4^i - 2^i + 1$ is a Kasami exponent (with $(i, n) = 1$) and w is not a cube (see [11]). The functions we obtain in this section are inequivalent to these functions and so they are new in this sense: Corollary 8 shows that the constructed vectorial bent functions are not CCZ-equivalent to the functions with Gold exponents indicated above; inequivalence to the functions above with Kasami eponents can be easily seen for any n divisible by 4 (because Kasami type bent functions are not defined then) and any n divisible by 6 since the constructed bent vectorial functions have algebraic degree 3 or 4 while for n divisible by 6 there exists no Kasami function of algebraic degree 3 or 4 (Kasami type bent functions have algebraic degree $i + 1$).

6 Conclusion

The notion of equivalence for APN and AB functions (and more generally for vectorial functions usable as S-boxes in block ciphers), called CCZ-equivalence, which seems to be in the same time the most general and the most adapted to this cryptographic framework, is delicate to handle: checking whether two given functions are CCZ-equivalent or not may be quite hard if they share the same CCZ-invariant parameters (while checking whether they are EA-equivalent or not is easier). Hence, identifying cases where CCZ-equivalence reduces to EA-equivalence is useful. We observe that, in the framework of bent functions, the complex CCZ-equivalence coincides with the simple EA-equivalence.

This seems to mean that, starting from known bent vectorial functions and using CCZ-equivalence, constructing new EA-inequivalent bent functions is impossible, contrary to what has been observed with APN functions. This is in fact possible (and this illustrates the nice possibilities offered by CCZ-equivalence) if instead of starting from bent functions, we use non-bent functions having bent components. Starting from Gold functions and considering two classes of APN functions which have been shown CCZ-equivalent to them, we derived two infinite classes of bent Boolean functions which are CCZ-inequivalent to the bent components of the Gold functions, and we also deduced new families of vectorial bent functions.

Acknowledgment We would like to thank Gregor Leander for useful discussions.

References

1. Biham E., Shamir A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991).
2. Bracken C., Byrne E., Markin N., McGuire G.: New families of quadratic almost perfect nonlinear trinomials and multinomials. Finite Fields Appl. **14**, 703–714 (2008).
3. Browning K.A., Dillon J.F., McQuistan M.T., Wolfe A.J.: An APN permutation in dimension six. Postproceedings of the 9th International Conference on Finite Fields and their Applications Fq'9. Contemporary Mathematics Journal of American Mathematical Society, vol. 518, pp. 33–42 (2010).
4. Budaghyan L., Carlet C.: CCZ-equivalence of single and multi output Boolean functions. Postproceedings of the 9th International Conference on Finite Fields and their Applications Fq'9. Contemporary Mathematics Journal of American Mathematical Society, vol. 518, pp. 43–54 (2010).
5. Budaghyan L., Helleseth T.: New perfect nonlinear multinomials over $\mathbf{F}_{p^{2k}}$ for any odd prime p. In: Proceedings of SETA 2008, Lecture Notes in Computer Science, vol. 5203, pp. 401–414 (2008).
6. Budaghyan L., Carlet C., Leander G.: Two classes of quadratic APN binomials inequivalent to power functions. IEEE Trans. Inform. Theory **54**(9), 4218–4229 (2008).
7. Budaghyan L., Carlet C., Leander G.: Constructing new APN functions from known ones. Finite Fields Appl. **15**(2), 150–159 (2009).
8. Budaghyan L., Carlet C., Pott A.: New classes of almost bent and almost perfect nonlinear functions. IEEE Trans. Inform. Theory **52**(3), 1141–1152 (2006).
9. Carlet C.: Vectorial Boolean Functions for Cryptography. In: Crama Y., Hammer P. (eds.) Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 398–469. Cambridge University Press, London (2010). Preliminary version available at http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.
10. Carlet C.: Boolean Functions for Cryptography and Error correcting codes. In: Crama Y., Hammer P. L. (eds.) Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", pp. 257–397. Cambridge University Press (2010).
11. Carlet C.: Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. Des. Codes Cryptogr. (this special issue).
12. Carlet C., Ding C.: Highly nonlinear mappings. Special issue "Complexity Issues in Coding and Cryptography", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday. J. Complex. **20**, 205–244 (2004).
13. Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**(2), 125–156 (1998).
14. Dillon J.F.: Elementary hadamard difference sets. Ph.D. Thesis, University of Maryland (1974).
15. Kyureghyan G., Pott A.: Some theorems on planar mappings. In: Proceedings of WAIFI 2008, Lecture Notes in Computer Science, vol. 5130, pp. 115–122 (2008).
16. Leander G.: Monomial bent functions. In: Proceedings of the Workshop on Coding and Cryptography 2005, pp. 462–470. Bergen (2005).
17. Leander G.: Monomial bent functions. IEEE Trans. Inf. Theory **52**(2), 738–743 (2006).
18. Matsui M.: Linear cryptanalysis method for DES cipher. In: Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, pp. 386–397 (1994).
19. Nyberg K.: Perfect non-linear S-boxes. In: Proceedings of EUROCRYPT' 91, Lecture Notes in Computer Science, vol. 547, pp. 378–386 (1992).
20. Nyberg K.: S-boxes and round functions with controllable linearity and differential uniformity. In: Proceedings of Fast Software Encryption, Lecture Notes in Computer Science, vol. 1008, pp. 111–130 (1994).