CCZ-equivalence and Boolean functions

Lilya Budaghyan* and Claude Carlet†

Abstract

We study further CCZ-equivalence of (n, m)-functions. We prove that for Boolean functions (that is, for $m = 1$), CCZ-equivalence coincides with EA-equivalence. On the contrary, we show that 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. Our result on Boolean functions allows us to study the natural generalization of CCZ-equivalence corresponding to the CCZ-equivalence of the indicators of the graphs of the functions. We show that it coincides with CCZ-equivalence.

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 came later in [2]), seems to be the proper notion of equivalence for vectorial functions used as S-boxes in cryptosystems and has led to new APN and AB functions. 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 to an optimal resistance to the differential

*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

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 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), then F' is also AB. In fact, these two central notions for the design of S-boxes in block ciphers, APNness and ABness, can be expressed in a natural way by means of the graph of the S-box and this is why CCZ-equivalence is the proper notion of equivalence in this framework.

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 $F' = L' \circ F \circ L + L''$ (if $L'' = 0$ and L, L' are linear, the functions are called linearly equivalent). EA-equivalence is a particular case of CCZ-equivalence [4].

In the present paper we investigate the question of knowing whether CCZ-equivalence of (n, m)-functions is strictly more general than their EA-equivalence. We already know that the answer to this question is yes when $n = m$ since every permutation is CCZ-equivalent to its inverse and, moreover, as shown in [2], CCZ-equivalence is still more general than the EA-equivalence of the functions or their inverses (when they exist). A result in the other sense has been proven in [1]: CCZ-equivalence coincides with EA-equivalence when applied to bent (n, m)-functions, that is, to functions whose derivatives $D_aF(x) = F(x) + F(x + a)$, $a \neq 0$, are balanced (i.e. uniformly distributed over $\mathbb{F}_2^m$; bent functions exist only for n even and $m \leq n/2$, see [6]). The question is open for general (n, m)-functions when $n \neq m$. In Subsection 2.1 we prove that the answer is also negative for (n, m)-functions when $m = 1$, that is, for Boolean functions. This poses then the question of knowing whether the case $m = 1$ is a particular case or if the same situation occurs for larger values of m. We give a partial answer to this question in Subsection 2.2 by showing that CCZ-equivalence of (n, m)-functions is strictly more general than their EA-equivalence when $n \geq 5$ and m is greater or equal to the smallest positive divisor of n different from 1.

The question of knowing whether a notion still more general than CCZ-equivalence for vectorial functions has been raised by several authors. A notion having potentially such property, that we call ECCZ-equivalence, is introduced and studied in Section 3.

2 CCZ-equivalence of (n, m)-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 $\mathbb{F}_{2^n}$ of degree smaller than 2^n

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

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,

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

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, $0 \leq k \leq 2^n-1$, the number $w_2(k)$ of nonzero coefficients k_s, $0 \leq k_s \leq 1$, 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,

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

The algebraic degree of a function (if it is not linear) is invariant under EA-equivalence but it is not preserved by CCZ-equivalence. This has been proved in [2]. Let us recall why the structure of CCZ-equivalence implies this: for an (n,m)-function F and an affine permutation $\mathcal{L}(x,y) = \big(L_1(x,y), L_2(x,y)\big)$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ the set $\mathcal{L}(G_F)$ equals $\{(F_1(x), F_2(x)) : x \in \mathbb{F}_2^n\}$ where $F_1(x) = L_1(x, F(x)), F_2(x) = L_2(x, F(x))$. It is the graph of a function if and only if the function F_1 is a permutation. The function CCZ-equivalent to F whose graph equals $\mathcal{L}(G_F)$ is then $F' = F_2 \circ F_1^{-1}$. The composition by the inverse of F_1 modifies in general the algebraic degree (examples are given in [2]).

2.1 CCZ-equivalence of Boolean functions

We first consider the question whether CCZ-equivalence is strictly more general than EA-equivalence for Boolean functions. Let a Boolean function f' be CCZ-equivalent to a Boolean function f and EA-inequivalent to it. Then there exist linear functions $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$, and $l : \mathbb{F}_2^n \to \mathbb{F}_2$, and elements $a \in \mathbb{F}_2^n \setminus \{0\}$, $\eta \in \mathbb{F}_2$, such that

$$\mathcal{L}(x,y) = \big(L(x) + ay, l(x) + \eta y\big) \tag{1}$$

is a linear permutation of $\mathbb{F}_2^n \times \mathbb{F}_2$, and for

$$F_1(x) = L(x) + af(x) \quad (2)$$
$$F_2(x) = l(x) + \eta f(x), \quad (3)$$

F_1 is a permutation of $\mathbb{F}_2^n$ and

$$f'(x) = F_2 \circ F_1^{-1}(x). \quad (4)$$

Hence we need characterizing the permutations of the form (2). Note that for any permutation (2) the function L must be either a permutation or 2-to-1. Thus, we have only two possibilities for the function F_1, that is, either

$$F_1(x) = L\big(x + L^{-1}(a)f(x)\big)$$

when L is a permutation, or

$$F_1(x) = L'\Big((x/b)^2 + x/b + L'^{-1}(a)f(x)\Big) \quad (5)$$

when L is 2-to-1 and its kernel equals $\{0, b\}$ where $b \in \mathbb{F}_{2^n}^*$, and L' is a linear permutation of $\mathbb{F}_{2^n}$ such that $L'\big((x/b)^2 + x/b\big) = L(x)$. Note that if we take $L^{-1} \circ F_1$ (when L is a permutation) or $L'^{-1} \circ F_1$ (when L is 2-to-1) in (4) instead of F_1 then we get $f' \circ L$ and $f' \circ L'$, respectively, which are EA-equivalent to f'. Therefore, without loss of generality we can neglect L and L'. Then (5) gives

$$F_1(x) = (x/b)^2 + x/b + af(x) \quad (6)$$
$$F_1(bx) = x^2 + x + af(bx) = x^2 + x + ag(x) \quad (7)$$

where $g(x) = f(bx)$. Hence it is sufficient to consider permutations (2) of the following two types

$$x + af(x) \quad (8)$$
$$x^2 + x + af(x). \quad (9)$$

A lemma will simplify the study of permutations (2):

Lemma 1 *Let n be any positive integer, a any nonzero element of $\mathbb{F}_{2^n}$ and f a Boolean function on $\mathbb{F}_{2^n}$.*
- The function $F(x) = x + af(x)$ is a permutation over $\mathbb{F}_{2^n}$ if and only if F is an involution.
- The function $F'(x) = x + x^2 + af(x)$ is a permutation over $\mathbb{F}_{2^n}$ if and only if $\mathrm{tr}_n(a) = 1$ and $f(x+1) = f(x) + 1$ for every $x \in \mathbb{F}_{2^n}$. Under this condition,

let H be any linear hyperplane of $\mathbb{F}_{2^n}$ not containing 1; for every $y \in \mathbb{F}_{2^n}$, there exists a unique element $\phi(y) \in \mathbb{F}_{2^n}$ such that $\phi(y) \in H$ and

$$\begin{array}{rcl} \phi(y) + (\phi(y))^2 = y & \text{if} & \mathrm{tr}_n(y) = 0 \\ \phi(y) = \phi(y+a) + 1 & \text{if} & \mathrm{tr}_n(y) = 1. \end{array}$$

Then ϕ is a linear automorphism of $\mathbb{F}_{2^n}$ and we have

$$F'^{-1}(y) = \phi(y) + \mathrm{tr}_n(y) + f(\phi(y))$$

for every $y \in \mathbb{F}_{2^n}$.

Proof. Let us assume that F is a permutation. We have

$$F \circ F(x) = x + af(x) + af(x + af(x)).$$

If $f(x) = 0$ then obviously $F \circ F(x) = x$. If $f(x) = 1$ then $F \circ F(x) = x + a + af(x+a)$. Moreover, we have $f(x+a) = 1$ since otherwise $F(x+a) = F(x)$ which contradicts F being a permutation. Hence, when $f(x) = 1$, we have also $F \circ F(x) = x$. Hence, $F^{-1} = F$.

If F' is a permutation over $\mathbb{F}_{2^n}$, then $\mathrm{tr}_n(a) = 1$ since otherwise we have $\mathrm{tr}_n(F'(x)) = 0$ for every $x \in \mathbb{F}_{2^n}$ (and F' is not surjective), and $f(x+1) = f(x) + 1$ for every x since if $f(x+1) = f(x)$ for some $x \in \mathbb{F}_{2^n}$, then $F'(x+1) = F'(x)$ and F' is not injective. Conversely, if $\mathrm{tr}_n(a) = 1$ and $f(x+1) = f(x) + 1$ for every $x \in \mathbb{F}_{2^n}$ then, for every $x, y \in \mathbb{F}_{2^n}$, we have $F'(x) = y$ if and only if:
- either $\mathrm{tr}_n(y) = f(x) = 0$ and x is the unique element of $\mathbb{F}_{2^n} \setminus supp(f)$ such that $x + x^2 = y$;
- or $\mathrm{tr}_n(y) = f(x) = 1$ and x is the unique element of $supp(f)$ such that $x + x^2 = y + a$.

Hence, F' is a permutation over $\mathbb{F}_{2^n}$.
Moreover, since $\mathrm{tr}_n(a) = 1$ and $f(x+1) = f(x)+1$ for every $x \in \mathbb{F}_{2^n}$, we have $F'^{-1}(y+a) = F'^{-1}(y) + 1$ for every $y \in \mathbb{F}_{2^n}$. The existence and uniqueness of $\phi(y)$ is straightforward. The restriction of ϕ to the hyperplane of equation $\mathrm{tr}_n(y) = 0$ is an isomorphism between this hyperplane and H. The restriction of ϕ to the hyperplane of equation $\mathrm{tr}_n(y) = 1$ is an isomorphism between this hyperplane and $\mathbb{F}_{2^n} \setminus H$. Hence ϕ is a linear automorphism of $\mathbb{F}_{2^n}$. Moreover, for every $x, y \in \mathbb{F}_{2^n}$, we have $F'(x) = y$ if and only if:
- either $\mathrm{tr}_n(y) = f(x) = 0$ and $x = \phi(y) + f(\phi(y))$ (indeed, if $\phi(y) \notin supp(f)$ then $\phi(y)$ is the unique element x of $\mathbb{F}_{2^n} \setminus supp(f)$ such that $x + x^2 = y$ and if $\phi(y) \in supp(f)$ then $\phi(y) + 1$ is the unique element x of $\mathbb{F}_{2^n} \setminus supp(f)$ such

that $x+x^2=y$ since $f(x+1)=f(x)+1$);
- or $\mathrm{tr}_n(y)=f(x)=1$ and

$$x=F'^{-1}(y+a)+1=\phi(y+a)+f(\phi(y+a))+1=\phi(y)+1+f(\phi(y)).$$

This completes the proof. $\square$

We deduce the main result of this subsection:

Theorem 1 *Two Boolean functions of $\mathbb{F}_{2^n}$ are CCZ-equivalent if and only if they are EA-equivalent.*

Proof. Assume that two Boolean functions f and f' on $\mathbb{F}_{2^n}$ are CCZ-equivalent and EA-inequivalent. Then there is a linear permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}^2$ such that (1)-(4) take place. We first assume that $\eta=1$.

In case L is a permutation, we have $F_1(x)=L\big(x+L^{-1}(a)f(x)\big)$ and therefore by Lemma 1

$$F_1^{-1}(x)=L^{-1}(x)+L^{-1}(a)f(L^{-1}(x)).$$

Then we have

$$\begin{aligned} f'(L(x)) &= l(F_1^{-1}(L(x)))+f(F_1^{-1}(L(x))) \\ &= l\big(x+L^{-1}(a)f(x)\big)+f\big(x+L^{-1}(a)f(x)\big). \end{aligned}$$

If $f(x)=0$ then $f'(L(x))=l(x)$. If $f(x)=1$ then we have $f(x+L^{-1}(a))=1$. Indeed, since a is assumed to be nonzero, and F_1 being a permutation, we have $L(x+L^{-1}(a)+L^{-1}(a)f(x+L^{-1}(a)))=F_1(x+L^{-1}(a))\neq F_1(x)=L(x+L^{-1}(a))$. Hence, $f'(L(x))=l(x)+l(L^{-1}(a))+1$ when $f(x)=1$. Therefore,

$$f'(L(x))=l(x)+\big(1+l(L^{-1}(a))\big)f(x).$$

Note that $l(L^{-1}(a))=0$. Indeed, if $l(L^{-1}(a))=1$ then the system of equations

$$\begin{aligned} L(x)+ay &= 0 \\ l(x)+y &= 0 \end{aligned}$$

has two solutions $(0,0)$ and $(L^{-1}(a),1)$ which contradicts $\mathcal{L}$ being a permutation. Hence, $f'(x)=l(L^{-1}(x))+f(L^{-1}(x))$ and f is EA-equivalent to f', a contradiction.

Let L be now 2-to-1. Then, as observed above, we can assume without loss of generality that (6) and (7) take place. Then, since $\mathcal{L}$ is bijective, we have $l(b)=1$ (otherwise, the vector $(b,0)$ would belong to the kernel of $\mathcal{L}$). By Lemma 1, we have $g(x+1)=g(x)+1$ for any $x\in\mathbb{F}_{2^n}$, that is, $f(bx+b)=f(bx)+1$ for any $x\in\mathbb{F}_{2^n}$, that is, $f(x+b)=f(x)+1$ for any $x\in\mathbb{F}_{2^n}$. By Lemma 1, the inverse of the function $x^2+x+ag(x)$ equals $\phi(x)+\mathrm{tr}_n(x)+g(\phi(x))$ for a certain linear permutation ϕ of $\mathbb{F}_{2^n}$. Then

$$F_1^{-1}(x)=b\big(\phi(x)+\mathrm{tr}_n(x)+f(b\ \phi(x))\big)$$

and therefore

$$\begin{aligned}
f'(x) &= l\Big(b\big(\phi(x)+\mathrm{tr}_n(x)+f(b\ \phi(x))\big)\Big)+f\Big(b\big(\phi(x)+\mathrm{tr}_n(x)+f(b\ \phi(x))\big)\Big)\\
&= l(b\phi(x))+\mathrm{tr}_n(x)+f\big(b\ \phi(x)\big)+f\big(b\ \phi(x)\big)+\mathrm{tr}_n(x)+f\big(b\ \phi(x)\big)\\
&= l(b\phi(x))+f(b\ \phi(x)).
\end{aligned}$$

This means that f and f' are EA-equivalent, a contradiction.

According to the observations above and to Lemma 1, if $\eta=0$ then we can reduce ourselves to the cases $f'(x)=l(x+af(x))$ and $f'(x)=l\Big(b\big(\phi(x)+\mathrm{tr}_n(x)+f(b\ \phi(x))\big)\Big)$. For the first case we necessarily have $l(a)=1$ and for the second case $l(b)=1$ since otherwise the kernel of $\mathcal{L}$ would not be trivial (it would contain $(a,1)$ and $(b,0)$ respectively). Thus, $f'(x)=l(x)+f(x)$ or $f'(x)=l(b\ \phi(x))+\mathrm{tr}_n(x)+f(b\ \phi(x))$, and therefore f and f' are EA-equivalent, a contradiction. $\square$

A Boolen function f of $\mathbb{F}_{2^n}$ can be considered as a function form $\mathbb{F}_{2^n}$ to itself. Hence it is a natural question whether an (n,n)-function f', which is CCZ-equivalent to f, is necessarily EA-equivalent to a Boolean function, or even EA-equivalent to f. The theorem below shows that the answer is positive.

Theorem 2 *Let f be a Boolen function of $\mathbb{F}_{2^n}$ and f' a function from $\mathbb{F}_{2^n}$ to itself. Then f and f' are CCZ-equivalent as (n,n)-functions if and only if they are EA-equivalent as (n,n)-functions.*

Proof. If f and f' are CCZ-equivalent as (n,n)-functions then their is a linear permutation $\mathcal{L}(x,y)=(L_1(x,y),L_2(x,y))$ of $\mathbb{F}_{2^n}^2$ such that $F_1(x)=L_1(x,f(x))$ is a permutation of $\mathbb{F}_{2^n}$ and $f'=F_2\circ\mathbb{F}_1^{-1}$ for $F_2(x)=L_2(x,f(x))$. As we saw above it is sufficient to consider only the cases

$$\begin{aligned}
L_1(x,y) &= x+ay, &(10)\\
L_1(x,y) &= (x/b)^2+x/b+ay, &(11)
\end{aligned}$$

where $a, b \in \mathbb{F}_{2^n}^*$. We have $L_2(x, y) = L'(x) + L''(y)$ for some linear functions L' and L'' from $\mathbb{F}_{2^n}$ to itself, and

$$F_2(x) = L'(x) + L''(f(x)) = L'(x) + L''(1)f(x).$$

Since $\mathcal{L}$ is a permutation then the system

$$\begin{aligned} x + ay &= 0 \\ L'(x) + L''(y) &= 0 \end{aligned}$$

in case (10), and the system

$$\begin{aligned} (x/b)^2 + x/b + ay &= 0 \\ L'(x) + L''(y) &= 0 \end{aligned}$$

in case (11), must have only $(0, 0)$ solution. Hence, $L'(a) \neq L''(1)$ for case (10) (since otherwise $(a, 1)$ is in the kernel of $\mathcal{L}$), and $L'(b) \neq 0$ for case (11) (since otherwise $(b, 0)$ is in the kernel of $\mathcal{L}$).

Using Lemma 1 in case (10) we get

$$\begin{aligned} f'(x) &= F_2 \circ F_1^{-1}(x) = L'\big(x + af(x)\big) + L''(1)f\big(x + af(x)\big) \\ &= L'(x) + \big(L'(a) + L''(1)\big)f(x) \end{aligned}$$

since $f(x + af(x)) = f(x)$ as we see it in the proof of Lemma 1. Hence f and f' are EA-equivalent as (n, n)-functions.

Applying Lemma 1 for case (11) we get

$$\begin{aligned} f'(x) &= F_2 \circ F_1^{-1}(x) = L'\Big(b\big(\phi(x) + \mathrm{tr}_n(x) + f(b\ \phi(x))\big)\Big) \\ &\quad + L''(1)f\Big(b\big(\phi(x) + \mathrm{tr}_n(x) + f(b\ \phi(x))\big)\Big) \\ &= L'(b\ \phi(x)) + L'(b)\,\mathrm{tr}_n(x) + L'(b)f(b\ \phi(x)) \\ &\quad + L''(1)f(b\ \phi(x)) + L''(1)\,\mathrm{tr}_n(x) + L''(1)f(b\ \phi(x)) \\ &= \Big(L'(b\ \phi(x)) + L'(b)\,\mathrm{tr}_n(x) + L''(1)\,\mathrm{tr}_n(x)\Big) + L'(b)f(b\ \phi(x)) \end{aligned}$$

since $f(x + b) = f(x) + 1$ as we see it from the proof of Lemma 1. Thus f and f' are EA-equivalent as (n, n)-functions. □

2.2 CCZ-equivalence and EA-equivalence of (n, m)-functions when $1 < m < n$

We first show in Proposition 1 that there exist values of (n, m) such that CCZ-equivalence is strictly more general than EA-equivalence. We extend then in Theorem 3, thanks to Proposition 2, the hypotheses under which this is true.

Proposition 1 *Let $n \geq 5$ and $m > 1$ be any divisor of n, or $n = m = 4$. Then for (n,m)-functions CCZ-equivalence is strictly more general than EA-equivalence.*

Proof. We need to treat the cases n odd and n even differently.
- Let n be any odd positive integer, m any divisor of n and

$$F(x) = \mathrm{tr}_{n/m}(x^3). \tag{12}$$

The linear function from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ to itself:

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

is an involution, and

$$F_1(x) = L_1(x, F(x)) = x + \mathrm{tr}_n(x) + \mathrm{tr}_n(x^3)$$

is an involution too (which is easy to check). Let:

$$F_2(x) = L_2(x, F(x)) = \mathrm{tr}_{n/m}(x^3) + \mathrm{tr}_n(x) + \mathrm{tr}_n(x^3)$$

then the function:

$$\begin{aligned} F'(x) &= F_2 \circ F_1^{-1}(x) = F_2 \circ F_1(x) \\ &= \mathrm{tr}_{n/m}(x^3) + \mathrm{tr}_{n/m}(x^2+x)\,\mathrm{tr}_n(x) + \mathrm{tr}_{n/m}(x^2+x)\,\mathrm{tr}_n(x^3) \end{aligned}$$

is CCZ-equivalent to F by definition.
The part $\mathrm{tr}_{n/m}(x^2+x)\,\mathrm{tr}_n(x^3)$ is nonquadratic for $n \geq 5$ and $m > 1$. Indeed,

$$\mathrm{tr}_{n/m}(x^2+x)\,\mathrm{tr}_n(x^3) = \sum_{\substack{0 \leq i < n \\ 0 \leq j < n/m}} x^{2^{i+1}+2^i+2^{jm}} + \sum_{\substack{0 \leq i < n \\ 0 \leq j < n/m}} x^{2^{i+1}+2^i+2^{jm+1}} \tag{13}$$

and for $n \geq 5$, $m > 1$, the item $x^{2^3+2^2+2^0}$ does not vanish in the sum above. By construction the (n,m)-functions F and F' are CCZ-equivalent. When $n \geq 5$ and $m > 1$ they are EA-inequivalent because they have different algebraic degrees.
- Let now n be any even positive integer, m any divisor of n and F be given by (12). The linear function

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

is an involution, and

$$F_1(x) = L_1(x, F(x)) = x + \mathrm{tr}_n(x^3)$$

is also involutive (this can be easily checked). Let:

$$F_2(x) = L_2(x, F(x)) = \mathrm{tr}_{n/m}(x^3)$$

then

$$\begin{aligned} F'(x) &= F_2 \circ F_1^{-1}(x) = F_2 \circ F_1(x) = \mathrm{tr}_{n/m}\left(\left(x + \mathrm{tr}_n(x^3)\right)^3\right) \\ &= \mathrm{tr}_{n/m}(x^3) + \mathrm{tr}_{n/m}(1)\,\mathrm{tr}_n(x^3) + \mathrm{tr}_{n/m}(x^2 + x)\,\mathrm{tr}_n(x^3). \end{aligned}$$

The part $\mathrm{tr}_{n/m}(x^2 + x)\,\mathrm{tr}_n(x^3)$ is nonquadratic when $n \geq 6$, $m > 1$, or when $n = m = 4$. Indeed, in these cases the item $x^{2^3+2^2+2^0}$ does not vanish in (13). Hence, the (n, m)-functions F and F' are CCZ-equivalent by construction, and when $n \geq 6$, $m > 1$, or when $n = m = 4$ they are EA-inequivalent because of the difference of their algebraic degrees. □

The next proposition will allow us to generalize the conditions under which the statement of Proposition 1 is valid.

Proposition 2 *If there exist CCZ-equivalent (n, m)-functions F and F' which are EA-inequivalent then for any positive integer k the $(n, m + k)$-functions $H(x) = (F(x), 0)$ and $H'(x) = (F'(x), 0)$ are also CCZ-equivalent and EA-inequivalent.*

Proof. Let

$$L(x, y) = (L_1(x, y), L_2(x, y))$$

be a linear permutation of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ which maps the graph of F to the graph of F'. Then we have:

$$\begin{aligned} F_1(x) &= L_1(x, F(x)), \\ F_2(x) &= L_2(x, F(x)), \\ F'(x) &= F_2 \circ F_1^{-1}(x), \end{aligned}$$

where F_1 is a permutation. Let

$$\psi(x, (y, z)) = (\psi_1(x, (y, z)), \psi_2(x, (y, z)))$$

be a function from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^k}$ to itself, where

$$\psi_1(x, (y, z)) = L_1(x, y) + L_0(z)$$

for some linear function L_0 from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^n}$, and where

$$\psi_2(x, (y, z)) = (L_2(x, y), z).$$

ψ is linear and it is a permutation; indeed its kernel is the set of solutions of the system of two linear equations

$$\begin{aligned} L_1(x,y) + L_0(z) &= 0 \\ (L_2(x,y), z) &= 0. \end{aligned}$$

From the second equation we get $z = 0$, and since L_0 is linear then $L_0(0) = 0$ and we come down to the system

$$\begin{aligned} L_1(x,y) &= 0 \\ L_2(x,y) &= 0 \end{aligned}$$

which has only solution $(0,0)$. Hence the kernel of ψ is trivial. Denote $H_1(x) = \psi_1(x, H(x))$ and $H_2(x) = \psi_2(x, H(x))$ then

$$H_1(x) = \psi_1(x, H(x)) = \psi_1\big(x, (F(x), 0)\big) = L_1(x, F(x)) + L_0(0) = F_1(x)$$

which is a permutation and

$$H_2(x) = \psi_2(x, H(x)) = \psi_2(x, (F(x), 0)) = \big(L_2(x, F(x)), 0\big) = (F_2(x), 0).$$

Hence,

$$H'(x) = H_2 \circ H_1^{-1}(x) = \big(F_2 \circ F_1^{-1}(x), 0\big) = (F'(x), 0)$$

is CCZ-equivalent to $H(x)$. If F and F' are EA-inequivalent then obviously H and H' are EA-inequivalent too. $\square$

Proposition 1 and Proposition 2 give

Theorem 3 *Let $n \geq 5$ and $k > 1$ be the smallest divisor of n. Then for any $m \geq k$, the CCZ-equivalence of (n,m)-functions is strictly more general than their EA-equivalence.*

In particular, when $n \geq 6$ is even, this is true for every $m \geq 2$.

Remark.
The paper [5] is dedicated to the study of permutations of the kind $G(x) + f(x)$ where f is a Boolean function of $\mathbb{F}_{2^n}$ and G is either a permutation or a linear function from $\mathbb{F}_{2^n}$ to itself. Lemma 1 gives us a description of the inverses of all such permutations:

Corollary 1 *Let L be a linear function from $\mathbb{F}_{2^n}$ to itself and f be a Boolean function of $\mathbb{F}_{2^n}$. If $F(x) = L(x) + f(x)$ is a permutation then F^{-1} is EA-equivalent to F.*

Corollary 2 *Let G be a permutation of $\mathbb{F}_{2^n}$ and f be a Boolean function of $\mathbb{F}_{2^n}$. If $F(x) = G(x) + f(x)$ is a permutation then*

$$F^{-1}(x) = G^{-1}(x) + G^{-1} \circ f \circ G^{-1}(x).$$

Proof. We have $F(x) = G \circ H(x)$, where $H(x) = x + G^{-1} \circ f(x)$ is a permutation. H is involutive by Lemma 1. Hence

$$F^{-1}(x) = H^{-1} \circ G^{-1}(x) = H \circ G^{-1}(x) = G^{-1}(x) + G^{-1} \circ f \circ G^{-1}(x).$$

□

3 Consequence on a notion of equivalence of vectorial functions whose definition is more general than CCZ-equivalence

It is not hard to check that CCZ-equivalence of functions is the same as EA-equivalence of the graphs of these functions. Indeed, for a given function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, let us denote the indicator of its graph G_F by 1_{G_F}, that is,

$$1_{G_F}(x, y) = \begin{cases} 1 & \text{if} \quad y = F(x) \\ 0 & \text{otherwise,} \end{cases}$$

1_{G_F} is a Boolean function over $\mathbb{F}_2^{n+m}$. It is obvious that when composing 1_{G_F} by an affine permutation $\mathcal{L}$ of $\mathbb{F}_2^{n+m}$ on the right, that is, taking $1_{G_F} \circ \mathcal{L}$, we are within the definition of CCZ- equivalence of functions. If we compose 1_{G_F} by an affine permutation $\mathcal{L}$ of $\mathbb{F}_2$ on the left, then we get $\mathcal{L} \circ 1_{G_F} = 1_{G_F} + b$ for $b \in \mathbb{F}_2$. Hence, we have only to prove that if for an (n, m)-function F' and for an affine Boolean function φ of $\mathbb{F}_2^{n+m}$

$$1_{G_{F'}}(x, y) = 1_{G_F}(x, y) + \varphi(x, y)$$

then F and F' are CCZ-equivalent. In case $m > 2$ we must have $\varphi = 0$ because 1_{G_F} and $1_{G_{F'}}$ have Hamming weight 2^n while, if φ is not null, it has then Hamming weight 2^{n+m-1} or 2^{n+m}, a contradiction, since $2^{n+m-1} > 2^{n+1}$. Thus, for $m > 2$ we get $F = F'$. Let us consider now the case $m = 1$. Then $1_{G_F}(x, y) = F(x) + y + 1$ and $\varphi(x, y) = A(x) + ay + b$ for some affine Boolean function A of $\mathbb{F}_2^n$ and $a, b \in \mathbb{F}_2$. Therefore,

$$1_{G_{F'}}(x, y) = 1_{G_F}(x, y) + \varphi(x, y) = F(x) + A(x) + (a + 1)y + b + 1.$$

If $a=1$ then $1_{G_{F'}}$ is not an indicator of a graph of a function since $1_{G_{F'}}(x,0) = 1_{G_{F'}}(x,1) = 1$ when $F(x)+A(x)=b$. If $a=0$ then $1_{G_{F'}}(x,y)=1$ if and only if $y=F(x)+A(x)+b$, that is, $F'(x)=F(x)+A(x)+b$ and F and F' are EA-equivalent and therefore CCZ-equivalent. Let now $m=2$. Then φ has Hamming weight 2^{n+1} while 1_{G_F} and $1_{G_{F'}}$ have Hamming weight 2^n. Therefore, $\varphi(x,F(x))=1$ for any $x\in\mathbb{F}_2^n$. Besides, since $1_{G_{F'}}$ is the indicator of the graph of a function then for any $x\in\mathbb{F}_2^n$ there is a unique $\alpha_x\in\mathbb{F}_4$, $\alpha_x\neq F(x)$, that $\varphi(x,\alpha_x)=1$. Withought loss of generality we can assume that $F(0)=0$. Then $\varphi(0,0)=\varphi(0,F(0))=1$. We also have $\varphi(0,\alpha_0)=1$ and $\varphi(0,\beta)=0$ for any $\beta\in\mathbb{F}_4\setminus\{0,\alpha_0\}$. Since φ is affine then for any $x\in\mathbb{F}_2^n$ we have $\varphi(x,F(x)+\alpha_0)=\varphi(x,F(x))+\varphi(0,\alpha_0)+1=1$ and $\varphi(x,F(x)+\beta)=\varphi(x,F(x))+\varphi(0,\beta)+1=0$. Thus, $1_{G_{F'}}(x,y)=1$ if and only if $y=F(x)+\alpha_0$, that is, $F'(x)=F(x)+\alpha_0$.

Hence, (n,m)-functions F and F' are CCZ-equivalent if and only if the graphs of F and F' are EA-equivalent. A natural question is to know whether CCZ-equivalence of the graphs is more general than their EA-equivalence.

Definition 1 *Two (n,m)-functions F and F' are called ECCZ-equivalent if the indicators of their graphs $G_F=\{(x,F(x));\,x\in F_2^n\}$ and $G_{F'}=\{(x,F'(x));\,x\in F_2^n\}$ are CCZ-equivalent.*

According to Theorem 1 we have:

Corollary 3 *Let F and F' be two (n,m)-functions. F and F' are ECCZ-equivalent if and only if they are CCZ-equivalent.*

References

[1] L. Budaghyan and C. Carlet. On CCZ-equivalence and its use in secondary constructions of bent functions. Preprint available at IACR ePrint Archive, number 2009/042.

[2] 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.

[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] P. Charpin, G. Kyureghyan. On a class of permutation polynomials over $\mathbb{F}_{2^n}$. *Proceedings of SETA 2008*, Lecture Notes in Computer Science 5203, pp. 368-376, 2008.

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