On relations between CCZ- and EA-equivalences

L. Budaghyan[a], M. Calderini[a], I. Villa[a]

[a]*Department of informatics, University of Bergen*

Abstract

In the present paper we introduce some sufficient conditions and a procedure for checking whether, for a given function, CCZ-equivalence is more general than EA-equivalence together with taking inverses of permutations. It is known from [7, 5] that for quadratic APN functions (both monomial and polynomial cases) CCZ-equivalence is more general. We prove hereby that for non-quadratic APN functions CCZ-equivalence can be more general (by studying the only known APN function which is CCZ-inequivalent to both power functions and quadratics). On the contrary, we prove that for pawer no-Gold APN functions, CCZ equivalence coincides with EA-equivalence and inverse transformation for $n \leq 8$. We conjecture that this is true for any n.

Keywords: CCZ-equivalence, EA-equivalence, APN, Boolean functions

MSC: 94A60, 06E30, 11T71

1. Introduction

Given n and m two positive integers, a function F from the finite field with 2^n elements to the finite field with 2^m elements is called a vectorial Boolean function, or an (n,m)-function and it is simply called Boolean function when $m = 1$. Boolean functions and Vectorial Boolean functions are useful objects since they have many applications in mathematics and information theory; in particular they are one of the fundamental entities investigated in cryptography. Nowadays it is of fundamental importance to exchange and store information in an efficient, secure and reliable manner and cryptographic primitives are indeed used to protect informations against eavesdropping, unauthorized changes and other misuses. In symmetric cryptography the design of ciphers is based on an appropriate composition of nonlinear Boolean functions. For example, in block ciphers the security depends on S-boxes which are (n,m)-functions. Among the attacks that can be performed on a block cipher, one of the most efficient is the differential attack, introduced by Biham and Shamir [1]. It is based on the study of how differences in an input can affect the resulting difference at the output. To minimize the success probability of this attack, the theory of vectorial Boolean functions has identified an ideal property for the S-box when $n = m$, that is, to be *Almost Perfect Non-linear* (APN).

Email addresses: `lilya.budaghyan@uib.no` (L. Budaghyan), `marco.calderini@uib.no` (M. Calderini), `irene.villa@uib.no` (I. Villa)

The role of APN functions is not just related to cryptography. There are indeed applications of APN functions in coding theory, projective geometry and theory of commutative semifields. For these reasons many different works have been focused on finding and constructing new families of APN functions.

The APN property is preserved by some transformations of functions, which define equivalence relations between vectorial Boolean functions. There are mainly two such equivalence notions, called extended affine equivalence (EA-equivalence) and Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence). EA-equivalence is a particular case of CCZ-equivalence and any permutation is CCZ-equivalent to its inverse.

It is investigated in [4, 7] when the CCZ-equivalence could produce more functions than applying only the EA-equivalence and the inverse transformation. In particular, in [4], Budaghyan proves that for the Gold functions it is possible to construct, using the EA-equivalence and the inverse transformation, a function which is not EA-equivalent to the starting function and its inverse. In [7, 5], the authors show that for quadratic APN functions (in particular Gold functions and $x^3+Tr(x^9)$)) the CCZ-equivalence is more general than the EA-equivalence with the inverse transformation.

In this work, we focus on investigating this problem for the case of non-quadratic functions. In particular, we characterize some linear permutations on $(\mathbb{F}_{2^n})^2$ which imply that the CCZ-equivalence between two functions, F and F' can be obtained via EA-equivalence and inverse transformation. We also introduce a procedure that, at least in small dimensions, permits to verify whether a sufficient condition for CCZ-equivalence to be restricted to EA-equivalence and inverse transformation holds. Using this procedure we are able to verify that also for APN function CCZ-inequivalent to a quadratic function the CCZ-equivalence is more general than the EA-equivalence together with the inverse. With the same procedure we verify that, for contrary, up to dimension 8 for all non-Gold power APN functions CCZ-equivalence coincides with EA-equivalence together with the inverse transformation. This leads to a conjecture that for all non-Gold power APN functions and the inverse function the CCZ-equivalence coincides with the EA-equivalence together the inverse transformation. We conclude the paper with some observations on CCZ-equivalence classes for functions with linear structures.

2. Preliminaries

Let $n \geq 2$, we denote by $\mathbb{F}_{2^n}$ the finite field with 2^n elements, by $\mathbb{F}_{2^n}^*$ its multiplicative group and by $\mathbb{F}_{2^n}[x]$ the polynomial ring defined over $\mathbb{F}_{2^n}$. Any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can be represented as a univariate polynomial of degree at most 2^n-1 in $\mathbb{F}_{2^n}[x]$, that is

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

For any i, $0 \leq i \leq 2^n-1$, the *2-weight* of i is the (Hamming) weight of its binary representation. It is well known that the algebraic degree of a function F is equal to the maximum 2-weight of the exponent i such that $c_i \neq 0$. Functions of algebraic degree 1 are called *affine* and of degree 2 *quadratic*. Linear functions are affine functions without the constant term and they can be represented as $L(x) = \sum_{i=0}^{n-1} c_i x^{2^i}$. A well known example of a linear function is the *trace* function

$$Tr(x) = x + x^2 + \cdots + x^{2^{n-1}},$$

in particular, the trace is a Boolean function, i.e $Tr : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Besides, for any $m \geq 1$ such that $m|n$ we can define the linear function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$

$$Tr_n^m(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}.$$

Let $\lambda \in \mathbb{F}_{2^n}^*$ and F be a function from $\mathbb{F}_{2^n}$ to itself, we define the λ-component of F as the Boolean function $F_\lambda : \mathbb{F}_{2^n} \to \mathbb{F}_2$ with $F_\lambda(x) = Tr(\lambda F(x))$.

For any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ we denote the *Walsh transform* in $a, b \in \mathbb{F}_{2^n}$ by

$$\mathscr{W}_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(ax+bF(x))}.$$

For any Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ the Walsh transform in $a \in \mathbb{F}_{2^n}$ is given by

$$\mathscr{W}_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(ax)+f(x)}.$$

With *Walsh spectrum* we refer to the set of all possible values of the Walsh transform. A Boolean function f is called bent if its Walsh spectrum corresponds to the set $\{\pm 2^{n/2}\}$. Since $\mathscr{W}_f(a)$ is an integer bent functions can exist only for even n.
If $\mathscr{W}_f(0) = 0$ then the Boolean function is called balanced. Note that a bent function cannot be balanced. For any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ it is well know that F is a permutation if and only if all its component functions are balanced.

We denote the *derivative* of F in the direction of $a \in \mathbb{F}_{2^n}^*$ by $D_aF(x) = F(x+a) + F(x)$ and the *image* of F by $\mathrm{Im}(F) = \{F(x) \,|\, x \in \mathbb{F}_{2^n}\}$.
The function F is called *almost perfect nonlinear* (APN) if for every $a \neq 0$ and every b in $\mathbb{F}_{2^n}$, the equation $D_aF(x) = b$ admits at most 2 solutions, or equivalently $|\mathrm{Im}(D_aF)| = 2^{n-1}$.

There are several equivalence relations of functions for which the APN property is preserved. Two functions F and F' from $\mathbb{F}_{2^n}$ to itself are called:

- *affine equivalence* if $F' = A_1 \circ F \circ A_2$ where the mappings $A_1, A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine permutations;
- *extended affine equivalent* (EA-equivalent) if $F' = F'' + A$, where the mappings $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is affine and F'' is affine equivalent to F;

- *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if for some affine permutation $\mathscr{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ the image of the graph of F is the graph of F', that is, $\mathscr{L}(G_F) = G_{F'}$, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{2^n}\}$.

Obviously, affine equivalence is included in the EA-equivalence, and it is also well known that EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivalent to its inverse [10]. The algebraic degree of a function (if it is not affine) is invariant under EA-equivalence but, in general, it is not preserved by CCZ-equivalence. In general, neither EA-equivalence nor CCZ-equivalence preserves the permutation property.

There are six known infinite families of power APN functions. They are presented in Table 1. Since these power functions have different algebraic degree they are EA-inequivalent. Instead the

Table 1: Known APN power functions x^d over $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions	Degree	Proven
Golden	2^i+1	gcd(i,n)=1	2	[17, 21]
Kasami	$2^{2i}-2^i+1$	gcd(i,n)=1	i+1	[18, 19]
Welch	2^t+3	$n=2t+1$	3	[13]
Niho	$2^t+2^{\frac{t}{2}}-1$, t even $2^t+2^{\frac{3t+1}{2}}-1$, t odd	$n=2t+1$	$\frac{t+2}{2}$ t+1	[14]
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$	[2, 21]
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$	$i+3$	[15]

CCZ-inequivalence is not so straightforward, but also for this case it was possible to prove some inequalities. In both [22] and [12] Yoshiara and Dempwolff show that two APN power functions are CCZ-equivalent if and only if they are *cyclotomic-equivalent*, i.e. they are EA-equivalent or one is EA-equivalent to the inverse of the second one. To be more precise if we consider x^k and x^l defined over $\mathbb{F}_{2^n}$ the functions are cyclotomic-equivalent if there exists an integer $0 \leq a < n$ such that $l \equiv k2^a \mod (2^n-1)$ or $kl \equiv 2^a \mod (2^n-1)$, when k is coprime with 2^n-1. Earlier, some results on CCZ-inequivalence between the functions in Table 1 were proven in [6].

Among these power functions, for the Gold power function x^{2^i+1}, in [7] it was shown that the CCZ-equivalence is more general than applying the EA-equivalence and the inverse transformation. For the other power functions it is an open problem.

3. Remarks on CCZ-equivalence

In this section we will report some remarks regarding the CCZ-equivalence that will be useful in the investigation of the relation between EA-equivalence and CCZ-equivalence. Without loss of generality, we assume that the affine permutation in the definition of CCZ-equivalence is linear. It means that using affine permutations instead of linear one we simply make a shift by a constant in the input and output of the resulting function.

Lemma 3.1. *Let $L_1, L_2 : (\mathbb{F}_{2^n})^2 \to \mathbb{F}_{2^n}$ be linear maps and $a, b \in \mathbb{F}_{2^n}$, such that $\mathscr{L}(x,y) = (L_1(x,y) + a, L_2(x,y) + b)$ is a permutation. Let F and F' be CCZ-equivalent functions such that $\mathscr{L}$ maps the graph of F to the graph of F'. Then the linear part $\mathscr{L}'$ of $\mathscr{L}$ maps the graph of F to the graph of $F''(x) = F'(x+a) + b$.*

Proof. Indeed, if for an affine permutation $\mathscr{L}(x,y) = (L_1(x,y) + a, L_2(x,y) + b)$, where $L_1, L_2 : (\mathbb{F}_{2^n})^2 \to \mathbb{F}_{2^n}$ are linear and $a, b \in \mathbb{F}_{2^n}$, the image of the graph of a function F is the graph of a function F', then by denoting $F_1(x) = L_1(x, F(x))$ and $F_2(x) = L_2(x, F(x))$ we get $F' = F_2 \circ F_1^{-1}(x+a) + b$ (since F_1 must be a permutation [7]). Hence, neglecting a and b we get a function F'' affine equivalent to F', that is, $F''(x) = F'(x+a) + b$.

□

We can describe a linear map $\mathscr{L}$ as a formal matrix

$$\mathscr{L} = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix}$$

where A_i are linear maps over $\mathbb{F}_{2^n}$ for $1 \le i \le 4$, and

$$\mathscr{L}(x,y) = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = (A_1(x) + A_2(y), A_3(x) + A_4(y)).$$

In particular,

$$F_1(x) = L_1(x, F(x)) = A_1(x) + A_2 \circ F(x) \tag{1}$$

and

$$F_2(x) = L_2(x, F(x)) = A_3(x) + A_4 \circ F(x). \tag{2}$$

We can make the following straightforward but important observations about F_1.

Observation 3.2. *The function F_1 in* (1) *is a permutation if and only if any of its component is balanced. In terms of Walsh transforma we have that F_1 is a permutation if and only if*

$$\mathscr{W}_{F_1}(0, \lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda A_1(x) + \lambda A_2 \circ F(x))} = 0, \quad \textit{for all } \lambda \in \mathbb{F}_{2^n}^*.$$

Denoting by L^* the adjoint operator of the a linear map L (i.e. $Tr(yL(x)) = Tr(xL^*(y))$ for all $x, y \in \mathbb{F}_{2^n}$), we have

$$\mathscr{W}_{F_1}(0, \lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(A_1^*(\lambda)x + A_2^*(\lambda)F(x))} = \mathscr{W}_F(A_1^*(\lambda), A_2^*(\lambda)) = \mathscr{W}_{F_{A_2^*(\lambda)}}(A_1^*(\lambda)) = 0. \tag{3}$$

In particular, we have that $\mathrm{Ker}(A_1^*) \cap \mathrm{Ker}(A_2^*) = \{0\}$ *and for all* $\lambda \in \mathrm{Ker}(A_1^*) \setminus \{0\}$, *the* $A_2^*(\lambda)$-*component of F, $F_{A_2^*(\lambda)}$, has to be balanced. Moreover, if F has no balanced components then A_1 has to be a linear permutation on $\mathbb{F}_{2^n}$.*

4. CCZ-equivalence and EA-equivalence

In [7], it has been proved that for quadratic APN functions the CCZ-equivalence is strictly more general than the EA-equivalence and inverse transformation (when it is possible). Such a result has been obtained by exhibiting APN functions which are CCZ-equivalent to the Gold functions $F(x) = x^{2^i+1}$.

In this section we provide a procedure which allows, at least in small dimension, to investigate if the CCZ-equivalence leads to more functions than applying EA-equivalence and inverse transformation.

Given a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ we want to construct a possible linear permutation

$$\mathscr{L} = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix}$$

mapping the graph of F onto the graph of a function F'. In particular, we want to construct the linear functions A_1 and A_2 on $\mathbb{F}_{2^n}$ so that $F_1(x) = L_1(x, F(x)) = A_1(x) + A_2 \circ F(x)$ is a permutation.

For any $\lambda \in \mathbb{F}_{2^n}$ we define the set

$$\mathcal{ZW}(\lambda) = \{a \in \mathbb{F}_{2^n} : \mathscr{W}_{F_\lambda}(a) = 0\}.$$

Then we can define the following set

$$S_F = \{\lambda \in \mathbb{F}_{2^n}^* : \mathcal{ZW}(\lambda) \neq \emptyset\} \cup \{0\}. \quad (4)$$

Remark 4.1. *It is easy to see that the set* $\mathrm{Im}(A_2^*)$*, for a* A_2^* *defined as in Observation 3.2, has to be contained in* S_F *(see* (3)*).*

Along this section we will denote the vector (sub)space over $\mathbb{F}_2$ generated by the elements $v_1, \ldots, v_m \in \mathbb{F}_{2^n}$ by $\mathrm{Span}(v_1, \ldots, v_m)$.

Now, to construct the possible functions F_1 we should consider all the vector subspace of S_F. Let U be a fixed subspace contained in S_F, this will be a possible candidate for $\mathrm{Im}(A_2^*)$.

Observation 4.2. *Without loss of generality, fixed any basis* $\{u_1, \ldots, u_k\}$ *of* U *(where* k *is the dimension of* U*) and fixed a basis* $\{\beta_1, ..., \beta_n\}$ *of* $\mathbb{F}_{2^n}$ *(as vector space over* $\mathbb{F}_2$*), we can suppose that* $A_2^*(\beta_i) = u_i$ *for* $i = 1, ..., k$ *and* $\mathrm{Ker}(A_2^*) = \mathrm{Span}(\beta_{k+1}, ..., \beta_n)$*.*
Indeed, suppose A_2^* *is such that* $A_2^*(w_i) = u_i$ *for* $i = 1, ..., k$ *and* $\mathrm{Ker}(A_2^*) = \mathrm{Span}(w_{k+1}, ..., w_n)$ *for some* $w_1, ..., w_n$ *linearly independent. Then, we can consider any* $\bar{L}$*, linear permutation, such that* $\bar{L}^*(\beta_i) = w_i$ *for all* i*. Now, if* $F_1(x) = A_1(x) + A_2(F(x))$ *is a permutation, we can consider* $F_1' = \bar{L} \circ F_1$*, which is again a permutation, and* $\bar{A_2}^* = (\bar{L} \circ A_2)^*$ *is s.t.* $\bar{A_2}^*(\beta_i) = u_i$ *for* $i = 1, ..., k$ *and* $\mathrm{Ker}(\bar{A_2}^*) = \mathrm{Span}(\beta_{k+1}, ..., \beta_n)$*.*

Remark 4.3. *As stated in [20, Theorem 2.3] for any linear polynomial $L(x)$ we have that, given a basis $\{\beta_1,...,\beta_n\}$ of $\mathbb{F}_{2^n}$, there exist unique $\theta_1,...,\theta_n$ in $\mathbb{F}_{2^n}$ such that $L(x) = \sum_{i=1}^n Tr(\beta_i x)\theta_i$. Then, we can construct the linear polynomial A_2^* from the image of the basis $\{\beta_1,...,\beta_n\}$ by solving the linear system*

$$\begin{aligned}&\textstyle\sum_{i=1}^n Tr(\beta_1\beta_i)\theta_i = A_2^*(\beta_1)\\ &\vdots\\ &\textstyle\sum_{i=1}^n Tr(\beta_n\beta_i)\theta_i = A_2^*(\beta_n).\end{aligned}$$

Now, we have fixed U and our function A_2^* (using Observation 4.2 and Remark 4.3) and we want to construct all possible A_1^* such that $F_1(x) = A_1(x) + A_2 \circ F(x)$ is a permutation. In the following we report the procedure to construct the matrices A_1^* (for fixed A_2^*). The steps of this procedure will be explained in the proof of Proposition 4.5.

Procedure 4.4.
For any $u \in U \setminus \{0\}$ we consider the set $\mathcal{ZW}(u)$, as defined before. To construct A_1 we need to determine the images of the vectors β_i's. In order to do that, we need to select any possible k-tuple $a_1 \in \mathcal{ZW}(u_1),...,a_k \in \mathcal{ZW}(u_k)$ such that

(P1) $\sum_{i=1}^k \lambda_i a_i \in \mathcal{ZW}(\sum_{i=1}^k \lambda_i u_i)$ *for any $\lambda_1,...,\lambda_k \in \mathbb{F}_2$, not all zero.*

These $a_1,...,a_k$ will be the images by A_1^* of $\beta_1,...,\beta_k$, respectively.
After that, for any of these k-tuples, we need to determine all possible $(n-k)$-tuples of elements $a_{k+1},...,a_n$ satisfying:

(P2) *$a_{k+1},...,a_n$ are linearly independent;*

(P3) *for any $a \in \mathrm{Span}(a_{k+1},...,a_n)$, $a + \sum_{i=1}^k \lambda_i a_i \in \mathcal{ZW}(\sum_{i=1}^k \lambda_i u_i)$, for any $\lambda_1,\ldots,\lambda_k \in \mathbb{F}_2$.*

Condition **(P3)** is equivalent to have

$$\mathrm{Span}(a_{k+1},...,a_n) \subseteq \sum_{i=1}^k \lambda_i a_i + \mathcal{ZW}\left(\sum_{i=1}^k \lambda_i u_i\right),$$

for any $\lambda_1,\ldots,\lambda_k \in \mathbb{F}_2$, where $a + \mathcal{ZW}(u) = \{a + v : v \in \mathcal{ZW}(u)\}$.

Proposition 4.5. *Let U be a subspace contained in S_F, where F is a function from $\mathbb{F}_{2^n}$ to itself and S_F defined as in* (4). *Then, there exists a permutation of $\mathbb{F}_{2^n}$ $F_1(x) = A_1(x) + A_2 \circ F(x)$, with A_1 and A_2 linear and $\mathrm{Im}(A_2^*) = U$, if and only if Procedure 4.4 applied to the space U is successful.*

Proof. Let us suppose that $F_1(x) = A_1(x) + A_2 \circ F(x)$ is a permutation and $\mathrm{Im}(A_2^*) = U$. From the Observation 4.2 without loss of generality we can suppose that $A_2^*(\beta_i) = u_i$ for $i = 1,...,k$ and $\mathrm{Ker}(A_2^*) = \mathrm{Span}(\beta_{k+1},...,\beta_n)$, where $\{u_1,\ldots,u_k\}$ is a basis of U fixed for the procedure. Then, we need to show that A_1^* is generated by the procedure. That is, we need to show that **(P1)**, **(P2)** and **(P3)** are satisfied.

Let $a_i = A_1^*(\beta_i)$ for $1 \le i \le n$. Suppose that **(P1)** is not satisfied, then there exist $\lambda_1, \dots, \lambda_k$ in $\mathbb{F}_2$, not all zero, such that $\sum_{i=1}^k \lambda_i a_i \notin \mathcal{ZW}(\sum_{i=1}^k \lambda_i u_i)$, which means that $\mathscr{W}_F(\sum_{i=1}^k \lambda_i a_i, \sum_{i=1}^k \lambda_i u_i) \neq 0$. Since

$$\mathscr{W}_F(\sum_{i=1}^k \lambda_i a_i, \sum_{i=1}^k \lambda_i u_i) = \mathscr{W}_F(A_1^*(\sum_{i=1}^k \lambda_i \beta_i), A_2^*(\sum_{i=1}^k \lambda_i \beta_i)) = \mathscr{W}_{F_1}(0, \sum_{i=1}^k \lambda_i \beta_i)$$

(see Observation 3.2) and F_1 is a permutation, this is not possible.
If **(P2)** is not satisfied we have that there exist $\lambda_{k+1}, \dots, \lambda_n$ in $\mathbb{F}_2$, not all zero, such that $\sum_{i=k+1}^n \lambda_i a_i = 0$. Then, $\sum_{i=k+1}^n \lambda_i \beta_i \in \mathrm{Ker}(A_1^*) \cap \mathrm{Ker}(A_2^*)$ and from Observation 3.2 this is not possible.
The last condition **(P3)** is similar to **(P1)**. Indeed, suppose that there exist $\lambda_1, \dots, \lambda_n$ in $\mathbb{F}_2$ such that $\sum_{i=1}^k \lambda_i a_i + \sum_{i=k+1}^n \lambda_i a_i \notin \mathcal{ZW}(\sum_{i=1}^k \lambda_i u_i)$. Then, we have

$$\begin{aligned}\mathscr{W}_{F_1}(0, \sum_{i=1}^n \lambda_i \beta_i) &= \mathscr{W}_F(A_1^*(\sum_{i=1}^n \lambda_i \beta_i), A_2^*(\sum_{i=1}^n \lambda_i \beta_i)) \\ &= \mathscr{W}_F(A_1^*(\sum_{i=1}^n \lambda_i \beta_i), A_2^*(\sum_{i=1}^k \lambda_i \beta_i)) \neq 0,\end{aligned}$$

$A_2^*(\sum_{i=1}^k \lambda_i \beta_i) = A_2^*(\sum_{i=1}^n \lambda_i \beta_i)$ since $\mathrm{Ker}(A_2^*) = \mathrm{Span}(\beta_{k+1}, ..., \beta_n)$).

Vice versa, if we are successful on generating, at least, one matrix A_1^* with Procedure 4.4, then from conditions **(P1)**, **(P2)** and **(P3)** it is easy to verify that for any $\lambda_1, \dots, \lambda_n$ in $\mathbb{F}_2$, not all zero,

$$\mathscr{W}_{F_1}(0, \sum_{i=1}^n \lambda_i \beta_i) = \mathscr{W}_F(A_1^*(\sum_{i=1}^n \lambda_i \beta_i), A_2^*(\sum_{i=1}^n \lambda_i \beta_i)) = \mathscr{W}_F(\sum_{i=1}^n \lambda_i a_i, \sum_{i=1}^n \lambda_i u_i) = 0.$$

Indeed, from condition **(P1)** we have $\mathscr{W}_{F_1}(0, \sum_{i=1}^n \lambda_i \beta_i) = 0$, for all possible $\lambda_1, \dots, \lambda_k$ not all zero and $\lambda_{k+1} = \cdots = \lambda_n = 0$. From condition **(P2)** we have that for all possible $\lambda_{k+1}, \dots, \lambda_n$ not all zero and $\lambda_1 = \cdots = \lambda_k = 0$, $\mathscr{W}_{F_1}(0, \sum_{i=1}^n \lambda_i \beta_i) = 0$. The last condition **(P3)** guarantees that $\mathscr{W}_{F_1}(0, \sum_{i=1}^n \lambda_i \beta_i) = 0$ when both $\lambda_1, \dots, \lambda_k$ are not all zero and $\lambda_{k+1}, \dots, \lambda_n$ are not all zero. □

On the other hand, if we cannot construct a matrix A_1 for all spaces $U \subseteq S_F$, we have that all the CCZ-transformations that we can apply to F are composition of EA-transformations and inverse transformations. Before proving it, we recall the following remark from [7]. Further, in Lemma 4.7 we extend Proposition 3 of [7].

Remark 4.6 (Remark 2 in [7]). *For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, if $\mathscr{L} = (L_1, L_2)$ and $\mathscr{L}' = (L_1, L_2')$ are permutations such that the function $L_1(x, F(x))$ is a permutation, then the functions defined by the graphs $\mathscr{L}(G_F)$ and $\mathscr{L}'(G_F)$ are EA-equivalent.*

In Proposition 3 of [7], the authors characterized which type of linear maps $\mathscr{L}$, admissible for a CCZ-transformation, give us the EA-equivalence of a function F' to a function F or to its inverse (if it exists). That is, they studied the linear maps, $\mathscr{L}$, that applied to the graph of F permit to obtain the graph of F' in the following cases

$$F' \sim_{EA} F \quad \text{and} \quad F' \sim_{EA} F^{-1} \stackrel{\text{inv}}{\to} F.$$

In the following lemma we extend this characterization to the case when we apply, again, an EA-transformation and the inverse transformation (if it is possible). That is, we study the maps, $\mathscr{L}$, that maps the graph of F onto the graph F' when

$$F' \sim_{EA} G \stackrel{\text{inv}}{\to} G^{-1} \sim_{EA} F \quad \text{and} \quad F' \sim_{EA} G \stackrel{\text{inv}}{\to} G^{-1} \sim_{EA} F^{-1} \stackrel{\text{inv}}{\to} F,$$

for some permutation G.

Lemma 4.7. *Let $F, F' : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. The function F' is EA-equivalent to the function F or to the inverse of F (if it exists) if and only if there exists a linear map $\mathscr{L} = (L_1, L_2)$ such that $\mathscr{L}(G_F) = G_{F'}$ and L_1 depends only in one variable, i.e. $L_1(x,y) = A_1(x)$ and A_1, A_4 are permutations if F' is EA-equivalent to F and $L_1(x,y) = A_2(y)$ and A_2, A_3 are permutation if F' is EA-equivalent to F^{-1}. While, we have*

$$F' \sim_{EA} G \stackrel{inv}{\to} G^{-1} \sim_{EA} F,$$

for some permutation G if and only if there exists a linear permutation $\mathscr{L} = (L_1, L_2)$ such that $\mathscr{L}(G_F) = G_{F'}$ and $L_1(x,y) = A_1(x) + A_2(y)$ with A_2 a permutation of $\mathbb{F}_{2^n}$.
Moreover, if F^{-1} exists, then we have

$$F' \sim_{EA} G \stackrel{inv}{\to} G^{-1} \sim_{EA} F^{-1} \stackrel{inv}{\to} F,$$

for some permutation G if and only if there exists a linear permutation $\mathscr{L} = (L_1, L_2)$ such that $\mathscr{L}(G_F) = G_{F'}$ and $L_1(x,y) = A_1(x) + A_2(y)$ with A_1 a permutation of $\mathbb{F}_{2^n}$

Proof. The first part is Proposition 3 in [7]. Note that the condition A_1, A_4 permutations (and similarly A_2, A_3 permutations) is equivalent to $\mathscr{L} = (L_1, L_2)$ be a permutation.

We will show the last two claims. Suppose F' is EA-equivalent to the function G which inverse is EA-equivalent to F, that is

$$F' \sim_{EA} G \stackrel{\text{inv}}{\to} G^{-1} \sim_{EA} F.$$

Recalling that in the inverse transformation we are applying the linear permutation over $(\mathbb{F}_{2^n})^2$ given by $Inv(x,y) = (y,x)$, from the first part of the lemma we can construct the permutation $\mathscr{L}$ given by

$$\begin{aligned}
&(A'_1(x), A'_3(x) + A'_4(y)) \circ (A_3(x) + A_4(y), A_1(x)) = \\
&= (A'_1 \circ A_3(x) + A'_1 \circ A_4(y), A'_3 \circ A_3(x) + A'_3 \circ A_4(y) + A'_4 \circ A_1(x)),
\end{aligned}$$

where $(A'_1(x), A'_3(x) + A'_4(y))$ maps G_G onto $G_{F'}$ and $(A_3(x) + A_4(y), A_1(x))$ maps G_F onto G_G. Since A'_1 and $A_4(x)$ are permutations also $A'_1 \circ A_4$ is a permutation.

Vice versa, let $\mathscr{L}(x,y) = (A_1(x)+A_2(y), A_3(x)+A_4(y))$ be a linear permutation of $(\mathbb{F}_{2^n})^2$ such that $\mathscr{L}(G_F) = G_{F'}$ and A_2 is permutation of $\mathbb{F}_{2^n}$. Consider the linear map $\mathscr{L}'(x,y) = (A_1(x)+A_2(y), x)$. $\mathscr{L}'$ is a linear permutation of $(\mathbb{F}_{2^n})^2$ since $A_2(x)$ and x are permutations. Moreover $F_1(x) = A_1(x)+A_2(F(x))$ is a permutation since $\mathscr{L}(G_F) = G_{F'}$. Then, F_1 is a permutation EA-equivalent to F and the function G defined by the graph $\mathscr{L}'(G_F)$, that is F_1^{-1}, is such that G^{-1} is EA-equivalent to F. From Remark 4.6 we obtain that F' and G are also EA-equivalent.

The case when G^{-1} is equivalent to F^{-1} is similar. Indeed, suppose

$$F' \sim_{EA} G \stackrel{\text{inv}}{\to} G^{-1} \sim_{EA} F^{-1} \stackrel{\text{inv}}{\to} F,$$

using the first part of the lemma we can construct the permutation $\mathscr{L}$ given by

$$\begin{aligned}&(A'_1(x), A'_3(x)+A'_4(y)) \circ (A_3(x)+A_4(y), A_2(y)) = \\ &(A'_1 \circ A_3(x) + A'_1 \circ A_4(y), A'_3 \circ A_3(x) + A'_3 \circ A_4(y) + A'_4 \circ A_2(y)),\end{aligned}$$

where $(A'_1(x), A'_3(x)+A'_4(y))$ maps G_G onto $G_{F'}$ and $(A_3(x)+A_4(y), A_2(y))$ maps G_F onto G_G. Since A'_1 and $A_3(x)$ are permutations also $A'_1 \circ A_3$ is a permutation.

On the other hand, suppose $\mathscr{L}(x,y) = (A_1(x)+A_2(y), A_3(x)+A_4(y))$ is a linear permutation of $(\mathbb{F}_{2^n})^2$ such that $\mathscr{L}(G_F) = G_{F'}$ with A_1 a permutation of $\mathbb{F}_{2^n}$.
As before, we can consider $\mathscr{L}'(x,y) = (A_1(x)+A_2(y), y)$, which is a permutation of $(\mathbb{F}_{2^n})^2$. Let G be defined by the graph $\mathscr{L}'(G_F)$, that is $G(x) = F \circ F_1^{-1}(x)$ with $F_1(x) = A_1(x) + A_2 \circ F(x)$. Since F is a permutation also G is a permutation and we obtain that $G_{G^{-1}} = Inv \circ \mathscr{L}'(G_F)$. From the first part of the lemma we have that G^{-1} is EA-equivalent to F^{-1} since $Inv \circ \mathscr{L}'(x,y) = (y, A_1(x) + A_2(y))$. □

Theorem 4.8. *Let F be a function from $\mathbb{F}_{2^n}$ to itself. If for any nonzero vector subspace U in S_F different from $\mathbb{F}_{2^n}$ it is not possible to construct any matrix $A_1^* \neq 0$ with Procedure 4.4, then any function F' CCZ-equivalent to F can be obtained from F applying only the EA-equivalence and inverse transformation iteratively.*

Proof. Using Procedure 4.4 we can obtain only functions $L_1(x,y) = A_1(x) + A_2(y)$ such that A_2 is either the zero function, when $U = \{0\}$, or a permutation, when $U = \mathbb{F}_{2^n}$. Otherwise, from Proposition 4.5 we cannot obtain L_1 such that $L_1(x, F(x))$ is a permutation of $\mathbb{F}_{2^n}$. Then, for any CCZ-transformation $\mathscr{L}$ such that $\mathscr{L}(G_F) = G_{F'}$ the function L_1 needs to satisfies one of the conditions in Lemma 4.7, implying that F' can be obtained from F applying only the EA-equivalence and inverse transformation iteratively. □

When F is also a permutation we have the following.

Theorem 4.9. *Let F be a permutation over $\mathbb{F}_{2^n}$. If for any nonzero vector subspace U in S_F different from $\mathbb{F}_{2^n}$ it is not possible to construct a matrix $A_1^* \neq 0$ of $\mathrm{rank}(A_1^*) < n$ with Procedure 4.4, then any function F' CCZ-equivalent to F can be obtained from F applying only the EA-equivalence and inverse transformation iteratively.*

Proof. In this case, from Procedure 4.4 we could obtain a function $L_1(x,y) = A_1(x) + A_2(y)$ for some space $U \neq \{0\}, \mathbb{F}_{2^n}$ in S_F. However, A_1 would be a permutation, and from the last part of Lemma 4.7 we have our claim. □

Applying the Procedure 4.4, using the software MAGMA, from Theorem 4.8 we obtain the following corollary.

Corollary 4.10. *Let $n \leq 8$ and $F(x) = x^d$ be an APN power function defined over $\mathbb{F}_{2^n}$, which is inequivalent to a Gold function. Then, for the function F the CCZ-equivalence coincide with the EA-equivalence together with the inverse transformation.*

Corollary 4.11. *Let $n \leq 6$ be even. Then, for the inverse function $F(x) = x^{2^n-2}$ the CCZ-equivalence coincide with the EA-equivalence together with the inverse transformation.*

From these two results we conjecture the following.

Conjecture 4.12. *Let $F(x) = x^d$ be a non-Gold APN power function or the inverse function over $\mathbb{F}_{2^n}$. Then, for F the CCZ-equivalence coincide with the EA-equivalence together with the inverse transformation.*

5. On functions not equivalent to quadratic functions

For quadratic APN functions it is known that applying the CCZ-equivalence it is possible to obtain functions which cannot be obtained using the EA-equivalence and the inverse transformation only, see for instance [7], for the case of Gold functions, or also the APN permutation in dimension six introduced by Dillon *et al.* in [3] which was constructed by applying the CCZ-equivalence to the so-called Kim function, that is quadratic (and inequivalent to a Gold function). In the following we provide an example which shows for the first time that CCZ-equivalence is more general than EA-equivalence together with inverse transformation also for non quadratic APN functions.

Let $n = 6$, and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be

$$\begin{aligned} F(x) =& x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + u^{14}((u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13}) + \\ & (u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13})^2 + (u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13})^4 + \\ & (u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13})^8 + (u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13})^{16} + \\ & (u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13})^{32} + (u^2x)^9 + (u^2x)^{18} + (u^2x)^{36} + x^{21} + x^{42}), \end{aligned}$$

where u is a primitive element of $\mathbb{F}_{2^n}$. The function F is the first (and only currently known) example of APN functions which is not CCZ-equivalent to a quadratic function and to power functions (see [16]). Using the procedure described in the previous section it is possible to construct the functions A_1 and A_2 given by

$$A_1(x) = u^{50}x^{32} + u^{51}x^{16} + u^{43}x^8 + ux^4 + u^{26}x^2 + u^{26}x$$

and

$$A_2(x) = u^{26}x^{32} + u^{17}x^{16} + u^{56}x^8 + u^9x^4 + u^{54}x^2 + u^{46}x,$$

so that $F_1(x) = L_1(x, F(x)) = A_1(x) + A_2 \circ F(x)$ is a permutation of $\mathbb{F}_{2^n}$. Now considering the function $F_2(x) = L_2(x, F(x)) = F(x)$ we have that F is CCZ-equivalente to $F' = F_2 \circ F_1^{-1}$ having univariate polynomial representation

$$\begin{aligned} F'(x) = & u^{41}x^{60} + u^{29}x^{58} + u^{46}x^{57} + u^3x^{56} + u^{39}x^{54} + u^{47}x^{53} + u^3x^{52} + u^{62}x^{51} + u^{54}x^{50} + \\ & u^{62}x^{49} + u^{53}x^{48} + u^{14}x^{46} + u^{39}x^{45} + u^{20}x^{44} + u^{26}x^{43} + u^{11}x^{42} + u^{31}x^{41} + u^{53}x^{40} + \\ & u^{59}x^{39} + u^{53}x^{38} + u^{41}x^{37} + u^{19}x^{36} + u^{58}x^{35} + u^2x^{34} + u^7x^{33} + u^{39}x^{32} + u^{15}x^{30} + \\ & u^{17}x^{29} + u^{45}x^{28} + u^{39}x^{27} + u^{57}x^{26} + u^{33}x^{25} + u^{61}x^{24} + u^{41}x^{23} + u^{50}x^{22} + u^{58}x^{21} + \\ & u^{55}x^{20} + u^{26}x^{19} + u^{17}x^{18} + u^{37}x^{17} + u^{30}x^{16} + ux^{15} + u^{46}x^{14} + u^{21}x^{13} + u^{13}x^{12} + \\ & u^{61}x^{11} + u^{20}x^{10} + x^9 + u^{61}x^8 + u^{32}x^7 + u^{44}x^6 + u^{62}x^5 + u^{16}x^4 + u^{48}x^3 + u^{58}x^2 + u^{37}x. \end{aligned}$$

The function F' cannot be constructed from F via EA-equivalence and inverse transformation. Indeed $F \nsim_{EA} F'$ since F has algebraic degree 3 and F' algebraic degree 4. Moreover, to apply the inverse transformation, at least once, we need $F \sim_{EA} G$ with G a permutation, but since F has quadratic components, as for example

$$\begin{aligned} Tr(F(x)) = & u^{15}x^{48} + u^{60}x^{40} + u^{36}x^{36} + u^{51}x^{34} + u^{30}x^{33} + u^{39}x^{24} + u^{30}x^{20} + \\ & u^{18}x^{18} + u^{57}x^{17} + u^{51}x^{12} + u^{15}x^{10} + u^9x^9 + u^{57}x^6 + u^{39}x^5 + u^{60}x^3, \end{aligned}$$

this cannot be possible (see [8, Corollary 3.8]).

6. Some remarks on functions with linear structures

In the previous section we showed that also for functions CCZ-inequivalent to a quadratic function the CCZ-equivalence is more general than the EA-equivalence with the inverse transformation. It is worth to note that the function studied in Section 5 has some quadratic components. In this section we will report some considerations that can explain why for functions with components having some linear structures it is more likely that CCZ-equivalence is more general than EA-equivalence with inverse transformation.

We recall that $\alpha \in \mathbb{F}_{2^n}$ is a *c-linear structure*, with $c \in \mathbb{F}_2$, of a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ if $f(x+\alpha) + f(x) = c$ for all $x \in \mathbb{F}_{2^n}$. For a vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ we say that F has a linear structure if there exists a component $Tr(\gamma F)$, with $\gamma \neq 0$, of F which has a linear structure.

In [11], the authors study permutation polynomials (PP) of type $G(x) + \gamma Tr(F(x))$. In particular when $G(x)$ is a linearized polynomial from the results in [11] we have directly the following.

Lemma 6.1 ([11]). *Let $L, F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with L a linear polynomial. Then we have the following properties:*

i) *if $L(x)+\gamma Tr(F(x))$ is PP then L is a PP or is a 2-to-1 map.*

ii) *If L is a PP, then $L(x)+\gamma Tr(F(x))$ is a PP if and only if $F(x)=R(L(x))$ for some polynomial R and γ is a 0-linear structure of $Tr(R(x))$ (and in particular $L(\gamma)$ is a 0-linear structure of $Tr(F(x))$).*

iii) *If L is a 2-to-1 map with kernel $\{0,\alpha\}$, then $L(x)+\gamma Tr(F(x))$ is a PP if and only if γ is not in the image of L and α is a 1-linear structure of $Tr(F(x))$.*

Corollary 6.2. *If $L(x)+\gamma Tr(F(x))$ is a PP then F has a linear structure.*

So, given a function F defined over $\mathbb{F}_{2^n}$ with a component having some linear structure, from Lemma 6.1 we can obtain some linear functions $L_1 : (\mathbb{F}_{2^n})^2 \to \mathbb{F}_{2^n}$ such that $F_1(x) = L_1(x,F(x))$ is a permutation. Indeed, another direct consequence of Lemma 6.1 is the following.

Proposition 6.3. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Then there exists a linear function $L_1(x,y) = A_1(x)+A_2(y)$ such that $L_1(x,F(x))$ is a permutation and A_2 has rank 1 if and only if F has at least one component with a linear structure.*

Proof. Since A_2 has rank 1, then $\mathrm{Im}(A_2) = \gamma\mathbb{F}_2$ for some $\gamma \in \mathbb{F}_{2^n}$. Moreover, any linear transformations from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is of the type $Tr(\lambda x)$ with $\lambda \in \mathbb{F}_{2^n}$. Thus, we can suppose that $L_1(x,y) = A_1(x)+\gamma Tr(\lambda y)$ for some $\gamma,\lambda \in \mathbb{F}_{2^n}$ and from Corollary 6.2 we have that if $F_1(x) = L_1(x,F(x))$ is a permutation, then F has a linear structure.

Viceversa, suppose that γ is a 0-linear structure of the component $Tr(\lambda F(x))$. Then

$$x+\gamma Tr(\lambda F(x))$$

is a PP for ii) of Lemma 6.1. Let now γ be a 1-linear structure of the component $Tr(\lambda F(x))$. Then, if $Tr(\gamma) = 1$ we have

$$x+\gamma Tr(\lambda F(x)+x)$$

is a PP for iii) of Lemma 6.1 (note that $\gamma \notin \mathrm{Im}(x+\gamma Tr(x))$). If $Tr(\gamma) = 0$, then we can consider any element θ such that $Tr(\gamma\theta) = 1$. Then, always for iii) of Lemma 6.1,

$$x+\gamma Tr(\theta x)+\gamma Tr(\lambda F(x))$$

is a PP. □

This result has been obtained, independently, in [9] Corollary 2 in terms of function twisting (introduced always in [9]).

From Proposition 6.3 we obtained a possible function $L_1(x,y) = A_1(x)+A_2(y)$ such that $F_1(x) = L_1(x,F(x))$ is a permutation, when F has a linear structure. In the following, we will construct a function F' CCZ-equivalent to F, using this type of linear function $L_1(x,y)$.

First of all, note that the functions constructed in Proposition 6.3

$$F_1(x) = x + \gamma Tr(\lambda F(x))$$

when γ is a 0-linear structure of the component $Tr(\lambda F(x))$, and

$$F_1'(x) = x + \gamma Tr(\lambda F(x) + \theta x),$$

with θ as in Proposition 6.3, when γ is a 1-linear structure, are involutions. Indeed,

$$\begin{aligned} F_1 \circ F_1(x) =& x + \gamma Tr(\lambda F(x)) + \gamma Tr(\lambda F(x + \gamma tr(\lambda F(x)))) \\ =& \begin{cases} x & \text{if } Tr(\lambda F(x)) = 0 \\ x + \gamma Tr(\lambda F(x) + \lambda F(x+\gamma)) = x & \text{if } Tr(\lambda F(x)) = 1 \end{cases} . \end{aligned}$$

It is similar for F_1', we just need to verify the cases $(Tr(\theta x), Tr(\lambda F(x))) = (0,0), (1,0), (0,1)$ and $(1,1)$.

Now, for the case $F_1(x) = x + \gamma Tr(\lambda F(x))$, we have $L_1(x,y) = x + \gamma Tr(\lambda y)$ and, considering the linear function $L_2(x,y) = y$, we get the linear permutation $\mathscr{L}(x,y) = (L_1(x,y), L_2(x,y))$. Denoting $F_2(x) = L_2(x, F(x)) = F(x)$, this permutation permits to obtain the equivalent function

$$F'(x) = F_2 \circ F_1(x) = F(x + \gamma Tr(\lambda F(x)) = F(x) + Tr(\lambda F(x))(F(x) + F(x+\gamma)). \tag{5}$$

Similarly, for $F_1'(x) = x + \gamma Tr(\lambda F(x) + \theta x)$ we can consider $L_2(x,y) = y + \gamma Tr(\theta x)$, that is $F_2(x) = F(x) + \gamma Tr(\theta x)$ and

$$\begin{aligned} F'(x) = F_2 \circ F_1'(x) =& F(x + \gamma Tr(\lambda F(x) + \theta x)) + \gamma Tr(x + \gamma Tr(\lambda F(x) + \theta x)) \\ =& F(x) + Tr(\lambda F(x) + \theta x)(F(x) + F(x+\gamma) + \gamma Tr(1)) + \gamma Tr(\theta x). \end{aligned} \tag{6}$$

We can note that in both cases we are multiplying the component $Tr(\lambda F(x))$ with the derivative $F(x) + F(x+\gamma)$, such a multiplication could change the degree of the resulting function. In the case of quadratic functions such a transformation could lead to a function of degree 3.
For the particular case of quadratic function, this has been also observed in [9] in terms of function twisting (see Section 6.3 in [9]).

In [7], the authors constructed some permutation polynomials as those described in Proposition 6.3. Applying these polynomials to the Gold power functions x^{2^i+1}, they obtained, in the same way described for (5) and (6), functions EA-inequivalent to any power functions.

7. Conclusions

We have investigated the problem if for a given generic (APN) function F the class of CCZ-equivalent functions can be obtained by the EA-equivalence and the inverse transformation. Such a problem was investigated also in [4, 5, 7] for the case of quadratic APN functions, in particular for the Gold functions. We characterized some linear permutations on $(\mathbb{F}_{2^n})^2$ which imply that the equivalence between two functions F and F' can be obtained via EA-equivalence and inverse transformation. We also gave a procedure to verify if a sufficient condition (Theorem 4.8), implying that the CCZ-equivalence coincides with EA-equivalence and inverse transformation, holds. Using this procedure we prove that also for APN functions CCZ-inequivalent to a quadratic the CCZ-equivalence can be more general than the EA-equivalence and inverse. With the same procedure we could verify, on the contrary, in dimensions up to 8 for the non-Gold APN power functions the class of CCZ-equivalent functions can be obtained using only the EA-equivalence and the inverse transformation. This leads to a conjecture that for all non-Gold APN power functions and the inverse function the CCZ-equivalence coincides with the EA-equivalence together with the inverse transformation.

References

[1] E. Biham, A. Shamir: *Differential Cryptanalysis of DES-like Cryptosystems*. J. Cryptology 4(1), 3-72 (1991)

[2] T. Beth, and C. Ding, *On almost perfect nonlinear permutations*, Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science, 765, Springer-Verlag, New York, 1993, pp. 65-76.

[3] K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe. *An APN permutation in dimension six*. Finite Fields: theory and applications, 518:33-42, 2010

[4] L. Budaghyan: *The simplest method for constructing APN polynomials EA-inequivalent to power functions*. In: C. Carlet, B. Sunar (eds.) WAIFI 2007. LNCS, vol. 4547, pp. 177-188. Springer, Heidelberg (2007)

[5] L. Budaghyan, C. Carlet, and G. Leander, *Constructing new APN functions from known ones*, Finite Fields and Their Applications, vol.15, issue 2, Apr. 2009, pp. 150-159.

[6] L. Budaghyan, C. Carlet, G.Leander, *On inequivalence between known power APN functions*. In: Masnyk-Hansen, O., Michon, J.-F., Valarcher, P., J.-B.Yunes (Eds.) Proceedings of the conference BFCA'08, Copenhagen.

[7] L. Budaghyan, C. Carlet, and A. Pott, *New classes of almost bent and almost perfect nonlinear polynomials.* IEEE Transactions on Information Theory 52.3 (2006): 1141-1152.

[8] M. Calderini, M. Sala, and I. Villa, *A note on APN permutations in even dimension.* Finite Fields and Their Applications 46 (2017): 1-16.

[9] A. Canteaut and L. Perrin, *On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting*, Cryptology ePrint Archive, Report 2018/713, `https://eprint.iacr.org/2018/713`, 2018.

[10] C. Carlet, P. Charpin, and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems.* Designs, Codes and Cryptography 15.2 (1998): 125-156.

[11] P. Charpin, G. Kyureghyan, On a class of permutation polynomials over F2n , in: SETA 2008, in: Lecture Notes in Comput. Sci., vol. 5203, Springer-Verlag, Berlin, 2008, pp. 368–376.

[12] U. Dempwolff, *CCZ equivalence of power functions*, submitted to Designs, Codes and Cryptography Mar. 2017

[13] H. Dobbertin, *Almost perfect nonlinear power functions over $GF(2^n)$: the Welch case*, IEEE Trans. Inform. Theory, 45, 1999, pp. 1271-1275.

[14] H. Dobbertin, *Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case*, Inform. and Comput., 151, 1999, pp. 57-72.

[15] H. Dobbertin, *Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5*, Proceedings of Finite Fields and Applications FQ5, 2000, pp. 113-121.

[16] Y. Edel, and A. Pott, *A new almost perfect nonlinear function which is not quadratic.* Adv. in Math. of Comm. 3.1 (2009): 59-81.

[17] R. Gold, *Maximal recursive sequences with 3-valued recursive cross-correlation functions*, IEEE Trans. Inform. Theory, 14, 1968, pp. 154-156.

[18] H. Janwa, and R. Wilson, *Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cycle codes*, Proceedings of AAECC-10, LNCS, vol. 673, Berlin, Springer-Verlag, 1993, pp. 180-194.

[19] T. Kasami, *The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes*, Inform. and Control, 18, 1971, pp. 369-394.

[20] S. Ling, L.J. Qu, *A note on linearized polynomials and the dimension of their kernels*, Finite Fields Appl. 18 (2012) 56–62.

[21] K. Nyberg, *Differentially uniform mappings for cryptography*, Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science 765, 1994, pp. 55-64.

[22] S. Yoshiara, *Equivalences of power APN functions with power or quadratic APN functions*, Journal of Algebraic Combinatorics, vol. 44, N. 3. Nov. 2016, pp. 561-585.