HAL
archives-ouvertes.fr

On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting

Anne Canteaut, Léo Perrin

▶ To cite this version:

Anne Canteaut, Léo Perrin. On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting. Finite Fields and Their Applications, Elsevier, 2019, 56, pp.209-246. 10.1016/j.ffa.2018.11.008 . hal-01953353

HAL Id: hal-01953353
https://hal.inria.fr/hal-01953353

Submitted on 12 Dec 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting*

Anne Canteaut, Léo Perrin†

Inria, Paris, France
{anne.canteaut,leo.perrin}@inria.fr

Abstract

Two vectorial Boolean functions are "CCZ-equivalent" if there exists an affine permutation mapping the graph of one to the other. It preserves many of the cryptographic properties of a function such as its differential and Walsh spectra, which is why it could be used by Dillon et al. to find the first APN permutation on an even number of variables. However, the meaning of this form of equivalence remains unclear. In fact, to the best of our knowledge, it is not known how to partition a CCZ-equivalence class into its Extended-Affine (EA) equivalence classes; EA-equivalence being a simple particular case of CCZ-equivalence.

In this paper, we characterize CCZ-equivalence as a property of the zeroes in the Walsh spectrum of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ or, equivalently, of the zeroes in its Difference Distribution Table. We use this framework to show how to efficiently upper bound the number of distinct EA-equivalence classes in a given CCZ-equivalence class. More importantly, we prove that it is possible to go from a specific member of any EA-equivalence class to a specific member of another EA-equivalence class in the same CCZ-equivalence class using an operation called *twisting*; so that CCZ-equivalence can be reduced to the association of EA-equivalence and twisting. Twisting a function is a simple process and its possibility is equivalent to the existence of a particular decomposition of the function considered. Using this knowledge, we revisit several results from the literature on CCZ-equivalence and show how they can be interpreted in light of our new framework.

Our results rely on a new concept, the "thickness" of a space (or linear permutation), which can be of independent interest.

Keywords: Boolean functions · CCZ-Equivalence · EA-equivalence · Twist · APN · Butterfly

1 Introduction

Boolean functions and vectorial Boolean functions are crucial components of most symmetric cryptosystems. Their differential and linear properties can be used to prove that a primitive such as a block cipher or a message authentication code is safe from differential [BS91a, BS91b] and linear [Mat94] cryptanalysis.

The *Difference Distribution Table (DDT)* of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a two-dimensional array of positive integers of size $2^n \times 2^m$ denoted δ_F such that $\delta_F(a, b)$ is the number of solutions of the equation

$$F(x + a) + F(x) = b \ .$$

*This paper was accepted for publication in *Finite Fields and their Applications*.

†The work of Léo Perrin was supported by a post-doc grant of the *Fondation Sciences Mathématiques de Paris (FSMP)*.

The maximum coefficient in the DDT for $a \neq 0$ is called the *differential uniformity* of F [Nyb94]. The lower it is, the more resilient a cipher using F may be against differential attacks. Similarly, its *Linear Approximation Table (LAT)* or *Walsh spectrum* is a two-dimensional array of signed integers of size $2^n \times 2^m$ denoted $\mathcal{W}_F$ such that

$$\mathcal{W}_F(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b \cdot F(x)} \ .$$

The maximum coefficient in the LAT for $b \neq 0$ is the *linearity* of F. Again, we want this coefficient to be as low as possible as this may improve the security of a cipher using F against linear attacks.

A function offering ideal protection against differential cryptanalysis is one for which the differential uniformity is minimal. The optimal differential uniformity is equal to 2 and the functions reaching this bound are called *Almost Perfect Non-linear (APN)* [NK93]. There are many known infinite classes of APN functions. For example, the Gold functions defined over the finite field $\mathbb{F}_{2^n}$ by the monomials of the form x^{2^i+1} with $\gcd(i,n) = 1$ are APN for all $n > 1$. However, when n is even, they are not permutations. In fact, whether there exists an APN permutation operating on an even number of variables is an open problem.

It was partially solved by Dillon et al. when they found an APN permutation of $\mathbb{F}_2^6$ [BDMW10]. A more general solution is still missing despite a decomposition of this permutation in [PUB16] which was followed by several generalizations of the corresponding structure [CDP17, FFW17, LTYW18].

The differential uniformity is preserved by different forms of equivalence between (vectorial) Boolean functions. For example, it is easy to see that *extended-affine equivalence* preserves it, where EA-equivalence is defined as follows.

Definition 1 (EA-Equivalence)**.** *Two functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are* extended-affine equivalent (EA-equivalent) *if there exist two affine permutations $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $B : \mathbb{F}_2^m \to \mathbb{F}_2^m$ and an affine function $C : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that*

$$F(x) = (B \circ G \circ A)(x) + C(x) \ .$$

The most general form of function equivalence that is known to preserve the differential uniformity is *CCZ-equivalence*, of which EA-equivalence is a particular case. It was named after Carlet, Charpin and Zinoviev who introduced it in [CCZ98].

Definition 2 (CCZ-Equivalence)**.** *Two functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are CCZ-equivalent if there exists an affine permutation $\mathcal{A}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ such that*

$$\left\{ (x, F(x)), x \in \mathbb{F}_2^n \right\} \ = \ \mathcal{A}\left(\left\{ (x, G(x)), x \in \mathbb{F}_2^n \right\} \right) \ .$$

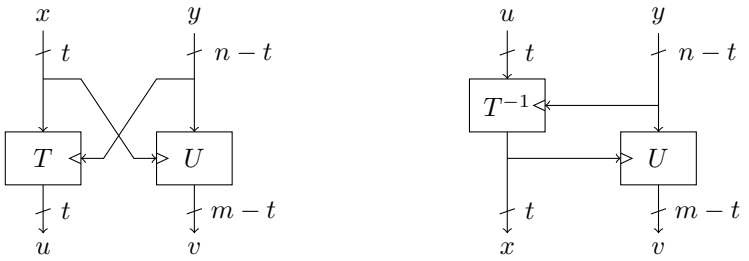
As EA-equivalence and CCZ-equivalence are equivalence relations, and since EA-equivalence is a particular case of CCZ-equivalence, it is possible to partition the space of all functions $\mathbb{F}_2^n \to \mathbb{F}_2^m$ into CCZ-equivalence classes and then to partition each CCZ-equivalence class into EA-equivalence classes. For brevity, we shorten "EA-equivalence class" into "EA-class" and "CCZ-equivalence class" into "CCZ-class".

CCZ-equivalence played a crucial role in allowing Dillon et al. to find an APN permutation on 6 bits. Indeed, they first found an APN quadratic function, the so-called "Kim mapping", and then built a permutation from it in such a way that the permutation had to be in the same CCZ-class. Since CCZ-equivalence preserves the differential uniformity, this permutation has to be APN as well.

Despite this usefulness, CCZ-equivalence is not well understood. It was shown by Budaghyan and Carlet [BC10] to be more general than EA-equivalence but, to the best of our knowledge, we do not even know how to partition the CCZ-class of a function into its EA-classes.

Our Contribution. In this paper, we characterize CCZ-equivalence by identifying a simple relation between special structures in the LAT of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ (or equivalently in its DDT) and the EA-classes of the functions CCZ-equivalent to it.

Furthermore, we show that it is possible to navigate between the EA-classes in the CCZ-class of a function using an operation which we call *t-twisting*, where $t \leq \min(m, n)$. As a consequence, we show that CCZ-equivalence can be fully described as the combination of two different forms of equivalences: EA-equivalence and twist-equivalence. Each t-twist equivalence class contains at most two functions, in which case they must have the structures described in Figures 1a and 1b where $T_y : \mathbb{F}_2^t \to \mathbb{F}_2^t$ must be a permutation for all $y \in \mathbb{F}_2^{n-t}$.



(a) F. **(b)** G.

Figure 1: *Two t-twist-equivalent functions.*

A t-twist is obtained by applying a particular matrix M_t called a *swap matrix* on $\{(x, F(x)), \forall x \in \mathbb{F}_2^n\}$. These swap matrices, together with the related concept of *thickness of a vector space*, will play a crucial role in our proofs. They may also be of independent interest: we show in particular that any vector space V of $\mathbb{F}_2^{n+m}$ of dimension n can be written

$$V = (\Lambda^T \times M_t)(\mathcal{V}) \ ,$$

where $\mathcal{V} = \{(x, 0), \forall x \in \mathbb{F}_2^n\}$, and where Λ is such that $\Lambda^T(\mathcal{V}) = \mathcal{V}$.

Using this framework, we revisit some results from the literature and show how they can be explained more intuitively with it. We are also able to provide upper and lower bounds for the number of EA-equivalence classes in the CCZ-equivalence class of any function.

Outline. The necessary notations and basic mathematical concepts are introduced in Section 2. We then present our framework linking structures in the LAT to EA-classes in Section 3. The remainder of the paper is based on this framework. Twisting and its relationship with CCZ-equivalence are described in Section 4 where we also introduce swap matrices and some of their properties. Section 5 presents some results on partitioning a CCZ-equivalence class into its constitutive EA-equivalence classes. We then revisit some results from the literature on CCZ-equivalence in light of our results in Section 6. Section 7 concludes the paper.

2 Preliminaries

We consider vectorial Boolean functions, that is functions mapping $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ for some non-zero m and n. For such a function F, the Difference Distribution Table (DDT) is a $2^n \times 2^m$ table δ_F of positive integers such that, for any $(a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$,

$$\delta_F(a, b) = \#\{x \in \mathbb{F}_2^n, F(x + a) + F(x) = b\} \ .$$

Similarly, the Linear Approximation Table (LAT) or Walsh spectrum is a $2^n \times 2^m$ table $\mathcal{W}_F$ of signed integers such that, for any $(a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$,

$$\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b \cdot F(x)} ,$$

where $y \cdot z$ denotes the scalar product of two elements $(y_0, ..., y_{k-1})$ and $(z_0, ..., z_{k-1})$ of $\mathbb{F}_2^k$ which is given by $y \cdot z = \sum_{i=0}^{k-1} y_i z_i$.

It is well-known [CV95, BN13] that the DDT and the squared LAT are related by a Fourier transform:

$$\mathcal{W}_F^2(\lambda, \mu) = \sum_{a \in \mathbb{F}_2^n} \sum_{b \in \mathbb{F}_2^m} (-1)^{a \cdot \lambda + b \cdot \mu} \delta_F(a, b) \quad (1)$$

$$\delta_F(a, b) = 2^{-(n+m)} \sum_{\lambda \in \mathbb{F}_2^n} \sum_{\mu \in \mathbb{F}_2^m} (-1)^{a \cdot \lambda + b \cdot \mu} \mathcal{W}_F^2(\lambda, \mu) . \quad (2)$$

If $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a function and $\alpha \in \mathbb{F}_2^m$ is not equal to 0 then $x \mapsto \alpha \cdot F(x)$ is a *component* of F. If the Hamming weight of α is one, the component is called a *coordinate*.

An element $u \in \mathbb{F}_2^n$ is a *c-linear structure* for a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ if $f(x + u) + f(x) = c$ for some constant $c \in \mathbb{F}_2$ and for all $x \in \mathbb{F}_2^n$.

We use I_k to denote the identity matrix operating on $\mathbb{F}_2^k$, i.e. a $k \times k$ binary matrix where the only non-zero coefficients are those on the diagonal.

We use Γ_F to denote the codebook of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, so that

$$\Gamma_F = \left\{ (x, F(x)) , x \in \mathbb{F}_2^n \right\} .$$

We let $\mathcal{V} = \{(x, 0), x \in \mathbb{F}_2^n\}$ and $\mathcal{V}^\perp = \{(0, x) \in \mathbb{F}_2^m\}$ be two orthogonal subspaces of $\mathbb{F}_2^n \times \mathbb{F}_2^m$.

2.1 Particular Linear Permutations

Two types of affine permutations of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ will play a crucial role in this paper: *EA* (and *EL*) mappings, and *admissible* mappings. In this paper, we always represent a linear function L from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$ by an $m \times n$-matrix M such that $L(x) = Mx$ where the input $x \in \mathbb{F}_2^n$ is seen as an n-bit column vector.

Definition 3 (EA-mapping, EL-mapping)**.** *We call EL-mapping of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ a linear permutation of this set whose matrix representation is of the shape*

$$\begin{bmatrix} a & 0 \\ b & c \end{bmatrix} ,$$

where a is an n-bit linear permutation, c is an m-bit linear permutation and $b : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a linear function. We call EA-mapping of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ an affine permutation of this set whose linear part is an EL-mapping.

The set of all EL-mappings (resp. EA-mappings) for given n and m is denoted $\mathcal{M}^{EL}$ (resp. $\mathcal{M}^{EA}$).

It is worth noticing that the inverse of an EL-mapping (resp. EA-mapping) is an EL-mapping (resp. EA-mapping) too because

$$\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}^{-1} = \begin{bmatrix} a^{-1} & 0 \\ c^{-1} b a^{-1} & c^{-1} \end{bmatrix} .$$

As the composition of two EL-mappings is also an EL-mapping and as the identity is one, we can conclude that $\mathcal{M}^{\mathrm{EL}}$ (resp. $\mathcal{M}^{\mathrm{EA}}$) is a group under composition. Furthermore, such permutations have a close relationship with the vector space $\mathcal{V} = \{(x, 0), x \in \mathbb{F}_2^n\}$ given by the following lemma.

Lemma 1. *EL-mappings are exactly the linear mappings whose transpose maps $\mathcal{V}$ to itself. Therefore, if $\mathcal{L}$ is a linear permutation of $\mathbb{F}_2^{n+m}$ such that $\mathcal{L}(\mathcal{V}) = \mathcal{V}$, then $\mathcal{L}^T \in \mathcal{M}^{EL}$.*

Two functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are CCZ-equivalent (resp. EA-equivalent) if and only if there exists an affine permutation $\mathcal{A}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ (resp. an EA-mapping) such that

$$\mathcal{A}(\Gamma_F) \;=\; \Gamma_G \;.$$

In general, given a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and an affine permutation $\mathcal{A}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$, there a priori does not exist a function G such that

$$\mathcal{A}\big(\{(x, F(x)), \forall x \in \mathbb{F}_2^n\}\big) = \{(x, G(x)), \forall x \in \mathbb{F}_2^n\} \;.$$

Indeed, it is necessary for G to be well-defined that the left-hand side of the output of $x \mapsto \mathcal{A}(x, F(x))$ is a permutation. As a consequence, only a few permutations $\mathcal{A}$ yield valid functions G. The following definition captures this intuition.

Definition 4 (Admissible affine permutations)**.** *Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. We say that the affine permutation $\mathcal{A}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ is* admissible for F *if we can define a function G such that*

$$\mathcal{A}\big(\Gamma_F\big) = \Gamma_G \;.$$

If $\mathcal{A}(x, y) = (\mathcal{A}_1(x, y), \mathcal{A}_2(x, y))$ with $\mathcal{A}_1 : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2^n$ and $\mathcal{A}_2 : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2^m$, then $\mathcal{A}$ is admissible for F if and only if $x \mapsto \mathcal{A}_1(x, F(x))$ is a permutation of $\mathbb{F}_2^n$.

For example, an EA-mapping is always admissible, which is why EA-equivalence is well-defined. On the other hand there are functions for which there are admissible mappings which are not EA-mappings. That is why CCZ-equivalence is more general than EA-equivalence.

Another simple type of admissible mapping corresponds to the functional inversion. Indeed, if P is a permutation of $\mathbb{F}_2^n$, then the following mapping $\mathcal{L}$ is admissible

$$\mathcal{L} = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}$$

as it maps the graph of P to that of P^{-1}.

CCZ-equivalence and equivalence of codes. The main cryptographic properties (e.g. the APN property, the linearity...) can be interpreted as conditions on some binary linear codes, as first shown in [CCZ98]. To this end, any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is associated to the linear binary code $\mathcal{C}_F$ of length 2^n defined by the following $(n + m + 1) \times 2^n$ generator matrix

$$G_F = \begin{bmatrix} 1 & \cdots & 1 & \cdots & 1 \\ 0 & \cdots & x_i & \cdots & x_{2^n-1} \\ F(0) & \cdots & F(x_i) & \cdots & F(x_{2^n-1}) \end{bmatrix}, \tag{3}$$

where $\{0, x_1, \ldots, x_{2^n-1}\} = \mathbb{F}_2^n$ and each entry in the matrix is viewed as a binary column-vector. In other words, $\mathcal{C}_F$ is the linear subspace of $\mathbb{F}_2^{2^n}$ spanned by the rows of G_F. It

is worth noticing that the code $\mathcal{C}_F$ has dimension $(n+m+1)$ if and only if F does not have any linear component, which is the situation we focus on [CCD00, Th. 2.7].

Obviously, two linear binary codes C_1 and $\mathcal{C}_2$ of length n and dimension k with generator matrices G_1 and G_2 are equal if and only if there exists some $k \times k$ invertible matrix M such that $G_2 = MG_1$. Moreover, two linear binary codes are said *equivalent* [MS77, Page 39] if they differ only in the order of symbols, i.e. if there exist an $n \times n$ permutation matrix P and a $k \times k$ invertible matrix M such that $G_2 = MG_1P$.

It directly follows from this definition that CCZ-equivalence coincides with the usual notion of equivalence between the corresponding codes $\mathcal{C}_F$ as pointed out in [BDKM09].

Proposition 1. *[BDKM09, Th. 6.2] Let F_1 and F_2 be two functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ without any linear component. Then, F_1 and F_2 are CCZ-equivalent if and only if the linear codes $\mathcal{C}_{F_1}$ and $\mathcal{C}_{F_2}$ are equivalent.*

More precisely, the affine permutation $\mathcal{A}$ of $\mathbb{F}_2^{n+m}$ of the form $\mathcal{A}(x) = Mx + c$ where M is an $(n+m) \times (n+m)$ invertible matrix and $c \in \mathbb{F}_2^{n+m}$ satisfies $\Gamma_G = \mathcal{A}(\Gamma_F)$ if and only if there exists a permutation matrix P such that $G_{F_2} = M' G_{F_1} P$ where

$$M' = \left[\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline c & & M & \end{array}\right] .$$

2.2 CCZ-Equivalence, DDT and LAT

In Section 3, we identify necessary and sufficient conditions for a mapping $\mathcal{A}$ to be admissible. As these conditions depend on the DDT and LAT of the function, we first recall some well-known results regarding them.

Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ and $\mathcal{A}$ be an affine permutation of $\mathbb{F}_2^n \times \mathbb{F}_2^m$:

$$\begin{array}{rcl} \mathcal{A} : \mathbb{F}_2^n \times \mathbb{F}_2^m & \to & \mathbb{F}_2^n \times \mathbb{F}_2^m \\ (x, y) & \mapsto & (\mathcal{A}_1(x, y), \mathcal{A}_2(x, y)) \end{array}$$

which is admissible for F. We define

$$F_1 : x \mapsto \mathcal{A}_1(x, F(x)) \text{ and } F_2 : x \mapsto \mathcal{A}_2(x, F(x))$$

and we note that, since $\mathcal{A}$ is admissible, F_1 is a permutation of $\mathbb{F}_2^n$. We can then define the function G from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ by

$$G = F_2 \circ F_1^{-1}(x) = \mathcal{A}_2\left(F_1^{-1}(x), F \circ F_1^{-1}(x)\right) .$$

Proposition 2. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be such that $\Gamma_G = \mathcal{A}(\Gamma_F)$ for some affine permutation $\mathcal{A}$ of $\mathbb{F}_2^{n+m}$. Let $\mathcal{L}$ denote the linear part of $\mathcal{A}$, i.e., $\mathcal{A}(x) = \mathcal{L}(x) + c$ for some constant $c \in \mathbb{F}_2^{n+m}$. Then the DDT and LAT of G are given by*

$$\begin{aligned} \delta_G(a, b) &= \delta_F(\mathcal{L}^{-1}(a, b)) , \\ \mathcal{W}_G(\alpha, \beta) &= (-1)^{c \cdot (\alpha, \beta)} \mathcal{W}_F(\mathcal{L}^T(\alpha, \beta)) . \end{aligned}$$

Proof. By definition, $\delta_G(a, b)$ equals the number of pairs (x, x') of elements in $\mathbb{F}_2^n$ such that

$$x + x' = a \text{ and } G(x) + G(x') = b$$

or equivalently, the number of $y = F_1^{-1}(x)$ and $y' = F_1^{-1}(x')$ such that

$$F_1(y) + F_1(y') = a \text{ and } F_2(y) + F_2(y') = b$$

This system corresponds to

$$\mathcal{L}_1\left(y+y', F(y)+F(y')\right) = a \text{ and } \mathcal{L}_2\left(y+y', F(y)+F(y')\right) = b$$

where $\mathcal{L}_1$ and $\mathcal{L}_2$ are the linear parts of $\mathcal{A}_1$ and $\mathcal{A}_2$. Equivalently

$$\left(y+y', F(y)+F(y')\right) = \mathcal{L}^{-1}(a,b) \ .$$

The number of pairs satisfying this equation is then $\delta_F(\mathcal{L}^{-1}(a,b))$.

Let us now look at the LAT. The value of $\mathcal{W}_G(\alpha,\beta)$ is determined by the number of $x \in \mathbb{F}_2^n$ such that

$$\beta \cdot G(x) + \alpha \cdot x = 0 \ .$$

By setting $y = F_1^{-1}(x)$, the left-hand term of this equation can be replaced by

$$\begin{aligned}
\beta \cdot F_2(y) + \alpha \cdot F_1(y) &= \beta \cdot \mathcal{A}_2(y, F(y)) + \alpha \cdot \mathcal{A}_1(y, F(y)) \\
&= \beta \cdot \mathcal{L}_2(y, F(y)) + \alpha \cdot \mathcal{L}_1(y, F(y)) + c \cdot (\alpha, \beta) \\
&= (\alpha, \beta) \cdot \mathcal{L}(y, F(y)) + c \cdot (\alpha, \beta) \\
&= \mathcal{L}^T(\alpha, \beta) \cdot (y, F(y)) + c \cdot (\alpha, \beta)
\end{aligned}$$

by using that, for any linear function $\mathcal{L}$ and any pair (x,y), $x \cdot \mathcal{L}(y) = \mathcal{L}^T(x) \cdot y$ where $\mathcal{L}^T$ is the linear function corresponding to the transpose of the matrix defining $\mathcal{L}$. □

As a consequence, if $\mathcal{A}$ is an EA-mapping then the correspondence between the DDT of F and that of G is given by an EL-mapping and the correspondence between their LATs is given by the transpose of an EL-mapping.

3 Table-Based Characterization of CCZ-Equivalence

In this section, we identify a relation between the mappings admissible for a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and the vector spaces of dimension n in the positions of the coefficients equal to 0 in its LAT. An identical relationship exists between EA-classes and vector spaces of zeroes of dimension m in the DDT. These are described in Theorem 1.

The relationship between these vector spaces and CCZ-equivalence was first hinted in [BDMW10] where Dillon *et al.* found an APN permutation in dimension six through finding a permutation in the CCZ-class of an APN function.

3.1 Vector Spaces of Zeroes

Recall that $\mathcal{V} = \{(x,0), x \in \mathbb{F}_2^n\}$ and $\mathcal{V}^\perp = \{(0,x) \in \mathbb{F}_2^m\}$ are two subspaces of $\mathbb{F}_2^n \times \mathbb{F}_2^m$, the first being of dimension n and the second of dimension m. Note that the span of $\mathcal{V} \cup \mathcal{V}^\perp$ is $\mathbb{F}_2^n \times \mathbb{F}_2^m$.

In this section, we investigate the roles played by some specific vector spaces found in sets defined via the LAT or the DDT of a function.

Definition 5 (Walsh Zeroes)**.** *Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. We call* Walsh zeroes of F *the set*

$$\mathcal{Z}_F = \left\{(\alpha,\beta) \in \mathbb{F}_2^n \times \mathbb{F}_2^m, \ \mathcal{W}_F(\alpha,\beta) = 0\right\} \cup (0,0) \ .$$

Definition 6 (Impossible Differential Set)**.** *For a function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, we denote $\mathcal{Z}_F^D$ the* impossible differential set of F*. It is defined as*

$$\mathcal{Z}_F^D = \{(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m, \ \delta_F(a,b) = 0\} \cup (0,0) \ .$$

Using the correspondence between the DDT and the squared LAT, we observe that these two sets are related in the following sense.

Proposition 3. *Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. Let V be a linear subspace of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ of dimension n. Then, $V \subseteq \mathcal{Z}_F$ if and only if $V^\perp \subseteq \mathcal{Z}_F^D$.*

Proof. Using Relation (1), we get that, for any linear subspace V of $\mathbb{F}_2^n \times \mathbb{F}_2^m$,

$$\begin{aligned}\sum_{(\lambda,\mu)\in V} \mathcal{W}_F^2(\lambda,\mu) &= \sum_{(\lambda,\mu)\in V} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^m} (-1)^{a\cdot\lambda+b\cdot\mu}\delta_F(a,b) \\ &= \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^m} \delta_F(a,b)\left(\sum_{(\lambda,\mu)\in V}(-1)^{a\cdot\lambda+b\cdot\mu}\right) \\ &= 2^{\dim(V)} \sum_{(a,b)\in V^\perp} \delta_F(a,b)\end{aligned}$$

where the last equality is deduced from the fact that

$$\sum_{(\lambda,\mu)\in V}(-1)^{a\cdot\lambda+b\cdot\mu} = \begin{cases} 2^{\dim(V)} & \text{if } (a,b)\in V^\perp \\ 0 & \text{otherwise.}\end{cases}$$

Obviously, $V \subseteq \mathcal{Z}_F$ if and only if

$$\sum_{(\lambda,\mu)\in V} \mathcal{W}_F^2(\lambda,\mu) = \mathcal{W}_F^2(0,0) = 2^{2n}.$$

Moreover, we have proved that

$$\sum_{(\lambda,\mu)\in V} \mathcal{W}_F^2(\lambda,\mu) = 2^{2n} \text{ if and only if } \sum_{(a,b)\in V^\perp} \delta_F(a,b) = 2^{2n-\dim V}\ .$$

Using that $\delta_F(0,0) = 2^n$, we deduce that, when $\dim V = n$, this equivalently means that $V^\perp \subseteq \mathcal{Z}_F^D$. □

Lemma 2 then shows that the Walsh zeroes (resp. the impossible differential sets) of two CCZ-equivalent functions are strongly related.

Lemma 2. *For two functions F and G mapping $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, if $\Gamma_G = \mathcal{A}(\Gamma_F)$ for some affine permutation $\mathcal{A}$ of $\mathbb{F}_2^{n+m}$, then*

$$\mathcal{Z}_G = (\mathcal{L}^T)^{-1}(\mathcal{Z}_F) \quad \text{and} \quad \mathcal{Z}_G^D = \mathcal{L}(\mathcal{Z}_F^D)\ ,$$

where $\mathcal{L}$ is the linear part of $\mathcal{A}$.

These sets must contain some specific vector spaces in all cases, as formally stated by the following proposition.

Proposition 4. *Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, let $\mathcal{Z}_F$ be its Walsh zeroes and let $\mathcal{Z}_F^D$ be its impossible differential set. Then the following is always true:*

$$\mathcal{V} \subseteq \mathcal{Z}_F \text{ and } \mathcal{V}^\perp \subseteq \mathcal{Z}_F^D\ .$$

Proof. We prove the proposition in terms of Walsh zeroes. The formulation in terms of impossible differential set then follows directly using Proposition 3.

If $(a,b) \in \mathcal{V}$, then $b = 0$. For all such elements with $a \neq 0$,

$$\mathcal{W}_F(a,b) = \sum_{x\in\mathbb{F}_2^n}(-1)^{a\cdot x+0\cdot F(x)} = \sum_{x\in\mathbb{F}_2^n}(-1)^{a\cdot x} = 0,$$

so that $(a,b) \in \mathcal{Z}_F$. As we have imposed $(0,0) \in \mathcal{Z}_F$, we conclude that $\mathcal{V} \subseteq \mathcal{Z}_F$ for any F. □

The following theorem is what most of our results are based on. It gives a simple necessary and sufficient condition for an affine mapping to be admissible.

Theorem 1. *Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, let $\mathcal{A}$ be an affine permutation of $\mathbb{F}_2^n \times \mathbb{F}_2^m$, and $\mathcal{L}$ its linear part. Then, the following three statements are equivalent:*

1. *$\mathcal{A}$ is admissible for F*
2. *$\mathcal{L}^T(\mathcal{V}) \subseteq \mathcal{Z}_F$*
3. *$\mathcal{L}^{-1}(\mathcal{V}^\perp) \subseteq \mathcal{Z}_F^D$.*

Proof. Recall that $\mathcal{A}$ is admissible for F if and only if $x \mapsto \mathcal{L}_1(x, F(x))$ is a permutation, where $\mathcal{L}(x, y) = (\mathcal{L}_1(x, y), \mathcal{L}_2(x, y))$.

1 $\Leftrightarrow$ 2. The function $x \mapsto \mathcal{L}_1(x, F(x))$ is a permutation if and only if all of its components are balanced, i.e. if and only if

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot \mathcal{L}_1(x, F(x))} = 0, \ \forall a \in (\mathbb{F}_2^n)^* \ ,$$

which can be re-written as

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{(a,0) \cdot \mathcal{L}(x, F(x))} = 0, \ \forall a \in (\mathbb{F}_2^n)^* \ .$$

Using the fact that $(a, b) \cdot \mathcal{L}(x, y) = \mathcal{L}^T(a, b) \cdot (x, y)$, we have that $\mathcal{L}$ (and $\mathcal{A}$) are admissible for F if and only if

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{\mathcal{L}^T(a,0) \cdot (x, F(x))} = 0, \ \forall a \in (\mathbb{F}_2^n)^* \ ,$$

which is equivalent to saying that $\mathcal{L}^T(\mathcal{V}) \subseteq \mathcal{Z}_F$.

2 $\Leftrightarrow$ 3. From Proposition 3, we have that $\mathcal{L}^T(\mathcal{V}) \subseteq \mathcal{Z}_F$ if and only if $\left(\mathcal{L}^T(\mathcal{V})\right)^\perp \subseteq \mathcal{Z}_F^D$. We now use the fact that an element x belongs to $\left(\mathcal{L}^T(\mathcal{V})\right)^\perp$ if and only if it satisfies for all $v \in \mathcal{V}$

$$x \cdot \mathcal{L}^T(v) = 0 \Leftrightarrow \mathcal{L}(x) \cdot v = 0 \ .$$

This equivalently means that $\mathcal{L}(x)$ belongs to $\mathcal{V}^\perp$, i.e., $x \in \mathcal{L}^{-1}(\mathcal{V}^\perp)$.

□

In terms of codes. It is well-known that the weight distribution of the code $\mathcal{C}_F$ associated to F carries exactly the same information as the squared Walsh spectrum of the function [CCZ98, BDKM09]. Indeed, the weights of all codewords in $\mathcal{C}_F$ correspond to

$$\mathcal{W} = \{\mathrm{wt}\left((\varepsilon, a, b)G_F\right), \ \varepsilon \in \mathbb{F}_2, a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m\}$$

where G_F is the generator matrix defined by (3). Using that

$$\mathrm{wt}\left((\varepsilon, a, b)G_F\right) = 2^{n-1} + (-1)^{\varepsilon+1}\mathcal{W}_F(a, b) \ ,$$

we deduce that

$$\mathcal{W} = \left\{2^{n-1} \pm \left|\mathcal{W}_F(a, b)\right|, \ a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m\right\} \ .$$

Therefore, the Walsh zeroes of F, $\mathcal{Z}_F$, correspond to the *balanced codewords* in $\mathcal{C}_F$. Moreover, any linear subspace of dimension n in $\mathcal{Z}_F$ coincides with a subcode of $\mathcal{C}_F$

of dimension $(n+1)$, composed of the all-zero word, the all-one word and balanced codewords. It is well-known that any code with this weight distribution is equivalent to the first-order Reed-Muller code (i.e., the extended Simplex code) [CV09]. It follows that Theorem 1 equivalently means that there is a correspondence between admissible mappings for F and the first-order Reed-Muller subcodes of $\mathcal{C}_F$. This property has been already observed by Dillon *et al.* [BDMW10] with a slightly different formulation since they focused on functions with $F(0) = 0$ and considered the simplex subcodes of a shortened version of $\mathcal{C}_F$.

3.2 A First Partition of CCZ-Classes

The mappings admissible for a given function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are then exactly the mappings whose transpose of the linear part maps $\mathcal{V}$ to a linear subspace of $\mathcal{Z}_F$. In order to further characterize the CCZ-class of F, we then gather together all affine permutations having the same $\mathcal{L}^T(\mathcal{V})$.

Definition 7. *Let V be a linear subspace of $\mathbb{F}_2^{n+m}$ such that $\dim V = n$. We denote by $\mathcal{S}(V)$ the set of all affine permutations of $\mathbb{F}_2^{n+m}$ whose linear part $\mathcal{L}$ satisfies $\mathcal{L}^T(\mathcal{V}) = V$.*

We have then proved that the set of all mappings admissible for F corresponds to the union of all $\mathcal{S}(V)$, where V varies in the set of all n-dimensional linear spaces in $\mathcal{Z}_F$.

The following lemma gives a simple relation between EA-classes and the sets $\mathcal{S}(V)$.

Lemma 3. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G' : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be three functions such that $\Gamma_G = \mathcal{A}(\Gamma_F)$ and $\Gamma_{G'} = \mathcal{A}'(\Gamma_F)$ for some affine permutations $\mathcal{A}$ and $\mathcal{A}'$ of $\mathbb{F}_2^{m+n}$.*

If both $\mathcal{A}$ and $\mathcal{A}'$ belong to the same $\mathcal{S}(V)$ for some n-dimensional linear space V, then G and G' are EA-equivalent.

Proof. Let $\mathcal{L}$ and $\mathcal{L}'$ denote the linear parts of $\mathcal{A}$ and $\mathcal{A}'$. The two affine permutations $\mathcal{A}$ and $\mathcal{A}'$ belong to the same $\mathcal{S}(V)$ if and only if $\mathcal{L}^T(\mathcal{V}) = \mathcal{L}'^T(\mathcal{V})$, or equivalently $((\mathcal{L}^T)^{-1} \circ \mathcal{L}'^T)(\mathcal{V}) = \mathcal{V}$. As $(\mathcal{L}' \circ \mathcal{L}^{-1})^T$ leaves $\mathcal{V}$ unchanged, Lemma 1 imposes the existence of an EL-mapping Λ such that $(\mathcal{L}' \circ \mathcal{L}^{-1}) = \Lambda$. We deduce that $\mathcal{L}' = \Lambda \times \mathcal{L}$.

We know from the hypothesis that $\Gamma_{G'} = \mathcal{L}'(\Gamma_F) + c'$ for some constant $c' \in \mathbb{F}_2^{n+m}$. Using the equality we established in the previous paragraph, we deduce that

$$\Gamma_{G'} = (\Lambda \circ \mathcal{L})(\Gamma_F) + c' = \Lambda(\Gamma_G + c) + c' = \Lambda(\Gamma_G) + c''$$

for some constant $c'' \in \mathbb{F}_2^{n+m}$. Since Λ is an EL-mapping, we thus have that G and G' are EA-equivalent. □

In other words, if two mappings $\mathcal{A}$ and $\mathcal{A}'$ are both admissible for F because of the same subspace of $\mathcal{Z}_F$, then applying them to the codebook of F yields two functions that are in the same EA-class. We deduce the following direct corollary.

Corollary 1. *The number of EA-classes in the CCZ-class of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is upper-bounded by the number of vector spaces of dimension n in $\mathcal{Z}_F$.*

While we have established that two admissible mappings in the same set $\mathcal{S}(V)$ lead to two functions in the same EA-class, the converse is not true. A simple counterexample appears when $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an involution. In this case,

$$\underbrace{\begin{bmatrix} I_n & 0 \\ 0 & I_n \end{bmatrix}}_{\mathcal{L}}(\Gamma_F) = \underbrace{\begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}}_{\mathcal{L}'}(\Gamma_F)$$

so that $\mathcal{L}$ and $\mathcal{L}'$ send Γ_F to the same EA-class (namely that of F) despite the fact that $\mathcal{L}(\mathcal{V}) = \mathcal{V} \neq \mathcal{L}'(\mathcal{V}) = \mathcal{V}^\perp$.

3.3 Thickness and its Properties

We now introduce a new quantity, named *thickness*, related to any vector space in $\mathbb{F}_2^{n+m}$ which is invariant under EL-mappings but *not* under general linear permutations of $\mathbb{F}_2^{n+m}$. We naturally extend this definition to obtain the *thickness of a linear permutation.*

Definition 8 (Thickness)**.** *Let V be a vector space of $\mathbb{F}_2^{n+m}$ of dimension n. We call* thickness of V *the dimension of the projection of V on $\mathcal{V}^\perp$. It is denoted $t(V)$. If $\mathcal{L}$ is a linear permutation of $\mathbb{F}_2^{n+m}$ such that $V = \mathcal{L}(\mathcal{V})$ and such that*

$$\mathcal{L} = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

then $t(V) = rank(c)$.

We thus define the thickness *of a linear permutation of $\mathbb{F}_2^{n+m}$ as the rank of its bottom left block matrix of dimension $m \times n$.*

The thickness of a vector space (or of a linear permutation) of $\mathbb{F}_2^{n+m}$ is an integer in $\{0, ..., \min(m, n)\}$.

This thickness has multiple properties formalized by the following lemma.

Lemma 4 (Thickness Properties)**.** *Thickness is not influenced by EL-mappings. More formally, the following two points always hold.*

1. *Let $\mathcal{L} : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ be a linear permutation and let Λ_1 and Λ_2 be two EL-mappings. Then*
$$t(\mathcal{L}) = t(\Lambda_2^T \times \mathcal{L} \times \Lambda_1^T) .$$
2. *Let $V \subset \mathbb{F}_2^{n+m}$ be a vector space of dimension n and Λ be an EL-mapping. Then $t(\Lambda^T(V)) = t(V)$.*

Proof. We prove the first point. The second follows directly.

Let Λ_1, Λ_2 and $\mathcal{L}$ be as in the lemma. Due to their structure, Λ_1^T and Λ_2^T are such that

$$\Lambda_1^T = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \text{ and } \Lambda_2^T = \begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix}$$

for some linear permutations a and a' (resp. c and c') of $\mathbb{F}_2^n$ (resp. $\mathbb{F}_2^m$). We also write

$$\mathcal{L} = \begin{bmatrix} d & e \\ f & g \end{bmatrix},$$

so that $t(\mathcal{L}) = \text{rank}(f)$ and that the bottom-left block matrix of $\Lambda_2^T \times \mathcal{L} \times \Lambda_1^T$ is equal to $c'fa$. As c' and a are permutations, we have that $\text{rank}(c'fa) = \text{rank}(f)$ and thus that $t(\mathcal{L}) = t(\Lambda_2^T \circ \mathcal{L} \circ \Lambda_1^T)$. □

It is worth noticing that we cannot alternatively consider the dimension of the projection of V on $\mathcal{V}$ instead of its projection on $\mathcal{V}^\perp$, since this second quantity is *not* invariant under EL-mappings.

We now use the concept of thickness to introduce a new quantity which is invariant under EA-equivalence but *not* under CCZ-equivalence.

Definition 9 (Thickness Spectrum of a Function)**.** *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function and let Σ_F be the set of all vector spaces of dimension n in $\mathcal{Z}_F$. The* thickness spectrum of F *is the set of all pairs of positive integers (t_i, N_i) such that, for all i:*

$$\#\{V \in \Sigma_F, t(V) = t_i\} = N_i > 0 .$$

For example, the thickness spectrum of a function always contains $(0, 1)$ as $\mathcal{V}$ is always in $\mathcal{Z}_F$ and it is the only space of dimension n with a thickness of 0.

Lemma 4 directly implies the following proposition.

Proposition 5. *If two functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are EA-equivalent, then they have the same thickness spectra.*

However, we will detail in Section 6.3 some examples of functions in the same CCZ-class with different thickness spectra. It then follows that such functions belong to distinct EA-classes.

4 Twist and CCZ-Equivalence

As we have established, a CCZ-class can be partitioned into its constitutive EA-classes using vector spaces of zeroes in the LAT or in the DDT of the function. In this section, we show that it is always possible to go from an EA-class to another in the same CCZ-class by applying a simple operation called *t-twisting*. Thus, together with EA-mappings, t-twists fully describe CCZ-equivalence.

The t-twist is closely related with a type of matrix called "swap matrix" which provides a link between the thickness of a vector space and a particular decomposition of it.

4.1 Function Twisting

In order to introduce *function twisting*, we first need to describe an object called *swap matrix*.

Let $e_0, ..., e_{p-1}$ be the canonical basis of $\mathbb{F}_2^p$ for any p. We define the linear projection $\rho_{i,j}$ as follows:

$$\rho_{i,j}\left(\sum_{k=0}^{p-1} \lambda_k e_k\right) = \sum_{k=i}^{j-1} \lambda_k e_k \ ,$$

so that $\rho_{0,t} + \rho_{t,p} = I_p$. If A is an $n \times n$ matrix, then $\rho_{i,j} \times A$ is obtained by setting all rows in A with index not in $\{i, ..., j-1\}$ to 0. Conversely, $A \times \rho_{i,j}$ is obtained by setting all columns with index not in $\{i, ..., j-1\}$ in A to 0.

Definition 10 (Swap Matrix)**.** *Let m, n be non-zero integers and let $t \leq \min(m, n)$. The t-*swap matrix*, denoted M_t, is an $(n+m)$-bit linear permutation defined as*

$$M_t = \begin{bmatrix} \rho_{t,n} & \rho_{0,t} \\ \rho_{0,t} & \rho_{t,m} \end{bmatrix} = \begin{bmatrix} 0 & 0 & I_t & 0 \\ 0 & I_{n-t} & 0 & 0 \\ I_t & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{m-t} \end{bmatrix} .$$

Swap matrices derive their name from the fact that they simply swap two t-bit parts of their input. Indeed, if (a, b, c, d) is a tuple from $\mathbb{F}_2^t \times \mathbb{F}_2^{n-t} \times \mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$ then

$$M_t \times [a \ b \ c \ d]^T \ = \ [c \ b \ a \ d]^T \ .$$

For any t, M_t is an orthogonal involution:

$$M_t = M_t^T = M_t^{-1} \ .$$

A particular case of such a matrix is obtained when $t = m = n$. In this case,

$$M_n = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}$$

and applying this matrix to Γ_F for a permutation $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ yields $\Gamma_{F^{-1}}$. Conversely, if $t = 0$ then M_0 is the identity.

Using such matrices for $0 \leq t \leq \min(m, n)$, we will be able to define a more general operation which we call *function twisting*. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function and let t be an integer such that $0 \leq t \leq \min(n, m)$. Then $\mathbb{F}_2^n$ can be identified with $\mathbb{F}_2^t \times \mathbb{F}_2^{n-t}$, $\mathbb{F}_2^m$ with $\mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$ and F can be written as

$$F(x, y) \;=\; (T_y(x), U_x(y)) \quad \text{where} \quad \begin{cases} \forall y \in \mathbb{F}_2^{n-t}, & T_y : \mathbb{F}_2^t \to \mathbb{F}_2^t \\ \forall x \in \mathbb{F}_2^t, & U_x : \mathbb{F}_2^{n-t} \to \mathbb{F}_2^{m-t}. \end{cases}$$

This decomposition is represented in Figure 2. We call (T, U) the *TU-projection of F for t*.

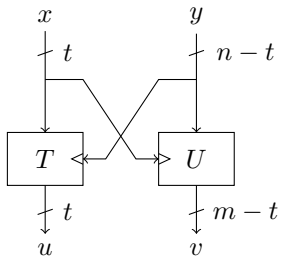


Figure 2: *TU projection.*

In [BLNW12], Bogdanov et al. showed that the existence of a balanced restriction of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is equivalent to a particular condition on $\mathcal{Z}_F$. In the following proposition, we state a particular case of their Proposition 1 and give a similar condition based on $\mathcal{Z}_F^D$.

Proposition 6. *Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, let t be an integer such that $1 \leq t \leq \min(n, m)$ and let (T, U) be the TU-projection of F for t.*

Then T_y is a permutation for all y if and only if

$$M_t(\mathcal{V}) \subseteq \mathcal{Z}_F \ .$$

Similarly, in terms of the DDT, T_y is a permutation for all y if and only if

$$M_t(\mathcal{V}^\perp) \subseteq \mathcal{Z}_F^D \ .$$

Proof. We prove the proposition using the impossible differential set. The case of the Walsh zeroes follows directly using Proposition 3.

The functions T_y are permutations for all y if and only if, for all nonzero $a \in \mathbb{F}_2^t$, it holds that

$$T_y(x + a) + T_y(x) \neq 0$$

for all $x \in \mathbb{F}_2^t$. As $F(x, y) = (T_y(x), U_x(y))$, $T_y(x + a) + T_y(x) \neq 0$ is equivalent to $F(x + a, y) + F(x, y) \neq (0, z)$ for all $(x, y, z) \in \mathbb{F}_2^t \times \mathbb{F}_2^{n-t} \times \mathbb{F}_2^{m-t}$. We deduce that T_y always being a permutation is equivalent to $\delta_F[(a, 0), (0, b)] = 0$ for all $(a, b) \neq (0, 0)$, which can be written $M_t(\mathcal{V}^\perp) \subseteq \mathcal{Z}_F^D$. □

Definition 11 (Function Twisting)**.** *Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, let t be an integer such that $1 \leq t \leq \min(m, n)$ and let (T, U) be the TU-projection of F for t.*

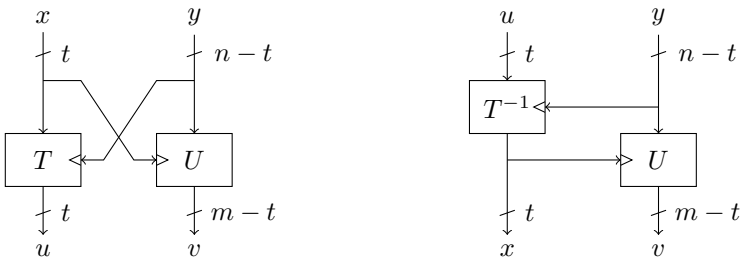
If T_y is a permutation for all $y \in \mathbb{F}_2^{n-t}$ then F is t-twist equivalent *to $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ defined as follows:*

$$G(x, y) \;=\; \left(T_y^{-1}(x), U_{T_y^{-1}(x)}(y)\right)$$

for any $(x, y) \in \mathbb{F}_2^t \times \mathbb{F}_2^{n-t}$. *In this case, it holds that*

$$\Gamma_G \;=\; M_t(\Gamma_F)\ .$$

This process is summarized in Figure 3.



(a) *Starting point.* **(b)** *End point.*

Figure 3: *Function twisting.*

Function twisting is its own inverse. Indeed, t-twisting G yields F' such that

$$F'(x,y) \;=\; \left(\left(T_y^{-1}\right)^{-1}(x), U_{T_y^{-1}\left((T_y^{-1})^{-1}(x)\right)}(y)\right) \;=\; (T_y(x), U_x(y)) \;=\; F(x,y)\ .$$

This is also a direct consequence of the fact that M_t is always an involution.

The link between swap matrix and t-twist has the following obvious consequence.

Lemma 5. *For any* $0 \leq t \leq \min(m,n)$, *t-twist equivalence is a particular case of CCZ-equivalence.*

This lemma can be seen as a generalization of Lemma 2 of [PUB16] which states the CCZ-equivalence of the closed and open butterfly structures.

To capture the fact that a function without a t-twist equivalent can be in the EA-class of a function which has one, we introduce the following notion.

Definition 12 (t-twistable function)**.** *Let* $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ *be a function. If there exists* $t \leq \min(m,n)$ *such that* F *is EA-equivalent to a function* F' *such that* $F'(x,y) = (T_y(x), U_x(y))$ *for some* t*-bit keyed permutation* T *and for all* $(x,y) \in \mathbb{F}_2^t \times \mathbb{F}_2^{n-t}$ *then we say that* F *is* t-twistable.

4.2 Some Special Twists

Some particular degenerate cases of function twisting are interesting as they have simple interpretations. They are listed in Section 4.2.1. Section 4.2.2 discusses the possibility of a 1-twist and shows its equivalence to the existence of linear structures.

4.2.1 Degenerate Cases

t = 0. In this case, no twist is actually performed as $M_t = I_{n+m}$. It is always possible.

t = m = n. As stated before, we have in this case

$$M_n = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}$$

and applying M_n to the graph of a permutation returns the graph of its functional inverse. In other words, an n-bit permutation is n-twistable.

$\mathbf{t = m}$, with $\mathbf{m < n}$. The case $n > m$ and $m = t$ can be seen as a generalization of the case of the functional inversion. In this case,

$$M_m = \begin{bmatrix} \rho_{m,n} & \rho_{0,m} \\ \rho_{0,m} & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & I_m \\ 0 & I_{n-m} & 0 \\ I_m & 0 & 0 \end{bmatrix}$$

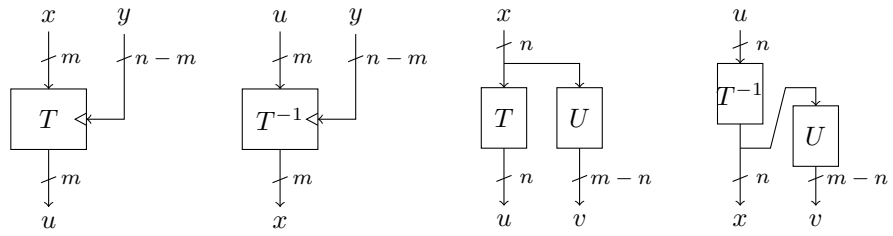
and M_m is admissible for $F : \mathbb{F}_2^m \times \mathbb{F}_2^{n-m} \to \mathbb{F}_2^m$ if and only if $F(x, y) = T_y(x)$ for some keyed permutation T. In this case, applying M_m to the graph of F returns the graph of $G : (x, y) \mapsto T_y^{-1}(x)$. Diagrams representing F and G are given in Figures 4a and 4b respectively.

Such a degenerate twist is observed for modular addition as explained in Section 6.1. It also exists in each S-Box of the DES [DES77] due to the fact that each of their row is a 4-bit permutation; so that they are all 4-twistable.

$\mathbf{n = t}$, with $\mathbf{m > n}$. In this case,

$$M_n = \begin{bmatrix} 0 & \rho_{0,n} \\ \rho_{0,n} & \rho_{n,m} \end{bmatrix} = \begin{bmatrix} 0 & I_n & 0 \\ I_n & 0 & 0 \\ 0 & 0 & I_{m-n} \end{bmatrix}$$

and M_n is admissible for $F : \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^{m-n}$ if and only if $F(x) = (T(x), U(x))$ for some permutation T. In this case, applying M_m to the graph of F returns the graph of $G : x \mapsto \big(T^{-1}(x), U(T^{-1}(x))\big)$. Diagram representing F and G are given in Figures 4c and 4d respectively.



(a) $t = m$. **(b)** $t = m$. **(c)** $t = n$. **(d)** $t = n$.

Figure 4: *Some degenerate cases of function twisting.*

4.2.2 On 1-Twistable Functions

Suppose that $t = 1$. In this case, we can give a better description of T_y using the following lemma.

Lemma 6. *A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is 1-twistable if and only if its EA-class contains $F' : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that*

$$F'(x, y) = \big(x + f(y), U_x(y)\big),\ \forall (x, y) \in \mathbb{F}_2 \times \mathbb{F}_2^{n-1}\ ,$$

where $f : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ is a Boolean function. In this case, F' is 1-twist equivalent to

$$G(x, y) \ = \ \big(x + f(y), U_{x+f(y)}(y)\big) \ = \ F'\big(x + f(y), y\big) + (f(y), 0)\ .$$

Proof. As we have established, F is 1-twistable if and only if it is EA-equivalent to F' such that $F'(x,y) = (T_y(x), U_x(y))$ for some T where T_y is a permutation of $\mathbb{F}_2$ for any $y \in \mathbb{F}_2^{n-1}$. As the only permutations of $\mathbb{F}_2$ are $x \mapsto x$ and $x \mapsto x+1$, there must exist a Boolean function f such that $T_y(x) = x + f(y)$. The lemma follows. □

We can deduce a simple relation between the fact that a function is 1-twistable and the existence of a linear structure.

Corollary 2. *A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ with $m, n \geq 2$ is 1-twistable if and only if some of its components have a linear structure.*

Proof. We simply need to show that F is EA-equivalent to F' such that

$$F'(x,y) = \big(x + f(y), U_x(y)\big),\ \forall (x,y) \in \mathbb{F}_2 \times \mathbb{F}_2^{n-1}\ ,$$

where $f : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ is a Boolean function if and only if there exists a component of F that has a linear structure. We will use that functions in a given EA-class have the same number of components with the same number of linear structures. Indeed, for $F' = A_2 \circ F \circ A_1 + A_0$, where the A_i are affine functions with linear parts L_i, we have that $u \in \mathbb{F}_2^n$ is a linear structure of $x \mapsto \lambda \cdot F'(x)$ if and only if $L_1(u)$ is a linear structure of $x \mapsto L_2^T(\lambda) \cdot F(x)$. This comes from the fact that

$$\lambda \cdot [F'(x+u) + F'(x)] = L_2^T(\lambda) \cdot [F(A_1(x) + L_1(u)) + F(A_1(x))] + \lambda \cdot L_0(u)\ .$$

$\Rightarrow$ Let F' be such that $F'(x,y) = \big(x + f(y), U_x(y)\big)$ and let F'_0 be its left-most bit. Then $F'_0(x+1, y) = x + 1 + f(y) = F'_0(x,y) + 1$. Thus, one coordinate of F' has a linear structure, implying that one component of F has a linear structure.

$\Leftarrow$ Suppose that one of the components of F has a linear structure: $(\alpha \cdot F)(z+u) + (\alpha \cdot F)(z) = \varepsilon$ for some $\alpha \in \mathbb{F}_2^m$, $u \in \mathbb{F}_2^n$ and $\varepsilon \in \mathbb{F}_2$. Then we choose a linear permutation L_1 of $\mathbb{F}_2^n$ such that $L_1(10\cdots0) = u$ and a linear permutation L_2 of $\mathbb{F}_2^m$ such that $L_2^T(10\cdots0) = \alpha$. Then, $10\cdots0$ is a linear structure of the left-most bit of $F' = L_2 \circ F \circ L_1 + L_0$ for any linear function L_0. Then, we choose for L_0 a function whose left-most coordinate ℓ is such that $\ell(10\cdots0) = \varepsilon + 1$. It follows that the left-most coordinate of $(F'(x + 10\cdots0) + F'(x))$ is given by

$$\begin{aligned} F'_0(x + 10\cdots0) + F'_0(x) &= L_2^T(10\cdots0) \cdot [F \circ L_1(x + 10\cdots0) + F \circ L_1(x)] \\ &\quad + \ell(10\cdots0) \\ &= \alpha \cdot [F(L_1(x) + u) + F(L_1(x))] + \varepsilon + 1 = 1\ . \end{aligned}$$

Then, the first coordinate of F' can be written as $(x,y) \mapsto x + f(y)$,

□

4.3 Swap Matrices and Space Thickness

It turns out that composing EA-mappings and functional twists is sufficient to fully describe CCZ-equivalence. We prove this statement in Section 4.4 but we first need to establish the following theorem which relates the thickness of a vector space to swap matrices. The remainder of this section then explores some consequences of this theorem.

Theorem 2. *Let $V \subseteq \mathbb{F}_2^{n+m}$ be a vector space of dimension n. Then there exists an EL-mapping Λ such that*

$$V = \big(\Lambda^T \times M_t\big)(\mathcal{V})\ ,$$

where $t = t(V) \leq \min(m,n)$.

Moreover, Λ can be written as

$$\Lambda = \begin{bmatrix} P & 0 \\ \rho_{0,t} \times \ell & Q \end{bmatrix}$$

for an n-bit linear permutation P, an m-bit linear permutation Q and a linear function $\ell : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

Proof. Let V be as defined in the theorem. Then there must exist two linear functions $L_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $L_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that

$$V = \left\{ \begin{bmatrix} L_1(x) \\ L_2(x) \end{bmatrix}, \forall x \in \mathbb{F}_2^n \right\} .$$

As by definition $t = \text{rank}(L_2)$, there exist two linear permutations Q' and R of $\mathbb{F}_2^m$ and $\mathbb{F}_2^n$ such that $L_2 = Q'\rho_{0,t}R$. We then let $y = R(x)$ in the previous expression and write

$$V = \left\{ \begin{bmatrix} L_1R^{-1}(y) \\ Q'\rho_{0,t}(y) \end{bmatrix}, \forall y \in \mathbb{F}_2^n \right\} .$$

Since $\rho_{0,t} + \rho_{t,n} = I_n$, we write $L_1R^{-1} = L_1R^{-1}\rho_{0,t} + L_1R^{-1}\rho_{t,n}$ and we further let $\ell' : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $P' : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be such that $\ell'\rho_{0,t} = L_1R^{-1}\rho_{0,t}$ and $L_1R^{-1}\rho_{t,n} = P'\rho_{t,n}$. We then have

$$V = \left\{ \begin{bmatrix} \ell'\rho_{0,t}(y) + P'\rho_{t,n}(y) \\ Q'\rho_{0,t}(y) \end{bmatrix}, \forall y \in \mathbb{F}_2^n \right\} . \tag{4}$$

Now, because Λ has the particular form given in the theorem, we have

$$\Lambda^T M_t = \begin{bmatrix} P^T & \ell^T\rho_{0,t} \\ 0 & Q^T \end{bmatrix} \times \begin{bmatrix} \rho_{t,n} & \rho_{0,t} \\ \rho_{0,t} & \rho_{t,m} \end{bmatrix} = \begin{bmatrix} P^T\rho_{t,n} + \ell^T\rho_{0,t} & P^T\rho_{0,t} \\ Q^T\rho_{0,t} & Q^T\rho_{t,m} \end{bmatrix} ,$$

so that

$$\Lambda^T M_t(\mathcal{V}) = \left\{ \begin{bmatrix} \ell^T\rho_{0,t}(x) + P^T\rho_{t,n}(x) \\ Q^T\rho_{0,t}(x) \end{bmatrix}, \forall x \in \mathbb{F}_2^n \right\} . \tag{5}$$

In order to prove the lemma, we simply need to show that Equations (4) and (5) can be made to be equal.

As Q' is a permutation, we can simply set $Q^T = Q'$. Similarly, as there is no specific condition on ℓ, we can freely set $\ell^T = \ell'$.

However, as P^T is assumed to be a permutation, we need to show that $P'\rho_{t,n}$ has rank $n - t$ to be able to set $P^T = P'$. Suppose that the image of $\{\rho_{t,n}(x), \forall x \in \mathbb{F}_2^n\}$ under $P'\rho_{t,n}$ is of dimension d. Using Equation (4), we deduce that $\dim(V) = t + d$. As we assume $\dim(V) = n$, it must then hold that $\text{rank}(P'\rho_{t,n}) = n - t$ so that there must exist a permutation P^T of $\mathbb{F}_2^n$ such that $P^T\rho_{t,n} = P'\rho_{t,n}$. We deduce the theorem. □

Below, we will use this theorem to study CCZ-equivalence. However, we first use it to derive a simple lemma which will allow us to interpret the results given in Section 3.3, especially the notion of thickness spectrum, in terms of vector spaces in the DDT rather than in the LAT. Intuitively and informally, the roles of $\mathcal{V}$ and $\mathcal{V}^\perp$ are swapped when we switch between vector spaces of zeroes in the DDT and in the LAT. Thus, we would expect the relevant quantity for the vector spaces in the DDT to be the dimension of the projection on $\mathcal{V}$ rather than on $\mathcal{V}^\perp$. This intuition is correct because of the following lemma.

Lemma 7. *Let U be a vector space of dimension n in $\mathbb{F}_2^{n+m}$ and let $U^\perp$ be its orthogonal. Note that $\rho_{0,n}(\mathbb{F}_2^{n+m}) = \mathcal{V}$ and $\rho_{n,n+m}(\mathbb{F}_2^{n+m}) = \mathcal{V}^\perp$. Then the following always holds:*

$$\dim\left(\rho_{0,n}(U^\perp)\right) = \dim\left(\rho_{n,n+m}(U)\right) = t(U) .$$

Proof. By definition of the thickness of U, we have that $\dim\left(\rho_{n,n+m}(U)\right) = t(U)$. Thus, we only need to show that

$$\dim\left(\rho_{0,n}(U^\perp)\right) = t(U)\ .$$

By applying Theorem 2, we derive the existence of an EL-mapping Λ such that $U = \Lambda^T M_t(\mathcal{V})$ where $t = t(U)$. Thus, we can write

$$U^\perp = \left((\Lambda^T M_t)^{-1}\right)^T (\mathcal{V}^\perp) = \Lambda^{-1} M_t(\mathcal{V}^\perp)\ .$$

The inverse of an EL-mapping is another EL-mapping, so there must exist linear permutations A and B of $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ as well as a linear function $C : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that

$$\Lambda^{-1} = \begin{bmatrix} A & 0 \\ C & B \end{bmatrix}\ ,$$

from which we deduce that

$$\begin{aligned}
\rho_{0,n}(U^\perp) &= \left(\begin{bmatrix} I_n & 0 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} A & 0 \\ C & B \end{bmatrix} \times \begin{bmatrix} \rho_{t,n} & \rho_{0,t} \\ \rho_{0,t} & \rho_{t,m} \end{bmatrix}\right)(\mathcal{V}^\perp) \\
&= \left(\begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} \rho_{t,n} & \rho_{0,t} \\ \rho_{0,t} & \rho_{t,m} \end{bmatrix}\right)(\mathcal{V}^\perp) \\
&= \begin{bmatrix} A\rho_{t,n} & A\rho_{0,t} \\ 0 & 0 \end{bmatrix}(\mathcal{V}^\perp)\ .
\end{aligned}$$

As $\mathcal{V}^\perp = \{(0,x), \forall x \in \mathbb{F}_2^m\}$, we deduce that $\dim\left(\rho_{0,n}(U^\perp)\right) = \mathrm{rank}(A\rho_{0,t}) = t$. The lemma follows. □

We directly deduce the following alternative formulation of Definition 9.

Corollary 3 (Thickness Spectrum in terms of DDT)**.** *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function and let Σ_F^D be the set of all vector spaces of dimension m in $\mathcal{Z}_F^D$. The* thickness spectrum *of F is the set of all pairs of positive integers (t_i, N_i) such that, for all i:*

$$N_i = \#\left\{V \in \Sigma_F^D, \dim(\rho_{0,n}(V)) = t_i\right\}.$$

4.4 Twisting and CCZ-Equivalence

Now, we use Theorem 2 to provide a complete description of CCZ-equivalence. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be two CCZ-equivalent functions such that $\Gamma_G = \mathcal{A}(\Gamma_F)$ for some affine permutation $\mathcal{A}$ of $\mathbb{F}_2^{n+m}$. As we have established in Theorem 1, this implies $\mathcal{L}^T(\mathcal{V}) \subseteq \mathcal{Z}_F$, where $\mathcal{L}$ is the linear part of $\mathcal{A}$.

Using Theorem 2, we find that there exists a positive integer $t \leq \min(m,n)$ and an EL-mapping Λ such that $\mathcal{L}^T(\mathcal{V}) = \Lambda^T M_t(\mathcal{V})$ as $\mathcal{L}^T(\mathcal{V})$ is a vector space of dimension n. We deduce that $(\Lambda^T M_t)^T = M_t\Lambda$ is an admissible mapping for F and thus that there exists a function G' such that $\Gamma_{G'} = (M_t \circ \Lambda)(\Gamma_F)$. Furthermore, since $\Lambda^T M_t(\mathcal{V}) = \mathcal{L}^T(\mathcal{V})$, we can apply Lemma 3 and thus obtain that G' is EA-equivalent to G. We conclude that there must exist an EA-mapping A such that $\Gamma_G = A(\Gamma_{G'})$, so that $\Gamma_G = (A \circ M_t \circ \Lambda)(\Gamma_F)$.

We deduce the following theorem which allows us to fully characterize CCZ-equivalence using only two types of operations.

Theorem 3 (A full description of CCZ-Equivalence)**.** *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be two CCZ-equivalent functions. Then we can obtain G from F (and vice-versa) by composing an EA transformation, a t-twist and an EA transformation.*

This result imposes that both functions F and G are EA-equivalent to functions that are twist-equivalent. We deduce the following corollary.

Corollary 4. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be two CCZ-equivalent functions that are not EA-equivalent. Then it is necessary that there exists some integer $1 \leq t \leq \min(m, n)$ such that both F and G are t-twistable.*

We can easily find which value of t is such that a function is t-twistable—if there is any—using the following corollary.

Corollary 5. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function. If $V \subseteq \mathcal{Z}_F$ is a vector space of dimension n then F is t-twistable where $t = t(V)$.*

Similarly, if $V' \subseteq \mathcal{Z}_F^D$ is a vector space of dimension m, then F is t-twistable where t is the dimension of the projection of V' on $\mathcal{V}$.

Remark 1. *It is well-known that, while it preserves the extended Walsh spectrum and differential spectrum, CCZ-equivalence does not preserve the algebraic degree. Because of Theorem 3 and because the algebraic degree is constant in an EA-class, the twist has to be responsible for this difference.*

Remark 2. *While it is* necessary *to perform a t-twist to leave an EA-class, it is not* sufficient.

Indeed, it is possible for two functions to be both t-twist equivalent and EA-equivalent. Consider a function $F : \mathbb{F}_2^t \times \mathbb{F}_2^{n-t} \to \mathbb{F}_2^n \times \mathbb{F}_2^{n-t}$ such that $F(x, y) = (T_y(x), U_x(y))$ for which T_y is always an involution of $\mathbb{F}_2^t$ and for which $U_x(y) = U(y)$ does not depend on x. Then a t-twist of F yields F' such that

$$F'(x, y) \;=\; \big(T_y^{-1}(x), U_{T_y^{-1}(x)}(y)\big) \;=\; \big(T_y(x), U(y)\big)\ , \tag{6}$$

so that $F' = F$. Such a function is such that $M_t(\mathcal{V}) \subset \mathcal{Z}_F$ and yet its CCZ-class may be reduced to a unique EA-class.

5 Partitioning CCZ-Classes

The question we now focus on is the partition of CCZ-classes into EA-classes. We have seen in Section 3.2 that the number of distinct EA-classes within a CCZ-class is at most the number of vector spaces of dimension n in $\mathcal{Z}_F$. Here, we combine the partition given by these vector spaces in $\mathcal{Z}_F$ with Theorem 3. It allows us to bound the number of EA-classes in the CCZ-class of a given function and gives us a simple description of all the admissible mappings of a function.

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function, let $\mathsf{Adm}(F)$ be the set of all admissible mappings for F, and let Σ_F be the set of all vector spaces of dimension n in $\mathcal{Z}_F$. Finally, recall that $\mathcal{M}^{\mathrm{EA}}$ denotes the set of all EA-mappings.

5.1 Theoretical Tools

In order to better understand the discrepancy between the number of EA-classes and the number of vector spaces of zeroes, we introduce two concepts: the automorphisms of a function and EA-similarity. The latter will capture the fact that, when functions F and G are EA-equivalent, there may exist $\mathcal{A} \notin \mathcal{M}^{\mathrm{EA}}$ such that $\Gamma_G = \mathcal{A}(\Gamma_F)$. Automorphisms will turn out to play a significant role in the study of EA-similarity.

Definition 13 (Automorphism for a function)**.** *For a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we call* automorphism for F *an affine permutation $\mathcal{A}$ of $\mathbb{F}_2^{n+m}$ such that $\mathcal{A}(\Gamma_F) = \Gamma_F$. The set of all such mappings is denoted* $\mathsf{Aut}(F)$*. It corresponds to the automorphism group [MS77, Page 229] of the associated code $\mathcal{C}_F$.*

This notion can be seen as a generalization of *self-equivalence* as defined in [BDBP03]; where a "self-equivalent" function is non-trivially affine equivalent to itself. If $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is self-equivalent in that sense, then there exist affine permutations $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $B : \mathbb{F}_2^m \to \mathbb{F}_2^m$ such that $F = B \circ F \circ A$. It thus corresponds to an automorphism of F because $\Gamma_F = \{(x, (B \circ F \circ A)(x)), x \in \mathbb{F}_2^n\} = \left\{\left(A^{-1}(y), (B \circ F)(y)\right), y \in \mathbb{F}_2^n\right\} = \mathcal{L}(\Gamma_F)$, where

$$\mathcal{L} = \begin{bmatrix} A^{-1} & 0 \\ 0 & B \end{bmatrix} .$$

The automorphism set of a given function has several properties given in the following lemma.

Lemma 8. *For a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $\mathsf{Aut}(F)$ is a group under composition. Furthermore, let $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be such that $\Gamma_G = \mathcal{A}(\Gamma_F)$ for some affine permutation $\mathcal{A}$. Then $\mathsf{Aut}(F)$ and $\mathsf{Aut}(G)$ are isomorphic as $\phi_{\mathcal{A}} : M \mapsto \mathcal{A}^{-1} \circ M \circ \mathcal{A}$ is an isomorphism such that $\mathsf{Aut}(G) = \phi_{\mathcal{A}}(\mathsf{Aut}(F))$.*

Proof. The identity is obviously in $\mathsf{Aut}(F)$. Furthermore, $\mathcal{L} \in \mathsf{Aut}(F)$ if and only if $\mathcal{L}(\Gamma_F) = \Gamma_F$, which is equivalent to $\Gamma_F = \mathcal{L}^{-1}(\Gamma_F)$ and thus to $\mathcal{L}^{-1} \in \mathsf{Aut}(F)$. Finally, if $\mathcal{L}$ and $\mathcal{L}'$ are in $\mathsf{Aut}(F)$, then $\mathcal{L}^{-1}(\Gamma_F) = \Gamma_F = \mathcal{L}'(\Gamma_F)$, so that $\mathcal{L} \circ \mathcal{L}' \in \mathsf{Aut}(F)$. As a consequence, $\mathsf{Aut}(F)$ is a group.

Let now $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $\mathcal{A} : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ be as in the lemma and let $\mathcal{L} \in \mathsf{Aut}(G)$. Then $\mathcal{L}(\Gamma_G) = \Gamma_G$, which is equivalent to $(\mathcal{L} \circ \mathcal{A})(\Gamma_F) = \mathcal{A}(\Gamma_F)$, so that $\mathcal{A}^{-1}\mathcal{L}\mathcal{A} = \phi_{\mathcal{A}}(\mathcal{L}) \in \mathsf{Aut}(F)$. As $\phi_{\mathcal{A}}$ is an isomorphism, the two groups are isomorphic. □

Definition 14 (EA-similarity)**.** *For a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we say that two mappings $\mathcal{A}$ and $\mathcal{A}'$ of $\mathsf{Adm}(F)$ are* EA-similar for F *if there exists an EA-mapping B such that*

$$\mathcal{A}(\Gamma_F) = (B \circ \mathcal{A}')(\Gamma_F) ,$$

so that the functions G and G' with codebooks $\mathcal{A}(\Gamma_F)$ and $\mathcal{A}'(\Gamma_F)$ are EA-equivalent.

For example, the identity as well as all other EA-mappings are always EA-similar. However, it is possible for two mappings $\mathcal{A}$ and $\mathcal{A}'$ to be EA-similar for a function without being EA-mappings as noticed in Remark 2. This is the case for instance of involutions.

Lemma 9. *For any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, EA-similarity for F is an equivalence relation.*

Proof. Let F be such a function and let $\mathcal{A}$ and $\mathcal{A}'$ be admissible mappings for F. As $\mathcal{A}(\Gamma_F) = (I_{n+m} \circ \mathcal{A})(\Gamma_F)$, EA-similarity is reflexive. If there is an EA-mapping B such that $\mathcal{A} = B\mathcal{A}'$ then $\mathcal{A}' = B^{-1}\mathcal{A}$ and, as B^{-1} is also an EA-mapping, EA-similarity is symmetric. Finally, let $\mathcal{A}_0, \mathcal{A}_1$ and $\mathcal{A}_2$ be admissible for F and verify both $\mathcal{A}_1(\Gamma_F) = B_1\mathcal{A}_0(\Gamma_F)$ and $\mathcal{A}_2(\Gamma_F) = B_2\mathcal{A}_0(\Gamma_F)$ for some EA-mappings B_1 and B_2. Then it holds that $B_1^{-1}\mathcal{A}_1(\Gamma_F) = B_2^{-1}\mathcal{A}_2(\Gamma_F) = \mathcal{A}_0(\Gamma_F)$, so that $\mathcal{A}_1(\Gamma_F) = B_1B_2^{-1}\mathcal{A}_2(\Gamma_F)$. As the product of two EA-mappings is an EA-mapping, we conclude that EA-similarity is also transitive. □

As EA-similarity is an equivalence relation, we can partition the set of all admissible mappings into its equivalence classes for this relation.

The equivalence classes for EA-similarity may be larger than $|\mathcal{M}^{\mathrm{EA}}|$. Indeed, there is a 1-to-1 correspondence between EA-similarity classes and EA-classes. As a consequence, the counter-example based on an involution can be reused here: if F is an involution of $\mathbb{F}_2^n$, then M_n is in the EA-similarity class of the identity although it is not in $\mathcal{M}^{\mathrm{EA}}$.

An affine permutation $\mathcal{A}'$ is EA-similar to an admissible mapping $\mathcal{A}$ if $\mathcal{A}'(\Gamma_F) = B\mathcal{A}(\Gamma_F)$ for an EA-mapping B. It means that the set of all $\mathcal{A}'$ EA-similar to $\mathcal{A}$ is the set of all $\mathcal{A}'$ such that $(\mathcal{A}^{-1}B^{-1}\mathcal{A}')(\Gamma_F) = \Gamma_F$, i.e. such that $\mathcal{A}^{-1}B^{-1}\mathcal{A}' \in \mathsf{Aut}(F)$. This is equivalent to having $\mathcal{A}' \in B\mathcal{A}(\mathsf{Aut}(F))$. We deduce the following lemma.

Lemma 10. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function and $\mathcal{A}$ be a mapping admissible for F. The set $E_F(\mathcal{A})$ of all affine permutations EA-similar to $\mathcal{A}$ for F can be written as*

$$E_F(\mathcal{A}) = \{B \circ \mathcal{A} \circ J, B \in \mathcal{M}^{EA}, J \in \mathsf{Aut}(F)\} .$$

Note that there may be repetition in this definition, i.e. different pairs (B, J) and (B', J') of $\mathcal{M}^{\mathrm{EA}} \times \mathsf{Aut}(F)$ such that $B \circ \mathcal{A} \circ J = B' \circ \mathcal{A} \circ J'$.

5.2 Partitioning

In Section 3.2, we have partitioned the set of all admissible mappings with respect to the vector spaces V of dimension n in $\mathcal{Z}_F$: let $\mathcal{S}(V)$ be the set of all affine permutations of $\mathbb{F}_2^{n+m}$ whose linear part $\mathcal{L}$ satisfies $\mathcal{L}^T(\mathcal{V}) = V$, and Σ_F be the set of all vector spaces of dimension n in $\mathcal{Z}_F$. Then,

$$\mathsf{Adm}(F) = \bigcup_{V \in \Sigma_F} \mathcal{S}(V) .$$

Moreover, Lemma 3 implies that all elements in a given $\mathcal{S}(V)$ are EA-similar. Therefore, each class $E_F(\mathcal{A})$ corresponds to a collection of sets $\mathcal{S}(V)$. We now refine this result as follows.

Proposition 7. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function, $\mathcal{A}$ be a mapping admissible for F, $\mathcal{L}$ be its linear part and $V = \mathcal{L}^T(\mathcal{V})$. The set $E_F(\mathcal{A})$ of all affine permutations EA-similar to $\mathcal{A}$ for F is given by*

$$E_F(\mathcal{A}) = \bigcup_{J \in \mathsf{Aut}_0(F)} \mathcal{S}(J^T(V)) ,$$

where $\mathsf{Aut}_0(F)$ is the set of all linear parts of the elements in $\mathsf{Aut}(F)$.

Proof. From Lemma 10, we have that

$$E_F(\mathcal{A}) = \{B \circ \mathcal{A} \circ J, B \in \mathcal{M}^{\mathrm{EA}}, J \in \mathsf{Aut}(F)\} .$$

Then, the linear part of any such $(B \circ \mathcal{A} \circ J)$ is of the form $(\Lambda \circ \mathcal{L} \circ J_0)$ for some $\Lambda \in \mathcal{M}^{\mathrm{EL}}$ and $J_0 \in \mathsf{Aut}_0(F)$. Its transpose then maps $\mathcal{V}$ to

$$(\Lambda \circ \mathcal{L} \circ J_0)^T(\mathcal{V}) = (J_0^T \circ \mathcal{L}^T \circ \Lambda^T)(\mathcal{V}) = (J_0^T \circ \mathcal{L}^T)(\mathcal{V}) = J_0^T(V) .$$

□

Some of the vector spaces $J^T(V)$ may be equal when J varies in $\mathsf{Aut}_0(F)$ but we have the following trivial bounds:

$$|\mathcal{M}^{\mathrm{EA}}| \ \leq \ |E_F(\mathcal{A})| \ \leq \ |\mathcal{M}^{\mathrm{EA}}| \times |\mathsf{Aut}(F)| . \tag{7}$$

We can now derive some bounds on the number of EA-classes., which improve Corollary 1.

Theorem 4 (Number of EA-classes in a CCZ-class)**.** *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function. Let Σ_F be the set of all vector spaces of dimension n in $\mathcal{Z}_F$ and e_F be the number of distinct EA-classes of functions that are CCZ-equivalent to F. Then the following holds:*

$$\frac{|\Sigma_F|}{|\mathsf{Aut}(F)|} \;\leq\; e_F \;\leq\; |\Sigma_F| \;.$$

Moreover, if $\mathsf{Aut}(F) \subseteq \mathcal{M}^{EA}$ then e_F is lower-bounded by the number of different thicknesses in the thickness spectrum of F, i.e.

$$\#\{t \;: 0 \leq t \leq n \;,\; \exists V \in \Sigma_F \text{ with } t(V) = t\} \;\leq\; e_F \;.$$

Proof. Let $s_F = |\Sigma_F|$ be the number of vector spaces of zeroes of dimension n in $\mathcal{Z}_F$. We can compute the total number of admissible mappings for F in two different ways:

$$\begin{aligned} |\mathsf{Adm}(F)| \;&=\; s_F \times |\mathcal{M}^{\mathrm{EA}}| \\ &= \sum_{e \;\in\; \{\text{EA-similarity classes of } F\}} |e| \;. \end{aligned}$$

Let e_F be the number of EA-classes in the CCZ-class of F. It is also equal to the number of EA-similarity classes for F in the set of all affine permutations of $\mathbb{F}_2^{n+m}$. Using the second expression and Equation (7), we deduce the following inequality:

$$|\mathsf{Adm}(F)| \;\leq\; e_F \times |\mathcal{M}^{\mathrm{EA}}| \times |\mathsf{Aut}(F)| \;.$$

We then use the fact that $|\mathsf{Adm}(F)| = s_F \times |\mathcal{M}^{\mathrm{EA}}|$ to obtain

$$s_F \times |\mathcal{M}^{\mathrm{EA}}| \;\leq e_F \times |\mathcal{M}^{\mathrm{EA}}| \times |\mathsf{Aut}(F)| \;,$$

leading to the first part of the theorem.

The second part of the theorem is a direct consequence of Proposition 7. Indeed, if $\mathsf{Aut}_0(F) \subseteq \mathcal{M}^{\mathrm{EL}}$, then all subspaces $J^T(V)$ have the same thickness as V (see Lemma 4). □

The situation where $\mathsf{Aut}(F) \subseteq \mathcal{M}^{\mathrm{EA}}$ is of special interest since it corresponds to a case where it is *necessary and sufficient* to perform a twist to leave the EA-class of a function. This situation occurs for instance for all APN quadratic power mappings, i.e., $x \mapsto x^{2^i+1}$ over $\mathbb{F}_{2^n}$ with $\gcd(i, n) = 1$, as proved by Berger and Charpin [BC96]. Then, we deduce the following corollary.

Corollary 6. *Let $F : x \mapsto x^{2^i+1}$ over $\mathbb{F}_{2^n}$ with $\gcd(i, n) = 1$ be an APN power mapping of degree 2. Then, $\mathsf{Aut}(F) \subseteq \mathcal{M}^{EA}$ and the number of EA-classes in the CCZ-class of F is lower-bounded by the number of different thicknesses in the thickness spectrum of F.*

Proof. The result is directly deduced from Proposition 5 in [BC96] which shows that $\mathsf{Aut}(F)$ is the semi-affine group $\mathrm{A\Gamma L}(1, 2^n)$. It is then easy to check that all transformations in this group belong to $\mathcal{M}^{\mathrm{EA}}$. □

6 Applications

We apply our new results to both reinterpret some known results and to provide several new ones. Section 6.1 revisits a result of Schulte-Geers on addition modulo 2^m; Section 6.2 provides new simpler proofs of some general results; and finally Section 6.3 focuses on quadratic APN functions.

6.1 Modular Addition

Let us first recall the result of Schulte-Geers.

Proposition 8 (Theorem 1 of [SG13]). *Let "$\boxplus$" denote addition modulo 2^m, "$+$" denote the XOR, let $n = 2m$, and let q be the quadratic function mapping an element (x, y) of $(\mathbb{F}_2^m)^2 = \mathbb{F}_2^n$ to*

$$q(x, y) = (0,\ x_0y_0,\ x_0y_0 + x_1y_1,\ \ldots,\ x_0y_0 + \ldots + x_{n-2}y_{n-2}).$$

Further, let $\Gamma_\boxplus$ and Γ_q be the graphs of those functions so that

$$\Gamma_\boxplus = \{(x, y, x \boxplus y), (x, y) \in \mathbb{F}_2^n\}$$
$$\Gamma_q = \{(x, y, q(x, y)), (x, y) \in \mathbb{F}_2^n\}.$$

Then it holds that $\Gamma_\boxplus = L(\Gamma_q)$, where

$$L = \begin{bmatrix} I_m & 0 & I_m \\ 0 & I_m & I_m \\ I_m & I_m & I_m \end{bmatrix} .$$

We can reinterpret this proposition in light of Theorem 3. First, we note that

$$L^{-1} = \underbrace{\begin{bmatrix} I_m & 0 & 0 \\ I_m & I_m & 0 \\ I_m & 0 & I_m \end{bmatrix}}_{A_1} \times \underbrace{\begin{bmatrix} 0 & 0 & I_m \\ 0 & I_m & 0 \\ I_m & 0 & 0 \end{bmatrix}}_{M_m} \times \underbrace{\begin{bmatrix} I_m & 0 & 0 \\ I_m & I_m & 0 \\ 0 & I_m & I_m \end{bmatrix}}_{A_2} ,$$

where the two outer matrices are EA-mappings and the center one is a degenerate swap matrix M_m where the bottom right corner is all zero because, in this case, $t = m$ is the output size.

As $L^{-1} = A_1 \times M_n \times A_2$, Proposition 8 implies $\Gamma_q = (A_1 \times M_n \times A_2) = \Gamma_\boxplus$. Let us look at the action of this matrix product on $\Gamma_\boxplus$. First, it holds that

$$\begin{aligned} A_2(\Gamma_\boxplus) &= \left\{ (x, x + y, (x \boxplus y) + y), (x, y) \in \mathbb{F}_2^n \right\} \\ &= \left\{ \big(x, z, (x \boxplus (x + z)) + x + z\big), (x, z) \in \mathbb{F}_2^n \right\} \\ &= \left\{ \big(x, z, T_z^\boxplus(x)\big), (x, z) \in \mathbb{F}_2^n \right\} , \end{aligned}$$

where $T_z^\boxplus(x) = (x \boxplus (x + z)) + x + z$. The swap incurred by M_n is possible if and only if $T_z^\boxplus$ is a permutation for all z. It is indeed the case and this permutation is in fact linear for each fixed z, as given by the following lemma.

Lemma 11. *Let $T_z^\boxplus$ be the function mapping $\mathbb{F}_2^m$ to itself defined by*

$$T_z^\boxplus(x) = (x \boxplus (x + z)) + x + z ,$$

where $z \in \mathbb{F}_2^m$. Then, for all z, $T_z^\boxplus$ is a linear permutation and so is its inverse. Furthermore, the function $(x, z) \mapsto T_z^\boxplus(x)$ has degree m and $(x, z) \mapsto (T_z^\boxplus)^{-1}(x)$ is quadratic.

Proof. As recalled in [SG13], $x \boxplus y = x + y + c(x, y)$, where $c(x, y)$ denotes the carry vector and is inductively defined by $c_0(x, y) = 0$ and $c_{i+1}(x, y) = \mathrm{maj}(x_i, y_i, c_i)$ where maj is the majority function such that $\mathrm{maj}(a, b, c) = ab + c(b + a)$. We also note that if $u = x \boxplus y$, then $c_i = u_i + x_i + y_i$, so that

$$u = x \boxplus y \ \text{ if and only if } \begin{cases} u_0 & = x_0 + y_0 \\ u_{i+1} & = x_{i+1} + y_{i+1} + \mathrm{maj}(x_i,\ y_i,\ u_i + x_i + y_i) \end{cases} .$$

Let $v = T_z^{\boxplus}(x) = (x \boxplus (x+z)) + x + z$. By substituting y for $x+z$ in the above, we first write

$$u = x \boxplus (x+z) \text{ if and only if } \begin{cases} u_0 & = z_0 \\ u_{i+1} & = z_{i+1} + \mathrm{maj}(x_i,\ x_i + z_i,\ u_i + z_i) \end{cases}$$

and then substitute u with $v + x + z$ to obtain

$$v = T_z^{\boxplus}(x) \text{ if and only if } \begin{cases} v_0 & = x_0 \\ v_{i+1} & = x_{i+1} + \mathrm{maj}(x_i,\ x_i + z_i,\ v_i + x_i)\ . \end{cases}$$

We can simplify the expression of v_{i+1} using that

$$\begin{aligned} \mathrm{maj}(x_i,\ x_i + z_i,\ v_i + x_i) &= x_i(x_i + z_i) + (x_i + x_i + z_i)(v_i + x_i) \\ &= x_i x_i + x_i z_i + z_i v_i + z_i x_i \\ &= x_i + z_i v_i\ , \end{aligned}$$

so that

$$v = T_z^{\boxplus}(x) \text{ if and only if } \begin{cases} v_0 & = x_0 \\ v_{i+1} & = v_i z_i + x_i + x_{i+1}\ . \end{cases}$$

A simple induction based on this result shows that v_i has degree 1 in x and degree $i+1$ in total as it contains the term $x_0 z_0 z_1 ... z_{i-1}$. Besides, since $T_z^{\boxplus}(0) = 0$, $T_z^{\boxplus}$ is linear for all z. Furthermore, the bit of highest algebraic degree in $(x, z) \mapsto T_z^{\boxplus}(x)$ is the bit of highest weight. It has index $m-1$ and thus degree m.

We also deduce that $T_z^{\boxplus}$ is invertible for all z as the bits of $x = (T_z^{\boxplus})^{-1}(v)$ can be computed one-by-one using that

$$x = (T_z^{\boxplus})^{-1}(v) \text{ if and only if } \begin{cases} x_0 & = v_0 \\ x_{i+1} & = x_i + v_{i+1} + z_i v_i\ . \end{cases} \tag{8}$$

While this induction formula is extremely similar to the one giving v as a function of x, it has a crucial difference: the only non-linear term in the expression of x_{i+1} does not involve x_i, meaning that we cannot have a sequence of multiplication whose length increases as i increases. Thus, $(x, y) \mapsto (T_z^{\boxplus})^{-1}(x)$ is quadratic. □

We deduce from Lemma 11 that

$$(M_n \times A_2)(\Gamma_{\boxplus}) \ = \ \left\{\left(T_z^{\boxplus}(x), z, x\right), (x, z) \in \mathbb{F}_2^n\right\} \ = \ \left\{\left(u, z, (T_z^{\boxplus})^{-1}(u)\right), (u, z) \in \mathbb{F}_2^n\right\}\ .$$

Since $L^{-1} = A_1 \times M_n \times A_2$, it holds that

$$\begin{aligned} L^{-1}(\Gamma_{\boxplus}) &= A_1\left(\left\{\left(u,\ z,\ (T_z^{\boxplus})^{-1}(u)\right), (u, z) \in \mathbb{F}_2^n\right\}\right) \\ &= \left\{\left(u,\ u+z,\ u + (T_z^{\boxplus})^{-1}(u)\right), (u, z) \in \mathbb{F}_2^n\right\} \\ &= \left\{\left(u,\ w,\ u + (T_{w+u}^{\boxplus})^{-1}(u)\right), (u, w) \in \mathbb{F}_2^n\right\}\ . \end{aligned}$$

Re-using Equation (8), i.e. the expression of $T_z^{\boxplus}$ we found in the proof of Lemma 11, we have that $a = (T_{w+u}^{\boxplus})^{-1}(u) + u$ if and only if

$$\begin{cases} a_0 + u_0 & = u_0 \\ a_{i+1} + u_{i+1} & = (a_i + u_i) + u_{i+1} + (u_i + w_i)u_i\ , \end{cases}$$

which is equivalent to

$$\begin{cases} a_0 & = 0 \\ a_{i+1} & = a_i + u_i w_i \ , \end{cases}$$

which is in turn the induction computing $a = q(u, w)$.

In light of these results, we can provide a new interpretation of Proposition 8. Indeed, the addition modulo 2^m is CCZ-equivalent to a quadratic function because $(x, y) \mapsto x \boxplus y$ is EA-equivalent to $(x, z) \mapsto (x \boxplus (x + z)) + x + z$, a function with a degenerate TU-decomposition where T takes the whole output and T_y is a permutation for all k. Then, $(x, y) \mapsto T_y^{-1}(x)$ is quadratic because the induction defining it is obtained by swapping the roles of the output and one of the inputs in the one defining $(x, y) \mapsto T_y(x)$. This breaks the unique chain of non-linear operation that appears when computing $T_y(x)$. As the chain is broken, the algebraic degree cannot increase and stays stuck at 2.

It may be possible to deduce a way to generate finite automata-based compression functions $(x, y) \mapsto F(x, y)$ with a degree which increases with the bit position and which are CCZ-equivalent to quadratic functions, those being hopefully easier to study.

6.2 Other Proofs of Some Known Results

In this section, we recall several simple results pertaining to CCZ-equivalence and prove them again using our framework.

Proposition 9 (Theorem 1 of [BC11])**.** *The CCZ-class of a bent function mapping $\mathbb{F}_2^n \to \mathbb{F}_2^m$ is limited to its EA-class.*

Proof. The coefficients of the Walsh spectrum of a bent function take only one non-zero value (up to its sign) except for those in $\mathcal{V}$. Thus, there cannot be another vector space of dimension n in $\mathcal{Z}_F$. □

Proposition 10 (Theorem 1 of [BC10])**.** *Two functions mapping $\mathbb{F}_2^n$ to $\mathbb{F}_2$ are CCZ-equivalent if and only if they are EA-equivalent.*

Proof. The only way for a Boolean function mapping n bits to 1 to have a non-trivial CCZ-equivalence class is for it to be t-twistable for some $1 \leq t \leq \min(1, n)$. In this case, it means it has to be 1-twistable. As we have established in Lemma 6, this happens if and only if $T_y(x) = x + f(y)$, so that in our case it would hold that $F(x, y) = x + f(y)$ for some Boolean function f. However, the result of twisting this function would be $G : \mathbb{F}_2^n \to \mathbb{F}_2$ such that $G(x, y) = T_y^{-1}(x) = x + f(y)$, i.e. F itself. As we have established, it is necessary to perform a twist in order to leave the EA-class of a function. However, the only possible one in this case fails to do so. As a consequence, the CCZ-class is reduced to a unique EA-class. □

Proposition 11 (Proposition 2 of [BC10])**.** *Let F and F' be two functions mapping $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ which are CCZ-equivalent but not EA-equivalent. Then for any integer k and any function $C : \mathbb{F}_2^n \to \mathbb{F}_2^k$, there exists $C' : \mathbb{F}_2^n \to \mathbb{F}_2^k$ such that the functions $G : x \mapsto (F(x), C(x))$ and $G' : x \mapsto (F'(x), C'(x))$ mapping $\mathbb{F}_2^n$ to $\mathbb{F}_2^{m+k}$ are CCZ-equivalent but not EA-equivalent.*

Proof. We consider without loss of generality the case where, for any $(x, y) \in \mathbb{F}_2^t \times \mathbb{F}_2^{n-t}$, $F(x, y) = (T_y(x), U_x(y))$ and $F'(x, y) = (T_y^{-1}(x), U_{T_y^{-1}(x)}(y))$. As F and F' are CCZ-equivalent but not EA-equivalent, such decompositions must exist for some members of their respective EA-classes.

In this context, we see that G and G' must both be t-twistable and we can further give an expression of C'. Indeed, G is such that

$$G(x, y) \ = \ \big(T_y(x), U_x(y), \ C(x, y)\big)$$

and t-twisting it yields G' such that

$$G'(x,y) \;=\; \left(T_y^{-1}(x), U_{T_y^{-1}(x)}(y),\; C\left(T_y^{-1}(x), y\right)\right) ,$$

so that $C'(x,y) = C\left(T_y^{-1}(x), y\right)$ for any $(x,y) \in \mathbb{F}_2^t \times \mathbb{F}_2^{n-t}$. Indeed, G and G' are not EA-equivalent. □

6.3 On Quadratic APN Functions

6.3.1 New Results

We can use Corollary 2 to study quadratic functions. First, we recall the following result from [MS77, Chapter 15].

Proposition 12. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a quadratic Boolean function. Let $\mathsf{LS}(f)$ be the linear space of f, i.e.*

$$\mathsf{LS}(f) \;=\; \{a \in \mathbb{F}_2^n, f(x+a) + f(x) = c, \forall x \in \mathbb{F}_2^n\} ,$$

where $c \in \mathbb{F}_2$. Then $s = \dim(\mathsf{LS}(f))$ has the parity of n and the maximum coefficient in the Walsh spectrum of f has absolute value $2^{(n+s)/2}$.

In the case where f is not bent, the maximum coefficient is strictly greater than $2^{(n+1)/2}$ and thus the linear space of f is not empty. As a consequence, we can apply Corollary 2 to obtain the following proposition.

Proposition 13. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a quadratic function. If it has at least one non-bent component then it is 1-twistable.*

It is worth noticing that a function derived from a quadratic function by any 1-twist has degree at most 3. Moreover, it follows from the expression of the resulting function given in Lemma 6 that it is very unlikely that it has degree 2.

On the other hand, if such functions are APN then some twists are impossible.

Proposition 14. *Let n be even and let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic APN function. Then F is never $n-1$-twistable.*

Proof. The second item in Corollary 3 of [BCCLC06] states that any APN quadratic function has at least $2(2^n - 1)/3$ bent components. Thus, as at most a third of the components of F have zeroes in their Walsh spectrum, it is impossible to find a vector space of dimension n in $\mathcal{Z}_F$ with a projection of dimension $n-1$ on $\mathcal{V}^\perp$. We deduce that an $(n-1)$-twist is always impossible. □

6.3.2 Revisiting the CCZ-Equivalence of Some Functions

We should not expect the members of the EA-classes obtained by twisting quadratic functions to be quadratic themselves as $(x,y) \mapsto \left(T_y^{-1}(x), U_{T_y^{-1}(x)}(y)\right)$ should a priori not be quadratic even when $(x,y) \mapsto (T_y(x), U_x(y))$ is. Indeed, the functional inverse of a quadratic function may have a higher degree and $(x,y) \mapsto U_{T_y^{-1}(x)}(y)$ should a priori not be quadratic since U has degree 2 and T_y^{-1} has degree at least 2. For instance, the functions obtained by applying any 1-twist to a quadratic function are expected to have degree 3. Informally, being quadratic is a brittle property which is unlikely to be preserved under twisting.

This observation provides a possible interpretation of the main result in [BBMN11]: the only quadratic functions which are CCZ-equivalent to Gold functions are EA-equivalent to it. This result was later generalized in [Yos17] to all power functions that are both plateaued, APN, and operate on an even block size. This class includes in particular quadratic APN functions. We recall his result below.

Proposition 15 (Theorem 3 of [Yos17]). *Let F and G be plateaued APN functions on $\mathbb{F}_{2^n}$ with n even. Assume that F is a power function, i.e. $F(x) = x^d$. Then F is CCZ-equivalent to G if and only if F is EA-equivalent to G.*

By combining this result with the fact that all automorphisms of an APN quadratic power mapping are EA-mappings (Corollary 6), we deduce the following.

Corollary 7. *Let $F : x \mapsto x^{2^i+1}$ over $\mathbb{F}_{2^n}$ with $\gcd(i, n) = 1$ be an APN power mapping of degree 2. Then, applying any admissible t-twist to F, with $t > 0$, leads to an APN function of degree at least 3.*

We can also use our framework to better understand results from [BL08] and [BCP06]. One of the results in this first paper is the following.

Lemma 12 ([BL08]). *The CCZ-class of $P_3 : x \mapsto x^3$ in $\mathbb{F}_2^5$ contains 3 distinct EA-classes.*

Experimentally, we found 64 vector spaces of zeroes of dimension 5 in $\mathcal{Z}_{P_3}$ of which 1 has thickness 0 ($\mathcal{V}$), 31 have thickness 4 and 32 have a thickness of 5. We looked at a member of the EA-class corresponding to each of these vector spaces and found that these could be sorted into 3 categories based on their thickness spectra. These are described in Table 1.

Representative	Algebraic Degree	Thickness Spectrum
x^3	2	$(0,1),(1,31),(5,32)$
F'	3	$(0,1),(1,1),(2,30),(4,32)$
$x^{1/3}$	3	$(0,1),(4,62),(5,1)$

Table 1: *EA-classes in the CCZ-class of x^3 for $n = 5$.*

The functions in the second class are obtained from x^3 by applying an EA-mapping followed by a 1-twist. The functions in the third one are obtained from x^3 via an EA-mapping followed by a 5-twist, i.e. a functional inversion.

We know a representative of the class obtained via a 1-twist thanks to Budaghyan et al.. Indeed, they showed in [BCP06] that the polynomial

$$F'(x) = x^{2^i+1} + (x^{2^i} + x)\mathrm{Tr}(x^{2^i+1} + x)$$

which maps $\mathbb{F}_{2^n}$ to itself ($n \geq 4$ odd, $\gcd(i, n) = 1$) is CCZ-equivalent to $G : x \mapsto x^{2^i+1}$ and, as such, APN. Using our terminology, they showed that the involution $\mathcal{L} : (\mathbb{F}_{2^n})^2 \to (\mathbb{F}_{2^n})^2$ defined for $a \neq 0$ by

$$\mathcal{L}(x, y) = \left(\ell_a(x, y), \ell_{a^{2^i+1}}(y, x)\right)$$

where $\ell_a : (\mathbb{F}_2^n)^2 \to \mathbb{F}_2^n$ is the linear function defined by

$$\ell_a(x, y) = x + a\mathrm{Tr}(xa^{-1}) + a\mathrm{Tr}(ya^{-(2^i+1)})$$

is admissible for G and showed that the graph of F' is obtained from that of G by applying $\mathcal{L}$ and then an EA-mapping to it. As the rank of the linear function $y \mapsto a\mathrm{Tr}(ya^{-(2^i+1)})$ is equal to 1, $\mathcal{L}^T$ has thickness 1, implying that it corresponds to a 1-twist and, for $n = 5$, it has to be in the EA-class corresponding to the second row of

Table 1. Besides, our Proposition 13 explains why such a twist is possible in the first place.

For $n \geq 4$ even and $\gcd(i, n) = 1$, they showed a similar result:

$$F''(x) = x^{2^i+1} + (x^{2^i} + x + 1)\mathrm{Tr}(x^{2^i+1})$$

is CCZ-equivalent to a Gold function. The corresponding admissible linear mapping is again defined for any non-zero $a \in \mathbb{F}_{2^n}$ by $\mathcal{L}(x, y) = \big(x + a\mathrm{Tr}(ya^{-(2^i+1)}),\ y\big)$. As before, the rank of the top right corner of the corresponding matrix is equal to 1, meaning that F'' is obtained from a Gold function via a 1-twist and some EA-mappings.

The bulk of [BCP06] consists in proofs of the CCZ-equivalence of the new functions they provide with the Gold function. However, as we have seen, applying a linear mapping to the graph of a function may yield a function in the same EA-class even when a twist is implied. Budaghyan et al. solved this problem by looking at the algebraic degree of their functions and showing that it was strictly greater than 2. As the algebraic degree is constant in an EA-class, the new function cannot be in that of the Gold functions. But this result can be directly deduced from Corollary 7 which shows that applying a 1-twist to $G : x \mapsto x^{2^i+1}$ with $\gcd(i, n) = 1$ leads to a function of degree at least 3, which cannot belong to the EA-class of G.

7 Conclusion

By looking at the interaction between CCZ-equivalence and both the DDT and LAT, we were able to derive several new results. In particular, we have shown that CCZ-equivalence is the combination of EA-equivalence and a new form of equivalence between two functions which we called t-twist equivalence. To prove this result, we have designed new theoretical tools such as swap matrices and space thickness which might be of independent interest. These results allowed us to reinterpret several results from the literature as well as to derive some new ones.

Using our results, the problem of exploring the EA-classes inside the CCZ-class of a function can be reduced to a search for vector spaces. Indeed, the ability to efficiently recover the vector spaces of dimension n in the Walsh zeroes of a function will directly allow us to iterate over all EA-classes. However, we may visit the same EA-class multiple times. In order to avoid this problem, we would need an efficient algorithm checking for the EA-equivalence of two functions.

Acknowledgement

We thank the reviewers as well as Christof Beierle for their comments. The work of Léo Perrin was supported by a grant from the *Fondation Sciences Mathématiques de Paris (FSMP)*.

References

[BBMN11] Carl Bracken, Eimear Byrne, Gary McGuire, and Gabriele Nebe. On the equivalence of quadratic APN functions. *Designs, Codes and Cryptography*, 61(3):261–272, Dec 2011.

[BC96] Thierry P. Berger and Pascale Charpin. The permutation group of affine-invariant extended cyclic codes. *IEEE Trans. Information Theory*, 42(6):2194–2209, 1996.

[BC10] Lilya Budaghyan and Claude Carlet. CCZ-equivalence of single and multi output boolean functions. In *Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications*, volume 518, pages 43–54. American Mathematical Society, 2010.

[BC11] Lilya Budaghyan and Claude Carlet. CCZ-equivalence of bent vectorial functions and related constructions. *Designs, Codes and Cryptography*, 59(1):69–87, Apr 2011.

[BCCLC06] Thierry P Berger, Anne Canteaut, Pascale Charpin, and Yann Laigle-Chapuy. On almost perfect nonlinear functions over $\mathbb{F}_2^n$. *IEEE Transactions on Information Theory*, 52(9):4160–4170, 2006.

[BCP06] Lilya Budaghyan, Claude Carlet, and Alexander Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 52(3):1141–1152, 2006.

[BDBP03] Alex Biryukov, Christophe De Cannière, An Braeken, and Bart Preneel. A toolbox for cryptanalysis: Linear and affine equivalence algorithms. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 33–50. Springer, Heidelberg, May 2003.

[BDKM09] K. A. Browning, J.F. Dillon, R.E. Kibler, and M. T. McQuistan. APN Polynomials and Related Codes. *J. of Combinatorics, Information and System Sciences*, 34(1-4):135–159, 2009.

[BDMW10] K. A. Browning, J.F. Dillon, M. T. McQuistan, and A. J. Wolfe. An APN permutation in dimension six. In *Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications*, volume 518, pages 33–42. American Mathematical Society, 2010.

[BL08] Marcus Brinkmann and Gregor Leander. On the classification of APN functions up to dimension five. *Designs, Codes and Cryptography*, 49(1):273–288, Dec 2008.

[BLNW12] Andrey Bogdanov, Gregor Leander, Kaisa Nyberg, and Meiqin Wang. Integral and multidimensional linear distinguishers with correlation zero. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 244–261. Springer, Heidelberg, December 2012.

[BN13] Céline Blondeau and Kaisa Nyberg. New links between differential and linear cryptanalysis. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 388–404. Springer, Heidelberg, May 2013.

[BS91a] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In Alfred J. Menezes and Scott A. Vanstone, editors, *Advances in Cryptology – CRYPTO'90*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, Heidelberg, August 1991.

[BS91b] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

[CCD00] Anne Canteaut, Pascale Charpin, and Hans Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on GF(2^m) and crosscorrelation of maximum-length sequences. *SIAM Journal on Discrete Mathematics*, 13(1):105–138, 2000.

[CCZ98] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[CDP17] Anne Canteaut, Sébastien Duval, and Léo Perrin. A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}. *IEEE Transactions on Information Theory*, 63(11):7575–7591, Nov 2017.

[CV95] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In Alfredo De Santis, editor, *Advances in Cryptology – EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pages 356–365. Springer, Heidelberg, May 1995.

[CV09] Yanling Chen and Han Vinck. Notes on reed-muller codes. arXiv 0901.2062, 2009.

[DES77] Data Encryption Standard. National Bureau of Standards, NBS FIPS PUB 46, U.S. Department of Commerce, January 1977.

[FFW17] Shihui Fu, Xiutao Feng, and Baofeng Wu. Differentially 4-uniform permutations with the best known nonlinearity from butterflies. *IACR Transactions on Symmetric Cryptology*, 2017(2):228–249, 2017.

[Hel94] Tor Helleseth, editor. *Advances in Cryptology – EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*. Springer, Heidelberg, May 1994.

[LTYW18] Yongqiang Li, Shizhu Tian, Yuyin Yu, and Mingsheng Wang. On the generalization of butterfly structure. *IACR Transactions on Symmetric Cryptology*, 2018(1):160–179, 2018.

[Mat94] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Helleseth [Hel94], pages 386–397.

[MS77] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*. North-Holland Publishing Company, 1977.

[NK93] Kaisa Nyberg and Lars R. Knudsen. Provable security against differential cryptanalysis (rump session). In Ernest F. Brickell, editor, *Advances in Cryptology – CRYPTO'92*, volume 740 of *Lecture Notes in Computer Science*, pages 566–574. Springer, Heidelberg, August 1993.

[Nyb94] Kaisa Nyberg. Differentially uniform mappings for cryptography. In Helleseth [Hel94], pages 55–64.

[PUB16] Léo Perrin, Aleksei Udovenko, and Alex Biryukov. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 93–122. Springer, Heidelberg, August 2016.

[SG13] Ernst Schulte-Geers. On CCZ-equivalence of addition mod 2^n. *Designs, Codes and Cryptography*, 66(1):111–127, Jan 2013.

[Yos17] Satoshi Yoshiara. Equivalences among plateaued APN functions. *Designs, Codes and Cryptography*, 85(2):205–217, Nov 2017.