Linear self-equivalence of the known families of APN functions: a unified point of view

Jules Baudrin, Anne Canteaut and Léo Perrin

Inria, Paris, France
name.surname@inria.fr

Abstract.
The *Kim mapping* is a quadratic vectorial Boolean function of 6 variables that attracted a lot of attention due to its CCZ-equivalence to the only known APN permutation in even dimension. Several attempts have been made to identify remarkable properties of this function, in the hope of finding useful generalizations that could work for higher dimensions. While none has yielded a new APN permutation, it has been found to have the so-called *subspace property*. It is also a *cyclotomic map*, and it is known to be linearly equivalent to a homogenous bivariate function, as captured by the so-called butterfly structure, or by the notion of biprojective mapping. It is also a linearly self-equivalent mapping.
In this paper, we re-frame all these properties (and several others) in terms of linear self-equivalence, each property corresponding to specific artifacts in the primary rational canonical form of linear bijections involved in the linear self-equivalence relationship. This insight allows us to show that this type of property is not specific to the Kim mapping at all: in fact, the vast majority of the known infinite families of APN functions turns out to exhibit properties of this type. We detail them, along with various algorithmic techniques that can be used to identify them in practice.

Keywords: APN functions · Differential uniformity · Linear equivalence · Cyclotomic mappints · Kim mapping

1 Introduction

Since the introduction of differential uniformity in the early 90's [NK93], the so-called *big APN problem* has remained open. It has a simple statement: does there exist a bijection F of $\mathbb{F}_2^{2k}$ such that the equation $F(x+a)+F(x)=b$ has at most two solutions x for all $a \neq 0$ and all b?

If the dimension equals $2k+1$ instead, or if we get rid of the constraint that F is a bijection, then many solutions are known. We need not look further than simple monomials, see for instance [Pot16, Table 3]. While many infinite families of non-bijective functions have been found, as we will see later, a solution to the big APN problem has so far remained elusive.

In 2009, Browning, Dillon, McQuistan & Wolfe [BDMW10] made a significant progress on this problem by finding a solution in dimension 6. As of today, the so-called *Dillon permutation* remains the only example (up to equivalence) of an APN bijection in even dimension. As a consequence, substantial effort has been devoted to the study of this specific permutation, and to how it was found, in the hopeof replicating its success.

Let $\mathbb{F}_q$ be the field of size q. The Dillon permutation was found starting from an already known [Dil09] quadratic function of $\mathbb{F}_{64}$, the so-called *Kim mapping*, and then exploring its equivalence class to find a permutation. The equivalence used in this case was *CCZ-equivalence* [CCZ98], and CCZ-equivalence to a permutation is now better understood

both in the particular case of the Kim mapping [PUB16], and in general [CP19]. The next natural step consists in identifying new quadratic APN functions[1] over larger fields of even degree in the hope that one of them turns out to be CCZ-equivalent to a permutation.

To this end, several methods have been proposed, for example the use of purely computational methods based on *Quadratic APN Matrices (QAM)* [YWL14, YP22]. However, another direction has consisted in identifying special properties of the Kim mapping, and then trying to find (infinite families of) functions with similar ones. This line of research includes several APN constructions like Göloğlu's trinomials and hexanomials [Göl15], "generalized Kim mappings" studied by Carlet [Car15], Kim-type mappings [CL21], (generalized) butterflies [PUB16, CDP17, FFW17, LTYW18, CPT19] and biprojective mappings [Göl22, GK21, Göl23], which have all been proved affine-equivalent to either a Gold monomial mapping or to the Kim mapping in dimension 6 [BHLS17, LLHQ21, CL21, Göl23]. Following another research direction, Beierle, Brinckmann and Leander have recently provided an in-depth analysis of *linearly self-equivalent APN mappings* [BBL21, BL22], and a classification for $n \leq 9$. Moreover, some of the new instances found this way then gave rise to new infinite families of APN functions [LK23].

Perhaps more surprisingly, the structural properties investigated in these works are also exhibited by functions which were not built to have them. Indeed, after investigating all known infinite families of APN functions, we have found that, a vast majority of them share the same very particular structure despite their very different representations: when they are defined over $\mathbb{F}_{2^n}$, a lot of them actually rely on the decomposition of $\mathbb{F}_{2^n}^*$ as a union of multiplicative cosets $\gamma\mathbb{F}_{2^k}^*$ of a subfield $\mathbb{F}_{2^k} \subset \mathbb{F}_{2^n}$. More precisely, they behave as a fixed power mapping on each of the multiplicative cosets. This property was notably exhibited for the Kim mapping. Indeed, the Kim mapping is defined by the following univariate form:

$$\kappa\colon \mathbb{F}_{64} \to \mathbb{F}_{64} \quad x \mapsto x^3 + x^{10} + ux^{24},$$

where u is a root of the primitive polynomial $X^6+X^4+X^3+X+1$. It was already noticed in [BDMW10] that it can be rewritten as $\kappa(x) = x^3P(x^7)$ (where $P(x) = ux^3 + x + 1$). It follows that the Kim mapping behaves over all cosets $\gamma\mathbb{F}_{2^3}$ as the power mapping $x \mapsto x^3$ over the subfield $\mathbb{F}_{2^3}$ (of cardinality $7+1$). As a more general consequence, because $x \mapsto x^3$ is a bijection over $\mathbb{F}_{2^3}$, the Kim mapping satisfies for any $\gamma \in \mathbb{F}_{2^6}$, $\kappa(\gamma\mathbb{F}_{2^3}) = \kappa(\gamma)\mathbb{F}_{2^3}$, which is called the *subspace property* [BDMW10].

While most infinite APN families share a particular structure related to the multiplicative cosets of a subgroup of $\mathbb{F}_{2^n}^*$, it is surprising that this was never explicitly exhibited and studied in a systematic manner. This is probably due to the different representations (univariate or multivariate) used for proving that these functions are APN, which seems to mean that they are of a different nature. The new point of view that we introduce in this paper then provides a way to unify many previous methodologies and definitions, while exhibiting new examples. In particular, our approach is related to the more general notion of *linear self-equivalence* [BBL21, BL22, BIK23, KKK23]. As a side effect, our work reinforces the following conjecture from [BBL21, Conjecture 1]: any APN permutation has a linearly self-equivalent CCZ-representative.

Outline and contributions. Before getting to the heart of the matter, we start by presenting the main definitions in Section 2. In particular, we begin from the well-known notion of homogeneity, which generalizes a property of power mappings to functions of the form $F\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}$. This property is involved in the definitions (or more precisely,

[1] We actually know a *single* APN function (up to equivalence) which is neither equivalent to a monomial nor to a quadratic function. This function operates on 6 bits and is known as the Brinckmann-Leander-Edel-Pott APN cubic function as it was independently discovered by the first two [BL08] and last two [EP09] authors. Whether other APN functions exist outside the CCZ-equivalence classes of monomials or of quadratic functions still remains an open question.

in equivalent characterizations that we detail later) of the *cyclotomic* and *biprojective* properties. They are respectively defined for functions of the form $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and of the form $F\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$ where $n = \ell k$. For this reason, it is hard to compare these notions, but also to relate them to properties of Boolean functions of the form $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$. Our goal is then to provide a unified point of view by relying on *linear self-equivalence*. A first step toward this objective is to precisely distinguish the cyclotomic property from the *subspace property*, which have been until now often mixed up.

In Section 3, we start our unification process by studying in detail the linear self-equivalences of cyclotomic or *ℓ-variate projective mappings*. To do so, we consider the linear mappings A, B involved in a linear self-equivalence relation $B \circ F \circ A = F$ of a function F, and we analyze the respective *similarity class* of A and B. The main tool at hand is a well-known *canonical form* of matrices based on the so-called *elementary divisors*. Because similarity can be studied up to isomorphisms of vector spaces, it provides a point of view well-suited to the study of functions defined over $\mathbb{F}_2^n$, $\mathbb{F}_{2^n}$ or even $\mathbb{F}_{2^k}^\ell$ with $n = \ell k$. This way, we derive three main theorems, namely Theorems 3 to 5, which not only give a clearer view of cyclotomic mappings and ℓ-variate projective mappings, but also provide definitions which do not depend on any specific input/output space $(\mathbb{F}_2^n, \mathbb{F}_{2^n}, \mathbb{F}_{2^k}^\ell)$ nor any specific bases.

In Section 4, we study the known infinite families of APN functions. The whole section is dedicated to a single main result (Theorem 6) which states that all members of almost all of these families are linearly equivalent (and in particular CCZ-equivalent) to a cyclotomic or an ℓ-variate projective mapping. Stated otherwise, despite their different initial representations (either univariate or multivariate), almost all of these families can be represented by particular linearly self-equivalent mappings. After commenting this result, its complete proof is provided.

The interest of these specific linearly self-equivalent mappings being established in Section 4, we continue in Section 5 to study their properties. In particular, we show how much linear self-equivalence can reflect on other properties of a function. The Walsh spectrum, differential spectrum, but also in the case of quadratic APN functions, the *ortho-derivative* and its associated spectra, inherit from such symmetries. Thus, we can show how to disprove the existence of a linearly self-equivalent representative among a given equivalence class, be it a CCZ-, EA-, or linear class.

In the end, in Section 6, we focus on a more specific case. After recalling some known facts about their Walsh spectra, we provide more detail about APN cyclotomic mappings, and in particular derive some necessary conditions to be APN. We also provide explicit formula for quadratic cyclotomic and ℓ-variate projective mappings.

We conclude by listing the main open questions that are spread out all along the paper.

2 Cyclotomic mappings, bi-projective mappings, linearly self-equivalent mappings, and subspace property

2.1 Preliminaries

In this section, we recap and introduce some notation. For any positive integers $0 \leq i \leq j$, we denote by $[\![i, j]\!]$ the set of integers ranging from i to j, *i.e.*, $[\![i, j]\!] := \{n \in \mathbb{N}, i \leq n \leq j\}$. The Hamming weight of an integer $i \geq 0$ is denoted by $\mathrm{wt}(n)$. Given two sets X, Y, we denote by $\mathcal{F}(X, Y)$ the set of functions from X to Y and by $|X|$ the cardinality of X.

We focus on the study of *vectorial Boolean functions*, that is of functions mapping n-bit words to m-bits words, which can be represented as: $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$, and more particularly to the case where $n = m$. In that case, the function can be uniquely represented by the *algebraic normal forms* (ANF) of its coordinates. Indeed, any Boolean function f

from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ can be uniquely represented by a polynomial $P \in \mathbb{F}_2[X_1, \ldots, X_n]/(X_1^2 + X_1, \ldots, X_n^2 + X_n)$ such that, for any $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$,

$$f(x_1, \ldots, x_n) = P(x_1, \ldots, x_n).$$

The *algebraic degree* of f is the degree of its ANF, while the degree of a vectorial function is the maximum degree of its coordinates. In particular, if not stated otherwise, the terminologies linear (or affine) and quadratic refer to functions whose ANF is of degree 1 or of degree 2.

The domain and codomain of a vectorial Boolean function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ can always be identified with other $\mathbb{F}_2$-spaces. Indeed, an $\mathbb{F}_2$-space isomorphism can always be built between two n-dimensional $\mathbb{F}_2$-spaces. In that case rather than focusing on $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$, we can instead look at $\pi_1 \circ F \circ \pi_2^{-1}$, where $\pi_1\colon \mathbb{F}_2^n \to V_1$ and $\pi_2\colon \mathbb{F}_2^m \to V_2$, where π_1, π_2 are $\mathbb{F}_2$-space isomorphims. If not stated otherwise, *isomorphism* always refers to an $\mathbb{F}_2$-linear bijection, *i.e.* a $\mathbb{F}_2$-vector space isomorphism. Handling several representations of the same functions will be a key point in our work for providing a unified point of view on several structural properties of vectorial functions.

When $n = m$, a specific choice is to choose $V_1 = V_2 = \mathbb{F}_{2^n}$, possibly with $\pi_1 = \pi_2$. In that case, F can be represented by a unique *univariate polynomial* $P \in \mathbb{F}_{2^n}[X]$ of (univariate) degree strictly smaller than 2^n. More generally, for any $k, \ell \geq 1$, any function $F\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}$ admits a unique *interpolating polynomial*, which is the unique polynomial $P \in \mathbb{F}_{2^k}[X_1, \cdots, X_\ell]$ which satisfies:

$$F(x_1, \cdots, x_\ell) = P(x_1, \cdots, x_\ell) \quad \forall\, x_1, \cdots, x_\ell \in \mathbb{F}_{2^k},$$

and has degree $d_i \leq 2^k - 1$ in each X_i. Given $u = (u_1, \cdots, u_\ell) \in [\![0, 2^k - 1]\!]^\ell$, the monomial $\prod_{i=1}^\ell X_i^{u_i}$ is denoted by $X^u := \prod_{i=1}^\ell X_i^{u_i}$.

The *trace* is a well-known linear mapping that plays a crucial role when working in finite fields.

Definition 1 (Trace function)**.** Let $n = \ell k$, $k > 1$. The trace function over $\mathbb{F}_{2^n}$ and relative to $\mathbb{F}_{2^k}$ is the function $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}$ from $\mathbb{F}_{2^n}$ to itself that is defined by:

$$\forall\, x \in \mathbb{F}_{2^n}, \quad \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(x) = \sum_{i=0}^{\ell-1} x^{2^{ik}}.$$

The graph of a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is denoted by $\mathcal{G}_F := \{(x, F(x)), x \in \mathbb{F}_2^n\}$. Given an affine mapping A, we denote by L_A its linear part, that is $L_A = A + A(0)$ and by c_A its constant term, *i.e.* $c_A = A(0)$. In order to study and classify vectorial Boolean functions in an effective manner we rely on the following equivalence relations.

Definition 2 (Linear, (extended) affine, and CCZ equivalence)**.** The functions F and G defined from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are said to be:

(i) *linearly equivalent* if there exist two $\mathbb{F}_2$-linear bijections A from $\mathbb{F}_2^n$ to itself and B from $\mathbb{F}_2^m$ to itself, such that $G = B \circ F \circ A$.

(ii) *affine equivalent* if there exist two $\mathbb{F}_2$-affine bijections A from $\mathbb{F}_2^n$ to itself and B from $\mathbb{F}_2^m$ to itself, such that $G = B \circ F \circ A$.

(iii) *extended affine-equivalent* if there exist two $\mathbb{F}_2$-affine bijections A from $\mathbb{F}_2^n$ to itself and B from $\mathbb{F}_2^m$ to itself, and an affine function $C\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that $G = B \circ F \circ A + C$.

(iv) *CCZ equivalent* if there exists an $\mathbb{F}_2$-affine bijection $\mathcal{A}$ from $\mathbb{F}_2^n \times \mathbb{F}_2^m$ to itself such that $\mathcal{A}(\mathcal{G}_F) = \mathcal{G}_G$.

Extended affine equivalence corresponds to CCZ equivalence restricted to affine mappings $\mathcal{A}$ whose linear part $\mathcal{L}$ is a lower triangular block matrix. More precisely $G = B \circ F \circ A + C$, if and only if $\begin{pmatrix} A^{-1} & 0 \\ CA^{-1} & B \end{pmatrix}(\mathcal{G}_F) = \mathcal{G}_G$. Similarly affine equivalence corresponds to CCZ equivalence restricted to affine mappings whose linear part is a diagonal block matrix: $G = B \circ F \circ A$ if and only if $\begin{pmatrix} A^{-1} & 0 \\ 0 & B \end{pmatrix}(\mathcal{G}_F) = \mathcal{G}_G$.

We denote by $\mathbf{GL}(V)$ the sets of all isomorphisms from the $\mathbb{F}_2$-space V to itself. In the paper, we will only use arbitrary vector spaces V when we voluntarily want to encompass the three cases of $\mathbb{F}_{2^k}^\ell$, $\mathbb{F}_2^n$, or $\mathbb{F}_{2^n}$ with $n = \ell k$. Otherwise, we prefer choosing one specific $\mathbb{F}_2$-space among the three previous ones. Similarly, the following definition enables us to compare the *linear-equivalence classes* of functions defined over possibly different domains.

Definition 3 (Linear-equivalence class)**.** Let $n = \ell k$ and F be a function from $\mathbb{F}_{2^k}^\ell$ to itself. Then, the linear-equivalence class of F is the subset of $\mathcal{F}(\mathbb{F}_2^n, \mathbb{F}_2^n)$ defined by:

$$\left\{\pi_1 \circ F \circ \pi_2^{-1}, \text{s.t } \pi_1, \pi_2 \colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_2^n \text{ are isomorphisms}\right\}.$$

By definition, the linear equivalence class of *any* function is *always* a subset of $\mathcal{F}(\mathbb{F}_2^n, \mathbb{F}_2^n)$. This notation has the big advantage that for any isomorphisms $\psi_1, \psi_2 \colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^{k'}}^{\ell'}$ with $k\ell = k'\ell'$, and any function $F \colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$, the linear-equivalence classes of F and $\psi_1 \circ F \circ \psi_2^{-1}$ coincide. Stated otherwise, the linear equivalence class of a function is independent of the choice of input and output bases, but also independent of the actual input or output spaces. This could be further generalized to functions $F \colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^{k'}}^{\ell'}$, where $(\ell, k) \neq (\ell', k')$, but in our context the domain and codomain will always be equal.

2.2 Homogeneity

In this section, we identify connections between various concepts that were still, to the best of our knowledge, unknown. They involve a lot of different properties that appear in different contexts, using different terminologies. These properties are also defined as properties of different objects (or representations), such as Boolean functions $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, univariate functions $F \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, or multivariate functions $F \colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$. In most of these properties, homogeneous functions are involved, one way or another.

Definition 4 (Homogeneous function with exponent d)**.** Let $k, \ell, d \geq 1$ be positive integers such that $d < 2^k$. Let F be a function from $\mathbb{F}_{2^k}^\ell$ to $\mathbb{F}_{2^k}$. The function F is said to be *homogeneous of exponent d* if it satisfies:

$$\forall (x_1, \cdots, x_\ell) \in \mathbb{F}_{2^k}^\ell, \quad \forall \varphi \in \mathbb{F}_{2^k}, \quad F(x_1\varphi, \cdots, x_\ell\varphi) = \varphi^d F(x_1, \cdots, x_\ell). \tag{1}$$

Remark 1. The functions defined in Definition 4 are sometimes known as homogeneous functions of degree d. However in our context, "degree" already refers to the univariate, multivariate or algebraic degree of a function. We then prefer using "exponent" instead.

Lemma 1. *Let $F \colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}$ and $d < 2^k$. Then, F is homogeneous of exponent d if and only if its interpolating polynomial $P = \sum_{u \in [\![0, 2^k-1]\!]^\ell} a_u X^u$ satisfies:*

$$\forall u \in [\![0, 2^k - 1]\!]^\ell \text{ s.t. } \sum_{i=1}^{\ell} u_i \not\equiv d \bmod (2^k - 1), \quad a_u = 0.$$

Proof. For any $u \in [\![0, 2^k - 1]\!]^\ell$, let us denote by $\Sigma(u)$ the integer sum defined by $\Sigma(u) := \sum_{i=1}^{\ell} u_i$. Let $\varphi \in \mathbb{F}_{2^k}$. Let us introduce the following functions:

$$G \colon (x_1, \cdots, x_\ell) \mapsto F(x_1\varphi, \cdots, x_\ell\varphi), \quad H \colon (x_1, \cdots, x_\ell) \mapsto \varphi^d F(x_1, \cdots, x_\ell).$$

Then G admits $P(X_1\varphi, \cdots, X_\ell\varphi)$ as interpolating polynomial and H admits $\varphi^d P$ as interpolating polynomial. By uniqueness of the interpolating polynomial, we deduce that the two polynomials are equal: $\forall u,\ a_u\varphi^{\Sigma(u)} = a_u\varphi^d$. Choosing for φ a primitive element of $\mathbb{F}_{2^k}$, we get that, for any $a_u \neq 0$, $\varphi^{\Sigma(u)} = \varphi^d$; in other words $\Sigma(u) \equiv d \bmod 2^k - 1$. Conversely, given any φ and any u with $\Sigma(u) \equiv d \bmod 2^k - 1$, we observe that $\prod_{i=1}^{\ell}(x_i\varphi)^{u_i} = \varphi^{\Sigma(u)}\prod_{i=1}^{\ell} x_i^{u_i} = \varphi^d \prod_{i=1}^{\ell} x_i^{u_i}$, which immediately implies the result. □

Example 1. When $\ell = 1$, homogeneous functions are exactly the monomials functions of the form $x \mapsto cx^d, \quad c \in \mathbb{F}_{2^k}$.

Example 2. Any homogeneous polynomial $P \in \mathbb{F}_{2^k}[X_1, \cdots, X_\ell]$ of degree d defines a homogeneous function $F\colon (\mathbb{F}_{2^n})^\ell \to \mathbb{F}_{2^n}$ of exponent d for any extension $\mathbb{F}_{2^n}$ of $\mathbb{F}_{2^k}$. However, the converse does not hold. For instance, $X_1^5X_2^2X_3^3 + X_1X_2X_3$ is not a homogeneous polynomial but still defines a homogeneous function $F\colon \mathbb{F}_8^3 \to \mathbb{F}_8$ of exponent 3 because $5 + 2 + 3 \equiv 10 \equiv 3 \bmod 7$.

2.3 Cyclotomic mappings

This section is devoted to a particular subclass of functions from $\mathbb{F}_{2^n}$ to itself, named *cyclotomic mappings*. After studying the main properties of this family, we will show that cyclotomic mappings over $\mathbb{F}_{2^n}$ with respect to $\mathbb{F}_{2^k}^*$, where k is a divisor of n, are characterized by a multivariate representation with homogeneous coordinates. We will see in Section 4, that these mappings play a major role in the known infinite families of APN functions.

Definition 5 (Cyclotomic mapping [Wan07])**.** Let $n \geq 1$ and let $\mathbb{G} \subset \mathbb{F}_{2^n}^*$ be a multiplicative subgroup. A mapping $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a *cyclotomic mapping of exponent d with respect to* $\mathbb{G}$ if $F(0) = 0$ and:

$$\forall\ \lambda \in \mathbb{F}_{2^n},\ \exists\ c_\lambda \in \mathbb{F}_{2^n}, \forall\ x \in \mathbb{G}, \quad F(\lambda x) = c_\lambda x^d.$$

Remark 2. For such a mapping, the original terminology introduced in [Wan07] is "cyclotomic mapping of order d and index $\frac{2^n-1}{|\mathbb{G}|}$". However, we prefer the wording of Definition 5 because "order" can also refer to the order of the group or of the function F, while "index" is also often overloaded.

Example 3. When n is even, the cyclotomic mappings of exponent 0 with respect to the subgroup $\mathbb{G} = \mathbb{F}_4^*$, which is of order 3, coincide with the so-called *canonical triplicate functions* studied in [BIK23, KKK23]. More generally, when d divides $2^n - 1$, the cyclotomic mappings of exponent 0 with respect to the group $\mathbb{G}$ of cardinality $|\mathbb{G}| = d$ coincide with the so-called *d-divisible* mappings studied in [KKK23], that is, functions that can be written as $x \mapsto P(x^d)$, for some P.

Definition 5 equivalently means that F acts on each coset of the subgroup $\mathbb{G}$ as the *fixed* monomial function $x \mapsto x^d$, up to a multiplicative constant. This is emphasized by the following equivalent definitions.

Lemma 2 (Equivalent definitions)**.** *Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $F(0) = 0$ and let $\mathbb{G} \subset \mathbb{F}_{2^n}^*$ be a subgroup of $\mathbb{F}_{2^n}^*$. Then, F is a cyclotomic mapping of exponent d with respect to $\mathbb{G}$ if and only if one of the following equivalent conditions holds:*

(i) $\forall\lambda \in \mathbb{F}_{2^n},\ \exists\ c_\lambda \in \mathbb{F}_{2^n}, \forall\ x \in \mathbb{G}, F(\lambda x) = c_\lambda x^d.$

(ii) $\forall\lambda \in \mathbb{F}_{2^n}, \forall\ x \in \mathbb{G}, F(\lambda x) = F(\lambda)x^d.$

(iii) *For any system Γ of representatives of $\mathbb{F}_{2^n}^*/\mathbb{G}$,*
$\forall\gamma \in \Gamma, \forall\ x \in \mathbb{G}, F(\gamma x) = F(\gamma)x^d.$

Proof. **(i) ⇔ (ii):** The fact that (i) implies (ii) is obtained by choosing $x = 1$, which leads to $c_\lambda = F(\lambda)$ for any $\lambda \in \mathbb{F}_{2^n}^*$. We then deduce that the first two definitions are equivalent.

(ii) ⇔ (iii): We only have to show that (iii) implies (ii): any $\lambda \in \mathbb{F}_{2^n}^*$ can be written $\lambda = \gamma y$ for some $\gamma \in \Gamma$ and $y \in \mathbb{G}$. Then, we deduce from (iii) that, for any $x \in \mathbb{G}$:

$$F(\lambda x) = F(\gamma x y) = F(\gamma) x^d y^d = F(\gamma y) x^d = F(\lambda) x^d \,.$$

□

Example 4. Let $\mathbb{F}_{2^k}$ be a subfield of $\mathbb{F}_{2^n}$. Because of the second characterization given in Lemma 2, we observe for instance that the trace $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}$ relative to $\mathbb{F}_{2^k}$, as well as any $\mathbb{F}_{2^k}$-linearized polynomial, are cyclotomic mappings of exponent 1 with respect to $\mathbb{F}_{2^k}^*$. The case $d = 1, \mathbb{G} = \mathbb{F}_{2^k}^*$ is a special case of Definition 5 corresponding to the former and more restrictive definition of cyclotomic mappings given in [NW05].

Any function $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $F(0) = 0$ is actually a cyclotomic mapping with respect to $\{1\}$. Therefore, we restrict ourselves to the nontrivial case where $\mathbb{G} \neq \{1\}$. Furthermore, any cyclotomic mapping with respect to $\mathbb{G}$ is also a cyclotomic mapping with respect to any subgroup of $\mathbb{G}$. We will then usually focus on the largest possible subgroup. We also notice that we can always consider $d < |\mathbb{G}|$ by replacing d by its remainder modulo $|\mathbb{G}|$.

It is also worth noting that, when the exponent d of a cyclotomic mapping F with respect to $\mathbb{G}$ is not coprime with the size of $\mathbb{G}$, then F is constant on each coset of the subgroup of order $t = \gcd(|\mathbb{G}|, d)$. This is detailed in the following definition and proposition.

Definition 6 (Almost t-to-1 mapping [KKK23])**.** Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and t be a divisor of $2^n - 1$. The function F is *almost t-to-1* if there exists a unique $y_0 \in \mathrm{Im}(F)$ such that:

$$\left|F^{-1}(\{y_0\})\right| = 1, \text{ and } \quad \forall\, y \in \mathrm{Im}(F) \setminus \{y_0\}\,, \left|F^{-1}(\{y\})\right| = t.$$

Proposition 1. *Let $\mathbb{G} \subset \mathbb{F}_{2^n}^*$ be a multiplicative subgroup of $\mathbb{F}_{2^n}^*$ and let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a cyclotomic mapping of exponent d with respect to $\mathbb{G}$ such that $t = \gcd(d, |\mathbb{G}|) > 1$. Then, F is constant on each coset of the subgroup $\mathbb{G}' \subset \mathbb{G}$ of size t. Equivalently, F is cyclotomic of exponent 0 with respect to $\mathbb{G}'$. Most notably, if F takes distinct non-zero values on each coset of $\mathbb{G}'$, then F is almost t-to-1.*

Proof. Since t is a divisor of $|\mathbb{G}|$, there exists a subgroup $\mathbb{G}' \subset \mathbb{G}$ of size t. Then, for any $\lambda \in \mathbb{F}_{2^n}$ and any $x \in \mathbb{G}'$:

$$F(\lambda x) = F(\lambda) x^d = F(\lambda)$$

since d is a multiple of $|\mathbb{G}'|$. □

Cyclotomic mappings can also be characterized by their univariate representation, as stated in the following well-known lemma.

Lemma 3 (Univariate characterization [Wan07, Lemma 1][Göl15, p.264])**.** *Let $\mathbb{G}$ be a multiplicative subgroup of $\mathbb{F}_{2^n}^*$ and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with interpolating polynomial $P = \sum_{i=0}^{2^n-1} a_i X^i$. The mapping F is a cyclotomic mapping of exponent d with respect to $\mathbb{G}$ if and only if one of the following equivalent conditions is satisfied:*

(i) *there exists $Q \in \mathbb{F}_{2^n}[X]$ such that $P(X) = X^d Q(X^{|\mathbb{G}|})$,*

(ii) *for any $i \in [\![0, 2^n - 1]\!]$ such that $i \not\equiv d \bmod |\mathbb{G}|$, $a_i = 0$.*

Proof. The two conditions are obviously equivalent. Let $s = |\mathbb{G}|$ and $2^n - 1 = ts$. Let α be a primitive element of $\mathbb{F}_{2^n}^*$, so that α^t generates $\mathbb{G}$.

($\Longleftarrow$) Let $\lambda = \alpha^i$ and $x = \alpha^{tj} \in \mathbb{G}$. Then:

$$\begin{aligned} F(\lambda x) &= P(\alpha^{i+tj}) = \alpha^{d(i+tj)} Q(\alpha^{s(i+tj)}) \\ &= (\alpha^{tj})^d \alpha^{di} Q(\alpha^{si}) = (\alpha^{tj})^d P(\alpha^i) = x^d F(\lambda), \end{aligned}$$

where the third equality is derived from $\alpha^{st} = 1$.

($\Longrightarrow$) Conversely, let $x \in \mathbb{G}$. From Lemma 2, we get for any $\lambda \in \mathbb{F}_{2^n}$:

$$\sum_{i=0}^{2^n-1} a_i \lambda^i x^i = P(\lambda x) = P(\lambda) x^d = \sum_{i=0}^{2^n-1} a_i x^d \lambda^i,$$

so that $\sum_{i=0}^{2^n-1} a_i (x^d + x^i) X^i$ is the null polynomial. Therefore if $a_i \neq 0$, using a generator x of $\mathbb{G}$, we get $x^{d-i} = 1$ and thus $i \equiv d \bmod |\mathbb{G}|$.

□

The polynomials described in Lemma 3 are sometimes known as Wan-Lidl polynomials [WL91] and have been extensively studied, and especially in the bijective case [AW07, BPW23, CC23, Lai07, WL91, Wan17].

Example 5. A binomial mapping over $\mathbb{F}_{2^n}$, $x \mapsto x^i + ax^j$ with $i < j$, is a cyclotomic mapping with respect to a nontrivial subgroup $\mathbb{G} \subset \mathbb{F}_{2^n}^*$ if and only if $\gcd(j-i, 2^n-1) > 1$. Indeed, from Lemma 3, this equivalently means that there exists a nontrivial subgroup $\mathbb{G} \subset \mathbb{F}_{2^n}^*$ such that $i \equiv j \bmod |\mathbb{G}|$. The largest subgroup $\mathbb{G}$ for which the property holds is then the subgroup of order $\gcd(j-i, 2^n-1)$.

Example 6. The *Kim-type mappings* defined[2] in [CL21] and also studied in [LLHQ21, Car15, Göl23], correspond to the mappings over $\mathbb{F}_{2^{2k}}$ with interpolating polynomials:

$$X^{3\cdot 2^k} + a_1 X^{2^{k+1}+1} + a_2 X^{2^k+2} + a_3 X^3, \ a_1, a_2, a_3 \in \mathbb{F}_{2^{2k}} \ .$$

Since all involved exponents are equal to 3 modulo $(2^k - 1)$, these mappings are cyclotomic mappings of exponent 3 with respect to $\mathbb{F}_{2^k}^*$. As we will show later in Proposition 15, the interpolating polynomials of all quadratic cyclotomic mappings defined over $\mathbb{F}_{2^{2k}}$ and of exponent 3 with respect to $\mathbb{F}_{2^k}^*$ can be written as:

$$a_0 X^{3\cdot 2^k} + a_1 X^{2^{k+1}+1} + a_2 X^{2^k+2} + a_3 X^3, \ a_0, a_1, a_2, a_3 \in \mathbb{F}_{2^{2k}} \ .$$

2.4 Cyclotomic mappings with respect to a subfield

Among all multiplicative subgroups, groups of units of subfields play a particular role. For the sake of simplicity, cyclotomic mappings with respect to the group of units of a subfield will be called *cyclotomic mappings with respect to a subfield*. For any subfield $\mathbb{F}_{2^k} \subset \mathbb{F}_{2^n}$, $\mathbb{F}_{2^n}$ can be seen as an $\mathbb{F}_{2^k}$-space of dimension $\ell := \frac{n}{k}$. In that case, a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can also be seen as a multivariate function, which leads to a multivariate characterization of cyclotomy.

Lemma 4 (Multivariate characterization)**.** *Let $n = \ell k$. Let $\pi \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}^\ell$ be an $\mathbb{F}_{2^k}$-linear bijection. Let $F \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and for all $i \in [\![1, \ell]\!]$, let $F_i \colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}$ denote the coordinates of $\pi \circ F \circ \pi^{-1}$. Then, F is a cyclotomic mapping of exponent $d < 2^k$ with respect to $\mathbb{F}_{2^k}$ if and only if, for any $i \in [\![1, \ell]\!]$, F_i is a homogeneous function of exponent d.*

[2] The terminology "Kim-type" originates from Chase and Lisoněk [CL21], while Carlet suggests "generalized Kim" for such functions *which are also APN* [Car15].

Proof. Let $(b_1, \cdots, b_\ell)$ be the $\mathbb{F}_{2^k}$-basis of $\mathbb{F}_{2^n}$ corresponding to π, *i.e.* the unique basis such that $\pi(b_i)$ is the element of $\mathbb{F}_{2^k}^\ell$ having all its coordinates equal to 0 except the i-th one, which is equal to 1. Then, the ℓ-variate coordinates $F_1, \ldots, F_\ell$ of $\pi \circ F \circ \pi^{-1}$ satisfy:

$$F(\lambda) = \sum_{i=1}^{\ell} F_i(\lambda_1, \cdots, \lambda_\ell) b_i, \quad \text{where } \lambda =: \sum_{i=1}^{\ell} \lambda_i b_i \text{ , with } \lambda_i \in \mathbb{F}_{2^k} \text{ for any } i.$$

($\Longrightarrow$) By hypothesis, F satisfies: $\forall \lambda \in \mathbb{F}_{2^n}\ \forall \varphi \in \mathbb{F}_{2^k}, F(\lambda\varphi) = F(\lambda)\varphi^d$, where equality also holds for $\varphi = 0$. Because $\varphi \in \mathbb{F}_{2^k}$, we have $\lambda\varphi = \sum_{i=1}^{\ell} (\lambda_i \varphi) b_i$. For any $i \in [\![1, \ell]\!]$, this then implies that:

$$\forall (\lambda_1, \cdots, \lambda_\ell) \in \mathbb{F}_{2^k}^\ell \quad \forall \varphi \in \mathbb{F}_{2^k} \quad F_i(\lambda_1\varphi, \cdots, \lambda_\ell\varphi) = \varphi^d F_i(\lambda_1, \cdots, \lambda_\ell);$$

or equivalently that all F_i are homogeneous functions of degree d.

($\Longleftarrow$) Conversely, we observe that, for any $\varphi \in \mathbb{F}_{2^k}$:

$$F(\lambda\varphi) = \sum_{i=1}^{\ell} F_i(\pi(\lambda\varphi)) b_i = \sum_{i=1}^{\ell} \varphi^d F_i(\pi(\lambda)) b_i = \varphi^d \sum_{i=1}^{\ell} F_i(\pi(\lambda)) b_i = \varphi^d F(\lambda),$$

where we use for the second equality the $\mathbb{F}_{2^k}$-linearity of π, and the homogeneity of F_i.

□

In that case, Lemma 4 provides an easy way to identify cyclotomic mappings through their multivariate polynomial representations. The previous characterizations of cyclotomic mapping with respect to a subfield are then summarized in the following theorem.

Theorem 1 (Cyclotomic mappings with respect to subfields)**.** *Let n, ℓ, k, d be positive integers such that $n = \ell k$ with $k > 1$ and $d < 2^k$. Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with interpolating polynomial $P = \sum_{i=0}^{2^n-1} a_i X^i$. Let $F = (F_1, \cdots, F_\ell)$ be any ℓ-variate representation of F where the i-th coordinate $F_i\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}$ has $P_i = \sum_{u \in [\![0, 2^k-1]\!]^\ell} a_{u,i} X^u$ as interpolating polynomial. The following statements are equivalent:*

- *F is a cyclotomic mapping of exponent d with respect to $\mathbb{F}_{2^k}$,*
- *$\forall\ \lambda \in \mathbb{F}_{2^n},\ \exists\ c_\lambda \in \mathbb{F}_{2^n},\ \forall\ \varphi \in \mathbb{F}_{2^k}, F(\lambda\varphi) = c_\lambda \varphi^d$,*
- *$\forall\ \lambda \in \mathbb{F}_{2^n},\ \forall\ \varphi \in \mathbb{F}_{2^k}, F(\lambda\varphi) = F(\lambda)\varphi^d$,*
- *For any system Γ of representatives of $\mathbb{F}_{2^n}^*/\mathbb{F}_{2^k}^*$, $\forall \gamma \in \Gamma,\ \forall\ \varphi \in \mathbb{F}_{2^k}, F(\gamma\varphi) = F(\gamma)\varphi^d$,*
- *$\exists\ Q \in \mathbb{F}_{2^n}[X], \quad P = X^d Q(X^{2^k-1})$,*
- *$\forall\ i \in [\![0, 2^n - 1]\!]$, such that $i \not\equiv d \bmod 2^k - 1$, $a_i = 0$,*
- *$\forall\ i \in [\![1, \ell]\!]$, F_i is a homogeneous function of exponent d,*
- *$\forall\ i \in [\![1, \ell]\!],\ \forall\ \varphi, x_1, \cdots, x_\ell \in \mathbb{F}_{2^k}, \quad F(x_1\varphi, \cdots, x_\ell\varphi) = \varphi^d F(x_1, \cdots, x_\ell)$,*
- *$\forall\ i \in [\![1, \ell]\!],\ \forall\ u \in [\![0, 2^k - 1]\!]^\ell$, such that $\sum_{i=1}^{\ell} u_i \not\equiv d \bmod 2^k - 1$, $a_{u,i} \neq 0$.*

As detailed in the following definition and proposition, the so-called (q, q)-*biprojective mappings* are particular cases of cyclotomic mappings.

Definition 7 (Biprojective mapping [Göl22, Göl23])**.** Let k, q, q', r, r' be positive integers such that $k > 1$, $q = 2^r, q' = 2^{r'}$ and $r, r' < k$. A function $F\colon \mathbb{F}_{2^k}^2 \to \mathbb{F}_{2^k}^2$ with bivariate representation $F(x, y) = (F_1(x, y), F_2(x, y))$ is a (q, q')-biprojective mapping if F_1 and F_2 have interpolating polynomials of the following forms:

$$F_1(x, y) = ax^{q+1} + bx^q y + cxy^q + dy^{q+1},$$
$$F_2(x, y) = ex^{q'+1} + fx^{q'} y + gxy^{q'} + hy^{q'+1},$$

with $a, b, c, d, e, f, g, h \in \mathbb{F}_{2^k}$.

Proposition 2 (Cyclotomic mappings and (q, q)-biprojective mappings [Göl23])**.** *Let $q = 2^r$. Then any (q, q)-biprojective mapping $F\colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ can be expressed as $\pi \circ G \circ \pi^{-1}$, where $G : \mathbb{F}_{2^{2k}} \to \mathbb{F}_{2^{2k}}$ is a cyclotomic mapping of exponent $q + 1$ with respect to $\mathbb{F}_{2^k}$ and $\pi\colon \mathbb{F}_{2^{2k}} \to \mathbb{F}_{2^k}^2$ is an $\mathbb{F}_{2^k}$-linear bijection.*

Proof. This is a direct corollary of the multivariate characterization of cyclotomic mappings. Indeed, we observe that any (q, q)-biprojective mapping F has homogeneous components of exponent $q + 1$. By choosing an $\mathbb{F}_{2^k}$-basis (b_1, b_2) of $\mathbb{F}_{2^{2k}}$, we can build the function $G\colon \mathbb{F}_{2^{2k}} \to \mathbb{F}_{2^{2k}}$ defined by:

$$\forall x, y \in \mathbb{F}_{2^k}, \quad G(b_1 x + b_2 y) = b_1 F_1(x, y) + b_2 F_2(x, y).$$

By construction, the function G is cyclotomic of exponent $q + 1$. With the mapping π defined by $\pi(b_1 x + b_2 y) = (x, y)$ for all x, y, we obtain: $F = \pi \circ G \circ \pi^{-1}$. □

Most notably, the previous proposition points out that the class of $(2, 2)$-biprojective functions coincides with the family of quadratic cyclotomic mappings of exponent 3 with respect to $\mathbb{F}_{2^{\frac{n}{2}}}$ mentioned in Example 6. Moreover, for $q = 2^r > 2$, the (q, q)-biprojective functions correspond to the *quadratic* cyclotomic mappings of exponent $(2^r + 1)$ with respect to $\mathbb{F}_{2^{\frac{n}{2}}}$, where quadratic refers to the algebraic degree of F. Most notably, this family includes as a subclass the so-called *(closed) generalized butterflies* introduced in [PUB16], studied in [CDP17, FFW17, LTYW18, CPT19], and defined by $F(x, y) = (F_1(x, y), F_1(y, x))$ with $F_1(x, y) = (x + \alpha y)^{2^r+1} + \beta y^{2^r+1}$.

2.5 Linearly self-equivalent mappings

When they are seen as functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, cyclotomic mappings correspond to a particular subclass of linearly self-equivalent mappings. This class of mappings has been extensively studied by Beierle, Brinkmann and Leander [BBL21, BL22] in order to find new APN mappings. In particular, they observed that all known APN permutations are CCZ-equivalent to a linearly self-equivalent APN permutation and conjecture in [BBL21, Conjecture 1] that this property always holds.

In the following, given $\mathbb{F}_2$-linear bijections A_i with $i \in [\![1, \ell]\!]$ from an $\mathbb{F}_2$-space V to itself, we denote by $\mathrm{diag}(A_1, \ldots, A_\ell)\colon V^\ell \to V^\ell$ the mapping defined by:

$$\forall (x_1, \ldots, x_\ell) \in V^\ell, \quad \mathrm{diag}(A_1, \ldots, A_\ell)(x_1, \ldots, x_\ell) := (A_1(x_1), \ldots, A_\ell(x_\ell)).$$

We also denote by $M_{\alpha,n}$ the multiplication mapping $x \mapsto x\alpha$ defined from $\mathbb{F}_{2^n}$ to itself.

Definition 8 (LE-automorphism group)**.** [CP19, BBL21] Let $n = \ell k$, $k > 1$. The *automorphism group* of a function $F : \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$ is the set $\mathrm{Aut}(F)$ of all $\mathbb{F}_2$-affine bijections σ from $\left(\mathbb{F}_{2^k}^\ell\right)^2$ to itself such that $\{(x, F(x)), x \in \mathbb{F}_{2^k}^\ell\}$ is invariant under σ.

The *LE-automorphism group* of F is the subgroup $\mathrm{Aut}_{\mathrm{LE}}(F)$ of $\mathrm{Aut}(F)$ composed of all automorphisms of the form $\mathrm{diag}(A, B)$ for some $\mathbb{F}_2$-linear bijections $A, B\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$.

Definition 9 (Linearly self-equivalent mappings [BBL21])**.** A function $F : \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$ is said to be *linearly self-equivalent* if $\mathrm{Aut}_{\mathrm{LE}}(F)$ is non-trivial, *i.e.*, there exist two $\mathbb{F}_2$-linear bijections $A, B \colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$ with $A \neq \mathrm{Id}$ or $B \neq \mathrm{Id}$ such that $B \circ F \circ A = F$.

Example 7. A cyclotomic mapping $F \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ of exponent d over a subgroup $\mathbb{G}$ satisfies for any $\alpha \in \mathbb{G}$:

$$M_{\alpha^{-d},n} \circ F \circ M_{\alpha,n} = F.$$

A (q, q')-biprojective function $G \colon (\mathbb{F}_{2^k})^2 \to (\mathbb{F}_{2^k})^2$ satisfies for any $\beta \in \mathbb{F}_{2^k}$:

$$\mathrm{diag}(M_{\beta^{q+1},k}, M_{\beta^{q'+1},k}) \circ G = G \circ \mathrm{diag}(M_{\beta,k}, M_{\beta,k}).$$

Both are therefore linearly self-equivalent mappings.

As in the case of Definition 3, this definition of linear self-equivalence is compatible with any change of basis, and any change of domain. Indeed, let $F \colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$. Then it holds that, for all $\mathbb{F}_2$-linear bijections $\pi_1, \pi_2 \colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^{k'}}^{\ell'}$,

$$\begin{aligned} \mathrm{diag}(A, B) \in \mathrm{Aut}_{\mathrm{LE}}(F) &\iff B\pi_1^{-1}\pi_1 F \pi_2^{-1}\pi_2 A^{-1} = F \\ &\iff (\pi_1 B \pi_1^{-1})(\pi_1 F \pi_2^{-1})(\pi_2 A^{-1} \pi_2^{-1}) = \pi_1 F \pi_2^{-1} \\ &\iff \mathrm{diag}\left(\pi_2 A \pi_2^{-1},\ \pi_1 B \pi_1^{-1}\right) \in \mathrm{Aut}_{\mathrm{LE}}\left(\pi_1 F \pi_2^{-1}\right). \end{aligned} \tag{2}$$

As a consequence of this formula, and as pointed out in [BBL21], classifying linearly self-equivalent mappings up to linear equivalence can leverage any similarity invariant of $\mathbf{GL}_n(\mathbb{F}_2)$, like the rational canonical form. We continue in this direction in Section 3.

Beforehand, we present another somehow-related property known as the *subspace property*, which is sometimes mistaken with cyclotomy.

2.6 Subspace property

The Kim mapping exhibited in [BDMW10] is a cyclotomic mapping of exponent 3 with respect to $\mathbb{F}_8$. Instead of this particular structure, Dillon *et al.* [BDMW10] highlight a more general property called the *subspace property*. In the following, we generalize it to any subgroup $\mathbb{G} \subset \mathbb{F}_{2^n}^*$ while it was originally defined in [BDMW10] for n even and $\mathbb{G} = \mathbb{F}_{2^{\frac{n}{2}}}^*$ only.

Definition 10 (Subspace property [BDMW10])**.** Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $\mathbb{G} \subset \mathbb{F}_{2^n}^*$ be a multiplicative subgroup of $\mathbb{F}_{2^n}^*$. A mapping F satisfies the $\mathbb{G}$-*subspace property* if, for all $\lambda \in \mathbb{F}_{2^n}$, $F(\lambda\mathbb{G}) = F(\lambda)\mathbb{G}$.

Because $0\mathbb{G} = \{0\}$, the definition implies that $F(\{0\}) = F(0)\mathbb{G}$, which necessarily means that $F(0) = 0$ for the cardinalities to be equal. A particular subclass of mappings satisfying the subspace property is formed by some so-called *generalized cyclotomic mappings*, which correspond to a generalization of the notion of cyclotomic mappings given in Definition 5. Indeed, while a cyclotomic mapping with respect to $\mathbb{G}$ acts as the same monomial mapping (up to a constant) over all cosets of $\mathbb{G}$, we may consider possibly different monomials for the different cosets, as in the following definition.

Definition 11 (Generalized cyclotomic mapping [BW22])**.** Let $\mathbb{G}$ be a subgroup of $\mathbb{F}_{2^n}^*$. A mapping $F \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called a generalized cyclotomic mapping with respect to $\mathbb{G}$ if $F(0) = 0$ and $\forall \lambda \in \mathbb{F}_{2^n}, \exists\, d_\lambda \in \mathbb{N},\ \forall\, x \in \mathbb{G}, F(\lambda x) = F(\lambda) x^{d_\lambda}$.

If $F(\lambda) \neq 0$, the value of $d_\lambda \bmod |\mathbb{G}|$ only depends on the coset of λ. Indeed, it holds that for any $y, x \in \mathbb{G}$:

$$F(\lambda y) x^{d_{\lambda y}} = F(\lambda y x) = F(\lambda) y^{d_\lambda} x^{d_\lambda} = F(\lambda y) x^{d_\lambda}.$$

Therefore, as in Lemma 2, an equivalent condition is that, for any γ in a system of representatives of $\mathbb{F}_{2^n}^*/\mathbb{G}$, there exists $d_\gamma \in \mathbb{N}$ such that:

$$\forall x \in \mathbb{G}, \quad F(\gamma x) = F(\gamma)x^{d_\gamma}.$$

Generalized cyclotomic mappings with respect to $\mathbb{G}$ then form a subclass of the mappings satisfying the $\mathbb{G}$-subspace property if their exponents are coprime with $|\mathbb{G}|$.

Lemma 5. *Let $\mathbb{G}$ be a subgroup of $\mathbb{F}_{2^n}^*$ and Γ be a system of representatives of $\mathbb{F}_{2^n}^*/\mathbb{G}$. A generalized cyclotomic mapping of exponents $d_\gamma, \gamma \in \Gamma$ with respect to $\mathbb{G}$ satisfies the $\mathbb{G}$-subspace property if and only if $\gcd(d_\gamma, |\mathbb{G}|) = 1$ for all $\gamma \in \Gamma$.*

Proof. Let F be a generalized cyclotomic mapping with respect to $\mathbb{G}$. By definition, for any $\lambda \in \mathbb{F}_{2^n}$, we have:

$$\begin{aligned} F(\lambda\mathbb{G}) &= \{F(\lambda x), x \in \mathbb{G}\} \\ &= \{x^{d_\lambda}F(\lambda), x \in \mathbb{G}\} \\ &= \{x^{d_\gamma}F(\lambda), x \in \mathbb{G}\} \end{aligned}$$

where $\gamma \in \Gamma$ is such that $\lambda \in \gamma\mathbb{G}$. It follows that $F(\lambda\mathbb{G}) = F(\lambda)\mathbb{G}$ if and only $x \mapsto x^{d_\gamma}$ is bijective over $\mathbb{G}$, or equivalently d_γ is coprime with $|\mathbb{G}|$. □

Most notably, this points out that the subspace property as defined by Göloğlu in [Göl15], and which actually corresponds to the definition of cyclotomic mapping of exponent (2^r+1) with respect to the subfield $\mathbb{F}_{2^{n/2}}$ for any $r \geq 1$, *does not coincide* with the original subspace property recalled in Definition 10. Indeed, such cyclotomic mappings satisfy the $\mathbb{F}_{2^{n/2}}^*$-subspace property if and only if $\frac{n}{2\gcd(r,n/2)}$ is odd. This is not the case for instance of the APN mappings satisfying Göloğlu's subspace property when n is a multiple of 4, since the APN condition (see Proposition 12) implies that r is coprime with $n/2$ and contradicts Lemma 5.

Therefore, we want to further clarify the differences between the subspace property and the properties of (generalized) cyclotomic mappings. To this aim, we now characterize, among all mappings satisfying the $\mathbb{G}$-subspace property, the ones corresponding to generalized cyclotomic mappings with respect to $\mathbb{G}$. This characterization first requires the following proposition.

Proposition 3. *Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $F(0) = 0$, let $\mathbb{G} \subset \mathbb{F}_{2^n}^*$ be a subgroup of $\mathbb{F}_{2^n}^*$ and Γ be a system of representatives of $\mathbb{F}_{2^n}^*/\mathbb{G}$. Then, F has the $\mathbb{G}$-subspace property if and only if one of the following equivalent conditions is satisfied:*

(i) $\forall \lambda \in \mathbb{F}_{2^n}$, $F(\lambda\mathbb{G}) = F(\lambda)\mathbb{G}$.

(ii) $\forall \gamma \in \Gamma$, $F(\gamma\mathbb{G}) = F(\gamma)\mathbb{G}$.

(iii) $\forall \lambda \in \mathbb{F}_{2^n}$, *there exists a bijection* $G_\lambda : \mathbb{G} \to \mathbb{G}$ *such that,* $\forall x \in \mathbb{G}$, $F(\lambda x) = F(\lambda)G_\lambda(x)$.

(iv) $\forall \gamma \in \Gamma$, *there exists a bijection* $G_\gamma : \mathbb{G} \to \mathbb{G}$ *such that,* $\forall x \in \mathbb{G}$, $F(\gamma x) = F(\gamma)G_\gamma(x)$.

Proof. **(i)** $\iff$ **(ii):** We only have to prove that (ii) implies (i). Let $\lambda \in \mathbb{F}_{2^n}$. Then, there exists $\gamma \in \Gamma$ such that $\lambda = \gamma x$. Then, $F(\lambda) \in F(\gamma)\mathbb{G}$. We then deduce that:

$$F(\lambda\mathbb{G}) = F(\gamma\mathbb{G}) = F(\gamma)\mathbb{G} = F(\lambda)\mathbb{G}\ .$$

(i) $\iff$ **(iii):** Let $\lambda \in \mathbb{F}_{2^n}$ such that $F(\lambda) \neq 0$. We consider the mapping $G_\lambda : \mathbb{G} \to \mathbb{F}_{2^n}$ defined by:

$$G_\lambda(x) = \frac{F(\lambda x)}{F(\lambda)}\ .$$

Then, $\mathrm{Im}(G_\lambda) = \mathbb{G}$ if and only if $F(\lambda\mathbb{G}) = F(\lambda)\mathbb{G}$. Moreover, when $F(\lambda) = 0$, $F(\lambda\mathbb{G}) = \{0\}$, which means that $F(\lambda x) = F(\lambda)G_\lambda(x)$ for any bijection $G_\lambda : \mathbb{G} \to \mathbb{G}$. Therefore, we derive that (i) and (iii) (resp. (ii) and (iv)) are equivalent.

□

It is worth noticing that, when $F(\lambda) \neq 0$, all the functions $G_\lambda : \mathbb{G} \to \mathbb{G}$ in the previous definitions satisfy $G_\lambda(1) = 1$, and the same can be assumed when $F(\lambda) = 0$.

An interesting case corresponds to the situation where all functions G_λ are identical when λ varies in a coset of $\mathbb{G}$. This situation characterizes the generalized cyclotomic mappings with respect to $\mathbb{G}$ within the family of all functions satisfying the $\mathbb{G}$-subspace property.

Theorem 2. *Let $\mathbb{G}$ be a subgroup of $\mathbb{F}_{2^n}^*$ and Γ be a system of representatives of $\mathbb{F}_{2^n}^*/\mathbb{G}$. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a mapping satisfying the $\mathbb{G}$-subspace property, i.e., for all $\lambda \in \mathbb{F}_{2^n}$, there exists a bijection $G_\lambda : \mathbb{G} \to \mathbb{G}$ such that, $\forall x \in \mathbb{G}$, $F(\lambda x) = F(\lambda)G_\lambda(x)$. Then, for all $\gamma \in \Gamma$ and all $\lambda \in \gamma\mathbb{G}$, $G_\lambda = G_\gamma$ if and only if F is a generalized cyclotomic mapping with respect to $\mathbb{G}$ of exponents d_λ with $\gcd(d_\lambda, |\mathbb{G}|) = 1$.*

Proof. **($\Longrightarrow$)** Let us first prove that, for any F satisfying the $\mathbb{G}$-subspace property, we have that, for any $\gamma \in \Gamma$ with $F(\gamma) \neq 0$, for all $\varphi, x \in \mathbb{G}$, $G_\gamma(\varphi x) = G_\gamma(\varphi)G_{\gamma\varphi}(x)$. By definition it holds that:

$$G_\gamma(\varphi x) = \frac{F(\gamma\varphi x)}{F(\gamma)} .$$

Moreover, $F(\gamma\varphi) \neq 0$ since $F(\gamma\varphi) \in F(\gamma)\mathbb{G}$, with $F(\gamma) \neq 0$. This leads to:

$$G_\gamma(\varphi)G_{\gamma\varphi}(x) = \frac{F(\gamma\varphi)}{F(\gamma)} \times \frac{F(\gamma\varphi x)}{F(\gamma\varphi)} = \frac{F(\gamma\varphi x)}{F(\gamma)} = G_\gamma(\varphi x) .$$

By hypothesis, we know that $G_{\gamma\varphi}(x) = G_\gamma(x)$. We then deduce that, for all $\varphi, x \in \mathbb{G}$, $G_\gamma(\varphi x) = G_\gamma(\varphi)G_\gamma(x)$ This means G_γ is a multiplicative permutation of $\mathbb{G}$ with $G_\gamma(1) = 1$. Let us consider $\varphi \in \mathbb{G}$ a given generator of $\mathbb{G}$. We observe that $G_\gamma(\varphi)$ can be written as $G_\gamma(\varphi) = \varphi^{d_\gamma}$ for some d_γ. It then implies that $G_\gamma(\varphi^{d'}) = G_\gamma(\varphi)^{d'} = (\varphi^{d_\gamma})^{d'} = (\varphi^{d'})^{d_\gamma}$, so that $G_\gamma(x) = x^{d_\gamma}$ for any $x \in \mathbb{G}$. The function G_γ is therefore a power mapping and d_γ is necessarily coprime with $|\mathbb{G}|$ because it is bijective. If $F(\gamma) = 0$, then any bijection G_γ can be used, including a power permutation. We then deduce that, for any $\lambda \in \mathbb{F}_{2^n}$, $\forall x \in \mathbb{F}$, $F(\lambda x) = F(\lambda)G_\gamma(x) = F(\lambda)x^{d_\gamma}$, i.e. F is a generalized cyclotomic mapping of exponents coprime with $\mathbb{G}$.

($\Longleftarrow$) Conversely, let F be a generalized cyclotomic mapping. Then for any $\lambda \in \mathbb{F}_{2^n}$, G_λ can be defined as $G_\lambda(x) = x^{d_\lambda}$ for any $x \in \mathbb{G}$. The equality $d_\lambda \equiv d_\gamma \bmod |\mathbb{G}|$ when $\lambda \in \gamma\mathbb{G}$ is already mentioned after Definition 11. Moreover, since the exponent d_γ is coprime with $|\mathbb{G}|$, $G_\lambda(x) = x^{d_\gamma}$ is a bijection on $\mathbb{G}$.

□

Theorem 2 enables us to have a clearer view of the situation. As a cyclotomic mapping with exponent coprime with $2^{\frac{n}{2}} - 1$, the Kim mapping appears to be a very particular case of function satisfying the $\mathbb{F}^*_{2^{\frac{n}{2}}}$-subspace property.

Contrary to cyclotomic mappings or biprojective mappings, the subspace property does not seem to imply (by definition) any kind of linear self-equivalence. For instance, let us consider the generalized cyclotomic mapping with respect to $\mathbb{F}_{2^3}$ and defined over $\mathbb{F}_{2^6}$ by:

$$F(x) = \begin{cases} x^3 & \text{if } x \in \alpha^i\mathbb{F}_{2^3} \text{ for any } i \in [\![0, 8]\!] \setminus \{1\} \\ x^5 & \text{if } x \in \alpha\mathbb{F}_{2^3} \end{cases} ,$$

where α is a primitive element with minimal polynomial $X^6 + X^4 + X^3 + X + 1$. It can be computationally verified that the automorphism group $\mathrm{Aut}(F)$ is trivial, and this in particular implies that this is also the case for $\mathrm{Aut}_{\mathrm{LE}}(F)$.

In the following, we rather continue studying linear self-equivalence. However, generalized cyclotomic mappings will still be mentioned in a few results in Section 6.1, when the generalization from the cyclotomic case is immediate.

3 Classification of some families of linearly self-equivalent mappings

This section is dedicated to a unified study of the cyclotomic mappings and biprojective mappings introduced in the previous section. More precisely, we study in detail the linear self-equivalences of such mappings. To do so, we consider the linear mappings A, B involved in a linear self-equivalence relation $B \circ F \circ A = F$ of a function F, and we analyze the respective *similarity class* of A and B. First, we will recall some properties of the *canonical form* of linear bijections.

3.1 Canonical forms of linear mappings

The family of companion matrices plays an important role when representing matrices up to similarity equivalence.

Definition 12 (Companion matrix)**.** Let $P(X) = X^n + \sum_{i=0}^{n-1} p_i X^i$ be a monic polynomial in $\mathbb{F}_2[X]$. Its *companion matrix* is the $n \times n$ matrix defined by:

$$C(P) = \begin{pmatrix} 0 & 0 & \cdots & 0 & p_0 \\ 1 & 0 & & \vdots & p_1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & & \ddots & 0 & p_{n-2} \\ 0 & \cdots & 0 & 1 & p_{n-1} \end{pmatrix}$$

In the following, we use the canonical representation of endomorphisms based on elementary divisors and which is sometimes known as the *primary rational canonical form*. This is an alternative to the one based on invariant factors (aka Frobenius normal form) and which is used in [BBL21]. Therefore, by *canonical form*, we now refer to the following well-known proposition.

Proposition 4 (Canonical form, elementary divisors [Her75, Page 308])**.** *Let V be an $\mathbb{F}_2$-space of dimension n. Let $A\colon V \to V$ be an $\mathbb{F}_2$-linear mapping with minimal polynomial $\prod_{i=1}^{r} P_i^{e_i}$ where $P_1, \ldots, P_r$ are distinct irreducible polynomials and all $e_i \geq 1$. Then, there exists an $\mathbb{F}_2$-basis of V in which the matrix M_A of A is of the form:*

$$M_A = \begin{pmatrix} R_1 & & \\ & \ddots & \\ & & R_r \end{pmatrix}, \text{with } R_i = \begin{pmatrix} C\left(P_i^{e_{i,1}}\right) & & \\ & \ddots & \\ & & C\left(P_i^{e_{i,s_i}}\right) \end{pmatrix},$$

where $e_i = e_{i,1} \geq e_{i,2} \geq \ldots \geq e_{i,s_i}$ for any i. The polynomials $P_i^{e_{i,j}}$ are called the elementary divisors of A. Such a decomposition is unique, up to a reordering of the blocks.

The previous theorem is stated for a generic $\mathbb{F}_2$-space V and this is on purpose. Indeed, this enables us to handle the three main cases on which we focus on in a single stroke:

functions from $\mathbb{F}_2^n$ to itself, functions from $\mathbb{F}_{2^n}$ to itself, and functions from $\mathbb{F}_{2^k}^\ell$ to itself with $n = \ell k$.

In the following, we denote by $\min(A)$ the *minimal polynomial* of any $\mathbb{F}_2$-linear endomorphism A. Also, the minimal polynomial of any $\alpha \in \mathbb{F}_{2^n}$ is denoted by $\min(\alpha)$.

Remark 3. Despite the name and notation, minimal polynomials of endomorphisms and the ones of elements of a finite field do not share all of their properties. As an example, the minimal polynomial $\min(\alpha)$ where $\alpha \in \mathbb{F}_{2^n}$ is always irreducible, while this is not the case of the minimal polynomial of a matrix. For instance, the minimal polynomial of an involutive matrix $A \neq \mathrm{Id}$ is $X^2 + 1 = (X + 1)^2$.

It is well-known (see for instance [MP13, pp. 311-312]) that, for any irreducible polynomial $P \in \mathbb{F}_2[X]$ of degree n, and any root $\alpha \in \mathbb{F}_{2^n}$ of P, there exists a basis of $\mathbb{F}_{2^n}$ such that the matrix of $M_{\alpha,n}$ is equal to $C(P)$. The following lemma generalizes this property, and will be very useful in our classification.

Lemma 6. *Let V be an $\mathbb{F}_2$-space of dimension n. Let $A\colon V \to V$ be an $\mathbb{F}_2$-linear mapping. Then the following statements are equivalent:*

(i) $\min(A)$ *is irreducible over* $\mathbb{F}_2$*,*

(ii) *there exists an irreducible polynomial $P \in \mathbb{F}_2[X]$ and an $\mathbb{F}_2$-basis in which the matrix of A is* $\mathrm{diag}(C(P), C(P), \ldots, C(P))$*,*

(iii) *there exists an irreducible polynomial $P \in \mathbb{F}_2[X]$ of degree d, $d \mid n$ such that for any root $\alpha \in \mathbb{F}_{2^n}$ of P, there exists an $\mathbb{F}_2$-linear bijection $\pi\colon V \to \mathbb{F}_{2^n}$ which satisfies: $\pi \circ A \circ \pi^{-1} = M_{\alpha,n}$.*

Proof. **(i) ⇔ (ii):** The first equivalence is a direct consequence of Proposition 4: if A has as unique type of block $C(P)$ for some irreducible P, this is necessarily its canonical form. Then it must hold that $\min(A) = P$ because P is the only irreducible factor of $\min(A)$ and it appears with highest power 1 in the canonical form. The minimal polynomial $\min(A)$ is therefore irreducible (and $\min(A) = P$). Conversely, if the minimal polynomial of A is irreducible, then there can be only one type of block in its canonical form, which is $C(\min(A))$.

(i & ii) ⟹ (iii): Let d be the degree of $\min(A)$. Because of the second characterization, d is the size of the blocks, and it must then divide n. The polynomial $\min(A)$ is then irreducible of degree d, and $\mathbb{F}_{2^d} \subset \mathbb{F}_{2^n}$ is thus its splitting field. Let s be such that $n = ds$. Let $\alpha \in \mathbb{F}_{2^d}$ be a root of $\min(A)$. Let $\beta_1, \ldots, \beta_s$ be an $\mathbb{F}_{2^d}$-basis of $\mathbb{F}_{2^n}$ so that any $x \in \mathbb{F}_{2^n}$ can be uniquely decomposed as $x = \sum_{i=1}^s x_i\beta_i$, with $x_1, \ldots, x_s \in \mathbb{F}_{2^d}$. Then for any $x \in \mathbb{F}_{2^n}$ it holds that:

$$M_{\alpha,n}(x) = \alpha x = \sum_{i=1}^{s} (\alpha x_i)\beta_i = \sum_{i=1}^{s} M_{\alpha,d}(x_i)\beta_i.$$

The multiplication $M_{\alpha,n}$ is then the application of $M_{\alpha,d}$ in parallel on each coset $\beta_i\mathbb{F}_{2^d}$. But in the basis $(1, \alpha, \ldots, \alpha^{d-1})$, $M_{\alpha,d}$ has $C(\min(A))$ as matrix. This means that $M_{\alpha,n}$ has $\mathrm{diag}(C(\min(A)), \ldots, C(\min(A)))$ as matrix in the basis $(\alpha^i\beta_j)_{i\in[\![0,d-1]\!],j\in[\![1,s]\!]}$. By hypothesis, this is also the case of A in some basis $(v_{i,j})_{i\in[\![0,d-1]\!],j\in[\![1,s]\!]}$ of V. The linear mapping π defined by $\pi(v_{i,j}) = \alpha^i\beta_j$ for any i, j satisfies the announced property.

(i) ⟸ (iii): Conversely, given P, α and π with the announced property, it holds that $\min(A) = \min(M_{\alpha,n})$. But for any $x \in \mathbb{F}_{2^n}$, it holds that:

$$P(M_{\alpha,n})x = P(\alpha)x = 0,$$

because α is a root of P. Therefore $\min(M_{\alpha,n}) \mid P$, but as P is irreducible, we deduce that $\min(M_{\alpha,n}) = P$, and thus $\min(A) = P$ is irreducible.

□

3.2 LE-automorphism groups of cyclotomic mappings

Using Eq. (2) and Lemma 6, we can now deduce the following correspondence between cyclotomic mappings and some linearly self-equivalent mappings.

Theorem 3. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and let $\mathbb{G}$ be a subgroup of $\mathbb{F}_{2^n}^*$. Then, the following properties are equivalent.*

(i) *F belongs to the linear-equivalence class of a cyclotomic mapping with respect to $\mathbb{G}$.*

(ii) *There exists $\mathrm{diag}(A, B) \in \mathrm{Aut}_{\mathrm{LE}}(F)$ such that $\min A$ and $\min B$ are irreducible polynomials and $\mathrm{ord}(A) = |\mathbb{G}|$ and $\mathrm{ord}(B)$ is a divisor of $|\mathbb{G}|$.*

Proof. **(i)** $\Longrightarrow$ **(ii)** Let $\alpha \in \mathbb{G}$ be a generator of $\mathbb{G}$. By assumption and by Eq. (2) there exists an integer d and two $\mathbb{F}_2$-linear bijections $\pi_1, \pi_2 \colon \mathbb{F}_2^n \to \mathbb{F}_{2^n}$ such that $\mathrm{diag}(A, B) \in \mathrm{Aut}_{\mathrm{LE}}(F)$ where A, B are defined by:

$$A = \pi_1^{-1} \circ M_{\alpha,n} \circ \pi_1, \qquad B = \pi_2^{-1} \circ M_{\beta,n} \circ \pi_2, \tag{3}$$

with $\beta = \alpha^d$. By Lemma 6, both $\min(A)$ and $\min(B)$ are irreducible. Furthermore, A (resp. B) has the same order as $M_{\alpha,n}$ (resp. $M_{\alpha^d,n}$) which is the multiplicative order of α (resp. α^d).

(i) $\Longleftarrow$ **(ii)** Conversely, if $\min(A), \min(B)$ are irreducible, because of Lemma 6, they can be decomposed as in Eq. (3), with α such that $\langle \alpha \rangle = \mathbb{G}$ and $\mathrm{ord}(\beta) \mid |\mathbb{G}|$. This implies that $\beta \in \mathbb{G}$ and it can then be written as $\beta = \alpha^d$ for some $0 \leq d < |G|$. Then Eq. (2) can be used in the opposite way to deduce that $\pi_2 \circ F \circ \pi_1^{-1}$ is cyclotomic with respect to $\mathbb{G}$.

□

In other words, any function F satisfying the second condition of Theorem 3 admits a univariate cyclotomic representation, if the identifications between $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ are properly chosen.

By classifying linearly self-equivalent APN permutations according to the Frobenius normal forms of their LE-automorphisms, Beierle *et al.* [BBL21] proved that any linearly self-equivalent APN permutation in dimension 8 is CCZ-equivalent to an APN permutation with an automorphism $\mathrm{diag}(A, B)$ of one of the following two types [BBL21, Th. 4]:

1. $A = B = \mathrm{diag}(C(P), C(P))$ with $P(X) = X^4 + X^3 + X^2 + X + 1$;
2. $A = B = \mathrm{diag}(I_2, C(Q), C(Q), C(Q))$ with $Q(X) = X^2 + 1$.

A direct consequence of Theorem 3 is that the functions of the first type correspond to the functions in the linear-equivalence class of a cyclotomic mapping of exponent 1 with respect to the subgroup $\mathbb{G} \subset \mathbb{F}_{2^4}$ of order 5 since P is an irreducible polynomial of degree 4 and order 5. The fact that the exponent can be chosen to be 1 comes from the freedom of choice in the previous proof for α, β among all elements satisfying $\mathrm{ord}(\alpha) = \mathrm{ord}(A)$ and $\mathrm{ord}(\beta) = \mathrm{ord}(B)$. Here we can choose $\alpha = \beta$.

3.3 LE-automorphism groups of biprojective mappings

We have proved that the linear-equivalence classes of cyclotomic mappings are characterized by automorphisms $\mathrm{diag}(A, B)$ such that the canonical forms of A and B have all their blocks equal. Now, we focus on the class of functions such that the primary rational canonical form of B has blocks $C(P_i)$ of the same size but with possibly different minimal polynomials. This enables us to characterize the following multivariate generalization of the notion of (q, q')-biprojective functions introduced and studied by Göloğlu [Göl22, Göl23].

Definition 13 (ℓ-variate projective mappings)**.** Let $n = \ell k$. Let $F\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$ and let $F_i\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}$, $1 \le i \le \ell$, denote its i-th coordinate. Then, F is an *ℓ-variate projective mapping* of exponents $(d_1, \ldots, d_\ell)$ with respect to $\mathbb{F}_{2^k}$ if, for all i, $1 \le i \le \ell$, F_i is a homogeneous function of exponent d_i.

Proposition 5. *Let ℓ, k, d, r, s be positive integers. Then:*

(i) *The family of ℓ-variate projective mappings of exponents $(d, \ldots, d)$ coincides with the family of cyclotomic mappings of exponent d with respect to $\mathbb{F}_{2^k}$.*

(ii) *The family of 2-variate projective mappings of exponents $(2^r + 1, 2^s + 1)$ with respect to $\mathbb{F}_{2^k}$ with algebraic degree 2 coincides with the family of $(2^r, 2^s)$-biprojective mappings.*

Proof. The first item is proved in Lemma 4. The proof of the second item is postponed to the proof of Proposition 16. □

We now characterize the linear-equivalence classes of multivariate projective mappings by their LE-automorphism group. Before stating the corresponding theorem, we recall the following well-known fact.

Lemma 7 (Degree and order of a minimal polynomial)**.** *Let α be an element of $\mathbb{F}_{2^n}$. Then the degree of its minimal polynomial is equal to the multiplicative order of 2 modulo $\mathrm{ord}(\alpha)$.*

Proof. By definition, the degree of $\min(\alpha)$ is the number of conjugates of α. As the conjugates can be enumerated as $\alpha, \alpha^2, \alpha^{2^2} \ldots$, the number of conjugates is given by the smallest $i \ge 1$ such that $\alpha^{2^i} = \alpha$, *i.e.* the smallest $i \ge 1$ such that $2^i \equiv 1 \bmod \mathrm{ord}(\alpha)$. In other words, the degree of $\min(\alpha)$ is the multiplicative order of 2 modulo $\mathrm{ord}(\alpha)$. □

Theorem 4. *Let $n = \ell k$ and let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then, the following properties are equivalent:*

(i) *F belongs to the linear-equivalence class of an ℓ-variate projective mapping of exponents $(d_1, \ldots, d_\ell)$ with respect to $\mathbb{F}_{2^k}$, and for any $1 \le i \le \ell$, the multiplicative order of 2 modulo $(2^k - 1)/\gcd(d_i, 2^k - 1)$ equals k.*

(ii) *There exists $\mathrm{diag}(A, B) \in \mathrm{Aut}_{\mathrm{LE}}(F)$ such that $\min(A)$ is a primitive polynomial of degree k and $\min(B)$ is a product of distinct irreducible polynomials of degree k.*

Proof. **(i)** $\implies$ **(ii)** By assumption, there exists $\mathrm{diag}(A, B) \in \mathrm{Aut}_{\mathrm{LE}}(F)$ such that A and B have the following forms:

$$A = \pi_1^{-1} \circ \mathrm{diag}(M_{\alpha,k}, \ldots, M_{\alpha,k}) \circ \pi_1,$$

$$B = \pi_2^{-1} \circ \mathrm{diag}(M_{\alpha^{d_1},k}, \ldots, M_{\alpha^{d_\ell},k}) \circ \pi_2,$$

where α is a primitive element of $\mathbb{F}_{2^k}$. Because of Lemma 6, the minimal polynomial of A is the minimal polynomial of α, and therefore a primitive polynomial of degree k. Let us denote by P_i the minimal polynomial of each α^{d_i}. By applying Lemma 6 to each coordinate of B, we observe that B has, as matrix representation, a diagonal

matrix where the block $C(P_i)$ appears $\frac{k}{\deg(P_i)}$ times (counted with multiplicities if some $P_i = P_j$ for some $i \neq j$). But, by hypothesis and because of Lemma 7, the degree of P_i is equal to k, so each block $C(P_i)$ appears once (again counted with multiplicity). This then corresponds to the canonical representation of B: $\min(B)$ is therefore the least common multiple of the minimal polynomials of the blocks, which is equal to the product of the *distinct* P_i.

(ii) $\implies$ **(i)** Conversely, by Lemma 6, any A such that $\min(A)$ is primitive and has degree k is similar to the multiplication by α where α is a generator of $\mathbb{F}_{2^k}^*$. This defines a mapping π_1. Moreover, any B such that $\min(B)$ is a product of distinct irreducible polynomials of degree k has a canonical representation of the form:

$$\mathrm{diag}(C(P_1), C(P_2), \ldots, C(P_\ell)),$$

where each P_i is an irreducible divisor of $\min(B)$. Each divisor must appear once, but some can appear several times. Therefore B is similar (for a mapping π_2) to the function $\mathrm{diag}(M_{\beta_1,k}, \ldots, M_{\beta_\ell,k})$ where each β_i is a root of P_i in $\mathbb{F}_{2^k}$. Moreover, since α is a generator of $\mathbb{F}_{2^k}^*$, any β_i can be written as α^{d_i}. This proves that $\pi_2 F \pi_1^{-1}$ is a projective mapping of exponents $(d_1, \ldots, d_\ell)$. Since P_i has degree k, k is the order of 2 modulo $\frac{(2^k-1)}{\gcd(d_i, 2^k-1)}$ by Lemma 7.

□

When $(2^k - 1)$ is a prime number, we obtain a simpler characterization of ℓ-variate projective mappings with respect to $\mathbb{F}_{2^k}$, without any restriction on the exponents $d_1, \ldots, d_\ell$. We use that the cycle structure of a linear mapping can be derived from its canonical form, as illustrated by the following lemma.

Lemma 8. *Let $A\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an $\mathbb{F}_2$-linear mapping. Then, the following properties are equivalent:*

(i) *The cycles of A, $\sigma_A(x_0) = (x_0, Ax_0, A^2x_0, \ldots)$, have the same length for all nonzero $x_0 \in \mathbb{F}_2^n$.*

(ii) *The minimal polynomial of A is a product of distinct irreducible polynomials of the same order.*

(iii) *A has $\mathrm{diag}(C(P_1), C(P_2), \ldots, C(P_\ell))$ as canonical form where all P_i are irreducible polynomials having the same order.*

Proof. The equivalence between (ii) and (iii) is a direct consequence of the canonical form (Proposition 4).

(i) $\implies$ **(ii)** It is well-known that, for any divisor Q of the minimal polynomial of A, there exists some $x_0 \neq 0$ such that Q is the minimal polynomial of the sequence $\sigma_A(x_0)$. We use that the period of a sequence $\sigma_A(x_0)$ with minimal polynomial $Q = P^2$ with P irreducible is $2 \times \mathrm{ord}(P)$, while the period of a sequence $\sigma_A(x_1)$ with minimal polynomial P is $\mathrm{ord}(P)$, e.g. [LN96, Theorem 8.63]. We then deduce that, if all $\sigma_A(x), x \neq 0$ have the same period, then all divisors of the minimal polynomial of A are square-free. Moreover, if the minimal polynomial of A has two irreducible divisors P_1 and P_2, then there exist x_1 and x_2 such that $\sigma_A(x_1)$ has period $\mathrm{ord}(P_1)$ and $\sigma_A(x_2)$ has period $\mathrm{ord}(P_2)$. It follows that all irreducible factors of the minimal polynomial of A have the same order.

(iii) $\implies$ **(i)** Because $P_1, \ldots, P_\ell$ are irreducible of same order, they are of the same degree k by Lemma 7, and $\mathbb{F}_{2^k}$ is a splitting field for all of them. By hypothesis A is similar to $M = \mathrm{diag}(M_{\alpha_1,k}, \ldots, M_{\alpha_\ell,k})$, where α_i is a root of P_i. The mappings A

and M share the same cycle type. But because each $M_{\alpha_i,k}$ acts independently from the others, we get that:

$$|\sigma_M(x_1,\dots,x_\ell)| = \operatorname{lcm}\left(\left|\sigma_{M_{\alpha_1}}(x_1)\right|,\dots,\left|\sigma_{M_{\alpha_\ell}}(x_\ell)\right|\right).$$

But for any $x, y \in \mathbb{F}_{2^k}^*$ and i, j, we get that:

$$\left|\sigma_{M_{\alpha_i}}(x)\right| = \operatorname{ord}(\alpha_i) = \operatorname{ord}(\alpha_j) = \left|\sigma_{M_{\alpha_j}}(y)\right|.$$

Therefore, whenever $(x_1,\dots,x_\ell) \neq (0,\dots,0)$, its order is the common order of the elements α_i.

□

As a consequence, we can characterize the matrices having a prime order by their minimal polynomials. These matrices play an important role: as shown in [BBL21, BL22], the classification of linearly self-equivalent functions can be reduced to the classification of functions having an automorphism in $\mathrm{Aut}_{\mathrm{LE}}$ with a prime order. It can then be checked from their Frobenius normal forms that all matrices considered in [BBL21, BL22] have a minimal polynomial of the form described in the following proposition.

Proposition 6. *Let A be an $n \times n$-invertible matrix. Then* $\operatorname{ord}(A)$ *is an odd prime if and only if the minimal polynomial of A is of the form $(X+1)P_1(X)\dots P_\ell(X)$ or $P_1(X)\dots P_\ell(X)$ where all P_i are distinct irreducible polynomials of the same prime order $p > 2$.*

Proof. $\Longrightarrow$ If $\operatorname{ord}(A)$ is a prime p, then all cycles of A have length 1 or p. Let k' denote the dimension of the linear space composed of all fixed points of A. If $k' = 0$, then all cycles $\sigma_A(x), x \neq 0$ have the same length, implying from Lemma 8, that the minimal polynomial of A is a product of distinct irreducible polynomials with the same order. Assume now that $k' > 0$. Since $\operatorname{ord}(A)$ is odd, the minimal polynomial of A is not divisible by $(X+1)^2$. Then, A is similar to $A' = \operatorname{diag}(\mathrm{Id}_{k'}, C)$ where C is an $(n-k') \times (n-k')$-matrix. By observing that, for any i, $(A')^i$ is similar to $\operatorname{diag}(\mathrm{Id}_{k'}, C^i)$, we deduce that C has no nonzero fixed points and that all cycles $\sigma_C(y_0)$ for $y_0 \neq 0$ have the same length p. We deduce from Lemma 8 that the minimal polynomial of C can be written as the product of distinct irreducible polynomials of order $p > 2$, or equivalently that the minimal polynomial of A has the form $(X+1)P_1(X)\dots P_\ell(X)$ where all P_i are distinct irreducible polynomials of order p.

$\Longleftarrow$ We only have to consider the case where the minimal polynomial of A is of the form $(X+1)P_1(X)\dots P_\ell(X)$ where all P_i are distinct irreducible polynomials of order $p > 2$, since the other case is a direct consequence of Lemma 8. The canonical form of A is then $\operatorname{diag}(\mathrm{Id}_{k'}, C(P_{i_1}), \dots, C(P_{i_s}))$ where the set $\{P_{i_j}, 1 \leq j \leq s\}$ coincides with $\{P_1,\dots,P_\ell\}$ with some (possible) multiplicities. Because all P_i are irreducible and coprime with $(X+1)$, the order of A is equal to the least common multiple of the orders of all irreducible factors of $\min(A)$, which is equal to $p > 2$.

□

Theorem 5. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $k > 1$ be a divisor of n such that $(2^k - 1)$ is a prime. Assume that the span of* $\mathrm{Im}(F)$ *has dimension n. Then, the following properties are equivalent:*

(i) *F belongs to the linear-equivalence class of an ℓ-variate projective mapping with respect to $\mathbb{F}_{2^k}$.*

(ii) *There exists* $\mathrm{diag}(A, B) \in \mathrm{Aut}_{\mathrm{LE}}(F)$ *such that* $\min(A)$ *is a primitive polynomial of degree* k.

Proof. **(i)** $\Longrightarrow$ **(ii)** The proof is similar to the same result in Theorem 4. Indeed, the hypothesis on the orders d_i in Theorem 4 was used only to prove the statement about the minimal polynomial of B.

(ii) $\Longrightarrow$ **(i)** Since there exists $\mathrm{diag}(A, B) \in \mathrm{Aut}_{\mathrm{LE}}(F)$ with $\mathrm{ord}(A) = 2^k - 1$, the order of the subgroup of $\mathrm{Aut}_{\mathrm{LE}}(F)$ generated by $\mathrm{diag}(A, B)$ is a multiple of $(2^k - 1)$. Therefore, there exists $\mathrm{diag}(A', B')$ in this subgroup of order $(2^k - 1)$. It follows that $\mathrm{lcm}(\mathrm{ord}(A'), \mathrm{ord}(B')) = 2^k - 1$ which is a prime. We deduce that either $\mathrm{ord}(A') = \mathrm{ord}(B') = 2^k - 1$, or exactly one matrix among A' and B' has order 1.

If $A' = \mathrm{Id}_n$, then $B' \circ F(x) = F(x)$ for all $x \in \mathbb{F}_{2^n}$. It follows that $\mathrm{Im}(F)$ is a subset of the set of fixed points of B', which is a vector space of dimension at most $(n-1)$ since $B' \neq \mathrm{Id}_n$. This situation is excluded by the hypotheses. If $B' = \mathrm{Id}_n$, then $F \circ A'(x) = F(x)$ where A' is a power of A. Since $\min(A)$ is a primitive polynomial of degree k, there exists an isomorphism $\pi : \mathbb{F}_{2^k}^{\ell} \to \mathbb{F}_2^n$, $n = k\ell$, such that $A = \pi \circ M_{\alpha,n} \circ \pi^{-1}$. Because $(2^k - 1)$ is a prime, α^s, for any $s < 2^k - 1$, is a primitive element of $\mathbb{F}_{2^k}$ too. This implies that $(\pi^{-1} \circ F \circ \pi) M_{\alpha^s} = (\pi^{-1} \circ F \circ \pi)$, i.e., $\pi^{-1} \circ F \circ \pi$ is an ℓ-variate projective mapping of orders $(0, 0, \ldots, 0)$ with respect to $\mathbb{F}_{2^k}$. Therefore, F belongs to the linear-equivalence class of an ℓ-variate projective mapping with respect to $\mathbb{F}_{2^k}$. More precisely, it is in the linear class of a cyclotomic mapping of exponent 0.

If $\mathrm{ord}(B') = 2^k - 1$ and $2^k - 1$ is an odd prime, then all cycles of B' have length 1 or $(2^k - 1)$. It follows from Proposition 6 that B' is similar to $B'' = \mathrm{diag}(\mathrm{Id}_{sk}, C(P_1), C(P_2), \ldots, C(P_{\ell-s}))$ where all P_i are irreducible polynomials of the same order, and therefore of the same degree k. Then, there is a function F' linearly equivalent to F such that $B'' \circ F' \circ A'' = F'$ where $A'' = \mathrm{diag}(C(P), \ldots, C(P))$ and P a primitive polynomial of degree k. This implies that there exists an isomorphism $\pi : \mathbb{F}_{2^k}^{\ell} \to \mathbb{F}_2^n$ such that $\pi \circ F' \circ \pi^{-1}$ is an ℓ-variate projective mapping of orders $(d_1, \ldots, d_\ell)$ with respect to $\mathbb{F}_{2^k}$ where the first s orders are zero and the other ones are determined by the roots of P_i, $1 \leq i \leq \ell - s$.

□

Just as in the case of Theorem 3, Theorem 5 enables us to determine the nature of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, from the nature of its LE automorphisms. Note that the condition on the dimension of $\langle \mathrm{Im}(F) \rangle$ is always satisfied by APN functions when $n > 2$.

Lemma 9 (Dimension of $\langle \mathrm{Im}(F) \rangle$ for APN functions)**.** *Let* $n > 2$ *and let* $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *be an APN function. Then* $\dim(\langle \mathrm{Im}(F) \rangle) = n$.

Proof. Let us suppose that $\dim(\langle \mathrm{Im}(F) \rangle) \leq n-1$. In that case, and up to linear equivalence, F can be seen as a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n-1}$. Because F is APN, for any $\Delta^{\mathrm{in}} \in \mathbb{F}_2^n, \Delta^{\mathrm{out}} \in \mathbb{F}_2^{n-1}$, the equation $F(x + \Delta^{\mathrm{in}}) + F(x) = \Delta^{\mathrm{out}}$ must have 0 or 2 solutions x. A pigeonhole argument proves that this number is equal to 2 for all $(\Delta^{\mathrm{in}}, \Delta^{\mathrm{out}})$. Therefore, F is perfect non-linear, because $2 = 2^{n-(n-1)}$. However, such functions exist only when the dimension of the input space is at least twice larger than the dimension of the input space [Nyb91]. In our case, this implies that $2(n-1) \leq n$, which is excluded because $n > 2$. □

Example 8 (Classes 51 & 55 of [BL22])**.** Classes 51 & 55 correspond to classes of linearly self-equivalent APN mappings over $\mathbb{F}_{2^8}$ presented in [BL22]. The functions in these classes satisfy $B \circ F \circ A = F$ for some (A, B) where A is the multiplication by an element α of order 3. By Lemma 6, the minimal polynomial of A is the minimal polynomial of α, *i.e.* $X^2 + X + 1$, which is of degree 2. Because $2^2 - 1 = 3$ is prime, Theorem 5 states that F

is linearly equivalent to a 4-variate projective mapping with respect to $\mathbb{F}_4$. For Class 51, the Frobenius form of B, which is given in [BL22], is $\mathrm{diag}(\mathrm{Id}_2,\ C(X^3+1),\ C(X^3+1))$. By Proposition 4, the canonical form of $C(X^3+1)$ is $\mathrm{diag}(C(X+1),\ C(X^2+X+1))$, because all irreducible divisors must appear at highest multiplicity, which is here equal to 1. Because $C(X+1)$ is the 1×1 matrix equal to 1, B is therefore similar to:

$$\mathrm{diag}(\mathrm{Id}_2,\ \mathrm{Id}_2,\ C(X^2+X+1),\ C(X^2+X+1)).$$

This matrix is a canonical form, and by uniqueness, the one of B. Class 51 then corresponds to 4-variate projective mappings of exponent $(0,0,1,1)$ with respect to $\mathbb{F}_4$. Similarly, Class 55 corresponds to 4-variate projective mappings of exponents $(0,0,0,1)$ with respect to $\mathbb{F}_4$.

The previous examples are (for now) sporadic examples of 4-variate APN functions. A thorough analysis of the examples coming from computational approaches such as the ones presented in [BL08, BBL21, BL22, YWL14, YP22] is left as future work. In the following, we focus on the infinite families of APN functions.

4 Linear self-equivalence among known infinite families of APN functions

4.1 Main theorem

Since we have established the relationships between the different properties considered when constructing APN functions, we can now analyse most of the infinite families of quadratic APN functions in light of the structure of their LE-automorphism groups. Most notably, while these families have been introduced with different representations (univariate or multivariate), our framework provides a unified view of these mappings which looked of very different natures at first glance. The polynomial forms of the families are presented in Tables 1 to 3. The constraints on their parameters are given in Appendix A. We prove the following theorem.

Theorem 6 (Infinite APN families and linear self-equivalence)**.** *Let us consider the 19 infinite APN families listed in Tables 1 and 2. Then:*

(i) *They all contain in their linear-equivalence classes a linearly self-equivalent representative.*

(ii) *More precisely, except for Families (BCL09a/b/c) when n is odd, each family contains a cyclotomic, or a 2, 3 or 4-variate projective mapping in its linear-equivalence class.*

(iii) *When n is odd, any function of (BCL09a/b/c) is linearly-equivalent to a function which commutes with the Frobenius automorphism $x\mapsto x^2$.*

Finally, all (APN) power mappings are cyclotomic and commute with the Frobenius automorphism.

A lot of subcases were already pointed out in several previous papers such as [Car11, BBL21, CBC21, Göl22, GK21, BIK23, KKK23]. In particular, and to the best of our knowledge, Carlet first pointed out in [Car11, Theorem 1] the relevance of studying functions of the form:

$$\begin{aligned} F(x,y) &= \left(xy, a_1x^{2^i+2^j}+b_1x^{2^i}y^{2^j}+c_1x^{2^j}y^{2^i}+d_1y^{2^i+2^j}\right)\\ &= \left(xy, (a_2x^{2^{j-i}+1}+b_2xy^{2^{j-i}}+c_2x^{2^{j-i}}y+d_2y^{2^{j-i}+1})^{2^i}\right), \end{aligned} \tag{4}$$

ID	Functions	Observations	References
(BCL08a)	$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$	cyclotomic	[BCL08, BCFL06]
(BCL08b)	$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$	cyclotomic	[BCL08, BCL06]
(BCV20)	$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}$	$\sim_{\text{lin}}$ biprojective	[BBMM08, BC08, BCV20]
(BCL09a)	$x^3 + a^{-1}\text{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$	cyclotomic/($\sim_{\text{lin}}$) frob.	[BCL09a]
(BCL09b)	$x^3 + a^{-1}\text{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9 + a^6x^{18})$	cyclotomic/($\sim_{\text{lin}}$) frob.	[BCL09b]
(BCL09c)	$x^3 + a^{-1}\text{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$	cyclotomic/($\sim_{\text{lin}}$) frob.	[BCL09b]
(BBMM11)	$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$	cyclotomic	[BBMM11]
(BCCCV20)	$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$	cyclotomic	[BCC+20]
(BHK20)	$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$	$\sim_{\text{lin}}$ biprojective	[BHK20]
(ZKLPT22)	$a\text{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\text{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$	$\sim_{\text{lin}}$ biprojective	[ZKL+22]

"frob." refers to commutation with the Frobenius automorphism $x \mapsto x^2$.

Table 1: Known infinite families of univariate quadratic APN functions over $\mathbb{F}_{2^n}$. The Gold mappings are omitted.

ID	Functions	Observations	References
(ZP13)	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$	$\sim_{\text{lin}}$ biprojective	[ZP13]
(T19)	$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$	$\sim_{\text{lin}}$ biprojective	[Tan19]
(CBC21)	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^{s+k/2}}y^{2^{k/2}} + axy^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$	$\sim_{\text{lin}}$ 4-projective	[CBC21]
(G22a)	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{2s}+1} + x^{2^{2s}}y + y^{2^{2s}+1} \end{pmatrix}$	biprojective	[Göl22]
(G22b)	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{3s}}y + xy^{2^{3s}} \end{pmatrix}$	biprojective	[Göl22]
(GK21)	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$	biprojective	[GK21]
(CLV22a)	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + ay^{2^s+1} \\ x^{2^{2s}+1} + ax^{2^{2s}}y + (1+a)^{2^s}xy^{2^{2s}} + ay^{2^{2s}+1} \end{pmatrix}$	biprojective	[CLV22]
(LK23a)	$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^s}z + yz^{2^s} \\ x^{2^s}z + y^{2^s+1} \\ xy^{2^s} + y^{2^s}z + z^{2^s+1} \end{pmatrix}$	3-projective $\sim_{\text{lin}}$ cyclotomic	[LK23]
(LK23b)	$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + yz^{2^s} \\ xy^{2^s} + z^{2^s+1} \\ x^{2^s}z + y^{2^s+1} + y^{2^s}z \end{pmatrix}$	3-projective $\sim_{\text{lin}}$ cyclotomic	[LK23]

Table 2: Known infinite families of bivariate or trivariate quadratic APN functions over $\mathbb{F}_{2^n}$

that is, functions that are linearly equivalent to a $(2, 2^{j-i})$-projective mapping. Carlet also proved in [Car11, Section 4.2.1] that previously known infinite families, namely the ones given in [BBMM08, BC08], and that are today included in the (BCV20) family [BCV20], fall within this category. As pointed out by Example 3, the works [GK21, BIK23] present proofs of cyclotomy of exponent 0 with respect to $\mathbb{F}_4$ for a lot of these families. In the following, we generalize them into cyclotomy or (bi-)projectiveness proofs over larger groups. Unlike these works however, we make (almost) no distinction between even or odd values for n.

We believe that such a general observation deserves to be in the spotlight. We therefore prove all the cases and give credit to authors of previous works (that we know of) in the proof. The proof is postponed to the following section. We first present a few observations about this result.

Remark 4. Theorem 6 mentions representatives in the linear equivalence classes, but all the representatives presented in the proof actually lie in an $\mathbb{F}_{2^k}$-linear equivalence class with $k > 1$. Furthermore, this is not an exhaustive result, and some functions of these families have linearly self-equivalent representatives of several types. Examples of this situation are presented in Remark 5.

The following informal corollary of Theorem 6 raises many open questions.

Corollary 1 ((Informal) Infinite APN families and linear self-equivalence)**.** *Almost all infinite families of APN functions have linearly self-equivalent representatives in their linear-equivalence class, whose LE-automorphism group contains* (A, B) *where* A, B *are either* $\mathbb{F}_{2^k}$*-linear with* $k > 1$ *with very particular minimal polynomials characterized in Theorem 4, or where both* A *and* B *coincide with the Frobenius automorphism.*

This observation is rather surprising. Indeed, from theoretical arguments, what we (for now) know is that any quadratic function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is always EA self-equivalent, see e.g. [BBMN11, Proposition 1], and even *extended-linear* self-equivalent if $F(0) = 0$, see e.g [KZ21, Proposition 2.2]. But this does not *a priori* imply the existence of a linearly self-equivalent mapping in their linear-equivalence class.

Problem 1. *Does the property described in Corollary 1 hold for the three families in Table 3? For the sporadic APN functions such as those in [BL08, BBL21, BL22, YWL14, YP22]?*

We show for instance in Example 10 below, that the Brickmann-Leander-Edel-Pott [BL08, EP09] cubic for $n = 6$ cannot be represented as a cyclotomic mapping nor as an ℓ-variate projective mapping. More generally, and in line with [BBL21, Conjecture 1], we raise the following open problem.

Problem 2. *Does the CCZ-equivalence class of any APN function contain a linearly self-equivalent mapping?*

Theorem 6 then unifies (almost) all the research directions followed to search for infinite APN families. Answering the question raised in Problem 2 would enable us to understand whether these directions are direct generalizations extrapolated from the monomial case, or whether they correspond to an inherent property of APN mappings. The specific cases highlighted in Problem 1 could help address this problem or give some clues toward a definite answer.

4.2 Proof of Theorem 6

This section proves Theorem 6. We proceed case by case and start with the most obvious ones.

Table 3: Remaining infinite families to classify.

ID	Functions	Obs.	Ref.
(CLV22b)	$(x,y) \mapsto \begin{pmatrix} x^3+xy+xy^2+ay^3 \\ x^5+xy+ax^2y^2+ax^4y+(1+a)^2xy^4+ay^5 \end{pmatrix}$	?	[CLV22]
(LZLQ22b)	$(x,y) \mapsto \begin{pmatrix} x^3+xy^2+y^3+xy \\ x^5+x^4y+y^5+xy+x^2y^2 \end{pmatrix}$	?	[LZLQ22]
(LZLQ22a)	$L(x)^{2^k+1}+bx^{2^k+1}$	?	[LZLQ22]

Power mapping. A power mapping is a cyclotomic mapping of exponent d with respect to $\mathbb{F}_{2^n}$ and it obviously commutes with $x \mapsto x^2$.

Multivariate Families. Among the bivariate and trivariate families given in Table 2, we directly observe from their polynomial forms that:

- (G22a) is $(2^s+1,\ 2^{2s}+1)$-projective,
- (G22b) is $(2^s+1,\ 2^{3s}+1)$-projective,
- (GK21) is $(2^s+1,\ 2^{2+\frac{k}{2}}+1)$-projective,
- (CLV22a) is $(2^s+1,\ 2^{2s}+1)$-projective,
- (LK23a) and (LK23b) are $(2^s+1,\ 2^s+1,\ 2^s+1)$-projective,

all of them being ℓ-variate projective mappings by construction. Note that Theorem 1 shows that (LK23a) and (LK23b) have a representative which is a cyclotomic mapping of exponent 2^s+1 with respect to $\mathbb{F}_{2^k}$ in their linear-equivalence class. Furthermore, the families (ZP13), (T19) and the polynomials defined by Eq. (4) and introduced by Carlet have been proven linearly-equivalent to biprojective mappings by Göloğlu [Göl22]. More precisely:

- for (ZP13), using the ($\mathbb{F}_{2^k}$-linear) mapping $L\colon (x,y) \mapsto (x, y^{2^{k-i}})$, we find a linear-equivalent function $F \circ L$ which is a $(2^s+1,\ 2^{k-i}+1)$-projective mapping,
- for (T19), using the ($\mathbb{F}_{2^k}$-linear) mapping $L\colon (x,y) \mapsto (x^{2^{k-2s}}, y)$, we find a linear-equivalent function $F \circ L$ which is a $(2^s+1,\ 2^{k-2s}+1)$-projective mapping,
- for the polynomials of Eq. (4), using the ($\mathbb{F}_{2^k}$-linear) mapping $L\colon (x,y) \mapsto (x,\ y^{2^k-i})$, we find a linear-equivalent function $L \circ F$ which is a $(2,\ 2^{i-j}+1)$-projective mapping.

(CBC21). As we can observe the first coordinate of this mapping has monomials of degree d where $d \equiv 2^s+1 \bmod 2^{\frac{k}{2}}-1$, but not modulo 2^k-1. When substituting each monomial with $x \leftarrow a+\zeta b$, $y \leftarrow c+\zeta d$, with $\zeta \in \mathbb{F}_{2^k} \setminus \mathbb{F}_{2^{k/2}}$, and $a,b,c,d \in \mathbb{F}_{2^{k/2}}$, we observe that the obtained monomials in a,b,c,d are all of degree 2^s+1, because $a^{2^{k/2}} = a$ and the same holds for b,c,d. The same holds for the second coordinate. Therefore, the functions of (CBC21) are linearly equivalent to $(2^s+1,\ 2^s+1,\ 2,\ 2)$-projective mappings.

Let us now focus on the univariate families.

(BCL09a/b/c). First of all the families (BCL09a), (BCL09b) (BCL09c) were for instance identified as canonical triplicates when n is even in [BIK23], and their image set was studied in [KKK23]. When n is even, they correspond to cyclotomic mappings. More precisely:

- when n is even, (BCL09a), (BCL09b), (BCL09c) are made of cyclotomic mappings of exponent 0 with respect to $\mathbb{F}_4$, because they can be written as $P(x^3)$,
- when n is odd, it is observed in the original paper [BCL09b, Section II.B] that, when a takes different values, all the obtained functions within a fixed family (BCL09a), (BCL09b) or (BCL09c) are linearly-equivalent. We can actually focus on the case $a = 1$, by using $x \mapsto a^{\frac{1}{3}}x$ as a change of variables. In that case, the corresponding function has all its coefficients in $\mathbb{F}_2$, and therefore commutes with the Frobenius automorphism.

(BCL08a/b). Non-trivial linear self-equivalences were identified for Families (BCL08a) and (BCL08b) in [BBL21, Examples 2 & 3]. They can be reinterpreted as proofs of cyclotomy. Indeed, let us look at the difference between both exponents modulo $2^k - 1$. We observe that:

$$(2^{(3-i)k+s} + 2^{ik}) - (2^s + 1) \equiv 2^s + 1 - 2^s - 1 \equiv 0 \bmod 2^k - 1.$$

From Theorem 1, Family (BCL08a) is a family of cyclotomic mappings of exponent $2^s + 1$ with respect to $\mathbb{F}_{2^k}$, where $n = 3k$. Similarly, we obtain:

$$(2^{(4-i)k+s} + 2^{ik}) - (2^s + 1) \equiv 2^s + 1 - 2^s - 1 \equiv 0 \bmod 2^k - 1.$$

Therefore, Family (BCL08b) is a family of cyclotomic mappings of exponent $2^s + 1$ with respect to $\mathbb{F}_{2^k}$, where $n = 4k$.

(BCCCV20) & (BBMM11). If we look at Family (BCCCV20), we observe that the monomials appearing in the polynomials are:

$$x^{2^{2k+1}+1},\ x^{2^{k+1}+1},\ x^{2^{2k}+2},\ x^{2^k+2},\ \text{and } x^3\ ,$$

so thatthat its exponents are all equal to 3 modulo $2^k - 1$. This implies that the family consists exclusively of cyclotomic mappings of exponent 3 with respect to $\mathbb{F}_{2^k}$, where $n = 3k$. Regarding Family (BBMM11), the same applies, but we need to take into account some of the constraints on the parameters. Since $n = 3k$, we can look at cyclotomy with respect to $\mathbb{F}_{2^3}$. First, we reduce all the exponents modulo $2^3 - 1$ and obtain in that case: $2^s + 1,\ 2^{2k} + 1,\ 2^{2k} + 1,\ 2^s + 1$ because $k + s \equiv 0 \bmod 3$ by construction. Furthermore, again by construction, we have that $\gcd(3, k) = 1$, which implies $k \not\equiv 0 \bmod 3$. From these two constraints, we deduce that either $k \equiv 1$ and $s \equiv 2$, or, $k \equiv 2$ and $s \equiv 1$. In any case, it holds that $s \equiv 2k \bmod 3$. This proves that all exponents are equal modulo $2^3 - 1$, and the family then consists of cyclotomic mappings of exponent $2^{s'} + 1 \in \{3, 5\}$ with respect to $\mathbb{F}_{2^3}$ where s' is the remainder of s modulo 3.

(ZKLPT22). This family lies among bivariate families as well. Indeed, by definition, $a \notin \mathbb{F}_{2^k}^*$ (see Table 8), so (a, a^{2^k}) is an $\mathbb{F}_{2^k}$-basis of $\mathbb{F}_{2^n}$ where $n = 2k$. We observe that for any $\varphi \in \mathbb{F}_{2^k}, x \in \mathbb{F}_{2^n}$, we then have:

$$\begin{aligned} F(\varphi x) &= a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}\left(b(\varphi x)^{2^i+1}\right) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}\left(c(\varphi x)^{2^s+1}\right) \\ &= a\varphi^{2^i+1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}\left(bx^{2^i+1}\right) + a^{2^k}\varphi^{2^s+1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}\left(cx^{2^s+1}\right), \end{aligned}$$

because $\varphi^{2^i+1}, \varphi^{2^s+1} \in \mathbb{F}_{2^k}$. It is then linearly equivalent to a $(2^i + 1,\ 2^s + 1)$-projective mapping.

(BCV20). Let F be the function defined by $F(x) = ax^{2^k+1}+x^{2^s+1}+x^{2^{s+k}+2^k}+bx^{2^{k+s}+1}+b^{2^k}x^{2^s+2^k}$ where $n = 2k$ for some $k \geq 1$. Let $\alpha \in \mathbb{F}_{2^n}$ be a primitive element, and let us consider the $\mathbb{F}_{2^k}$-basis $(1, \alpha)$ and its dual basis (β_1, β_α) which satisfies:

$$\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_1 \cdot 1) = 1, \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_1 \cdot \alpha) = 0, \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_\alpha \cdot 1) = 0, \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_\alpha \cdot \alpha) = 1.$$

In particular, we observe that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_\alpha) = 0$, in other words, it holds that $\beta_\alpha = \beta_\alpha^{2^k}$, or stated otherwise that $\beta_\alpha \in \mathbb{F}_{2^k}$. Let $\gamma \in \mathbb{F}_{2^n}$, and let us focus on $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\gamma F)$. Let $x \in \mathbb{F}_{2^n}$. Then it holds that:

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\gamma F(x)) =& \gamma(ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}) + \\ & \gamma^{2^k}(ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k})^{2^k} \\ =& \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\gamma a)x^{2^k+1} + \lambda x^{2^s+1} + \lambda x^{2^{s+k}+2^k} + b\lambda x^{2^{s+k}+1} + b^{2^k}\lambda x^{2^s+2^k},\end{aligned}$$

where $\lambda = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\gamma)$. This simply comes from the fact that $x^{2^{2k}} = x$. We can therefore express the two coordinates of F with respect to the $\mathbb{F}_{2^k}$-basis $(1, \alpha)$ as :

$$\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_1 F(x)) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_1 a)x^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{s+k}+1} + b^{2^k}x^{2^s+2^k},$$

because $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_1) = 1$, but also:

$$\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_\alpha F(x)) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_\alpha a)x^{2^k+1},$$

because $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_\alpha) = 0$. Let us introduce the linear bijection $L\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ that is defined by:

$$\forall x, y \in \mathbb{F}, \quad L(x + \alpha y) = \left(x + \frac{\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_1 a)}{\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_\alpha a)} y\right) + \alpha y.$$

By construction, $a \notin \mathbb{F}_{2^k}$ (see Table 7), but as $\beta_\alpha \in \mathbb{F}_{2^k}$, we deduce that $\beta_\alpha a \notin \mathbb{F}_{2^k}$, and therefore $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_\alpha a) \neq 0$, so that L is well-defined. We then observe that:

$$\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_1 \cdot L \circ F(x)) = x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{s+k}+1} + b^{2^k}x^{2^s+2^k}, \text{and}$$

$$\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_\alpha \cdot L \circ F(x)) = \beta_\alpha \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(a)x^{2^k+1}.$$

In particular, the bivariate terms that can appear in the 1-coordinate of $L \circ F$ are terms of degree $2^s + 1$ because all exponents e of its univariate monomials satisfy $e \equiv 2^s + 1 \bmod 2^k - 1$. Similarly, the bivariate terms that can appear in the α-coordinate are terms of degree 2. Therefore $L \circ F$ is a $(2^s + 1, 2)$ biprojective APN function.

(BHK20). Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be defined by $F(x) = x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$ where $n = 2k$ for some $k \geq 1$. We proceed in a manner similar to the previous proof, except that we use the fact that a is by definition an element of order 3, so $a^2 = a^{-1}$, and also that k is odd, see Table 8. Let $\gamma \in \mathbb{F}_{2^n}$, $x \in \mathbb{F}_{2^n}$. Then it holds that:

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\gamma F(x)) &= \gamma(x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}) + \\ &\quad \gamma^{2^k}(x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}})^{2^k} \\ &= (\gamma + \gamma^{2^k}a)x^3 + (\gamma a + \gamma^{2^k})x^{2^{s+i}+2^i} + \\ &\quad (\gamma a^{-1} + \gamma^{2^k})x^{2^{k+1}+2^k} + (\gamma + \gamma^{2^k}a^{-1})x^{2^{s+i+k}+2^{i+k}} \\ &= (\gamma + \gamma^{2^k}a)(x^3 + a^{-1}x^{2^{k+1}+2^k}) + \\ &\quad (\gamma a + \gamma^{2^k})(x^{2^{s+i}+2^i} + a^{-1}x^{2^{s+i+k}+2^{i+k}})\end{aligned}$$

In particular, the terms x^3 and $x^{2^{k+1}+2^k}$ appear if and only if $\gamma + \gamma^{2^k} a \neq 0$. Stated otherwise, if $\gamma \neq 0$, both terms do not appear if and only if $\gamma^{2^k-1} = a^{-1}$, *i.e.* if and only if γ is a (2^k-1)-th root of a^{-1}. Such a root exists. Indeed, if β is a primitive element of $\mathbb{F}_{2^n}^*$, then $\beta^{\frac{2^n-1}{3}}$ is a generator of $\mathbb{F}_{2^2}^*$ and it can be rewritten as $\beta^{\frac{2^n-1}{3}} = (\beta^{\frac{2^k+1}{3}})^{2^k-1}$. In particular, because k is odd, $\frac{2^k+1}{3}$ is an integer, so this precisely states that $\beta^{\frac{2^k+1}{3}}$ or $(\beta^{\frac{2^k+1}{3}})^2$ is a (2^k-1)-th root of a^{-1}. Similarly, the terms $x^{2^{s+i}+2^i}$ and $x^{2^{s+i+k}+2^{i+k}}$ do not appear in $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\gamma F)$ if and only if γ is a (2^k-1)-th root of a. Finally, $(\beta^{\frac{2^k+1}{3}}, \beta^{\frac{2(2^k+1)}{3}})$ is an $\mathbb{F}_{2^k}$-basis of $\mathbb{F}_{2^n}$, because $\frac{\beta^{\frac{2(2^k+1)}{3}}}{\beta^{\frac{2^k+1}{3}}} = \beta^{\frac{2^k+1}{3}} \notin \mathbb{F}_{2^k}$. In this basis, the coordinates are homogeneous of exponent 3 and $2^i(2^s+1)$ respectively, because the monomials in each coordinate are of degree equal to 3 and $2^i(2^s+1)$ modulo 2^k-1.

This concludes our proof. □

Remark 5. As already mentioned, some functions in these classes have multiple linearly self-equivalent representatives of different natures. For example, a single function can be at the same time linearly-equivalent to a cyclotomic mapping, but also to a function which commutes with the Frobenius automorphism. It can also happen that a single representative has two types of linear self-equivalence. For instance as mentioned in [BCL09b, Section II.B], when n is even Family (BCL09a) can be split into two distinct linear classes. Indeed all functions are either linearly-equivalent to the function with $a = 1$, or to the one where a is a fixed primitive element of $\mathbb{F}_{2^n}$. In the first case, the representative with $a = 1$ is cyclotomic, but it also commutes with the Frobenius automorphism, because[3] its coefficients are in $\mathbb{F}_2$. The same also holds when n is even for Families (BCL09b), (BCL09c).

Another example can be derived from (BBMM11). We showed that this class is composed of cyclotomic mappings of exponent 3 or 5 with respect to $\mathbb{F}_{2^3}$. However, if $b = c = 0$, then only two terms remain and their exponents are both equal to 2^s+1 modulo 2^k-1. These specific functions are therefore cyclotomic with respect to $\mathbb{F}_{2^3}$, but also with respect to $\mathbb{F}_{2^k}$.

Finally, for Family (BCV20), on top of the biprojective property, according to the results reported in [BIK23, Section 7], the functions were computationally proven linearly-equivalent to cyclotomic mappings of exponent 0 with respect to $\mathbb{F}_4$, up to dimension 12.

5 Properties of mappings having a linearly self-equivalent representative

In the previous section, we pointed out the importance of linear self-equivalence, especially for the study of APN functions. We highlight in this section some properties which are consequences of the existence of a linearly self-equivalent mapping within the linear-equivalence class of a function. We first present how the symmetries inherent to this pattern can be captured by other means than the polynomial representation.

5.1 Image set and Walsh spectrum of linearly self-equivalent mappings

If a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is linearly self-equivalent, then its image set is very constrained. For instance, some properties of F can be derived from the cycle structures of the involved linear mappings. A first trivial property is the following one.

Proposition 7. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $\mathrm{diag}(A, B) \in \mathrm{Aut}_{\mathrm{LE}}(F)$. Then, the image set of F can be partitioned into cycles of B. Most notably, the image set of F is invariant under B.*

[3] The functions commuting with $x \mapsto x^2$ are precisely the functions whose coefficients are in $\mathbb{F}_2$. Note that APN functions of this specific form are classified up to dimension 9 in [YKBL20].

Proof. It holds that: $F(\mathbb{F}_2^n) = B \circ F \circ A^{-1}(\mathbb{F}_2^n) = B(F(\mathbb{F}_2^n))$, so $F(\mathbb{F}_2^n)$ is invariant under B. This precisely states that $F(\mathbb{F}_2^n)$ is a disjoint union of cycles of B. □

This result does not bring any new information in the case where F is bijective, but is helpful when F is not bijective, which is the case of most known APN functions. In the following, we highlight how linear self-equivalence can be captured as a property of the *Walsh transform* of the function F.

Definition 14 (Walsh transform)**.** Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. The Walsh transform of f is the function $W_f\colon \mathbb{F}_2^n \to \mathbb{Z}$ defined by:

$$\forall \alpha \in \mathbb{F}_2^n, \quad W_f(\alpha) := \sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha \cdot x + f(x)},$$

where the dot $\cdot$ corresponds to a given scalar product, typically to the coordinate-wise dot product: $\alpha \cdot x = \sum_{i=1}^n a_i x_i \in \mathbb{F}_2$.

The Walsh transform of a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is given by the Walsh transforms of all of the components of F. More precisely, for any $\alpha \in \mathbb{F}_2^n, \beta \in \mathbb{F}_2^m$, the Walsh *coefficient* of F with respect to (α, β) is defined by:

$$W_F(\alpha, \beta) := W_{\beta \cdot F}(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha \cdot x + \beta \cdot F(x)}.$$

Remark 6. We can also adapt the definition of the Walsh transform to functions of the form $G\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ (resp. $H\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$), so that the Walsh coefficients can be enumerated using $\alpha, \beta \in \mathbb{F}_{2^n}$ (resp. $\alpha, \beta \in \mathbb{F}_{2^k}^\ell$), instead of $\alpha, \beta \in \mathbb{F}_2^n$. In that case, it suffices to replace the standard dot product by a scalar product defined over $\mathbb{F}_{2^n}$ (resp. $\mathbb{F}_{2^k}^\ell$). Over $\mathbb{F}_{2^n}$, we can then consider the scalar product defined by:

$$\forall\, x, y \in \mathbb{F}_{2^n}, \quad x \cdot y = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(xy).$$

Over $\mathbb{F}_{2^k}^\ell$, we use the one defined by:

$$\forall\, z, t \in \mathbb{F}_{2^n}, \quad z \cdot t = (z_1, \ldots, z_\ell) \cdot (t_1, \ldots, t_\ell) = \sum_{i=1}^{\ell} \mathrm{Tr}_{\mathbb{F}_{2^k}/\mathbb{F}_2}(z_i t_i). \tag{5}$$

In the following, we denote by A^* the *adjoint operator* of a linear mapping A, for a given scalar product, *i.e.*, the linear mapping such that,

$$x \cdot A(y) = A^*(x) \cdot y, \ \forall x, y\ .$$

It is well-known that the Walsh coefficients of a mapping $B \circ F \circ A$ in the linear-equivalence class of F are in one-to-one correspondence with the Walsh coefficients of F. This implies that linear self-equivalence is captured by some spectral symmetries.

Lemma 10 (Spectral characterization of linear self-equivalence)**.** *Let A, B be bijective linear mappings from $\mathbb{F}_2^n$ to itself. Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then $B \circ F \circ A = F$ if and only if:*

$$\forall \alpha \in \mathbb{F}_2^n, \forall \beta \in \mathbb{F}_2^n, \quad W_F\left((A^{-1})^*(\alpha), B^*(\beta)\right) = W_F(\alpha, \beta).$$

Proof. The Walsh coefficient of the left-hand side is precisely the Walsh coefficient of $B \circ F \circ A$ in (α, β). It is then a consequence of the fact that two functions are equal if and only if their Walsh transforms are equal. □

Corollary 2. *Let A, B be bijective linear mappings from $\mathbb{F}_2^n$ to itself. Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be such that $B \circ F \circ A = F$. Let $\mathcal{L}$ be the function from $\mathbb{F}_2^n \times \mathbb{F}_2^n$ to itself that is defined by:*

$$\forall\ x, y \in \mathbb{F}_2^n, \quad \mathcal{L}(x, y) = \left((A^{-1})^*(x), B^*(y)\right)$$

Assume that the lengths of the cycles $\sigma_{\mathcal{L}}(x_0, y_0)$, for all nonzero $(x_0, y_0) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$, are divisible by L. Then each value v in the multiset

$$\{\!\{W_F(\alpha, \beta),\ \text{s.t. } \alpha, \beta \in \mathbb{F}_{2^n},\ (\alpha, \beta) \neq (0, 0)\}\!\}$$

appears $L \cdot t_v$ times for some $t_v \geq 1$. In that case, the greatest common divisor of the numbers of occurrences of the values in the Walsh spectrum is divisible by L.

Proof. Let $(\alpha, \beta) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ be such that $(\alpha, \beta) \neq (0, 0)$. By assumption, the multiset $\{\!\{W_F(\mathcal{L}^i(\alpha, \beta)), i \in [\![0, L-1]\!]\}\!\}$ contains the single value $W_F(\alpha, \beta)$ with multiplicity λL. Indeed, because $\sigma_{\mathcal{L}}(\alpha, \beta)$ is of length λL, this value corresponds to λL distinct Walsh coefficients. The divisibility is then an immediate consequence of the fact that the multiset $\{\!\{W_F(\alpha, \beta),\ s.t.\ (\alpha, \beta) \neq (0, 0)\}\!\}$ can be partitioned according to the decomposition of $\mathcal{L}$ into cycles with disjoint supports. □

Corollary 3 (Walsh coefficients of a cyclotomic mapping)**.** *Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a cyclotomic mapping of exponent d with respect to $\mathbb{G} \subset \mathbb{F}_{2^n}^*$. Then:*

$$\forall \alpha, \beta \in \mathbb{F}_{2^n}, \forall x \in \mathbb{G}, \quad W_F(\alpha, \beta x^d) = W_F(\alpha x^{-1}, \beta).$$

Furthermore, the greatest common divisor of the numbers of occurrences of the values in the Walsh spectrum is divisible by $\frac{|\mathbb{G}|}{\gcd(d, |\mathbb{G}|)}$ for $d > 0$, and by $|\mathbb{G}|$ when $d = 0$.

Proof. In the case of a cyclotomic mapping of exponent d with respect to $\mathbb{G}$ we can choose $A^{-1} = M_{x,n}$ where $x \in \mathbb{G}$ and $B = M_{x^d,n}$. The relation between the Walsh coefficients is then a direct consequence of Lemma 10. Moreover, the cycle decomposition of $(A^{-1})^*$ (resp. of B^*) is the same as the cycle decomposition of A (resp. of B). Starting from a nonzero element, all cycles of A have length $\mathrm{ord}(x)$, and all cycles of B have length $\mathrm{ord}(x^d)$. If $d \neq 0$, then

$$\mathrm{ord}(x^d) = \frac{\mathrm{ord}(x)}{\gcd(d, \mathrm{ord}(x))}\ .$$

Most notably, we deduce the result by choosing for x a generator of $\mathbb{G}$. When $d = 0$, all cycles of $\mathcal{L} = \left((A^{-1})^*(x), y\right)$ have length $|\mathbb{G}|$. □

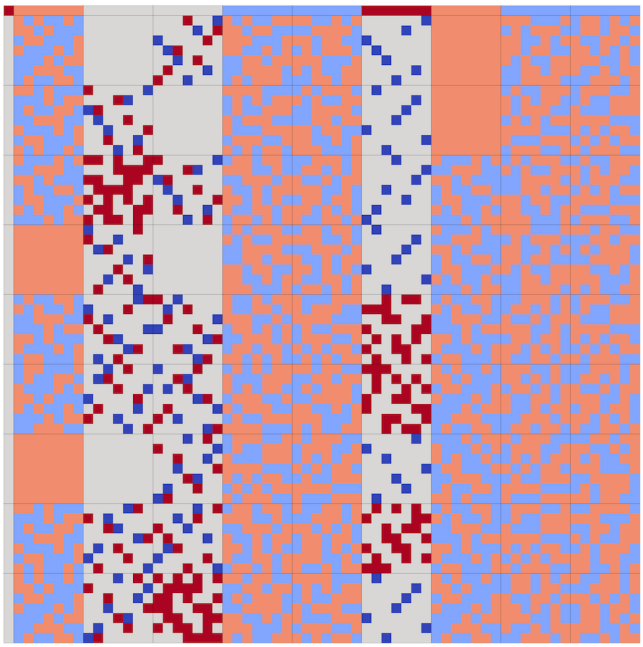
The following corollary can be proved in a similar manner.

Corollary 4 (Walsh coefficients of an ℓ-variate projective mapping)**.** *Let $F\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$ be an ℓ-variate projective mapping of exponents $(d_1, \ldots, d_\ell)$ with respect to $\mathbb{F}_{2^k}$. Then:*

$$\forall \alpha, \beta \in \mathbb{F}_{2^k}^\ell, \forall x \in \mathbb{F}_{2^k}^*, \quad W_F\left(\alpha, \left(\beta_1 x^{d_1}, \ldots, \beta_\ell x^{d_\ell}\right)\right) = W_F\left(\left(\alpha_1 x^{-1}, \ldots, \alpha_\ell x^{-1}\right), \beta\right).$$

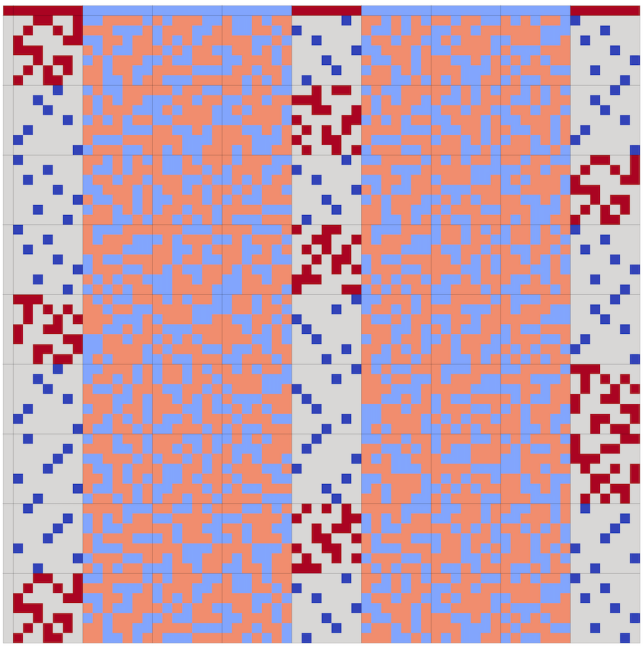
Furthermore, if there exists $x \in \mathbb{F}_{2^k}^*$ such that $\gcd(d_i, \mathrm{ord}(x)) = 1$ for all $i \in [\![1, \ell]\!]$, then the greatest common divisor of the numbers of occurrences of the values in the Walsh spectrum is divisible by $\mathrm{ord}(x)$.

The symmetries highlighted in Corollary 3 appear very clearly in the graphical representations of the linear approximation table (LAT) of the Kim mapping and of the Gold power mapping $x \mapsto x^3$ over $\mathbb{F}_{64}$ that are depicted in Figs. 1 and 2. The same property can be stated for the differential distribution table (DDT) of a linearly self-equivalent mapping.



The Walsh coefficients $W_F(\alpha, \beta)$ are enumerated cosets by cosets, β along the x-axis and α along the y-axis.

Figure 1: LAT of the Kim mapping.



The Walsh coefficients $W_F(\alpha, \beta)$ are enumerated cosets by cosets, β along the x-axis and α along the y-axis.

Figure 2: LAT of the mapping $x \mapsto x^3$ over $\mathbb{F}_{64}$.

Lemma 11 (Linear equivalence and DDT)**.** *Let $A, B\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be bijective linear mappings. Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$. If F satisfies $B \circ F \circ A = F$, then:*

$$\forall \alpha \in \mathbb{F}_2^n, \forall \beta \in \mathbb{F}_2^n, \quad \delta_F(\alpha, \beta) = \delta_F(A(\alpha), B^{-1}(\beta)),$$

where $\delta_F(\alpha, \beta) = |\{x \in \mathbb{F}_2^n, F(x+\alpha) + F(x) = \beta\}|$.

As in Corollary 3, the divisibility of the number of occurrences in the differential spectrum (with non-zero coefficients) also holds for cyclotomic mappings. These properties were already used in a cryptographic context in [JKK+22]. Indeed, in this paper, the authors use this redundancy among the Walsh and differential spectra to avoid going through all the coefficients while computing the linearity and the differential uniformity of the functions they study.

In our case, these properties can be used as a tool to search for signs of existence of linearly self-equivalent representatives within an equivalence class. Indeed, the Walsh spectrum is preserved by linear equivalence and the differential and extended Walsh spectra are preserved by CCZ-equivalence. However, APN functions all share the same differential spectrum, so this is of low interest. Furthermore, most of the APN functions in the infinite families that we know also share the same Walsh spectrum, see for instance [BCCLC06, KKK23, BIK23].

5.2 Ortho-derivatives of linearly self-equivalent mappings

We then see how to capture linear self-equivalence in another way by using the so-called *ortho-derivative* of quadratic functions.

Definition 15 (Ortho-derivative [CCP22, CCP24])**.** Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic function. We say that $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is *an* ortho-derivative for F if, for any x and Δ in $\mathbb{F}_2^n$:

$$\pi(\Delta) \cdot (F(x) + F(x+\Delta) + F(0) + F(\Delta)) = 0$$

The set of all ortho-derivatives of F is denoted by $\Pi(F)$.

Note that $\Pi(F)$ is actually a vector space, as the zero function is obviously an ortho-derivative and it is stable by the addition of functions.

As the Walsh transform, an ortho-derivative depends on a specific scalar product. For any function $F\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$, it can as well be defined with a scalar product over $\mathbb{F}_{2^k}^\ell$, for instance according to the one defined by Eq. (5).

In the case of a quadratic APN function, because the image set of any non-zero derivative is a hyperplane, there exists a single *non-trivial* ortho-derivative, that is $\pi \in \Pi(F)$ such that $\pi(0) = 0$ and $\pi(a) \neq 0$ for any $a \neq 0$. In the following, we refer to this single non-trivial ortho-derivative as *the* ortho-derivative of a quadratic APN function.

The main advantage of the ortho-derivative of a quadratic function is its behavior within a given EA-equivalence class.

Proposition 8 (Ortho-derivative and EA class [CCP22, Proposition 36])**.** *Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic function, $A, B\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be bijective affine mappings, and $C\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an affine function. Let π_F be an ortho-derivative of F. Let G and τ be defined as:*

$$G = B \circ F \circ A + C, \quad \tau = (L_B^*)^{-1} \circ \pi_F \circ L_A,$$

where L_A, L_B are the linear parts of A, B. Then τ is an ortho-derivative of G, that is, $\tau \in \Pi(G)$. In other words, we have:

$$\Pi(G) = (L_B^*)^{-1} \Pi(F) L_A.$$

Corollary 5. *Let F be a quadratic APN function. Let G be EA-equivalent to F. Then their unique non-zero ortho-derivative are linearly equivalent.*

In our case, this also implies the following easy, but important proposition.

Proposition 9. *Let F be a quadratic APN function. Let us suppose that F is linearly self-equivalent: $B \circ F \circ A = F$. Let G be EA-equivalent to F: $G = D \circ F \circ E + C$. Then:*

(i) *the ortho-derivative of F is linearly self-equivalent: $(B^{-1})^* \circ \pi_F \circ A = \pi_F$.*

(ii) *the ortho-derivative of G is linearly self-equivalent.*

Proof. By a direct application of Proposition 8, we obtain $(B^{-1})^* \circ \pi_F \circ A = \pi_F$, because A, B are linear and, $\pi_G = (L_D^*)^{-1} \circ \pi_F \circ L_E$, *i.e.* $L_D^* \circ \pi_G \circ L_E^{-1} = \pi_F$. By substituting π_F in the formula deduced from self equivalence, we obtain:

$$(B^{-1})^* \circ L_D^* \circ \pi_G \circ L_E^{-1} \circ A = L_D^* \circ \pi_G \circ L_E^{-1},$$

or equivalently:

$$\left((L_D^*)^{-1} \circ (B^{-1})^* \circ L_D^*\right) \circ \pi_G \circ \left(L_E^{-1} \circ A \circ L_E\right) = \pi_G. \tag{6}$$

□

In the case of a cyclotomic mapping, or more generally of an ℓ-variate projective mapping, we obtain the following interpretation of the previous proposition.

Corollary 6 (Ortho-derivatives of ℓ-variate projective mappings)**.** *Let $F\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$ be a quadratic APN function. Let us suppose that F is an ℓ-variate projective mapping with exponents $(d_1, \ldots, d_\ell)$. Then π_F is an ℓ-variate projective mapping with exponents $(-d_1, \ldots, -d_\ell)$, where the exponents are considered modulo $2^k - 1$. In particular, the ortho-derivative of a quadratic APN cyclotomic mapping of exponent d is cyclotomic of exponent $-d$, and the ortho-derivative of the power mapping $x \mapsto x^d$ is the power mapping $x \mapsto x^{-d}$.*

Proof. First, we observe that for any $x, y, z \in \mathbb{F}_{2^n}$: $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(x(yz)) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}((yx)z)$, so the multiplication $M_{y,n}$ is its own adjoint, for any $y \in \mathbb{F}_{2^n}$. When looking at functions $F\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$, we can use $(x, y) \mapsto \sum_{i=1}^{\ell} \mathrm{Tr}_{\mathbb{F}_{2^k}/\mathbb{F}_2}(x_i y_i)$ as the scalar product, which immediately yields the announced result by using Proposition 9. □

In particular, both the linear approximation table (LAT) and the difference distribution table (DDT) of such ortho-derivatives inherit from the symmetries mentioned in Corollary 3 and Lemma 11. Contrary to the initial quadratic APN functions, their ortho-derivatives are neither quadratic, nor APN. In particular, there is *a priori* no reason for ortho-derivatives to share the same differential spectrum or extended Walsh spectrum. In practice, two functions in two distinct EA-equivalence classes have distinct spectra. This is the reason why these spectra are used as strong invariants of EA-equivalence class for quadratic APN functions, for instance in [CCP22, Table VII], [BIK23, Tables 3 & 4], or [BL22, YP22].

In our case, if the divisibility condition mentioned in Corollary 3 does not hold for the ortho-derivative, this proves that the function we consider is not EA-equivalent to a cyclotomic mapping. On the other hand, as there is no known reason for such a structure to randomly occur, this could provide a way to detect the existence of a possible self-equivalent representative.

Example 9 (Quadratic APN functions of the Banff list)**.** Among the 13 representatives of quadratic APN functions in 6 variables, as given in Banff list [Dil09], we can exclude the existence of cyclotomic mappings in the EA-equivalence classes of 9 of them by studying

the differential spectra and Walsh spectra of their ortho-derivatives. Indeed, as shown in Table 4, in these 9 cases, for at least one of the two spectra, the greatest common divisor of the numbers of occurrences of each value is equal to 1. The four others classes are represented by:

$$\begin{aligned}
P_2 &= X^3,\\
P_3 &= X^3 + a^{11}X^6 + aX^9,\\
P_4 &= a^7X^3 + X^5 + a^3X^9 + g^4X^{10} + X^{17} + a^6X^{18}, \text{ and}\\
P_5 &= X^3 + X^{10} + aX^{24},
\end{aligned}$$

where a is a root of $X^6 + X^4 + X^3 + X + 1$ and where the GCDs corresponding to P_i are given on row $\#i$ of Table 4. Among them, P_2 is the cube power mapping, and P_3 is a cyclotomic mapping of exponent 0 with respect to $\mathbb{F}_4$, but the GCD for the Walsh spectrum of its ortho-derivative is 21 and the one for the differential spectrum is 63, which might suggest a property related to $\mathbb{F}_8$ or to the group $\mathbb{G}$ with 21 elements. The representative P_4 is not cyclotomic but the GCDs are in that case equal to 21 and 14, which again suggests a property related to $\mathbb{F}_8$. The polynomial P_5 is the Kim mapping, which is cyclotomic of exponent 3 with respect to $\mathbb{F}_8$.

Table 4: Divisibilities of the numbers of occurrences of each value in the Walsh spectrum of the 6-bit APN functions from the Banff list, and of the Walsh and differential spectra of their ortho-derivatives.

ID	GCD for Walsh spectrum of F	GCDs for Walsh and differential spectra of the ortho-derivative π_F	Number of mappings
#1	42	(1, 1)	7
#2	42	(84, 63)	1
#3	42	(21, 63)	1
#4	42	(21, 14)	1
#5	42	(28, 21)	1
#6	42	(1, 2)	1
#7	1	(2, 1)	1

Table 5: Divisibilities of the numbers of occurrences of each value in the Walsh spectrum of the 9-bit APN functions from [BL22], and of the Walsh and differential spectra of their ortho-derivatives.

ID	GCD for Walsh spectrum of F	GCDs for Walsh and differential spectra of the ortho-derivative π_F	Number of mappings
#1	4088	(7, 7)	33
#2	4088	(1, 1)	2

In light of Theorem 6, the previous example shows that (most of) the known infinite families of quadratic APN functions have very specific properties. **J:** J'ai trié le tableau 7 (et au passage corrigé car il y avait les 6-bit dedans aussi), est-ce que ça vous va ? J'ai aussi précisé la phrase suivante. This is also highlighted in Table 6 with the 8-bit APN functions found in [BL22, YP22, YWL14]. In particular, while the functions from [BL22] are all linearly self-equivalent, none of them, except maybe the two whose GCDs appear on

Table 6: Divisibilities of the numbers of occurrences of each value in the Walsh spectrum of the 8-bit APN functions from [BL22] (upper half) and [YP22, YWL14] (lower half), and of the Walsh and differential spectra of their ortho-derivative.

ID	GCD for Walsh spectrum of F	GCDs for Walsh and differential spectra of the ortho-derivative π_F	Number of mappings
BL-1	340	(1, 3)	8667
BL-2	2	(1, 3)	3206
BL-3	340	(1, 6)	403
BL-4	4	(1, 3)	311
BL-5	340	(1, 1)	204
BL-6	2	(1, 1)	45
BL-7	340	(1, 12)	26
BL-8	4	(1, 6)	11
BL-9	4	(1, 1)	11
BL-10	340	(1, 15)	10
BL-11	340	(1, 2)	7
BL-12	1	(1, 3)	4
BL-13	340	(1, 24)	3
BL-14	2	(1, 15)	3
BL-15	2	(1, 6)	3
BL-16	340	(1, 5)	2
BL-17	340	(1, 30)	2
BL-18	340	(5, 15)	2
BL-19	340	(2, 2)	1
BL-20	2	(1, 5)	1
BL-21	4	(2, 3)	1
QAM-1	340	(1, 1)	12201
QAM-2	2	(1, 1)	796
QAM-3	340	(1, 2)	359
QAM-4	340	(1, 3)	160
QAM-5	340	(1, 4)	17
QAM-6	2	(1, 3)	14
QAM-7	4	(1, 1)	14
QAM-8	340	(1, 6)	8
QAM-9	340	(1, 5)	8
QAM-10	340	(1, 12)	3
QAM-11	4	(1, 3)	2
QAM-12	340	(1, 10)	2
QAM-13	340	(85, 510)	1
QAM-14	340	(85, 1020)	1
QAM-15	340	(5, 60)	1
QAM-16	340	(2, 2)	1
QAM-17	340	(1, 24)	1
QAM-18	340	(1, 8)	1
QAM-19	2	(1, 2)	1

row BL-18, is EA-equivalent to a non-trivial cyclotomic mapping. On the other hand, we observe in Table 5 that out of the 35 known 9-bit quadratic APN functions from [BL22], 33 could potentially be EA-equivalent to cyclotomic mappings with respect to $\mathbb{F}_8$.

5.3 Searching for linearly self-equivalent mappings within an EA- or CCZ-equivalence class

We now discuss how we could determine in the general (non-quadratic) case whether a function is EA-equivalent or CCZ-equivalent to a cyclotomic mapping or to an ℓ-variate projective mapping.

The following approach is in line with the proof of Proposition 9. Let F be linearly self-equivalent: $B \circ F \circ A = F$. Let G be EA-equivalent to F such that they satisfy $F = D \circ G \circ E + C$. Then it holds that:

$$B \circ (D \circ G \circ E + C) \circ A = D \circ G \circ E + C,$$

or equivalently:

$$B \circ D \circ G \circ E \circ A = D \circ G \circ E + C + B \circ C \circ A.$$

By composing the output by D^{-1} and the input by E^{-1}, this is equivalent to:

$$(D^{-1} \circ B \circ D) \circ G \circ (E \circ A \circ E^{-1}) = G + D^{-1}(C + B \circ C \circ A) \circ E^{-1}.$$

In other words, G is EA self-equivalent. Furthermore $D^{-1} \circ B \circ D$ is an affine mapping with $L_D^{-1} \circ B \circ L_D$ as linear part, and a similar property holds for $E \circ A \circ E^{-1}$. This implies that the minimal polynomials of the involved transformations are preserved by EA-equivalence. This can again give proofs of the non-existence of cyclotomic (or ℓ-variate projective) representatives within an EA-equivalence class.

Actually, the same technique can be adapted to the case of CCZ-equivalence.

Proposition 10 (Functions CCZ-equivalent to a linearly self-equivalent one)**.** *Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a linearly self-equivalent mapping satisfying $B \circ F = F \circ A$ for some linear bijections A, B. Let G be CCZ-equivalent to F. Then:*

(i) *G is CCZ self-equivalent.*

(ii) *There exists an $\mathbb{F}_2$-affine bijective mapping $\mathcal{A}\colon (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2$ with linear part $\mathcal{L}$ such that $\mathcal{A}(\mathcal{G}_G) = \mathcal{G}_G$, and $\mathcal{L}$ is similar to $\mathrm{diag}(A, B)$. Most notably, $\mathrm{diag}(A, B)$ and $\mathcal{L}$ have the same canonical form and $\min(\mathcal{L}) = \mathrm{lcm}(\min(A), \min(B))$.*

Proof. From the two hypotheses, it holds that:

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \mathcal{G}_F = \mathcal{G}_F, \quad \text{and } \mathcal{A}(\mathcal{G}_G) = \mathcal{G}_F,$$

for some affine bijection $\mathcal{A}\colon (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2$. By substituting $\mathcal{G}_F$ by $\mathcal{A}(\mathcal{G}_G)$ in the first equality, we obtain:

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \circ \mathcal{A}(\mathcal{G}_G) = \mathcal{A}(\mathcal{G}_G) \quad \Longleftrightarrow \quad \mathcal{A}^{-1} \circ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \circ \mathcal{A}(\mathcal{G}_G) = \mathcal{G}_G.$$

In other words, G is CCZ self-equivalent. Furthermore, the linear part of the affine mapping $\mathcal{A}^{-1} \circ \mathrm{diag}(A, B) \circ \mathcal{A}$ is $\mathcal{L}^{-1} \circ \mathrm{diag}(A, B) \circ \mathcal{L}$, which is similar to $\mathrm{diag}(A, B)$. In particular, $\mathcal{L}$ and $\mathrm{diag}(A, B)$ have the same minimal polynomial, which is the least common multiple of the ones of A and B. □

Contrary to ortho-derivatives which are not defined for functions of degree more than 2, this method can be applied to any function.

Example 10 (Brinckmann-Leander-Edel-Pott APN cubic [BL08, EP09])**.** Let us consider the well-known Brinckmann-Leander-Edel-Pott APN cubic for $n = 6$ [BL08, EP09]. Then there is neither cyclotomic nor ℓ-variate projective mapping in its CCZ-equivalence class. Indeed, its 7 non-trivial automorphisms share the same elementary divisors, which are $X+1$ with multiplicity 2 and $(X+1)^2$ with multiplicity 5. In particular, if a linearly self-equivalent function exists in its CCZ-equivalence class, then, according to Proposition 10, the canonical form of $\mathrm{diag}(A, B)$ is the same as the one of $\mathcal{L}$. But the canonical form of $\mathrm{diag}(A, B)$ is the concatenation of the ones of A and B. This implies that the canonical form of A is made of blocks $C(X+1)$ or $C\left((X+1)^2\right)$ with at least one block $C\left((X+1)^2\right)$. Therefore, because of Proposition 4, $\min(A) = (X+1)^2$. Thus $\min(A)$ is not irreducible which contradicts the hypotheses of Theorem 3 for the cyclotomic case, and the ones of Theorem 5 for the ℓ-variate projective case. Indeed, the only non-trivial subfields of $\mathbb{F}_{2^6}$ are $\mathbb{F}_{2^2}$ and $\mathbb{F}_{2^3}$, with both 2^2-1 and 2^3-1 being prime.

In particular, this example generalizes the well-known fact that this function is not CCZ-equivalent to a monomial mapping. Actually, these non-LE automorphisms correspond to the 7 affine derivatives of the Brinckmann-Leander-Edel-Pott cubic. By definition, any such automorphism corresponds to a triangular block matrix with a diagonal made of identity blocks:

$$\begin{pmatrix} \mathrm{Id} & 0 \\ L & \mathrm{Id} \end{pmatrix} + \begin{pmatrix} \Delta^{\mathrm{in}} \\ \Delta^{\mathrm{out}} \end{pmatrix} \in \mathrm{Aut}(F),$$

where L is the linear part of the derivative $D_{\Delta^{\mathrm{in}}}F$ and Δ^{out} its constant term (see e.g [BBMM11]). In particular, the linear part of such an EA automorphism is involutive: its canonical form is therefore only made of blocks $C(X+1)$ and $C((X+1)^2)$. The argument used in the previous example can therefore be generalized. Indeed, from an EA automorphism related to an affine derivative of a function F, we can never prove the existence of a linearly self-equivalent function G in its CCZ-equivalence class, where G satisfies $B \circ G \circ A = G$, with *non-involutive* A and/or B. Conversely, if the only non-trivial automorphisms of a function come from its affine derivatives, neither cyclotomic nor ℓ-variate cyclotomic mapping exists in its CCZ-equivalence class. This also implies the non-existence of representatives that commute with the Frobenius automorphism because $x \mapsto x^2$ is not involutive.

A lot of questions still remain open. For instance, this does not rule out the existence of a linearly self-equivalent mapping G in the CCZ-equivalence class of this cubic, it only proves that if such a mapping G exists, it satisfies $B \circ G \circ A = G$ for two involutions A and B. However, in light of Theorem 6, it proves that this cubic is very different from the other known APN functions. The most interesting problem that remains is the following one.

Problem 3 (From CCZ self-equivalence to linear self-equivalence)**.** *Given a CCZ self-equivalent function, is it possible to use its automorphisms to find a linearly self-equivalent function in the same CCZ-equivalence class?*

6 (Quadratic) APN mappings

6.1 APN (generalized) cyclotomic mappings

We have shown in Section 4 that many families among the known APN functions are linearly equivalent to a cyclotomic mapping. We then further study these mappings since they seem to play a particular role among all known APN mappings. Note that the differential uniformity of cyclotomic mappings was investigated by Chen and Coulter [CC23] recently, but their results do not provide any relevant information for our parameters in characteristic 2. We thus continue studying the link between those two properties. Since

the generalization is straightforward, we state the results in a more general context, such as the one of generalized cyclotomic mappings.

6.1.1 Necessary conditions to be APN

First of all, an APN generalized cyclotomic mapping with respect to a subfield $\mathbb{F}_{2^k}$ has a single preimage for 0.

Proposition 11. *Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a generalized cyclotomic mapping with respect to $\mathbb{F}_{2^k}$. Assume that there exists $\lambda \neq 0$ such that $F(\lambda) = 0$. Then the differential uniformity of F is at least 2^k.*

Proof. We observe that, for any $\varphi \in \mathbb{F}_{2^k}$, we have $F(\lambda\varphi + \lambda) + F(\lambda\varphi) = 0$. □

In particular an APN generalized cyclotomic mappping with respect to $\mathbb{F}_{2^k}$ must satisfy $F^{-1}(\{0\}) = \{0\}$. Furthermore, it must be based on APN monomials over $\mathbb{F}_{2^k}$.

Lemma 12. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a generalized cyclotomic mapping with respect to a subfield $\mathbb{F}_{2^k}$. If F is APN, then all its exponents d_λ, $\lambda \neq 0$, defined in Definition 11 are such that $x \mapsto x^{d_\lambda}$ is APN on $\mathbb{F}_{2^k}$.*

Proof. Suppose that there exists a coset $\lambda\mathbb{F}_{2^k}$, $\lambda \neq 0$, such that $G_\lambda : x \mapsto x^{d_\lambda}$ is not APN on $\mathbb{F}_{2^k}$. Then, there exist $\varphi_1, \varphi_2 \in \mathbb{F}_{2^k}$ such that $\delta_{G_\lambda}(\varphi_1, \varphi_2) > 2$. Using that, for any $\varphi \in \mathbb{F}_{2^k}$,

$$F(\lambda\varphi + \lambda\varphi_1) + F(\lambda\varphi) = F(\lambda)\left(G_\lambda(\varphi + \varphi_1) + G_\lambda(\varphi)\right),$$

we deduce that there exist more than two $\varphi \in \mathbb{F}_{2^k}$ such that

$$F(\lambda\varphi + \lambda\varphi_1) + F(\lambda\varphi) = F(\lambda)\varphi_2$$

implying that F is not APN. □

This explains the fact that the exponents of the cyclotomic mappings in most of the infinite families are Gold exponents. Note that the stability of $\mathbb{F}_{2^k}$ with respect to addition is used in the previous proof, this is the reason why it cannot (at least directly) be adapted to the more general case of cyclotomic mappings with respect to generic groups $\mathbb{G}$.

The case of subfields of even dimension is very peculiar. Indeed, we can in that case derive necessary conditions from the fact that an APN function F must satisfy:

$$|\mathrm{Im}(F)| \geq \begin{cases} \frac{2^n+1}{3} & \text{if } n \text{ is odd} \\ \frac{2^n+2}{3} & \text{if } n \text{ is even} \end{cases}, \tag{7}$$

see for instance [CHP17, Cze20, KKK23].

Proposition 12. *Let k be an even divisor of n and F be a cyclotomic mapping with respect to $\mathbb{F}_{2^k}$. Let Γ be a system of representatives of the multiplicative cosets of $\mathbb{F}_{2^k}$. If F is APN then:*

- *F does not satisfy the $\mathbb{F}_{2^k}$-subspace property,*
- *F is cyclotomic of exponent 0 with respect to $\mathbb{F}_4$,*
- *all $F(\gamma)$, $\gamma \in \Gamma$ belong to different cosets of $\mathbb{F}_{2^k}$,*
- *F is almost 3-to-1 with $F^{-1}(0) = \{0\}$.*

Proof. Lemma 12 states that $x \mapsto x^d$ is APN over $\mathbb{F}_{2^k}$. The first point is then a consequence of the well-known[4] fact that there does not exist any APN bijective monomial for even dimension. Furthermore, because k is even, we have that $\gcd(d, 2^k - 1) = 3$, which implies that the exponent of each monomial of F is divisible by 3. By Proposition 1, F is cyclotomic of exponent 0 with respect to $\mathbb{F}_4$, and therefore constant on each coset of $\mathbb{F}_4$. Because of Eq. (7), F is then necessarily almost 3-to-1, or equivalently, all $F(\gamma), \gamma \in \Gamma$ belong to different cosets of $\mathbb{F}_{2^k}$. □

This proposition can actually be refined in the case of *plateaued functions*, which generalize the case of quadratic functions.

Definition 16 (Plateaued function [ZZ99])**.** Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$. The function f is said to be *plateaued* if there exists a positive integer $c > 0$ such that for any $\alpha \in \mathbb{F}_2^n$, $W_f(\alpha) \in \{0, \pm c\}$. In that case, $c = 2^i$, with $i \geq \frac{n}{2}$ and it is called the *amplitude* of f. A vectorial function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called plateaued if all its non-zero components are plateaued.

In the case of the functions of Proposition 12 *that are also plateaued*, it can be proved [KKK23] that they all share the same Walsh spectrum, which is the Walsh spectrum of the APN Gold mappings. However, this is not true in the general case. An example of this situation is Dobbertin's power function over $\mathbb{F}_{2^{10m}}$, $m \geq 1$, with exponent $d = 2^{8m} + 2^{6m} + 2^{4m} + 2^{2m} - 1$ [Dob01]. As any power function, this function is a cyclotomic mapping. For instance, it can be written as $x^3 x^{(2^{8m}-1)+(2^{6m}-1)+(2^{4m}-1)+(2^{2m}-1)}$, but the four terms of the second exponent are divisible by $2^{2m} - 1$ so it is cyclotomic of exponent 3 with respect to $\mathbb{F}_{2^{2m}}$. It is also almost 3-to-1 by the previous proposition, however it is known that its Walsh spectrum is not $2^{n/2}$ divisible [CCD00]. Then, its Walsh spectrum cannot be the one of the APN Gold mappings and its form is only conjectured [BCC+22, Conjecture 29].

6.1.2 Spectral properties of (generalized) cyclotomic mappings

For generalized cyclotomic mappings with respect to a subfield, we can easily express the Walsh coefficients in terms of the Walsh coefficients of the power functions $x \mapsto x^{d_\lambda}$.

Proposition 13. *Let $n = \ell k$ and $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a generalized cyclotomic mapping with respect to $\mathbb{F}_{2^k}$. Let $d_\gamma, \gamma \in \Gamma$ denote its exponents as defined in Definition 11, where Γ is a system of representatives of the multiplicative cosets of $\mathbb{F}_{2^k}$. For any $\alpha, \beta \in \mathbb{F}_{2^n}$, we have:*

$$W_F(\alpha, \beta) = -\sum_{i=1}^{\ell-1} 2^{ik} + \sum_{\gamma \in \Gamma} W_{\mathbb{F}_{2^k}, x^{d_\gamma}}\left(\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\alpha\gamma), \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta F(\gamma))\right).$$

[4] An elegant and straight-forward proof of this fact can be found in [KKK23, Corollary 4]. It is based on Eq. (7).

Proof. A direct computation yields:

$$\begin{aligned}
W_F(\alpha,\beta) &= \sum_{\lambda\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\alpha\lambda+\beta F(\lambda))} \\
&= (-1)^0 + \sum_{\gamma\in\Gamma}\sum_{\varphi\in\mathbb{F}_{2^k}^*} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\alpha\gamma\varphi+\beta F(\gamma\varphi))} \\
&= 1 + \sum_{\gamma\in\Gamma}\left(\sum_{\varphi\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\alpha\gamma\varphi+\beta F(\gamma\varphi))} - 1\right) \\
&= (1-|\Gamma|) + \sum_{\gamma\in\Gamma}\sum_{\varphi\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\alpha\gamma\varphi+\beta F(\gamma\varphi))} \\
&= -\sum_{i=1}^{\ell-1} 2^{ik} + \sum_{\gamma\in\Gamma}\sum_{\varphi\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\alpha\gamma\varphi+\beta F(\gamma)\varphi^{d_\gamma})} \\
&= -\sum_{i=1}^{\ell-1} 2^{ik} + \sum_{\gamma\in\Gamma} W_{\mathbb{F}_{2^k},x^{d_\gamma}}\left(\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\alpha\gamma), \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta F(\gamma))\right);
\end{aligned}$$

where we successively used the multiplicative decomposition using Γ, changed the sum over $\mathbb{F}_{2^k}^*$ into a sum over $\mathbb{F}_{2^k}$, used Definition 11, and finally the trace linearity. □

Proposition 14 (Walsh coefficients in zero)**.** *Let $n = \ell k$. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a generalized cyclotomic mapping with bijective exponents with respect to $\mathbb{F}_{2^k}$. Let $\beta \in \mathbb{F}_{2^n}^*$ and $\mathcal{K}(\beta) = \left|\{\gamma \in \Gamma : \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta F(\gamma)) = 0\}\right|$. Then:*

$$W_F(0,\beta) = 2^k\left(\mathcal{K}(\beta) - \sum_{i=0}^{\ell-2} 2^{ik}\right).$$

Proof. By Proposition 13, $W_F(0,\beta)$ can be expressed as:

$$W_F(0,\beta) = -\sum_{i=1}^{\ell-1} 2^{ik} + \sum_{\gamma\in\Gamma} W_{\mathbb{F}_{2^k},x^{d_\gamma}}\left(0, \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta F(\gamma))\right).$$

Moreover, $x \mapsto x^{d_\gamma}$ is a bijection over $\mathbb{F}_{2^k}$ and thus, $W_{\mathbb{F}_{2^k},x^{d_\gamma}}(0,\lambda) = 2^k \cdot \mathbf{1}_0(\lambda)$. Then:

$$W_F(0,\beta) = -\sum_{i=1}^{\ell-1} 2^{ik} + 2^k\left|\left\{\gamma\in\Gamma \text{ s.t. } \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta F(\gamma)) = 0\right\}\right|.$$

□

When n is even and $k = n/2$, the Walsh coefficients in zero are directly derived from the number of preimages by F of the multiplicative cosets of $\mathbb{F}_{2^k}$.

Corollary 7 (Walsh coefficients in zero when $k = n/2$)**.** *Let $n = 2k$ be an even integer and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a generalized cyclotomic mapping with bijective exponents with respect to $\mathbb{F}_{2^k}$. Then, for any $\beta \in \mathbb{F}_{2^n}^*$, we have:*

$$W_F(0,\beta) = 2^k(\mathcal{K}(\beta) - 1), \quad \textit{with} \quad \mathcal{K}(\beta) = \left|\Gamma \cap F^{-1}(\beta^{-1}\mathbb{F}_{2^k})\right|.$$

Most notably, if F is a plateaued APN function, there are at least $\frac{2(2^k+1)}{3}$ cosets of $\mathbb{F}_{2^k}^*$ with 0 or 2 preimages by F.

Proof. We know from Proposition 14 that $W_F(0,\beta) = 2^k(\mathcal{K}(\beta)-1)$. Since $k = n/2$, $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta F(\gamma)) = \beta F(\gamma)+(\beta F(\gamma))^{2^k} = 0$ if and only if $\beta F(\gamma) \in \mathbb{F}_{2^k}$, i.e., $F(\gamma) \in \beta^{-1}\mathbb{F}_{2^k}$. We deduce that: $\mathcal{K}(\beta) = \left|\Gamma \cap F^{-1}(\beta^{-1}\mathbb{F}_{2^k})\right|$. If F is APN then by Proposition 11, $F^{-1}(\{0\}) = \{0\}$. In that case this implies that: $\mathcal{K}(\beta) = \left|\Gamma \cap F^{-1}(\beta^{-1}\mathbb{F}_{2^k}^*)\right|$, which is the number of cosets of $\mathbb{F}_{2^k}^*$ mapped onto $\beta^{-1}\mathbb{F}_{2^k}^*$. □

Corollary 8. *Let $n = 2k$ be an even integer and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a generalized cyclotomic mapping with bijective exponents with respect to $\mathbb{F}_{2^k}$. Then its linearity satisfies:*

$$\mathcal{L}(F) \geq 2^k \left(\max_{\beta\in\Gamma}(\left|\Gamma \cap F^{-1}(\beta^{-1}\mathbb{F}_{2^k})\right| - 1\right).$$

Example 11. We exhaustively looked at the 63 mappings over $\mathbb{F}_{64}$ of the form $x \mapsto x^3 + x^{10} + ux^{24}$, where $u \neq 0$. Eight of them can be proven non-APN thanks to Proposition 11, because a coset is set onto $\{0\}$. For the remaining ones, we computed the multiset $\{\!\{\mathcal{K}(\beta),\ \beta \in \Gamma\}\!\}$ where Γ is a system of representatives of the multiplicative cosets of $\mathbb{F}_{2^k}^*$. The possible values for this multiset are:

$$\begin{aligned}
M_1 &= \{\!\{0,\ 0,\ 1,\ 1,\ 1,\ 1,\ 1,\ 2,\ 2\}\!\},\\
M_2 &= \{\!\{0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 1,\ 3,\ 3\}\!\},\\
M_3 &= \{\!\{0,\ 0,\ 0,\ 1,\ 1,\ 1,\ 1,\ 2,\ 3\}\!\},\\
M_4 &= \{\!\{0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 2,\ 2,\ 3\}\!\},\\
M_5 &= \{\!\{0,\ 0,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 3\}\!\},\\
M_6 &= \{\!\{1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1\}\!\},
\end{aligned}$$

In this specific case, it holds that $\frac{2(2^k+1)}{3} = \frac{2\times 9}{3} = 6$. This implies that if a function has as spectrum M_1, M_2, M_3, M_5 or M_6, then it cannot be APN. The spectrum M_4 cannot be rule out. In practice, it is obtained for the six roots u of $X^6+X^4+X^3+X+1$ and the associated functions are in that case (CCZ-equivalent to) the Kim mapping, and therefore APN.

The functions considered in this example are quadratic cyclotomic mappings with respect to the subfield $\mathbb{F}_{2^{\frac{n}{2}}} \subset \mathbb{F}_{2^n}$, with n even. As detailed below and due to a recent result of Göloğlu [Göl23], no new APN functions can be found in this family. However, the previous results are more general and could hopefully lead to the finding of new APN functions outside of this specific family.

6.2 APN cyclotomic mappings of degree 2

As already mentioned, quadratic APN functions are relatively better understood than the general case. It is therefore interesting to look at this subcase in the context of cyclotomic mappings.

First of all, as already mentioned by Göloğlu [Göl15, p.264] in a less general case, quadratic cyclotomic mappings with respect to subfields can easily be characterized by refining Lemma 3.

Proposition 15 (Quadratic cyclotomic mappings w.r.t subfields)**.** *Let $\mathbb{F}_{2^k} \subset \mathbb{F}_{2^n}$. Let $d < 2^k - 1$. Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a quadratic cyclotomic mapping of exponent d with respect to $\mathbb{F}_{2^k}$. Then,* $\mathrm{wt}(d) \leq 2$. *Furthermore if $d = 2^{e_1} + 2^{e_2}$, $e_1 \neq e_2$ then F is of the form:*

$$F\colon x \mapsto \sum_{i=0}^{\ell-1}\sum_{j=0}^{\ell-1} \lambda_{i,j} x^{2^{ki+e_1}+2^{kj+e_2}}, \qquad \text{for some } \lambda_{i,j} \in \mathbb{F}_{2^n}.$$

Proof. Let $(2^k-1)s+d = 2^u+2^v$ be an exponent of weight exactly 2, which appears in the univariate form of F. By Lemma 3 we get $d \equiv 2^{u'}+2^{v'} \bmod 2^k-1$ where u', v' are the Euclidean remainders of u and v modulo k. If $u'=v'=k-1$ then $d \equiv 2^k \equiv 1 \bmod 2^k-1$ and therefore $d=1$. Otherwise, $2^{u'}+2^{v'} < 2^k-1$ and $d=2^{u'}+2^{v'}$ which is of weight at most 2.

In the case where $\mathrm{wt}(d)=2$, F does not contain any linear monomial x^{2^w} as it would imply $d=2^{w'}$ (where $w' \equiv w \bmod k$), which is a contradiction. Furthermore $F(0)=0$ so all monomials of F have degree exactly 2. In that case, for any term $x^{2^u+2^v}$ in F, we get $d \equiv 2^{u'}+2^{v'} \bmod 2^k-1$ with $u' \neq v'$ (otherwise $\mathrm{wt}(d)=1$, which is excluded). Since $2^{u'}+2^{v'} < 2^k-1$, we deduce $2^{e_1}+2^{e_2} := d = 2^{u'}+2^{v'}$. This means that there exist i,j such that $\{u,v\} = \{ki+e_1, kj+e_2\}$. But u,v are such that $2^u+2^v < 2^{\ell k}-1$ so necessarily $i,j \in [\![0,\ell-1]\!]$. □

Lemma 12 implies that the case where $\mathrm{wt}(d)=1$ is not interesting if we are looking for APN cyclotomic mappings, as $x \mapsto x^d$ is linear in that case. When $\mathrm{wt}(d)=2$, we can always write $d=2^a(2^s+1)$ but a can be arbitrarily set to 0. Indeed, $F = x^{2^a(2^s+1)}P(x^{2^k-1})$ is APN if and only if the linearly-equivalent cyclotomic mapping $F(x^{2^{n-a}}) = x^{2^s+1}Q(x^{2^k-1})$ is APN where $Q = P(x^{2^{n-a}})$. We then deduce the following corollary.

Corollary 9 (Quadratic APN cyclotomic mappings and Gold exponents)**.** *Studying APN cyclotomic mappings whose exponent is a Gold exponent over $\mathbb{F}_{2^k}$ $d=2^s+1$, $\gcd(s,k)=1$ is sufficient to study quadratic APN cyclotomic mappings with respect to $\mathbb{F}_{2^k}$.*

For even n, the family of quadratic cyclotomic mappings with respect to $\mathbb{F}_{2^{\frac{n}{2}}}$, described in Proposition 15, has already received a lot of attention [Göl15, Car15, BHLS17, LLHQ21, CL21, Göl23]. As shown in Proposition 15, they also include the so-called "Kim-type" functions introduced by Carlet in [Car15, Section 3.7] who raised the question of the existence of APN functions in this family.

Most notably, the list of all quadratic APN cyclotomic mappings w.r.t $\mathbb{F}_{2^{\frac{n}{2}}}$, n even, is now known to be complete. Cyclotomic mappings of exponent 3 are all affine-equivalent to either x^3 or $x^{2^{k-1}+1}$ [CL21, LLHQ21], and thus never CCZ-equivalent to a permutation [GL20]. The general case, with exponent $d=2^s+1$, has been recently classified by Göloğlu [Göl23], as he classified all APN $(2^s+1, 2^s+1)$-projective mappings, which coincide with quadratic cyclotomic mappings with respect to $\mathbb{F}_{2^{\frac{n}{2}}}$ (see Proposition 2). His result shows that a quadratic cyclotomic mapping with respect to the subfield $\mathbb{F}_{2^k} \subset \mathbb{F}_{2^n}$ where $n=2k$ is APN if and only if it is equivalent to some specific Gold mapping (depending on the parities of k and s) *except* when $n=6$, where it can also be equivalent to the Kim mapping.

This implies that there is no hope to find new APN functions over $\mathbb{F}_{2^n}$, n even, among the quadratic cyclotomic mappings w.r.t $\mathbb{F}_{2^{\frac{n}{2}}}$. However, some families presented in Tables 1 and 2 contain functions that are equivalent to cyclotomic mappings but not to Gold mappings. This is the case for instance of Families (LK23a) and (LK23b) in Table 2, which consist of quadratic cyclotomic mappings with respect to $\mathbb{F}_{2^{\frac{n}{3}}}$ for n divisible by 3. This also applies to more general biprojective mappings. Another interesting idea would be to try to build cyclotomic mappings $\mathbb{F}_{2^k} \subset \mathbb{F}_{2^{2k}}$, with non-quadratic APN exponents, corresponding to other APN monomial functions. The results that we just presented in this section open the door to new research directions as they are more general than the case $n=2k$, with F quadratic.

Similarly to Proposition 15, we provide the generic form of the polynomials corresponding to quadratic ℓ-variate projective mappings, based on the following lemma.

Lemma 13 (Quadratic multivariate functions)**.** *Let $F\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$ be quadratic. Then each multivariate monomial in the coordinates of F is of the form $X_i^{u_i}X_j^{u_j}$ with $i \neq j$ and $\mathrm{wt}(u_i)=\mathrm{wt}(u_j)=1$, or of the form $X_i^{u_i}$ with $\mathrm{wt}(u_i) \leq 2$.*

Proof. Let $(\alpha_1, \dots, \alpha_\ell)$ be an $\mathbb{F}_{2^k}$-basis of $\mathbb{F}_{2^n}$ with $n = \ell k$. Let us consider the linearly equivalent function $\widetilde{F}$ defined by:

$$\widetilde{F}(x) = \sum_{i=1}^{\ell} \alpha_i F_i(x_1, \dots, x_\ell),$$

for any $x = \sum_{i=1}^{\ell} \alpha_i x_i$. By construction, $F_i(x_1, \dots, x_\ell) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\beta_i F(x))$ for some β_i. The function $x \mapsto F(x)^{2^j}$ contains univariate monomials whose exponents are the ones of F multiplied by 2^j. This transformation does not change the Hamming weight of the exponents so $x \mapsto F(x)^{2^j}$ is of algebraic degree at most 2. Moreover, we observe that $(\sum_{i=1}^{\ell} \alpha_i x_i)^{2^a} = \sum_{i=1}^{\ell} \alpha_i^{2^a} x_i^{2^a}$, so a linear univariate monomial X^{2^a} can only produce multivariate monomials with a single variable, and whose exponent is of Hamming weight 1. Similarly, we observe that:

$$\left(\sum_{i=1}^{\ell} \alpha_i x_i\right)^{2^a+2^b} = \sum_{i,j=1}^{\ell} \alpha_i^{2^a} x_i^{2^a} \cdot \alpha_j^{2^b} x_j^{2^b},$$

so a quadratic univariate monomial $X^{2^a+2^b}$ only produces multivariate monomials $X_i^{2^a} X_j^{2^b}$ with $i \neq j$ or monomials $X_i^{2^a+2^b}$. □

As a direct consequence, we obtain the following proposition.

Proposition 16 (Quadratic ℓ-variate projective mappings)**.** *Let $F\colon \mathbb{F}_{2^k}^{\ell} \to \mathbb{F}_{2^k}^{\ell}$ be a quadratic ℓ-variate projective mappings. Then its exponents $(d_1, \dots, d_\ell)$ satisfy $\mathrm{wt}(d_i) \leq 2$ for all i. Moreover, in a homogeneous coordinate of exponent $2^s + 1$, only the terms $X_i X_j^{2^s}$ with $i \neq j$ and $X_i^{2^s+1}$ can appear. Most notably, the family of 2-variate projective mappings of exponents $(2^r + 1, 2^s + 1)$ with respect to $\mathbb{F}_{2^k}$ with algebraic degree 2 coincides with the family of $(2^r, 2^s)$-biprojective mappings defined in Definition 7.*

Propositions 15 and 16 then allow the search for new quadratic APN ℓ-variate projective mappings, $\ell > 2$, from their polynomial representations. We believe that this opens a promising direction for finding new APN mappings.

7 Conclusion

We have developed a methodology for studying linear self-equivalence of any vectorial Boolean function, regardless of whether it is represented as a univariate polynomial, or a multivariate polynomial over a Cartesian product of finite fields of characteristic 2. This enabled us to show that most known infinite families of quadratic APN functions are linearly equivalent to functions with highly structured linear self-equivalence, unlike for instance in the sporadic examples found in [BL22]. This begs the question: Is linear self-equivalence a side effect of the techniques used to find new infinite families of APN permutations, or is it an inherent property of (quadratic) APN functions?

Even if cyclotomic mappings and ℓ-variate projective mappings have been investigated for ℓ at most equal to 4, our results show that increasing the value of ℓ could be a direction worth exploring to find new APN functions.

Another direction that has received but a fraction of the attention of the community at this stage is that of non-quadratic functions. The differential properties of quadratic functions are inherently easier to study thanks to the affine nature of the derivatives in this case. Still, could the structure provided by self-linear equivalence give us the practical tools we need to provide meaningful results about such functions?

References

[AW07] Amir Akbary and Qiang Wang. On polynomials of the form $x^r f(x^{(q-1)/l})$. *International Journal of Mathematics and Mathematical Sciences*, 2007, 2007.

[BBL21] Christof Beierle, Marcus Brinkmann, and Gregor Leander. Linearly self-equivalent APN permutations in small dimension. *IEEE Transactions on Information Theory*, 67(7):4863–4875, 2021.

[BBMM08] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields and Their Applications*, 14(3):703–714, 2008.

[BBMM11] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. A few more quadratic APN functions. *Cryptography and Communications*, 3(1):43–53, 2011.

[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, 2011.

[BC08] Lilya Budaghyan and Claude Carlet. Classes of quadratic APN trinomials and hexanomials and related structures. *IEEE Transactions on Information Theory*, 54(5):2354–2357, 2008.

[BCC+20] Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S. Coulter, and Irene Villa. Constructing APN functions through isotopic shifts. *IEEE Transactions on Information Theory*, 66(8):5299–5309, 2020.

[BCC+22] Lilya Budaghyan, Marco Calderini, Claude Carlet, Diana Davidova, and Nikolay S. Kaleyski. On two fundamental problems on APN power functions. *IEEE Transactions on Information Theory*, 68(5):3389–3403, 2022.

[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.

[BCFL06] Lilya Budaghyan, Claude Carlet, Patrick Felke, and Gregor Leander. An infinite class of quadratic APN functions which are not equivalent to power mappings. In *2006 IEEE International Symposium on Information Theory*, pages 2637–2641, 2006.

[BCL06] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Another class of quadratic APN binomials over $\mathbb{F}_{2^n}$: the case n divisible by 4. Cryptology ePrint Archive, Report 2006/428, 2006.

[BCL08] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Transactions on Information Theory*, 54(9):4218–4229, 2008.

[BCL09a] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Constructing new APN functions from known ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.

[BCL09b] Lilya Budaghyan, Claude Carlet, and Gregor Leander. On a construction of quadratic APN functions. In *2009 IEEE Information Theory Workshop*, pages 374–378, 2009.

[BCV20] Lilya Budaghyan, Marco Calderini, and Irene Villa. On equivalence between known families of quadratic APN functions. *Finite Fields and Their Applications*, 66:101704, 2020.

[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 Their Appl.*, volume 518, pages 33–42. American Mathematical Society, 2010.

[BHK20] Lilya Budaghyan, Tor Helleseth, and Nikolay Kaleyski. A new family of APN quadrinomials. *IEEE Transactions on Information Theory*, 66(11):7081–7087, 2020.

[BHLS17] Lilya Budaghyan, Tor Helleseth, Nian Li, and Bo Sun. Some results on the known classes of quadratic APN functions. In Said El Hajji, Abderrahmane Nitaj, and El Mamoun Souidi, editors, *Codes, Cryptology and Information Security - C2SI 2017*, volume 10194 of *Lecture Notes in Computer Science*, pages 3–16. Springer, 2017.

[BIK23] Lilya Budaghyan, Ivana Ivkovic, and Nikolay S. Kaleyski. Triplicate functions. *Cryptography and Communications*, 15(1):35–83, 2023.

[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.

[BL22] Christof Beierle and Gregor Leander. New instances of quadratic APN functions. *IEEE Transactions on Information Theory*, 68(1):670–678, 2022.

[BPW23] Alexander Bors, Daniel Panario, and Qiang Wang. Functional graphs of generalized cyclotomic mappings of finite fields. arXiv 1108.1873, 2023.

[BW22] Alexander Bors and Qiang Wang. Generalized cyclotomic mappings: Switching between polynomial, cyclotomic, and wreath product form. *Communications in Mathematical Research*, 38(2):246–318, 2022.

[Car11] Claude Carlet. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. *Designs, Codes and Cryptography*, 59(1-3):89–109, 2011.

[Car15] Claude Carlet. Open questions on nonlinearity and on APN functions. In Çetin Kaya Koç, Sihem Mesnager, and Erkay Savaş, editors, *Arithmetic of Finite Fields*, pages 83–107, Cham, 2015. Springer International Publishing.

[CBC21] Marco Calderini, Lilya Budaghyan, and Claude Carlet. On known constructions of APN and AB functions and their relation to each other. *Rad Hrvatske akademije znanosti i umjetnosti. Matematičke znanosti*, 25:79–105, 2021.

[CC23] Li-An Chen and Robert S. Coulter. Bounds on the differential uniformity of the Wan-Lidl polynomials. *Cryptography and Communications*, 15(6):1069–1085, 2023.

[CCD00] Anne Canteaut, Pascale Charpin, and Hans Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbb{F}_{2^m}$, and crosscorrelation of maximum-length sequences. *SIAM J. Discret. Math.*, 13(1):105–138, 2000.

[CCP22] Anne Canteaut, Alain Couvreur, and Léo Perrin. Recovering or testing extended-affine equivalence. *IEEE Transactions on Information Theory*, 68(9):6187–6206, 2022.

[CCP24] Anne Canteaut, Alain Couvreur, and Léo Perrin. On the properties of the ortho-derivatives of quadratic functions. In *WCC 2024: The Thirteenth International Workshop on Coding and Cryptography*, pages 99–110, Perugia, Italy, June 2024. https://wcc2024.sites.dmi.unipg.it/WCC_proceedings.pdf.

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

[CHP17] Claude Carlet, Annelie Heuser, and Stjepan Picek. Trade-offs for s-boxes: Cryptographic properties and side-channel resilience. In Dieter Gollmann, Atsuko Miyaji, and Hiroaki Kikuchi, editors, *Applied Cryptography and Network Security - ACNS 2017*, volume 10355 of *Lecture Notes in Computer Science*, pages 393–414. Springer, 2017.

[CL21] Benjamin Chase and Petr Lisonek. Kim-type APN functions are affine equivalent to Gold functions. *Cryptography and Communications*, 13(6):981–993, 2021.

[CLV22] Marco Calderini, Kangquan Li, and Irene Villa. Two new families of bivariate APN functions. *arXiv preprint arXiv:2204.07462*, 2022.

[CP19] Anne Canteaut and Léo Perrin. On CCZ-equivalence, extended-affine equivalence, and function twisting. *Finite Fields and Their Applications*, 56:209–246, 2019.

[CPT19] Anne Canteaut, Léo Perrin, and Shizhu Tian. If a generalised butterfly is APN then it operates on 6 bits. *Cryptography and Communications*, 11(6):1147–1164, 2019.

[Cze20] Ingo Czerwinski. On the minimal value set size of APN functions. Cryptology ePrint Archive, Report 2020/705, 2020.

[Dil09] John Dillon. APN polynomials: an update. In *International Conference on Finite fields and applications - Fq9*, July 2009.

[Dob01] Hans Dobbertin. Almost perfect nonlinear power functions on GF(2^n): A new case for n divisible by 5. In Dieter Jungnickel and Harald Niederreiter, editors, *Finite Fields and Applications*, pages 113–121, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[EP09] Yves Edel and Alexander Pott. A new almost perfect nonlinear function which is not quadratic. *Adv. Math. Commun.*, 3(1):59–81, 2009.

[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.

[GK21] Faruk Göloğlu and Lukas Kölsch. Equivalences of biprojective almost perfect nonlinear functions. *arXiv preprint arXiv:2111.04197*, 2021.

[GL20] Faruk Göloğlu and Philippe Langevin. Almost perfect nonlinear families which are not equivalent to permutations. *Finite Fields and Their Applications*, 67:101707, 2020.

[Göl15] Faruk Göloğlu. Almost perfect nonlinear trinomials and hexanomials. *Finite Fields and Their Applications*, 33:258–282, 2015.

[Göl22] Faruk Göloğlu. Biprojective almost perfect nonlinear functions. *IEEE Transactions on Information Theory*, 68(7):4750–4760, 2022.

[Göl23] Faruk Göloğlu. Classification of (q, q)-biprojective APN functions. *IEEE Transactions on Information Theory*, 69(3):1988–1999, 2023.

[Her75] Israel Nathan Herstein. *Topics in algebra*. John Wiley & Sons, 1975.

[JKK+22] Jaeseong Jeong, Chang Heon Kim, Namhun Koo, Soonhak Kwon, and Sumin Lee. On cryptographic parameters of permutation polynomials of the form $x^r h(x^{(2^n-1)/d})$. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 105-A(8):1134–1146, 2022.

[KKK23] Lukas Kölsch, Björn Kriepke, and Gohar M. Kyureghyan. Image sets of perfectly nonlinear maps. *Designs, Codes and Cryptography*, 91(1):1–27, 2023.

[KZ21] Christian Kaspers and Yue Zhou. The number of almost perfect nonlinear functions grows exponentially. *J. Cryptol.*, 34(1):4, 2021.

[Lai07] Yann Laigle-Chapuy. Permutation polynomials and applications to coding theory. *Finite Fields and Their Applications*, 13(1):58–70, 2007.

[LK23] Kangquan Li and Nikolay Kaleyski. Two new infinite families of APN functions in trivariate form. *IEEE Transactions on Information Theory*, 2023.

[LLHQ21] Kangquan Li, Chunlei Li, Tor Helleseth, and Longjiang Qu. A complete characterization of the APN property of a class of quadrinomials. *IEEE Transactions on Information Theory*, 67(11):7535–7549, 2021.

[LN96] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1996.

[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.

[LZLQ22] Kangquan Li, Yue Zhou, Chunlei Li, and Longjiang Qu. Two new families of quadratic APN functions. *IEEE Transactions on Information Theory*, 68(7):4761–4769, 2022.

[MP13] Gary L. Mullen and Daniel Panario, editors. *Handbook of Finite Fields*. CRC Press, 2013.

[NK93] Kaisa Nyberg and Lars R. Knudsen. Provable security against differential cryptanalysis (rump session). In Ernest F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 566–574, Santa Barbara, CA, USA, August 16–20, 1993. Springer, Berlin, Heidelberg, Germany.

[NW05] Harald Niederreiter and Arne Winterhof. Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields. *Discret. Math.*, 295(1-3):161–171, 2005.

[Nyb91] Kaisa Nyberg. Perfect nonlinear S-boxes. In Donald W. Davies, editor, *EUROCRYPT'91*, volume 547 of *LNCS*, pages 378–386, Brighton, UK, April 8–11, 1991. Springer, Berlin, Heidelberg, Germany.

[Pot16] Alexander Pott. Almost perfect and planar functions. *Des. Codes Cryptogr.*, 78(1):141–195, 2016.

[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, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 93–122, Santa Barbara, CA, USA, August 14–18, 2016. Springer, Berlin, Heidelberg, Germany.

[Tan19] Hiroaki Taniguchi. On some quadratic APN functions. *Designs, Codes and Cryptography*, 87:1973–1983, 2019.

[Wan07] Qiang Wang. Cyclotomic mapping permutation polynomials over finite fields. In Solomon W. Golomb, Guang Gong, Tor Helleseth, and Hong-Yeop Song, editors, *Sequences, Subsequences, and Consequences*, pages 119–128, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[Wan17] Qiang Wang. A note on inverses of cyclotomic mapping permutation polynomials over finite fields. *Finite Fields and Their Applications*, 45:422–427, 2017.

[WL91] Daqing Wan and Rudolf Lidl. Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure. *Monatshefte für Mathematik*, 112:149–163, 1991.

[YKBL20] Yuyin Yu, Nikolay S. Kaleyski, Lilya Budaghyan, and Yongqiang Li. Classification of quadratic APN functions with coefficients in $\mathbb{F}_2$ for dimensions up to 9. *Finite Fields and Their Applications*, 68:101733, 2020.

[YP22] Yuyin Yu and Léo Perrin. Constructing more quadratic APN functions with the QAM method. *Cryptography and Communications*, 14(6):1359–1369, 2022.

[YWL14] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions. *Designs, Codes and Cryptography*, 73(2):587–600, 2014.

[ZKL+22] Lijing Zheng, Haibin Kan, Yanjun Li, Jie Peng, and Deng Tang. Constructing new APN functions through relative trace functions. *IEEE Transactions on Information Theory*, 68(11):7528–7537, 2022.

[ZP13] Yue Zhou and Alexander Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43–60, 2013.

[ZZ99] Yuliang Zheng and Xian-Mo Zhang. Plateaued functions. In Vijay Varadharajan and Yi Mu, editors, *Information and Communication Security - ICICS'99*, volume 1726 of *Lecture Notes in Computer Science*, pages 284–300. Springer, 1999.

A Infinite families of quadratic APN functions

The polynomial representations of the known infinite families of APN functions, together with the conditions on their parameters to actually be APN are presented in Tables 7 to 10. In the following, we provide more details on these conditions when they do not fit in the tables, but also on the precise references where these results were found.

In the following, for $n = \ell k$, we denote by $S_{\ell,k} = \frac{2^n-1}{2^k-1} = \sum_{i=0}^{\ell-1} 2^{ik}$.

(BCL08a). See [BCL08, Corollary 1].

(BCL08b). See [BCL08, Theorem 2].

(BCV20). See [BCV20, Lemma 3.17].

(BCL09a). See [BCL09a, Corollary 1] [BCL09b, Corollaries 3 & 4].

(BBMM11). See [BBMM11, Theorem 2.1].

(BCCCV20). See [BCC+20, Theorem VI.3 & Equation 16].

(BHK20). See [BHK20, Corollary 1].

(ZKLPT22). The conditions for this family of quadratic APN functions are numerous. We therefore recall the original statement by the authors.

Theorem 7 (Family (ZKLPT22))**.** *[ZKL+22, Theorem 2] Let $n = 2k$ with $k \geq 1$ odd. Let i be a positive integer such that $\gcd(n, i) = 1$. Let $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$ and $b, c \in \mathbb{F}_{2^n}$ such that $bc \neq 0$. Let $F_{i,s,a,b,c} \colon x \to a\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(cx^{2^s+1})$. If one of the following conditions is verified, then $F_{i,s,a,b,c}$ is APN over $\mathbb{F}_{2^n}$:*

1. *b is not a cube and:*
   (a) *$s = 3i$ and $\frac{c}{b^{2^{2i}-2^i+1}} \in \mathbb{F}_{2^k}^*$ or,*
   (b) *$s = k - 2i$ and $\frac{c^{2^{2i}}}{b^{2^i-1}} \in \mathbb{F}_{2^k}^*$ or,*
   (c) *$s = k + 2i$ and $cb^{2^i-1} \in \mathbb{F}_{2^k}^*$ or,*
   (d) *$i = 1$, $s = (k-2)^{-1} \bmod n$, and $\frac{c^{2^s-1}}{b^{2^{2s}}} \in \mathbb{F}_{2^k}^*$ or,*
   (e) *$s = k$ and $c \notin \mathbb{F}_{2^k}$*
2. *or, $s = n - i$ and $\frac{c^{2^i}}{b} \notin \mathbb{F}_{2^k}$.*

(LZLQ22a). See [LZLQ22, Theorem 6].

(LZLZ22b). See [LZLQ22, Theorem 5].

(ZP13). See [ZP13, Corrolary 2].

(T19). See [Tan19, Theorem 3].

(CBC21). See [CBC21, Theorem 6.2].

(G22a). See [Göl22, Theorem III.2 $\mathcal{F}_1$].

(G22b). See [Göl22, Theorem III.2 $\mathcal{F}_2$].

(GK21). See [GK21, Theorem 1].

(CLV22a). See [CLV22, Theorem 3].

(CLV22b). See [CLV22, Theorem 4].

(LK23a/b). The conditions for these two families of quadratic APN functions are too numerous for the table. We therefore recall the original statements by the authors.

Theorem 8 (Family (LK23a) [LK23, Theorem 1]). *Let* $\gcd(s,k)=1$ *and*

$$F\colon (x,y,z)\mapsto (x^{2^s+1}+x^{2^s}z+yz^{2^s}, x^{2^s}z+y^{2^s+1}, xy^{2^s}+y^{2^s}z+z^{2^s+1}).$$

Assume that the polynomials P_1,P_2,P_3 *have no root in* $\mathbb{F}_{2^k}$ *and* P_4 *have no root in* $\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$ *where* $q=2^s$ *and* P_1,P_2,P_3,P_4 *are defined by:*

$$\begin{aligned}
P_1 &= X^{q^2+q+1}+X+1,\\
P_2 &= X^{q^2+q+1}+X^{q^2}+1,\\
P_3 &= X^{q^2+q+1}+X^{q^2+1}+X^{q+1}+X+1\\
P_4 &= X^{q^2+q+1}+XY^{q^2+q}+XY^q+X^{q^2+q}+X^qY^{q^2}\\
&\quad +X^{q^2}Y+Y^{q^2+q+1}+Y^{q^2+q}+Y^{q^2}+Y^q+1.
\end{aligned}$$

Then F *is APN.*

Theorem 9 (Family (LK23b) [LK23, Theorem 9]). *Let* $\gcd(s,k)=1$ *and*

$$F\colon (x,y,z)\mapsto (x^{2^s+1}+xy^{2^s}+yz^{2^s}, xy^{2^s}+z^{2^s+1}, x^{2^s}z+y^{2^s+1}+y^{2^s}z).$$

Assume that the polynomials P_1,P_2,P_3 *have no root in* $\mathbb{F}_{2^k}$ *and* P_4 *have no root in* $\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$ *where* $q=2^s$ *and* P_1,P_2,P_3,P_4 *are defined by:*

$$\begin{aligned}
P_1 &= X^{q^2+q+1}+X^{q+1}+X^q+X+1,\\
P_2 &= X^{q^2+q+1}+X^{q^2}+1,\\
P_3 &= X^{q^2+q+1}+X+1,\\
P_4 &= X^{q^2+q+1}+X^{q+1}Y^{q^2}+XY^q+X^qY^{q^2}+X^{q^2}Y\\
&\quad +X^{q^2}+Y^{q^2+q+1}+Y^{q^2+1}+Y^{q^2+q}+Y^{q^2}+1.
\end{aligned}$$

Then F *is APN.*

ID	Functions	Conditions to be APN	References
(BCL08a)	$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$	**Field:** $n = 3k$ (*i.e.* $\ell = 3$), $k \geq 4$, $\gcd(3,k) = 1$ **Exponent:** $\gcd(s,n) = 1$ (Gold for $\mathbb{F}_{2^n}$) **Others:** $sk \equiv i \bmod 3, i \in \{1,2\}$, $\mathrm{ord}(a) = S_{3,k}$	[BCL08, BCFL06]
(BCL08b)	$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$	**Field:** $n = 4k$ (*i.e.* $\ell = 4$), $k \geq 3$, k odd (so $\gcd(4,k) = 1$) **Exponent:** $\gcd(s,n) = 1$ (Gold for $\mathbb{F}_{2^n}$) **Others:** $sk \equiv i \bmod 4, i \in \{1,3\}$, $\mathrm{ord}(a) = S_{4,k}$	[BCL08, BCL06]
(BCV20)	$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}$	**Field:** $n = 2k$. **Exponent:** $\gcd(s,k) = 1$ (Gold for $\mathbb{F}_{2^k}$) **Others:** $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, $X^{2^s+1} + bX^{2^s} + b^{2^k}X + 1$ has no root x s.t $x^{2^k+1} = 1$.	[BC08, BCV20]
(BCL09a)	$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$	$a \neq 0$	[BCL09a]
(BCL09b/c)	$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9 + a^6x^{18})$ $x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$	**Field:** $n = 3k$ **Exponent:** - **Others:** $a \neq 0$	[BCL09b]
(BBMM11)	$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$	**Field:** $n = 3k$, $\gcd(3,k) = 1$. **Exponent:** $\gcd(s,n) = 1$ (Gold for $\mathbb{F}_{2^n}$), $3 \mid (k+s)$ **Others:** a primitive in $\mathbb{F}_{2^n}$. $b, c \in \mathbb{F}_{2^k}, bc \neq 1$.	[BBMM11]

Table 7: Known infinite families of univariate quadratic APN functions over $\mathbb{F}_{2^n}$ (1/2). The Gold mappings are omitted.

ID	Functions	Conditions to be APN	References
(BCCCV20)	$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$	**Field:** $n = 3k$. **Exponent:**. **Others:** see [BCC+20, Theorem VI.3].	[BCC+20]
(BHK20)	$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$	**Field:** $n = 2k$, k odd, $3 \nmid k$. **Exponent:** If i is even, $s \in \left\{k-2,\ k,\ n-1,\ (k-2)^{-1} \bmod n\right\}$. If i odd, $s \in \left\{k+2, n-1, (k+2)^{-1} \bmod n\right\}$. **Others:** a of order 3.	[BHK20]
(ZKLPT22)	$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$	**Field:** $n = 2k$, k odd. **Exponent:** $\gcd(i, n) = 1$ **Others:** $a \notin \mathbb{F}_{2^k}, bc \neq 0$. i, s, b, c satisfy the conditions of Theorem 7.	[ZKL+22]
(LZLQ22a)	$L(x)^{2^k+1} + bx^{2^k+1}$	**Field:** $n = 3k$. **Exponent:** $\gcd(s, k) = 1$ (Gold for $\mathbb{F}_{2^k}$). **Others:** $a^{\frac{2^n-1}{2^k-1}} \neq 1$, $b \in \mathbb{F}_{2^k}^*$. $L\colon x \mapsto x^{2^{k+s}} + ax^{2^s} + x$ bijection over $\mathbb{F}_{2^n}$.	[LZLQ22]

Table 8: Known infinite families of univariate quadratic APN functions over $\mathbb{F}_{2^n}$ (2/2).

ID	Functions	Conditions to be APN	References
(ZP13)	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$	**Field:** $n = 2k$. k even. **Exponent:** $\gcd(s,k) = 1$ (Gold for $\mathbb{F}_{2^k}$), i even. **Others:** $a \in \mathbb{F}_{2^k}$ and non-cubic.	[ZP13]
(T19)	$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$	**Field:** $n = 2k$. $k \geq 2$. **Exponent:** $\gcd(s,k) = 1$ (Gold for $\mathbb{F}_{2^k}$). **Others:** $a \in \mathbb{F}_{2^k}, b \in \mathbb{F}_{2^k}^*$ such that $X^{2^s+1} + aX + b$ has no root in $\mathbb{F}_{2^k}$.	[Tan19]
(CBC21)	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^{s+k/2}}y^{2^{k/2}} + axy^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$	**Field:** $n = 2k$. k even. **Exponent:** $\gcd(s,k) = 1$ (Gold for $\mathbb{F}_{2^k}$), $s < \frac{k}{2}$. **Others:** $a, b \in \mathbb{F}_{2^k}$ such that $(bX^{2^s+1} + aX^{2^s} + 1)^{2^{k/2}+1} + X^{2^{k/2}+1}$ has no root in $\mathbb{F}_{2^k}$.	[CBC21]
(G22a)	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{2s}+1} + x^{2^{2s}}y + y^{2^{2s}+1} \end{pmatrix}$	**Field:** $n = 2k$ **Exponent:** $\gcd(3s,k) = 1$.	[Göl22]
(G22b)	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{3s}}y + xy^{2^{3s}} \end{pmatrix}$	**Field:** $n = 2k$, k odd. **Exponent:** $\gcd(3s,k) = 1$.	[Göl22]
(GK21)	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$	**Field:** $n = 2k$, $k \equiv 2 \bmod 4$. **Exponent:** $\gcd(s,k) = 1$. **Others:** $a \in \mathbb{F}_{2^{k/2}}^*$, $b \in \mathbb{F}_{2^k}$, b non-cubic such that $b^{2^s+2^{s+\frac{k}{2}}} \neq a^{2^s+1}$	[GK21]

Table 9: Known infinite families of multivariate quadratic APN functions over $\mathbb{F}_{2^n}$ (1/2).

ID	Functions	Conditions to be APN	References
(LZLQ22b)	$(x,y) \mapsto \begin{pmatrix} x^3+xy^2+y^3+xy \\ x^5+x^4y+y^5+xy+x^2y^2 \end{pmatrix}$	**Field:** $n=2k$, $\gcd(k,3)=1$.	[LZLQ22]
(CLV22a)	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1}+xy^{2^s}+ay^{2^s+1} \\ x^{2^{2s}+1}+ax^{2^{2s}}y+(1+a)^{2^s}xy^{2^{2s}}+ay^{2^{2s}+1} \end{pmatrix}$	**Field:** $n=2k$. **Exponent:** $\gcd(s,k)=1$. **Others:** $a \in \mathbb{F}_{2^k}$ s.t. $X^{2^s+1}+X+a$ has no root in $\mathbb{F}_{2^k}$.	[CLV22]
(CLV22b)	$(x,y) \mapsto \begin{pmatrix} x^3+xy+xy^2+ay^3 \\ x^5+xy+ax^2y^2+ax^4y+(1+a)^2xy^4+ay^5 \end{pmatrix}$	**Field:** $n=2k$. **Others:** $a \in \mathbb{F}_{2^k}$ s.t. X^3+X+a has no root in $\mathbb{F}_{2^k}$.	[CLV22]
(LK23a)	$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1}+x^{2^s}z+yz^{2^s} \\ x^{2^s}z+y^{2^s+1} \\ xy^{2^s}+y^{2^s}z+z^{2^s+1} \end{pmatrix}$	**Field:** $n=3k$. **Exponent:** $\gcd(s,k)=1$. **Others:** The polynomials of Theorem 8 have no root in $\mathbb{F}_{2^k}$ or $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.	[LK23]
(LK23b)	$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1}+xy^{2^s}+yz^{2^s} \\ xy^{2^s}+z^{2^s+1} \\ x^{2^s}z+y^{2^s+1}+y^{2^s}z \end{pmatrix}$	**Field:** $n=3k$. **Exponent:** $\gcd(s,k)=1$. **Others:** The polynomials of Theorem 9 have no root in $\mathbb{F}_{2^k}$ or $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.	[LK23]

Table 10: Known infinite families of multivariate quadratic APN functions over $\mathbb{F}_{2^n}$ (2/2).