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

Jules Baudrin[1,2], Anne Canteaut[2] and Léo Perrin[2]

[1] Université Paris-Saclay, UVSQ, CNRS, Laboratoire de mathématiques de Versailles, Versailles, France
name.surname@uvsq.fr
[2] Inria, Paris, France
name.surname@inria.fr

Abstract. The Kim mapping, which belongs to the only known CCZ-equivalence class in even dimension that contains an APN bijection, and the APN bijections in dimension 9 exhibited by Beierle and Leander in [BL22], all have a univariate representation corresponding to a *cyclotomic mapping* (aka Wan-Lidl polynomial), and they are all linearly-equivalent to functions with a highly-structured multivariate representation. In this paper, we show that functions having these properties, which correspond to multivariate projective mappings, i.e. multivariate functions whose coordinates are homogeneous, actually appear in the CCZ-equivalence classes of almost all known infinite families of APN functions. However, this behavior is not inherent to the APN property. Indeed, we prove that the vast majority of the known sporadic examples of APN functions in dimension 6 and 8, including almost all APN functions whose automorphism group is reduced to the automorphisms derived from their affine derivatives, are not CCZ-equivalent to an affinely self-equivalent function.

Keywords: APN functions · Differential uniformity · Linear equivalence · CCZ equivalence · Cyclotomic mappings · Multivariate projective mapping

1 Introduction

Since the introduction of differential uniformity in the early 1990s [NK93], the so-called *big APN problem* has remained open. Its formulation is deceptively simple: 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? A major breakthrough came in 2009 when Browning, Dillon, McQuistan, and Wolfe [BDMW10] discovered such a bijection in dimension 6. Known as the *Dillon permutation*, it remains to date the only known example (up to equivalence) of an APN bijection in even dimension. This result was obtained by starting from a quadratic APN function of $\mathbb{F}_{2^6}$, the so-called *Kim mapping* [Dil09], and then searching for a permutation within its *CCZ-equivalence* class [CCZ98]. Therefore, this result has motivated a significant line of research aimed at identifying new quadratic APN functions[1] over larger fields of even dimension, with the hope that some may be CCZ-equivalent to permutations.

A natural strategy has been to identify special properties of the Kim mapping:

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

[1] We actually know a *single* APN function (up to equivalence) which is neither CCZ-equivalent to a monomial nor to a quadratic function. This function operates on 6 bits and is known as the Brinkmann-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.

where u is a root of the primitive polynomial $X^6 + X^4 + X^3 + X + 1$. Many works have sought to identify (infinite families of) functions, exhibiting similar structural features. This line of research includes several APN constructions such as [Göl15, Car15, CL21], which are based on the specific form of the exponents in the univariate representation of κ. Indeed, it was already noted in [BDMW10] that this function could be expressed as $\kappa(x) = x^3 P(x^7)$, for $P(x) = ux^3 + x + 1$. This is then a special case of cyclotomic mappings [Wan07], aka Wan-Lidl polynomials [WL91]. Some other APN constructions inspired by Dillon's work, such as [PUB16, CDP17, FFW17, LTYW18, CPT19, Göl22, GK25, Göl23], rely on the structure of the bivariate representation of a function linearly equivalent to κ.

While following a different research direction based on computational classification techniques for *linearly self-equivalent APN mappings* [BBL21] for a small number of variables, Beierle and Leander [BL22] discovered two new quadratic APN bijections over $\mathbb{F}_{2^9}$, and have observed that the exponents in their univariate representations were also all congruent to 3 modulo 7. These functions were later shown [BCLP22] to be extended-affine equivalent to functions admitting highly-structured trivariate representations. Exploiting this trivariate representation led to the extension of these sporadic examples into two constructions of APN functions [LK23] that were recently generalized in wider trivariate APN families [GK26].

Surprisingly, this similarity was never explicitly exhibited and studied in a systematic manner. In this work, we first show that the fact that both the Kim mapping over $\mathbb{F}_{2^6}$ and of the APN bijections over $\mathbb{F}_{2^9}$ in [BL22] are linearly equivalent to functions with simple bivariate or trivariate representations, is a direct consequence of their univariate representation as cyclotomic mappings. More generally, most previously defined constructions, including most generalizations of the Kim mapping, correspond to *multivariate projective mappings*, that is, to functions $F\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$ with $n = \ell k$ having ℓ homogeneous coordinates. Moreover, we point out that this structure, which is equivalent to the existence of a CCZ-equivalent function having a very particular subgroup in its automorphism group, appears in almost all infinite families of APN functions that are known so far. However, this is not the case of the vast majority of the sporadic examples of APN functions obtained by computer search. In other words, the functions with this structure provide good candidates when searching for APN mappings, but the picture drawn by the obtained mappings is far from being representative of the general behavior of APN mappings.

We also bring to ligth the fact that being CCZ-equivalent to a cyclotomic mapping, or to a multivariate projective mapping, is a much stronger property than having automorphisms of a prescribed order, or with prescribed elementary divisors. Indeed, given a function F, detecting the existence of an EA- or CCZ-equivalent function G having a specific linear self-equivalence is a difficult question. This is related to the more general open problem raised by Beierle, Brinkmann and Leander [BBL21] on the existence of a linearly self-equivalent representative in the CCZ-equivalence class of any APN quadratic mapping. Here, we provide a negative answer to this question. Most notably, focusing on the APN functions whose automorphism group is reduced to the automorphisms derived from its affine derivatives, which is the case of the vast majority of the currently known APN functions, we provide a necessary condition for the existence of an affinely self-equivalent function within the corresponding CCZ-equivalence class, and we deduce that this situation rarely occurs.

Outline. In Section 2, we introduce the main definitions starting from homogeneity, which serves as the foundation for *cyclotomic*, *biprojective*, and *multivariate projective* mappings, to the self-equivalent nature of such functions. In Section 3, we establish that all members of almost all known infinite families of APN functions are CCZ-equivalent to a cyclotomic or multivariate projective mapping. Then in Section 4, we successively address the question of (dis)proving the existence of linear self-equivalent mappings in an

affine, extended-affine and CCZ-equivalence class. We conclude in Section 5 by outlining a number of open questions that arise throughout the paper.

2 Cyclotomic mappings, multivariate projective mappings and linearly self-equivalent mappings

2.1 Preliminaries

In this section, we recall some definitions and introduce the 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 $n \geq 0$ is denoted by $\mathrm{wt}(n)$ and the cardinality of a set X by $|X|$.

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 adjectives 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 $\pi_2 \circ F \circ \pi_1^{-1}$, 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.* an $\mathbb{F}_2$-vector space isomorphism. Handling several representations of the same functions will help provide 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 $P \in \mathbb{F}_{2^k}[X_1, \ldots, X_\ell]$ satisfying

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

with degree $d_i \leq 2^k - 1$ in each X_i.

The graph of a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is denoted by $\Gamma_F := \{(x, F(x)), x \in \mathbb{F}_2^n\}$. In order to study and classify vectorial Boolean functions in an effective manner we rely on the following equivalence relations.

Definition 1 (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 $G = B \circ F \circ A + C$, and

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

It is worth noting that affine bijections $\mathcal{A}$ from $\mathbb{F}_2^n \times \mathbb{F}_2^m$ to itself do not all lead to a CCZ-equivalent function: it must hold that $\mathcal{A}(\Gamma_F)$ is the graph of a function. When it is the case $\mathcal{A}$ is said to be *admissible* [CP19, Definition 4] for F.

2.2 Homogeneity

This section provides a detailed review of several properties that arise across different contexts and are often referred to using varying terminologies. These properties may be defined on different mathematical objects or representations, such as vectorial 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 $F\colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$. Our objective is to clarify the relationships and interdependencies between these notions, which are frequently used implicitly in the literature and have occasionally led to confusion (see Remark 3). Some of the results in this section are well-known but scattered across many papers. We thus prefer to recall them, and refer either to the initial proofs or to the ones in [Bau24, Chapter 6].

Many of these properties involve homogeneous functions in one way or another.

Definition 2 (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:

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

Remark 1. The functions defined in Definition 2 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:*

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

Example 1. Any homogeneous polynomial $P \in \mathbb{F}_{2^k}[X_1, \ldots, X_\ell]$ 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, $X_1^5 X_2^2 X_3^3 + X_1 X_2 X_3$ 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 examining 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 3, that these mappings play a major role in the known infinite families of APN functions.

Definition 3 (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:

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

or equivalently,

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

The fact that $c_\lambda = F(\lambda)$ is obtained by choosing $x = 1$ in the definition. Definition 3 equivalently means that F behaves on each coset of the subgroup $\mathbb{G}$ as the *fixed* monomial function $x \mapsto x^d$, up to a multiplicative constant.

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 3 because "order" can also refer to the order of the group, while "index" is also often overloaded. ▷

Example 2. 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 t divides $2^n - 1$, the cyclotomic mappings of exponent 0 with respect to the group $\mathbb{G}$ of cardinality $|\mathbb{G}| = t$ coincide with the so-called *t-divisible* mappings [KKK23], that is, functions that can be written as $x \mapsto P(x^t)$, for some P. ▷

Example 3. Let $\mathbb{F}_{2^k}$ be a subfield of $\mathbb{F}_{2^n}$. We observe for instance that the trace relative to $\mathbb{F}_{2^k}$, namely $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(x) = \sum_{i=0}^{\ell-1} x^{2^{ik}}$, 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 3 corresponding to the former and more restrictive definition of cyclotomic mappings given in [NW05]. ▷

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 and we always restrict ourselves to the nontrivial case where $\mathbb{G} \neq \{1\}$. 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 4 (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 2 (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 $i \not\equiv d \bmod |\mathbb{G}|$, $a_i = 0$.*

The polynomials described in Lemma 2 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].

While not explicitly mentioned, the case of quadratic cyclotomic mappings with respect to a subfield $\mathbb{F}_{2^k}$ has already attracted a lot of interest, especially when $k = \frac{n}{2}$ [CL21, LLHQ21, Car15, Göl23] or when $k = \frac{n}{3}$ [BL22, BCLP22]. In that case, Lemma 2 can be refined to obtain an explicit univariate form, as already mentioned by Göloğlu [Göl15, p.264] in a less general case.

Proposition 2 (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:*

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

The proof, which relies on explicitly determining the exponents of Hamming weight 2 of the univariate form, can be found *e.g.* in [Bau24, Proposition 6.82].

Example 4 (Kim-type mappings)**.** 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:

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

According to Proposition 2, this corresponds (up to a constant multiplication) to the subclass of quadratic cyclotomic mappings (defined over $\mathbb{F}_{2^{2k}}$) of exponent 3 with respect to $\mathbb{F}_{2^k}$ whose univariate form contains the monomial $X^{3\cdot 2^k}$. ▷

Remark 3 (Cyclotomic mappings and the subspace property). The previous example generalizes the Kim mapping exhibited in [BDMW10] which is indeed a quadratic cyclotomic mapping (of exponent 3 with respect to $\mathbb{F}_8$). Instead of this particular structure, Dillon *et al.* [BDMW10] highlight a related but *distinct* property, called the *subspace property*, which states that for all $\lambda \in \mathbb{F}_{2^n}$, the Kim mapping κ satisfies $\kappa(\lambda\mathbb{F}_{2^k}^*) = \kappa(\lambda)\mathbb{F}_{2^k}^*$, where $n = 6, k = 3$. In [Bau24, Section 6.1.6], this definition (generalized to any subgroup $\mathbb{G}$ of $\mathbb{F}_{2^n}^*$) is compared in detail with cyclotomic mappings, since these notions have often been mixed up in former works [Göl15]. ▷

Example 5 (The Beierle-Leander 9-bit APN bijections)**.** In [BL22], Beierle & Leander exhibited two quadratic APN bijections over $\mathbb{F}_{2^9}$ which are defined as:

$$F_0(x) = x^3 + u^2x^{10} + ux^{24} + u^4x^{80} + u^6x^{136}$$
$$F_1(x) = x^3 + ux^{10} + u^2x^{17} + u^4x^{80} + u^5x^{192}\,,$$

where $u \in \mathbb{F}_{2^9}$ is a root of $X^3 + X + 1$. Since all exponents in these two polynomials are congruent to 3 modulo $2^3 - 1$, they correspond to cyclotomic mappings of exponent 3 with respect to $\mathbb{F}_{2^3}$. ▷

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

2.4 Cyclotomic mappings with respect to a subfield

Among all subgroups of $\mathbb{F}_{2^n}^*$, the multiplicative groups of subfields, $\mathbb{F}_{2^k}^*$, play a particular role. For the sake of simplicity, cyclotomic mappings with respect to $\mathbb{F}_{2^k}^*$ (for some divisor k of n) 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 the following multivariate characterization of cyclotomy (see e.g. [Bau24, Lemma 6.17] for a proof).

Lemma 3 (Multivariate characterization)**.** *Let $n = \ell k$. Let $\pi_1, \pi_2 \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}^\ell$ be $\mathbb{F}_{2^k}$-linear bijections. 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 $\pi_2 \circ F \circ \pi_1^{-1}$. 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.*

It is worth noting that the previous lemma holds when π_1, π_2 are $\mathbb{F}_{2^k}$-linear, but *a priori* not if they are $\mathbb{F}_2$-linear. In other words, in most cases, this multivariate polynomial representation does not offer a straightforward criterion for determining whether a given mapping is linearly equivalent to a cyclotomic mapping. This issue will be investigated in Section 4.

Example 6 (The Beierle-Leander 9-bit APN bijections, continued)**.** The two quadratic APN bijections over $\mathbb{F}_{2^9}$ of [BL22] have been further studied in [BCLP22] where the authors present trivariate representations of these functions of the form

$$C_u \colon (\mathbb{F}_{2^3})^3 \to (\mathbb{F}_{2^3})^3, (x, y, z) \mapsto (x^3 + uy^2z, y^3 + uxz^2, z^3 + ux^2y)$$

for two distinct values of $u \in \mathbb{F}_{2^3} \setminus \{0, 1\}$. This corresponds to multivariate representations of cyclotomic mapping with respect to $\mathbb{F}_{2^{\frac{n}{3}}}$, as described in Lemma 3. ▷

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

Definition 5 (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 $a, b, c, d, e, f, g, h \in \mathbb{F}_{2^k}$.

The following proposition is a direct corollary of the multivariate characterization of cyclotomic mappings.

Proposition 3 (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 $\pi_2 \circ G \circ \pi_1^{-1}$, 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 $\pi_1, \pi_2 \colon \mathbb{F}_{2^{2k}} \to \mathbb{F}_{2^k}^2$ are $\mathbb{F}_{2^k}$-linear bijections.*

Proof. We observe that any (q, q)-biprojective mapping F has homogeneous components of exponent $q + 1$. By choosing two $\mathbb{F}_{2^k}$-bases (a_1, a_2) and (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:

$$\forall x, y \in \mathbb{F}_{2^k}, \quad G(a_1 x + a_2 y) = b_1 F_1(x, y) + b_2 F_2(x, y).$$

By construction, the function G is cyclotomic of exponent $q + 1$. With the mappings π_1, π_2 defined by $\pi_1(a_1 x + a_2 y) = (x, y)$ and $\pi_2(b_1 x + b_2 y) = (x, y)$ for all x, y, we obtain: $F = \pi_2 \circ G \circ \pi_1^{-1}$. □

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 4. 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 $\mathbb{F}_{2^{\frac{n}{2}}}$. 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 $F_1(x,y) = (x+\alpha y)^{2^r+1} + \beta y^{2^r+1}$.

The definition of biprojective mappings, that was introduced and studied by Göloğlu [Göl22, Göl23], is limited to functions with two quadratic homogeneous coordinates. The following natural generalization covers any number of coordinates of any algebraic degree, and in particular cyclotomic mappings with respect to subfields $\mathbb{F}_{2^k}$ for which $[\mathbb{F}_{2^n} : \mathbb{F}_{2^k}] > 2$.

Definition 6 (Multivariate 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-projective mapping* of exponents $(d_1, \dots, d_\ell)$ 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.

Multivariate projective mappings capture the previously defined notions of cyclotomic mappings and of biprojective mappings. An equivalent (up to naming convention) and as natural notion of "multiprojective map" has also been recently and independently proposed by Göloğlu & Kölsch recently [GK26].

Proposition 4. *Let ℓ, k, d, r, s be positive integers. Then:*

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

(ii) *The family of 2-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 presented in Definition 5.*

The first item is a rewriting of Lemma 3 while the second one is a direct consequence of the fact that the exponents $(d_1, \dots, d_\ell)$ of a *quadratic* ℓ-projective mappings must satisfy $\mathrm{wt}(d_i) \le 2$ for all i, and that the multivariate form of a homogeneous coordinate of exponent 2^s+1 can only contain the terms $X_i X_j^{2^s}$ with $i \neq j$ and $X_i^{2^s+1}$ in that case. This is for instance proven in [Bau24, Lemma 6.84].

2.5 Linearly self-equivalent mappings

The previously introduced multivariate projective mappings and in particular cyclotomic mappings correspond to a 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 mapping 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 $\mathbb{F}_2^n$ to itself, we denote by $\mathrm{diag}(A_1, \dots, A_\ell)$ the mapping from $(\mathbb{F}_2^n)^\ell$ to itself defined by:

$$\forall (x_1, \dots, x_\ell) \in (\mathbb{F}_2^n)^\ell, \quad \mathrm{diag}(A_1, \dots, A_\ell)(x_1, \dots, x_\ell) := (A_1(x_1), \dots, A_\ell(x_\ell)) \ .$$

Definition 7 (Automorphism group [CP19, BBL21])**.** Let $n = \ell k$, $k \ge 1$. 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 $\mathcal{A}$ from $\left(\mathbb{F}_{2^k}^\ell\right)^2$ to itself such that the graph of F, $\Gamma_F := \{(x, F(x)), x \in \mathbb{F}_{2^k}^\ell\}$, is invariant under $\mathcal{A}$.

We denote by $\mathrm{Aut}_{\mathrm{EA}}(F)$ (resp. $\mathrm{Aut}_{\mathrm{EL}}(F)$) the subgroup of $\mathrm{Aut}(F)$ composed of all automorphisms whose linear part is a *lower-triangular* 2×2 block matrix (resp. and whose

constant term is zero). Similarly, we denote by $\mathrm{Aut}_{\mathrm{Aff}}(F)$ (resp. $\mathrm{Aut}_{\mathrm{Lin}}(F)$) the subgroup of automorphisms whose linear part is a *diagonal* 2×2 block matrix (resp. and whose constant term is zero).

What we refer to as $\mathrm{Aut}_{\mathrm{Lin}}(F)$ is sometimes referred to as $\mathrm{Aut}_{\mathrm{LE}}(F)$ (see [CP19, BBL21], where LE stands for linear equivalence). We prefer the notation $\mathrm{Aut}_{\mathrm{Lin}}(F)$ which avoids the ambiguity between LE and EL. Our notation reflects the fact that F is respectively EA-, EL-, affinely, or linearly self-equivalent if and only if the corresponding subgroup $\mathrm{Aut}_{\mathrm{EA}}(F), \mathrm{Aut}_{\mathrm{EL}}(F), \mathrm{Aut}_{\mathrm{Aff}}(F)$ or $\mathrm{Aut}_{\mathrm{Lin}}(F)$ is non-trivial.

Definitions 3, 5 and 6 can then be restated as the existence of very-specific cyclic subgroups of $\mathrm{Aut}_{\mathrm{Lin}}(F)$, or equivalently as specific linearly self-equivalent mappings. In the following, $M_{\alpha,n}$ denotes the multiplication mapping $x \mapsto x\alpha$ defined from $\mathbb{F}_{2^n}$ to itself.

Proposition 5 (Cyclotomic and projective mappings in terms of linear self-equivalences)**.** *Let F be a function from $\mathbb{F}_{2^n}$ to itself and G be a function from $\mathbb{F}_{2^k}^\ell$ to itself. Let $\langle\alpha\rangle = \mathbb{G} < \mathbb{F}_{2^n}^*$ be a multiplicative subgroup generated by α and β be a primitive element of $\mathbb{F}_{2^k}$, $\langle\beta\rangle = \mathbb{F}_{2^k}^*$. Then:*

1. *F is cyclotomic of exponent d with respect to $\mathbb{G}$ if and only if*

$$\mathrm{diag}(M_{\alpha,n}, M_{\alpha^d,n}) \in \mathrm{Aut}_{\mathrm{Lin}}(F)\,.$$

2. *G is an ℓ-projective mapping of exponents $(d_1, \ldots, d_\ell)$ if and only if*

$$\mathrm{diag}(M_{\beta,k}, \ldots, M_{\beta,k}, M_{\beta^{d_1},k}, \ldots, M_{\beta^{d_\ell},k}) \in \mathrm{Aut}_{\mathrm{Lin}}(G)\,.$$

In particular, if one of the two previous items holds, then $\mathrm{Aut}_{\mathrm{Lin}}(F)$ or $\mathrm{Aut}_{\mathrm{Lin}}(G)$ admits a cyclic subgroup whose order divides $2^n - 1$.

These assertions rely on the fact that, if $\mathcal{A} \in \mathrm{Aut}_{\mathrm{Lin}}(F)$, then $\mathrm{Aut}_{\mathrm{Lin}}(F)$ necessarily admits $\langle\mathcal{A}\rangle$ as a subgroup.

As already hinted by the multiple examples provided in this section, it seems that numerous APN functions have cyclotomic mappings and more generally multivariate projective mappings within their CCZ-equivalence classes. These highly structured mappings actually correspond to convenient representatives of a CCZ-equivalence class, leading to a better understanding of symmetries of these functions. It is therefore tempting to find such a representative within an equivalence class if it exists, or to disprove its existence. This is the direction taken in the rest of the paper.

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

3.1 Main theorem

In the previous section, we clarified the relationships between many properties that have been, sometimes indirectly, used to study and construct examples of APN functions. In this section, we turn our attention to infinite families of quadratic APN functions. These functions have been introduced under various representations, either univariate or multivariate, as part of a (largely successful) effort to diversify the known instances of APN functions, as shown[3] in Tables 1 and 2. However the variety of the forms of the representatives of CCZ-equivalence classes complicates comparisons and hinders a better understanding of these families as a whole. In this section, we prove that almost all of

[3]The detailed constraints on the parameters of the families are given in Section A.

the CCZ-equivalence classes coming from the known infinite families actually contain linearly self-equivalent representatives that are highly structured and closely related, as they correspond to multivariate projective mappings, cyclotomic mappings or functions commuting with the Frobenius automorphism.

Theorem 1 (Infinite APN families and linear self-equivalence)**.** *Let us consider the 18 infinite APN families listed in Table 1. Then:*

(i) *For all families, except for Families (BCL09a/b/c) when n is odd, the listed representatives are linearly-equivalent to a cyclotomic, or a 2, 3 or 4-projective mapping.*

(ii) *When n is odd, the representatives for Families (BCL09a/b/c) are 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.

These 18 families account for the vast majority of the 21 infinite families of APN functions currently known[4] (to the best of our knowledge).

A lot of subcases of Theorem 1 were already pointed out in several previous papers such as [Car11, BBL21, CBC21, Göl22, GK25, BIK23, KKK23, GK26]. 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:

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

that is, functions that are linearly equivalent to a 2-projective mapping with exponents $(2, 2^{j-i}+1)$. Carlet also proved in [Car11, Section 4.2.1] that some 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 2, the works [GK25, 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.

Before detailing the proof of Theorem 1, we discuss a few questions raised by this result concerning these infinite families and APN functions in general. Firstly, Theorem 1 clearly highlights the relationships between the earliest APN power mappings, the subsequent APN cyclotomic mappings (which locally behave like power mappings) and, more recently, the multivariate APN projective mappings whose coordinates are homogeneous. In particular, it reveals strong structural properties shared by all these families, properties that have often been used implicitly but almost never formally mentioned. Therefore, this result provides a shared framework to encompass functions that were designed in very different manners and thus a way to study them *as a whole*. As an example, it could be beneficial to go further in the study of the intersections between families and for counting the number of known CCZ-equivalence classes of APN functions. Indeed, as demonstrated in [KZ21, KZ22, GK25], it is possible to study equivalences between biprojective mappings and therefore count the number of inequivalent functions within a family or between families. While [GK25, Remark 4.9] indicates that cyclotomic mappings with respect to $\mathbb{F}_{2^{\frac{n}{2}}}$ could be handled in the same way, Theorem 1 reinforces the interest of generalizing these results even further to ℓ-projective mappings where $\ell > 2$, so that (almost) all infinite families can be taken into account. Even considering ℓ-projective APN mappings with

[4] With the monomial families excluded.

Table 1: Known infinite families of quadratic APN functions.

ID / Ref.	Functions	Comment
(BCL08a) [BCL08]	$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$	cyclotomic
(BCL08b) [BCL08]	$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$	cyclotomic
(BCV20) [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
(BCL09a) [BCL09a]	$x^3 + a^{-1}\text{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$	cyclotomic / ($\sim_{\text{lin}}$) frob.
(BCL09b) [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.
(BCL09c) [BCL09b]	$x^3 + a^{-1}\text{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$	cyclotomic / ($\sim_{\text{lin}}$) frob.
(BBMM11) [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
(BCCCV20) [BCC+20]	$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$	cyclotomic
(BHK20) [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
(ZKLPT22) [ZKL+22]	$a\text{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\text{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$	$\sim_{\text{lin}}$ biprojective
(ZP13) [ZP13]	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$	$\sim_{\text{lin}}$ biprojective
(T19) [Tan19]	$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$	$\sim_{\text{lin}}$ biprojective
(CBC21) [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
(G22a) [Göl22]	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{2s}+1} + x^{2^{2s}}y + y^{2^{2s}+1} \end{pmatrix}$	biprojective
(G22b) [Göl22]	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{3s}}y + xy^{2^{3s}} \end{pmatrix}$	biprojective
(GK21) [GK25]	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$	biprojective
(CLV22a) [CLV22]	$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + ay^{2^s+1} \\ x^{2^{2s}+1} + ax^{2^{2s}}y + (1+a)^{2^s}xy^{2^{2s}} + ay^{2^{2s}+1} \end{pmatrix}$	biprojective
(GK26) [GK26]	$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{2^s}z + bx^{2^s}y + cx^{2^s}z \\ ay^{2^s+1} + z^{2^s}x + bz^{2^s}y + cx^{2^s}y \\ z^{2^s+1} + x^{2^s}y \end{pmatrix}$	3-projective $\sim_{\text{lin}}$ cyclotomic

The Gold mappings are omitted. The detailed descriptions are provided in Appendix A. "frob." refers to commutation with the Frobenius automorphism $x \mapsto x^2$.

Table 2: 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]

$\ell > 4$ seems to be of interest to try to find new families and introduce more variety in the known APN functions.

Secondly, it appears from the numerous examples of APN functions in dimension 8 found in [YWL14, BBL21, BL22, YP22, BLL+25] that most of known classes of APN functions are not CCZ-equivalent to cyclotomic mappings or multivariate projective mappings. Indeed, 7 out of 13 APN functions from the Banff list or 3,795,716 out of the 3,808,491 quadratic APN functions in dimension 8 found in [YWL14, BBL21, BL22, YP22, BLL+25] (see Theorem 6 in Section 4) have an automorphism group of order 2^n which implies that a CCZ-equivalent cyclotomic or multivariate projective mapping cannot exist in these cases, since 2^n has no odd divisor. It then follows that the known infinite families of APN mappings are extremely specific, and present many symmetries. Therefore, finding an infinite family of APN functions which are not CCZ-equivalent to multivariate projective mappings would be of major interest. Moreover, understanding whether the existence of a permutation within the CCZ-equivalence class of the Kim mapping is somehow related to the fact that it is a cyclotomic mapping, or whether this is a pure coincidence, may be helpful to confirm or disprove the existence of APN permutations in higher even dimensions.

3.2 Proof of Theorem 1

This section proves Theorem 1. We proceed case by case and start with the most obvious ones. While we mention representatives found in the linear equivalence classes of the original representatives, all the representatives that we exhibit below actually lie in the $\mathbb{F}_{2^k}$-linear equivalence class of the original representatives for some $k > 1$.

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 1, 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,
- (GK26) is $(2^s+1,\ 2^s+1,\ 2^s+1)$-projective,

all of them being multivariate projective mappings by construction. Note that Lemma 3 shows that (GK26) has 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. (2) 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. (2), 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. Thus, 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 $\mathbb{F}_2$, which equivalently means that it 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 Lemma 3, 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 that their 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 projective families as well. Indeed, by definition, $a \notin \mathbb{F}_{2^k}^*$ (see Table 4), 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 4), 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 $F(x) = x^3 + ax^{2^{s+i}+2^i} + a^2 x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$ 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 4. Let $\gamma \in \mathbb{F}_{2^n}$, $x \in \mathbb{F}_{2^n}$. Then it holds that:

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

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 are absent 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 4. While we identify some particular self-equivalences, some of the functions in these classes also have (linearly) self-equivalent representatives of other natures, see e.g. [BCL09b, Section II.B].

▷

Obviously, a natural open problem is to address the three families among the 22 known families of APN functions that are not captured by Theorem 1,

Problem 1. *Do the CCZ-equivalence classes of the three infinite APN families described in Table 2 contain multivariate projective mappings ?*

The next section details why solving this type of problem cannot be addressed in general with simple classical properties such as the order of the automorphism group of the function, or similarity invariants of the automorphisms.

4 On the (non-)existence of linearly self-equivalent mappings in a CCZ- or EA-equivalence class

As already noted, an immediate corollary of Theorem 1 is that APN functions belonging to almost all infinite families admits a cyclic automorphism subgroup $\mathbb{G}$ of order[5] dividing $2^n - 1$. However, we will show in the following that the existence of such a subgroup of $\mathrm{Aut}(F)$ does not guarantee that F is CCZ-equivalent to a cyclotomic or multivariate projective mapping, or even to a linearly self-equivalent mapping. This question is related to the following more general problem, raised by Beierle, Brinkmann and Leander, both for quadratic functions, and for APN functions.

Problem 2 (Adapted from [BBL21, Section 3.1])**.** *For a quadratic (resp. APN) function F with a non-trivial automorphism in $\mathrm{Aut}(F)$, does there always exist a CCZ-equivalent function G with a non-trivial automorphism in $\mathrm{Aut}_{\mathrm{Lin}}(G)$?*

This general question is motivated by the fact that all quadratic functions, as well as all known APN functions, have a non-trivial automorphism group. More precisely, all of them are CCZ-equivalent to an extended-linear self-equivalent function. Indeed, all but one of the known APN CCZ-equivalence classes contain either a power mapping which linearly self-equivalent, or a quadratic function which is always EA self-equivalent [BBMN11, Proposition 1], and even *extended-linear* self-equivalent if $F(0) = 0$ [KZ21, Proposition 2.2]. This is due to the existence of an affine derivative $D_a F(x) \coloneqq F(x) + F(x + a)$ is equivalent to the existence of an EA self-equivalence $B \circ F \circ A + C = F$, where $A = B = \mathrm{Id}_n$. The only known exception is the CCZ-equivalence class of the Brinkmann-Leander-Edel-Pott [BL08, EP09] cubic mapping for $n = 6$, which is neither equivalent to a monomial nor to a quadratic mapping but which is known to admit a representative with 8 affine derivatives and is therefore EA self-equivalent.

In the following, through the study of $\mathrm{Aut}(F)$, we analyze if there exists in the linear, EA- or CCZ-equivalence class of F, a linearly self-equivalent function G, i.e., such that $\mathrm{Aut}_{\mathrm{Lin}}(G) \neq \{\mathrm{Id}\}$. This in particular enables us to provide a negative answer to Problem 2.

4.1 Linearly self-equivalent mappings up to equivalence

In the following, we denote by $\sim$ the similarity relation for endomorphisms and for any affine map A, we denote by L_A its linear part defined by $L_A = A + A(0)$. Calligraphic letters will be reserved for affine maps over $(\mathbb{F}_2^n)^2$. Let us consider two CCZ-equivalent functions F and G from $\mathbb{F}_2^n$ to itself, i.e., there exists an admissible mapping $\mathcal{A}$ over $\mathbb{F}_2^{2n}$ such that $\mathcal{A}(\Gamma_F) = \Gamma_G$. In that case, it is well-known that $\mathrm{Aut}(G) = \mathcal{A}\mathrm{Aut}(F)\mathcal{A}^{-1}$. Therefore, if F is linearly self-equivalent, then G is CCZ self-equivalent and satisfies

$$\mathcal{A}^{-1} \circ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \circ \mathcal{A}(\Gamma_G) = \Gamma_G \,, \tag{3}$$

for some linear bijections A, B. Recall from Definition 7 that extended-affine equivalence corresponds to CCZ equivalence restricted to affine mappings $\mathcal{A}$ whose linear part $\mathcal{L}$ is a lower-triangular block matrix. Such triangular mappings are often called EL-mappings [CP19, Definition 3] (or EA-mapping in the affine case). Similarly, affine equivalence corresponds to CCZ equivalence restricted to affine mappings whose linear part is a diagonal block matrix.

The following simple proposition characterizes the existence of a linearly (and even affinely) self-equivalent function in an affine equivalence class.

[5] In the case of mappings commuting with the Frobenius automorphism, this subgroup is instead of order n.

Proposition 6 (Affine self-equivalence and affine equivalence)**.** *Let* $F, G\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ *be two affine equivalent functions,* i.e. *there exists* $\mathcal{A}\colon (x,y) \mapsto \begin{pmatrix} C & 0 \\ 0 & D \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}$ *such that* $\mathcal{A}(\Gamma_F) = \Gamma_G$ *where* C, D *are linear bijections over* $\mathbb{F}_2^n$ *and* $(c,d) \in (\mathbb{F}_2^n)^2$*. Then,* $\mathrm{Aut}_{\mathrm{Aff}}(G) = \mathcal{A}\mathrm{Aut}_{\mathrm{Aff}}(F)\mathcal{A}^{-1}$.

In particular, for any linear bijections A, B*, there exists* $\mathcal{B} \in \mathrm{Aut}_{\mathrm{Aff}}(F)$ *such that* $L_{\mathcal{B}} = \mathrm{diag}(A', B')$ *with* $A \sim A'$*,* $B \sim B'$ *if and only if there exists a function* H *in the affine equivalence class of* F*, such that* $\mathrm{diag}(A, B) \in \mathrm{Aut}_{\mathrm{Lin}}(H)$.

Proof. This is an immediate consequence of Equation (3), together with the facts that invertible block-diagonal matrices form a group and that any invertible block-diagonal mapping is admissible (as it corresponds to an affine equivalence). □

However, when it comes to an EA-equivalence class, an affine self-equivalence is no longer preserved and a priori becomes an EA self-equivalence.

Proposition 7 (Affine self-equivalence and EA-equivalence)**.** *Let* F, G *be two EA-equivalent functions,* i.e. *there exists an EA-mapping* $\mathcal{A}$ *such that* $\mathcal{A}(\Gamma_F) = \Gamma_G$*. Then,* $\mathrm{Aut}_{\mathrm{EA}}(G) = \mathcal{A}\mathrm{Aut}_{\mathrm{EA}}(F)\mathcal{A}^{-1}$.

In particular, if $\mathcal{B} \in \mathrm{Aut}_{\mathrm{Aff}}(F)$ *with* $L_{\mathcal{B}} = \mathrm{diag}(A, B)$ *for some linear bijections* A, B*, then there exists* $\mathcal{B}' \in \mathrm{Aut}_{\mathrm{EA}}(G)$ *with* $L_{\mathcal{B}'} = \begin{pmatrix} A' & 0 \\ C & B' \end{pmatrix}$ *for some* A', B', C *such that* $A' \sim A$ *and* $B' \sim B$.

Proof. This is again a consequence of the fact that invertible lower-triangular block matrices form a group and that conjugation within this group preserves the similarity classes of each of the diagonal blocks. □

More generally, determining whether a mapping F with a non-trivial automorphism $\mathcal{B}$ is in the same CCZ-equivalence class as a mapping G with a non-trivial group $\mathrm{Aut}_{\mathrm{Lin}}(G)$ is not obvious. While it is rather easy to know whether there exists some $\mathcal{A}$ such that $\mathcal{A} \circ \mathcal{B} \circ \mathcal{A}^{-1}$ has an appropriate block-diagonal form, it is much more difficult to determine whether some of these $\mathcal{A}$ are admissible for F. Otherwise, $\mathcal{A}(\Gamma_F)$ is not the graph of a function.

Before proceeding to more fine-grained results for the case of CCZ- and EA-equivalence classes, we start by identifying the similarity invariants of the mappings A and B in the case of cyclotomic and multivariate projective mappings. This provides an effective rephrasing of Proposition 6 which is better-suited to efficiently find such a representative in an affine equivalence class. These similarity invariants will also be valuable for studying CCZ- and EA-equivalence classes in Section 4.3.

4.2 Similarity invariants for cyclotomic and multivariate projective mappings

In the following, we denote by $\min(A)$ the *minimal polynomial* of any $\mathbb{F}_2$-linear endomorphism A. The minimal polynomial of any field element $\alpha \in \mathbb{F}_{2^n}$ is also denoted by $\min(\alpha)$ (despite the fact that they do no share all of their properties). The companion matrix of a monic polynomial $P \in \mathbb{F}_2[X]$ is denoted by $C(P)$.

To identify the automorphisms associated to cyclotomic or multivariate projective mappings, we rely on their *primary rational canonical form* and their *elementary divisors*. This is an alternative to the Frobenius normal form and invariant factors, used for instance in [BBL21]. By *canonical form*, we thus refer to the following well-known proposition.

Proposition 8 (Canonical form, elementary divisors [Her75, Page 308])**.** *Let* $A\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ *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* $\mathbb{F}_2^n$ *in which the matrix of* A *is of the form:*

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

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.*

4.2.1 The case of cyclotomic mappings

By Proposition 6, a function F is in the linear equivalence class of a cyclotomic mapping if and only if F admits a linear self-equivalence $B \circ F = F \circ A$ where $A \sim M_{\alpha,n}$ and $B \sim M_{\alpha^d,n}$. The elementary divisors of the multiplication by a constant are well-known and recalled in the following lemma, which can be proven in the same way as [MP13, pp. 311-312] or [Hou18, Theorem 1.14].

Lemma 4. *Let* $A\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ *be an* $\mathbb{F}_2$*-linear mapping. Then the following statements are equivalent:*

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

(ii) A *admits a single elementary divisor* P, *with multiplicity* $\frac{n}{\deg(P)}$, *and* P *is irreducible.*

(iii) A *is similar to* $M_{\alpha,n}$ *for some* $\alpha \in \mathbb{F}_{2^n}^*$.

Any triple (A, P, α) *for which equivalence holds satisfies* $\mathrm{ord}(A) = \mathrm{ord}(P) = \mathrm{ord}(\alpha)$.

Sketch proof. **(i)** $\Leftrightarrow$ **(ii)** is a direct consequence of Proposition 8. **(ii)** $\Leftrightarrow$ **(iii)** comes from the fact that for any $\alpha \in \mathbb{F}_{2^n}$, $M_{\alpha,n}$ can always be seen as $\mathrm{diag}(M_{\alpha,d}, \ldots, M_{\alpha,d})$ where $\mathbb{F}_{2^d} = \mathbb{F}_2(\alpha) \subset \mathbb{F}_{2^n}$. □

For cyclotomic mappings, Proposition 6 can thus be rephrased as follows.

Theorem 2. *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* $\mathrm{diag}(A, B) \in \mathrm{Aut}_{\mathrm{Lin}}(F)$ *such that* $\min A$ *and* $\min B$ *are irreducible polynomials,* $\mathrm{ord}(A) = |\mathbb{G}|$ *and* $\mathrm{ord}(B)$ *is a divisor of* $|\mathbb{G}|$.

In other words, any function F *satisfying* ***(ii)*** *admits a univariate cyclotomic representation, if the identifications between* $\mathbb{F}_2^n$ *and* $\mathbb{F}_{2^n}$ *are properly chosen.*

Proof. A mapping G is cyclotomic with respect to $\mathbb{G}$ if and only if it satisfies $M_{\alpha^d} \circ G = G \circ M_\alpha$ for some generator α of $\mathbb{G}$. This is then a direct consequence of Lemma 4 and of the fact that $\beta = \alpha^d$ if and only if $\beta \in \mathbb{G} \iff \mathrm{ord}(\beta) \mid |\mathbb{G}|$. □

Example 7 (Linearly self-equivalent APN bijections in dimension 8)**.** By classifying linearly self-equivalent APN permutations according to the Frobenius normal forms of the elements of $\mathrm{Aut}_{\mathrm{Lin}}(F)$, 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. $A = B = \mathrm{diag}(\mathrm{Id}_2, C(Q), C(Q), C(Q))$ with $Q(X) = X^2 + 1$.

The second case was recently proven to be impossible since $\mathrm{rank}(L_A + \mathrm{Id}) + \mathrm{rank}(L_B + \mathrm{Id})$ is too small in that case, see [BBF+25, Corollary 3 & Remark 1]. A direct consequence of Theorem 2 is that any linearly self-equivalent APN permutation in dimension 8, is necessarily a cyclotomic mapping of exponent $d = 1$ with respect to the subgroup $\mathbb{G} \subset \mathbb{F}_{2^4}^*$ of order 5, (up to linear-equivalence). Indeed, P is here an irreducible polynomial of degree 4 and order 5. The fact that $d = 1$ is obtained by choosing $\alpha = \beta$ which is a valid choice since any α, β such that $\mathrm{ord}(\alpha) = \mathrm{ord}(A)$ and $\mathrm{ord}(\beta) = \mathrm{ord}(B)$ are correct choices. ▷

4.2.2 The case of multivariate projective mappings

We now extend the previous characterization of cyclotomic mappings up to linear equivalence to the case of multivariate projective mappings. To do so, as a direct corollary of Lemma 4, we obtain the following characterization of the linear mappings that are similar to $\mathrm{diag}(M_{\beta_1,k}, \dots, M_{\beta_\ell,k})$.

Lemma 5. *Let $A \colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$ be an $\mathbb{F}_2$-linear mapping. Let $P_1, \dots, P_s$ be the distinct elementary divisors of A appearing with respective multiplicity $m_1, \dots, m_s$. Then A is similar to $\mathrm{diag}(M_{\beta_1,k}, \dots, M_{\beta_\ell,k})$ for some $\beta_1, \dots, \beta_\ell \in \mathbb{F}_{2^k}$ if and only if for any $1 \le i \le s$, P_i is irreducible, $\deg(P_i)$ divides k, and $\frac{k}{\deg(P_i)}$ divides m_i.*

Proof. ($\Longrightarrow$) Applying Lemma 4 ℓ times in parallel, we observe that the unique elementary divisor of each block $M_{\beta_i,k}$ is irreducible and its degree divides k. Furthermore $m_i = \frac{k}{\deg(P_i)} |\{j \in [\![1, s]\!] \text{ st. } \min(\beta_j) = \min(\beta_i)\}|$, implying the divisibility property.

($\Longleftarrow$) Conversely, because $\deg(P_i) \mid k$ and $\frac{k}{\deg(P_i)} \mid m_i$, the polynomials P_i's can be grouped in sets of $\frac{k}{\deg(P_i)}$, to form blocks of size k. The rest follows from Lemma 4. □

Theorem 3. *Let $n = \ell k$ and $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then, the following properties are equivalent:*

(i) *F is linearly-equivalent to an ℓ-variate projective mapping with respect to $\mathbb{F}_{2^k}$.*

(ii) *There exists $\mathrm{diag}(A, B) \in \mathrm{Aut}_{\mathrm{Lin}}(F)$ such that:*

- *$\min(A)$ is a primitive polynomial of degree k,*
- *$\min(B)$ is square-free, each of its irreducible factors P_i satisfies $\deg(P_i) \mid k$, and its multiplicity m_i as elementary divisor satisfies $\frac{k}{\deg(P_i)} \mid m_i$.*

Proof. The proof is identical to the proof of Theorem 2 by replacing the usage of Lemma 4 by Lemma 5 when it comes to B. □

Remark 5. As already observed, the cyclotomic case corresponds to a particular case of multivariate projective mappings. Indeed, it corresponds to the case where $\min(B)$ admits a single irreducible divisor. In that case, the divisibility conditions are redundant. ▷

When $(2^k - 1)$ is a prime number, we obtain a much simpler characterization of multivariate projective mappings with respect to $\mathbb{F}_{2^k}$.

Theorem 4. *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 is linearly-equivalent to a multivariate projective mapping with respect to $\mathbb{F}_{2^k}$.*

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

Proof. The implication **(i)** $\implies$ **(ii)** is already proven in Theorem 3, so we only prove **(ii)** $\implies$ **(i)**. Since there exists $\mathrm{diag}(A, B) \in \mathrm{Aut}_{\mathrm{Lin}}(F)$ with $\mathrm{ord}(A) = 2^k - 1$, the order of the subgroup of $\mathrm{Aut}_{\mathrm{Lin}}(F)$ 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.

The case $A' = \mathrm{Id}_n$. 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.

The case $B' = \mathrm{Id}_n$. If $B' = \mathrm{Id}_n$, then $F \circ A'(x) = F(x)$ where A' is a power of A, $A' = A^s$ with $0 < s < 2^k - 1$. Since $\min(A)$ is a primitive polynomial of degree k, A is similar to $M_{\alpha,n}$ for some generator α of $\mathbb{F}_{2^k}^*$, according to Lemma 4. Therefore A' is similar to $(M_{\alpha,n})^s = M_{\alpha^s,n}$. Because $\mathrm{ord}(M_{\alpha^s,n}) = 2^k - 1$ is a prime, α^s is also a primitive element of $\mathbb{F}_{2^k}$. As in the proof of Theorem 2, this implies that F is linearly-equivalent to a cyclotomic mapping of exponent 0, or equivalently to an ℓ-variate projective mapping of orders $(0, 0, \ldots, 0)$ with respect to $\mathbb{F}_{2^k}$.

The case $\mathrm{ord}(B') = 2^k - 1$. If $\mathrm{ord}(B') = 2^k - 1$ and $2^k - 1$ is an odd prime, then all cycles of B' have length 1 or $(2^k - 1)$. Under canonical form, this implies that each block $C(P)$ has order 1 or $2^k - 1$. It is well-known that $\mathrm{ord}(C(P)) = \mathrm{ord}(P)$ (*e.g.* [LN96, Lemma 8.26]) and that $\mathrm{ord}(P^e)$ with $e > 1$ is necessarily a composite number (*e.g.* [LN96, Theorem 3.8]). Therefore, the canonical form of B' is of the form $\mathrm{diag}(\mathrm{Id}_{sk}, C(P_1), C(P_2), \ldots, C(P_{\ell-s}))$ where all P_i are irreducible polynomials of the same order $(2^k - 1)$, and therefore of the same degree k. By applying Lemma 5 to the canonical form of B', we conclude that F is linearly-equivalent to an ℓ-variate projective mapping of exponents $(d_1, \ldots, d_\ell)$ with respect to $\mathbb{F}_{2^k}$ where the first s exponents are zero and the other ones are determined by the roots of the P_i's. □

Just as in the case of Theorem 2, Theorem 4 enables us to determine whether F is a multivariate projective mapping from the nature of its automorphisms in $\mathrm{Aut}_{\mathrm{Lin}}(F)$. Note that the condition on the dimension of $\langle \mathrm{Im}(F) \rangle$ is always satisfied by APN functions when $n > 2$, see for instance [PRKv26, Prop. 5.1].

Example 8 (Classes 51 & 55 of [BL22])**.** In their work [BL22], Beierle and Leander searched for linearly self-equivalent APN mappings over $\mathbb{F}_{2^8}$. To do so, the involved linear mappings (A, B) are chosen under Frobenius form, see [BL22, Lemma 2]. Once a pair (A, B) is fixed, they exhaustively searched for APN functions satisfying $B \circ F = F \circ A$. Among the found linearly self-equivalent APN mappings, some of them actually correspond to multivariate projective mappings. This is the case of the functions in the so-called Class 51 and Class 55. Indeed, for both classes, A is chosen as $A = M_{\alpha,n}$ for some generator α of $\mathbb{F}_4^*$ and therefore $\min(A)$ is irreducible by Lemma 4. Furthermore, because $2^2 - 1 = 3$ is prime, Theorem 4 states that F is linearly equivalent to a 4-variate projective mapping with respect to $\mathbb{F}_4$.

For instance, for Class 51, $B = \mathrm{diag}(\mathrm{Id}_2,\ C(X^3+1),\ C(X^3+1))$. As per Proposition 8, its canonical form is $B' = \mathrm{diag}(\mathrm{Id}_2,\ \mathrm{Id}_2,\ C(X^2+X+1),\ C(X^2+X+1))$. 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-projective mappings of exponents $(0, 0, 0, 1)$ with respect to $\mathbb{F}_4$. These sporadic examples might be extended to 4-variate infinite families, as it was done in [LK23] for the 3-variate APN functions found in [BL22, BCLP22]. ▷

4.3 Linear self-equivalences up to EA and CCZ-equivalences

The detection of cyclotomic and multivariate projective mappings in a linear equivalence class being completely handled in the previous section, we now address the cases of EA-

and CCZ-equivalences.

This is actually in line with Problem 2, i.e., the existence of a linearly self-equivalent mapping within the CCZ-equivalence class of any quadratic or APN function. Most notably, in this section, we prove that the question raised in Problem 2 does not have a positive answer for many APN functions.

We will also show that the study of linearly self-equivalent functions in a CCZ-equivalence class does not reduce to a mere study of elementary divisors. For instance, we identify a function in the Banff list [Dil09] whose automorphism group contains a cyclic subgroup of order 7 with elements all similar to $\mathrm{diag}(M_{\alpha,n}, M_{\alpha^d,n})$, but we can prove that no cyclotomic mapping exists in its CCZ-equivalence class.

4.3.1 Linearly self-equivalent mappings up to EA-equivalence

Let us fist recall from Definition 1 that an *EL-mapping* [CP19, Definition 3] is a bijective linear mapping of the form $\begin{pmatrix} A & 0 \\ C & B \end{pmatrix}$ where A and B are invertible. Equivalently, a bijective linear mapping is an EL-mapping if and only if the space $V = \{0\} \times \mathbb{F}_2^n$ is an invariant subspace of L, *i.e.* $L(V) = V$ [CP19, Lemma 1]. This characterization immediately implies the following lemma and proposition.

Lemma 6. *Let $\mathcal{L} = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix}$ be an EL-mapping. Then, there exists an EL-mapping $\mathcal{P}$ such that $\mathcal{P}\mathcal{L}\mathcal{P}^{-1} = \begin{pmatrix} A' & 0 \\ 0 & B' \end{pmatrix}$ if and only if $V = \{0\} \times \mathbb{F}_2^n$ admits an $\mathcal{L}$-invariant complement.*

Proof. A lower-triangular change of basis corresponds to changing from one complement of V to another. The matrix obtained is block-diagonal if and only if the chosen complement is $\mathcal{L}$-invariant. □

Proposition 9 (Affine self-equivalence up to EA-equivalence)**.** *Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $\mathcal{A} \in \mathrm{Aut}_{\mathrm{EA}}(F)$ where $L_{\mathcal{A}} = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix}$. Then the following assertions are equivalent:*

(i) *There exists an EA-mapping $\mathcal{P}$ such that $\mathcal{P}\mathcal{A}\mathcal{P}^{-1} \in \mathrm{Aut}_{\mathrm{Aff}}(G)$, where G is defined by the relation $\mathcal{P}(\Gamma_F) = \Gamma_G$.*

(ii) *$V = \{0\} \times \mathbb{F}_2^n$ admits an $L_{\mathcal{A}}$-invariant complement.*

(iii) *The equation $XA + BX = C$ admits a solution X.*

Proof. The equivalence **(i)** $\Leftrightarrow$ **(ii)** is a direct corollary of the previous lemma since the linear part of $\mathcal{P}\mathcal{A}\mathcal{P}^{-1}$ is $L_{\mathcal{P}}L_{\mathcal{A}}L_{\mathcal{P}}^{-1}$ which is an EL-mapping. The automorphism $\mathcal{P}\mathcal{A}\mathcal{P}^{-1}$ thus corresponds to an affine self-equivalence of G if and only if its linear part is block-diagonal.

Regarding the equivalence **(ii)** $\Leftrightarrow$ **(iii)**, we observe that if $L_{\mathcal{P}} = \begin{pmatrix} J & 0 \\ X & K \end{pmatrix}$, then

$$L_{\mathcal{P}}L_{\mathcal{A}}L_{\mathcal{P}}^{-1} = \begin{pmatrix} JAJ^{-1} & 0 \\ (XA + KC)J^{-1} + KBK^{-1}XJ^{-1} & KBK^{-1} \end{pmatrix}.$$

Since we are only interested in the block diagonal form (and not the actual values of the diagonal blocks), and because the conjugation by $\mathrm{diag}(J, K)$ preserves block diagonal mappings, we can assume without loss of generality that $L_{\mathcal{P}}$ is of the form $L_{\mathcal{P}} = \begin{pmatrix} \mathrm{Id}_n & 0 \\ X & \mathrm{Id}_n \end{pmatrix}$ and therefore that $L_{\mathcal{P}}L_{\mathcal{A}}L_{\mathcal{P}} = \begin{pmatrix} A & 0 \\ XA + C + BX & B \end{pmatrix}$. The bottom left-hand block is therefore zero if and only if $XA + BX = C$. □

Remark 6. Given an endomorphism $\mathcal{L}$ of $\mathbb{F}_2^{2n}$, the $\mathcal{L}$-invariant subspaces correspond to the $\mathbb{F}_2[\mathcal{L}]$-submodules of $\mathbb{F}_2^{2n}$ where the scalar multiplication $\mathbb{F}_2[\mathcal{L}] \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ is given by $(P, v) \mapsto P(\mathcal{L})(v)$, see *e.g.* [DF04, Sec.10.1, pp340-341]. The fact that some $\mathcal{L}$-invariant subspaces do not admit any $\mathcal{L}$-invariant complement is then equivalent to the fact that the basis-extension theorem does not hold in general for modules [DF04, Chapter 12]. ▷

In the case of EA-equivalence, the previous characterization provides an efficient computational answer to our problem: determining whether such a mapping $\mathcal{P}$ exists (and finding it if it is the case) boils down to solving the matrix equation $XA + BX = C$ for the unknown X, which corresponds to an affine system with n^2 binary unknowns. For $n \leq 9$, as relevant in the study of sporadic APN functions, such systems can be solved almost instantly on a personal computer.

When $L_{\mathcal{A}}$ is *semi-simple*, i.e., if $\min(L_{\mathcal{A}})$ is square-free, then the previous system always admits a solution. Indeed, it is well-known that the minimal polynomial of an endomorphism $\mathcal{L}$ is square-free if and only if any $\mathcal{L}$-invariant subspace admits an $\mathcal{L}$-invariant complement, see *e.g.* [HK71, Sec 7.5, Thm 11]. This sufficient condition is particularly important in our context since Theorems 2 and 3 state that cyclotomic and multivariate projective mappings admit semi-simple automorphisms.

Corollary 1. *Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $\mathcal{A} \in \mathrm{Aut}_{\mathrm{EA}}(F)$ such that $\min(L_{\mathcal{A}})$ is square-free. Then there exists an affinely self-equivalent function G in the EA-equivalence class of F.*

Example 9. Among the 13 representatives of quadratic APN functions in 6 variables, as given in the Banff list [Dil09], let us consider $F = a^7X^3+X^5+a^3X^9+a^4X^{10}+X^{17}+a^6X^{18}$, where a is a root of $X^6 + X^4 + X^3 + X + 1$. It can be computationally verified that this function admits 7 EL automorphisms, which thus form a cyclic subgroup of $\mathrm{Aut}(F)$. The elementary divisors of the 6 non-trivial ones are identical and equal to $P_1 = X^3 + X + 1$ and $P_2 = X^3 + X^2 + 1$, both with multiplicity two. Their minimal polynomial $\mu = P_1P_2$ is thus square-free, so Corollary 1 implies that F admits a linearly self-equivalent representative G in its EL-equivalence class. More precisely, G satisfies $B' \circ G = G \circ A'$ where $A' \sim B' \sim \begin{pmatrix} C(P_1) & 0 \\ 0 & C(P_2) \end{pmatrix}$. This is a consequence of the fact that the non-trivial EL-automorphisms of F are of the form $\mathcal{L} = \begin{pmatrix} A & 0 \\ \star & B \end{pmatrix}$ where $A \sim B \sim \begin{pmatrix} C(P_1) & 0 \\ 0 & C(P_2) \end{pmatrix}$ and that the conjugation of $\mathcal{L}$ by an EL mapping preserves the similarity classes of the diagonal blocks, as shown in the proof of Proposition 9. Moreover, it is worth noting that this EL mapping can always be chosen so that $A' = B'$. This implies that F does not admit any cyclotomic mapping with respect to $\mathbb{F}_{2^3}$ in its EL-equivalence class, since it would imply "exchanging" a block $C(P_1)$ of A with a block $C(P_2)$ of B (or the other way around) which is impossible with an EL change-of-basis. ▷

4.3.2 Linearly self-equivalent mappings up to CCZ-equivalence

The situation becomes more intricate with CCZ-equivalence. This clearly appears by comparing the function in the previous example, with another APN function of 6 variables, the so-called open butterfly [PUB16], which is affine-equivalent to Dillon's APN permutation and also has an automorphism whose diagonal blocks are both similar to $\mathrm{diag}(C(P_1), C(P_2))$. Indeed, this open butterfly is CCZ-equivalent to the Kim mapping, κ, which is cyclotomic of order 3 with respect to $\mathbb{F}_{2^3}$, and therefore satisfies $B \circ \kappa = \kappa \circ A$ with $A \sim \mathrm{diag}(C(P_1), C(P_1))$ and $B \sim \mathrm{diag}(C(P_2), C(P_2))$. On the other hand, the function from Example 9 does not admit any cyclotomic nor multivariate projective mapping in its CCZ equivalence class, as shown in the following proposition. This implies that the existence of a cyclic group of $\mathrm{Aut}(F)$ whose elements have their elementary divisors as described in Theorems 2 and 3, is not sufficient to claim that F is CCZ-equivalent to a cyclotomic or multivarivate projective mapping.

Proposition 10. *The APN function $F\colon \mathbb{F}_2^6 \to \mathbb{F}_2^6$ defined in Example 9 is such that* $\mathrm{Aut}(F)$ *contains a cyclic subgroup whose elements have their elementary divisors as described in Theorems 2 and 3, and its CCZ-equivalence class does not contain any a cyclotomic or multivarivate projective mapping.*

To prove this proposition, we recall the following results.

Lemma 7 ([CP19, Theorem 3])**.** *Let F, G be two CCZ-equivalent functions. Then G can be obtained from F by composing an EA-mapping, a t-twist, for some $0 < t \leq n$, and an EA-mapping, where a t-twist is defined by the following matrix*

$$\mathcal{T}_t = \begin{pmatrix} 0 & 0 & \mathrm{Id}_t & 0 \\ 0 & \mathrm{Id}_{n-t} & 0 & 0 \\ \mathrm{Id}_t & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathrm{Id}_{n-t} \end{pmatrix}.$$

Note that contrary to an EA-mapping, a t-twist may be not admissible for a given function F. It will also be convenient to observe that $\mathcal{T}_t$ is involutive. In the following, if the derivative of F with respect to s, namely $D_aF : x \mapsto F(x) + F(x+a)$, is affine, we denote by $\mathcal{D}_a^F$, the associated EA-automorphism of F, namely:

$$\begin{aligned} \mathcal{D}_a^F \coloneqq \mathbb{F}_2^n \times \mathbb{F}_2^n &\to \mathbb{F}_2^n \times \mathbb{F}_2^n \\ (x, y) &\mapsto (x + a, D_aF(x) + y)\ . \end{aligned}$$

By construction, the linear part of $\mathcal{D}_a^F$ is lower-triangular with Id_n as diagonal blocks and the matrix associated to $x \mapsto D_aF(x) + D_aF(0)$ as bottom left-hand block.

Proposition 11 ([KZ21, Proposition 2.3 & Lemma 2.4])**.** *Let $n \geq 4$. Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic function such that $F(0) = 0$. Then,*

$$\mathrm{Aut}(F) = \mathrm{Aut}_{\mathrm{EA}}(F) = \mathrm{Aut}_{\Delta}(F) \rtimes \mathrm{Aut}_{\mathrm{EL}}(F)\,,$$

where $\mathrm{Aut}_{\Delta}(F) \coloneqq \left\{\mathcal{D}_a^F, a \in \mathbb{F}_2^n\right\}$ is the subgroup derived from the affine derivatives of F.

Note that, since any automorphism of a quadratic APN function F is an EA-automorphism, we can always eliminate the constant term and assume that it is an EL-automorphism, at the cost of changing the representative in the EA-equivalence class.

Proof of Proposition 10. Let us consider the CCZ-equivalence class of $F = a^7X^3 + X^5 + a^3X^9 + a^4X^{10} + X^{17} + a^6X^{18}$ that is already presented in Example 9 and prove that there is no multivariate projective mapping in its CCZ-equivalence class. From Proposition 11, it is sufficient to consider the following automorphism in $\mathrm{Aut}_{\mathrm{Lin}}(G)$ where G is EL-equivalent to F:

$$\mathcal{L} = \begin{pmatrix} C(P_1) & 0 & 0 & 0 \\ 0 & C(P_2) & 0 & 0 \\ 0 & 0 & C(P_1) & 0 \\ 0 & 0 & 0 & C(P_2) \end{pmatrix}.$$

If there exists a multivariate projective mapping derived from $\mathcal{L}$ in the CCZ-equivalence class of F, then it is necessarily a cyclotomic mapping $\mathcal{L}'$ of the form described below and there must exist an admissible mapping $\mathcal{A}$ for G such that:

$$\mathcal{A} \times \mathcal{L} \times \mathcal{A}^{-1} = \begin{pmatrix} C(P_i) & 0 & 0 & 0 \\ 0 & C(P_i) & 0 & 0 \\ 0 & 0 & C(P_j) & 0 \\ 0 & 0 & 0 & C(P_j) \end{pmatrix} =: \mathcal{L}'\,,$$

with $\{i,j\} = \{1,2\}$. Since the unique fixed point of $\mathcal{L}$ is 0, $\mathcal{A}$ is necessarily linear because $\mathcal{A}\mathcal{L}\mathcal{A}^{-1}(0) = \mathcal{L}'(0) = 0$. Observe that $\mathcal{T}$ defined below is a particular solution $\mathcal{A}$ of the equation $\mathcal{A}\mathcal{L}\mathcal{A}^{-1} = \mathcal{L}'$:

$$\mathcal{T} = \begin{pmatrix} \mathrm{Id}_3 & 0 & 0 & 0 \\ 0 & 0 & \mathrm{Id}_3 & 0 \\ 0 & \mathrm{Id}_3 & 0 & 0 \\ 0 & 0 & 0 & \mathrm{Id}_3 \end{pmatrix}.$$

This implies that $\mathcal{A}\mathcal{L}\mathcal{A}^{-1} = \mathcal{L}'$ can be equivalently written as $\mathcal{A}\mathcal{T}^{-1}\mathcal{L}'\mathcal{T}\mathcal{A}^{-1} = \mathcal{L}'$, that means that $\mathcal{A}\mathcal{T}^{-1}$ commutes with $\mathcal{L}'$. The set of solutions $\mathcal{A}$ for $\mathcal{A}\mathcal{L}\mathcal{A}^{-1} = \mathcal{L}'$ is therefore $\mathrm{C}_{\mathbf{GL}_n(\mathbb{F}_2)}(\mathcal{L}')\mathcal{T}$, where the centralizer $\mathrm{C}_{\mathbf{GL}_{2n}(\mathbb{F}_2)}(\mathcal{L}')$ is the set of invertible matrices commuting with $\mathcal{L}'$. However, $\mathrm{C}_{\mathbf{GL}_{2n}(\mathbb{F}_2)}(\mathcal{L}')$ is only made of block diagonal matrices and we postpone the proof of this fact for the sake of clarity. Since any block diagonal mapping is admissible for any function, this implies that there exists an admissible mapping satisfying $\mathcal{A} \times \mathcal{L} \times \mathcal{A}^{-1} = \mathcal{L}'$ if and only if $\mathcal{T}$ is admissible for some function EA-equivalent to F, or equivalently that F is 3-twistable. However, it can be computationally verified that this is not the case by computing the thickness spectrum [CP19, Definition 9] of F, which thus proves that F is not CCZ-equivalent to any bivariate projective mapping.

We finish by proving that $\mathrm{C}_{\mathbf{GL}_{2n}(\mathbb{F}_2)}(\mathcal{L}')$ is indeed made of block diagonal matrices $\mathrm{diag}(A,B)$ (where each of the four $\frac{n}{2} \times \frac{n}{2}$ sub-blocks of A belongs to $\mathbb{F}_2[C(P_i)]$ and the sub-blocks of B belong to $\mathbb{F}_2[C(P_j)]$ with $j \neq i$). Indeed, for any $k \in \{1,2\}$, P_k is irreducible so it holds that $\mathrm{C}_{\mathbf{GL}_n(\mathbb{F}_2)}(C(P_k)) = \mathbb{F}_2[C(P_k)]$, see e.g. [HK71, Ex. 8 Sec 7.2]. Furthermore, since P_i and P_j are irreducible and distinct then the non-diagonal blocks are zero because $MC(P_i) = C(P_j)M$ if and only if $M = 0$. Indeed, $MC(P_i) = C(P_j)M$ implies that $MQ(C(P_i)) = Q(C(P_j))M$ for any polynomial Q. Choosing $Q = P_i$, we obtain $0 = P_i(C(P_j))M$. Finally, we observe that $P_i(C(P_j))$ is invertible since P_i and P_j are coprime and therefore $M = 0$. □

4.4 Linear self-equivalence and automorphims derived from affine derivates

In the following, we focus on automorphisms derived from affine derivatives. As already reported at the end of Section 3.1, the reason is that in the vast majority of the cases, the automorphism group of the known sporadic APN functions is often reduced to such automorphisms. We thus address the question of transforming an automorphism derived from an affine derivative $\mathcal{D} \in \mathrm{Aut}_\Delta(F)$ to a block-diagonal automorphism by conjugation with an admissible admissible for F. Proposition 9 implies that $\mathcal{D}$ cannot be transformed by conjugation by an EA-mapping to an automorphism whose linear part is block-diagonal, in the non-trivial cases where its lower-right part is non-zero. This implies that, for finding a block-diagonal automorphism associated to $\mathcal{D}$, it is necessary to look outside the initial EA-equivalence class. Because the existence of affine derivatives is preserved by EA-equivalence, we can then assume without loss of generality that the function F we consider admits such a derivative *and* that F is twist-equivalent to a function outside its EA-equivalence class. The following two lemmas will be useful.

Lemma 8. *Let $0 < t < n$. Let $\mathcal{T}_t, \mathcal{D}$ be the following $2n \times 2n$ matrices:*

$$\mathcal{T}_t = \begin{pmatrix} 0 & 0 & \mathrm{Id}_t & 0 \\ 0 & \mathrm{Id}_{n-t} & 0 & 0 \\ \mathrm{Id}_t & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathrm{Id}_{n-t} \end{pmatrix} \qquad D = \begin{pmatrix} \mathrm{Id}_t & 0 & 0 & 0 \\ 0 & \mathrm{Id}_{n-t} & 0 & 0 \\ C_1 & C_2 & \mathrm{Id}_t & 0 \\ C_3 & C_4 & 0 & \mathrm{Id}_{n-t} \end{pmatrix}.$$

Then

$$\mathcal{T}_t D \mathcal{T}_t = \begin{pmatrix} \mathrm{Id}_t & C_2 & C_1 & 0 \\ 0 & \mathrm{Id}_{n-t} & 0 & 0 \\ 0 & 0 & \mathrm{Id}_t & 0 \\ 0 & C_4 & C_3 & \mathrm{Id}_{n-t} \end{pmatrix}. \tag{4}$$

Lemma 9. *Let $0 < t < n$, and C be a $(n-t) \times t$ matrix, and $\mathcal{D}$ be the following matrix:*

$$\mathcal{D} = \begin{pmatrix} \mathrm{Id}_t & 0 \\ C & \mathrm{Id}_{n-t} \end{pmatrix}.$$

Then the elementary divisors of $\mathcal{D}$ are $X+1$ with multiplicity $\mu_1 = n - 2 \times \mathrm{rank}(C)$ and X^2+1 with multiplicity $\mu_2 = \mathrm{rank}(C)$.

Proof. D is involutive so its minimal polynomial is X^2+1 and its elementary divisors are therefore necessarily $X+1$ with some multiplicity μ_1 and X^2+1 with multiplicity μ_2. Because of the size of the associated companion blocks, it must hold that $\mu_1 + 2\mu_2 = n$. Furthermore, by a double-counting argument of the dimension of the fixed-points space, we get $\mu_1 + \mu_2 = \dim(\ker(C)) + n - t$. Indeed, $\mathcal{D}(x,y) = (x,y)$ if and only if $(x,y) \in \ker(C) \times \mathbb{F}_2^{n-t}$. This leads to the announced multiplicities. □

Using these two lemmas, we obtain the following characterization.

Proposition 12. *Let n be even. Let $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ that admits an affine derivative $D_a F$ of rank $n-1$ for some $a \in \mathbb{F}_2^n$. Let $\mathcal{D}_a^F \in \mathrm{Aut}_\Delta(F)$ be the corresponding automorphism. Let $\mathcal{T}_t$ be an admissible t-twist mapping. Then there exists an EA-mapping $\mathcal{P}$ such that $\mathcal{P}\mathcal{T}_t\mathcal{D}_a^F\mathcal{T}_t\mathcal{P}^{-1} \in \mathrm{Aut}_{\mathrm{Aff}}(G)$, where G is defined by $\mathcal{P}\mathcal{T}_t(\Gamma_F) = \Gamma_G$, if and only if*

$$t = \frac{n}{2} \quad \textit{and} \quad \mathcal{D}_a^F = \left(\begin{array}{cc|c} \mathrm{Id}_{n/2} & 0 & 0 \\ 0 & \mathrm{Id}_{n/2} & \\ \hline 0 & C_2 & \mathrm{Id}_n \\ C_3 & C_4 & \end{array}\right). \tag{5}$$

Proof. By Equation (4), $\mathcal{T}_t\mathcal{D}_a^F\mathcal{T}_t$ must satisfy $C_1 = 0$. Indeed, otherwise $\mathcal{T}_t\mathcal{D}_a^F\mathcal{T}_t$ would not be lower-triangular, and then for any EA-mapping $\mathcal{P}$, $\mathcal{P}(\mathcal{T}_t\mathcal{D}_a^F\mathcal{T}_t)\mathcal{P}^{-1}$ would not be lower-triangular, and in particular not block-diagonal. Furthermore, for $\mathcal{T}_t\mathcal{D}_a^F\mathcal{T}_t$ to become block-diagonal by conjugation with an EA-mapping $\mathcal{P}$, it is necessary that the elementary divisors of $\mathcal{T}_t\mathcal{D}_a^F\mathcal{T}_t$ (or equivalently of $\mathcal{D}_a^F$) are exactly the concatenation of the elementary divisors of the diagonal blocks of $\mathcal{T}_t\mathcal{D}_a^F\mathcal{T}_t$, namely of A, B defined as follows:

$$A = \begin{pmatrix} \mathrm{Id}_t & C_2 \\ 0 & \mathrm{Id}_{n-t} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} \mathrm{Id}_t & 0 \\ C_3 & \mathrm{Id}_{n-t} \end{pmatrix}.$$

By Lemma 9, since D_aF has rank $n-1$ the elementary divisors of $\mathcal{D}_a^F$ are X^2+1 with multiplicity $n-1$ and $X+1$ with multiplicity 2. For A and B (for which Lemma 9 also applies), the multiplicity of X^2+1 is upper-bounded by $\min(n-t, t)$ because $\mathrm{rank}(C_2)$ and $\mathrm{rank}(C_3)$ are both at most $\min(n-t,t) \leq \lfloor \frac{n}{2} \rfloor$. If $\mathrm{rank}(C_2)$ and $\mathrm{rank}(C_3)$ are both strictly less than $\lfloor \frac{n}{2} \rfloor$ then $\mathrm{rank}(C_2) + \mathrm{rank}(C_3) \leq n-2$, and the total multiplicity of X^2+1 is not reached. So either $\mathrm{rank}(C_2)$ or $\mathrm{rank}(C_3)$ is equal to $\lfloor \frac{n}{2} \rfloor$. This in particular implies that $\min(n-t,t) = \lfloor \frac{n}{2} \rfloor$ which is equivalent to $t = \frac{n}{2}$ since n is even.

Conversely, assume that Equation (5) holds. Since $t = \frac{n}{2}$, the blocks C_2, C_3 and C_4 are square matrices. Because D_aF has rank $n-1$, exactly one of C_2 or C_3 has full rank and is therefore invertible. According to Proposition 9, the existence of an EA-mapping $\mathcal{P} = \begin{pmatrix} \mathrm{Id}_n & 0 \\ X & \mathrm{Id}_n \end{pmatrix}$ such that $\mathcal{P}\mathcal{T}_t\mathcal{D}_a^F\mathcal{T}_t\mathcal{P}^{-1}$ is equivalent to the existence of a matrix X

such that

$$\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}\begin{pmatrix} I & C_2 \\ 0 & I \end{pmatrix}+\begin{pmatrix} I & 0 \\ C_3 & I \end{pmatrix}\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & C_4 \end{pmatrix} \iff \begin{cases} X_1C_2=0, \\ C_3X_1=0, \\ X_3C_2+C_3X_2=C_4 \end{cases}.$$

Let us assume that C_2 is invertible. In that case, $X_1C_2=0$ is equivalent to $X_1=0$ and $X_3C_2+C_3X_2=C_4$ to $X_3=(C_4+C_3X_2)C_2^{-1}$ which always admits a solution. We prove in the similar manner that a solution to the system always exists if C_3 is invertible. □

Remark 7. When n is odd, then we similarly prove that $\min(t,n-t)$ must be equal to $\frac{n-1}{2}$, which implies that $t\in\{\frac{n-1}{2},\frac{n+1}{2}\}$. We also deduce that $C_1=0$. However, the reciprocal statement seems less evident: if $t=\frac{n\pm1}{2}$, then both C_2 and C_3 must have full rank $\frac{n-1}{2}$ so that D_aF reaches rank $n-1$. If $t=\frac{n-1}{2}$, since C_2 has t rows and C_3 t columns, they respectively admit a left inverse and a right inverse and the same reasoning as for the even case applies. On the other hand, if $t=\frac{n+1}{2}$, the solvability of $X_3C_2+C_3X_2=C_4$ cannot be addressed generically. ▷

Based on Propositions 9 and 12 we deduce the following results.

Theorem 5 (Automorphisms of sporadic APN functions in dimension 6)**.**

(i) *Out of the 13 quadratic APN mappings in dimension 6, 6 correspond to CCZ-equivalence classes that do not contain any affinely self-equivalent mapping. They correspond to the quadratic APN functions satisfying* $\mathrm{Aut}(F)=\mathrm{Aut}_\Delta(F)$.

(ii) *For the 7 remaining ones, there exists a quadratic function F in the CCZ equivalence class such that* $\mathrm{Aut}_{\mathrm{EL}}(F)=\mathrm{Aut}_{\mathrm{Lin}}(F)\neq\{\mathrm{Id}\}$.

(iii) *Out of these 13 CCZ-equivalence classes, the class of the Kim mapping is the only one containing quadratic functions F for which there exists $\mathcal{D}_a^F\in\mathrm{Aut}_\Delta(F)$ and an admissible mapping $\mathcal{A}$ such that $\mathcal{A}\mathcal{D}_a^F\mathcal{A}^{-1}\in\mathrm{Aut}_{\mathrm{Aff}}(G)$, where G is defined by $\mathcal{A}(\Gamma_F)=\Gamma_G$.*

(iv) *The Brinkmann-Leander-Edel-Pott APN cubic [BL08, EP09] does not admit any affinely self-equivalent mapping in its CCZ equivalence class.*

Theorem 6 (Automorphisms of sporadic APN functions in dimension 8)**.**

(i) *Out of the 3,808,491 CCZ-equivalence classes of APN functions in dimension 8 found in [YWL14, BBL21, YP22, BL22, BLL+25],* $12,775$ *admit a quadratic representative such that* $\mathrm{Aut}_{\mathrm{EL}}(F)\neq\{\mathrm{Id}\}$. *Each of them correspond to a CCZ-equivalence class that contains a quadratic function G such that* $\mathrm{Aut}_{\mathrm{EL}}(G)=\mathrm{Aut}_{\mathrm{Lin}}(G)$.

(ii) *The remaining* $3,795,716$ *functions do not admit any affinely self-equivalent mapping in their CCZ-equivalence class.*

Proof. Since most of the automorphisms are automorphisms from $\mathrm{Aut}_\Delta(F)$, the previous theorem was mainly obtained by verifying that Proposition 12 does not hold, mainly because most of the APN functions are not $\frac{n}{2}$-twistable. Whenever there exist automorphisms outside $\mathrm{Aut}_\Delta(F)$, $\mathrm{Aut}_{\mathrm{EL}}(F)$ is computed. From there, we explore each EA-equivalence class within the CCZ-equivalence class of F using sboxU and derive $\mathrm{Aut}_{\mathrm{EL}}(G)=\mathcal{A}\mathrm{Aut}_{\mathrm{EL}}(F)\mathcal{A}^{-1}$ for some admissible mapping $\mathcal{A}$. We then verify for each automorphism if Item **(iii)** of Proposition 9 applies or not. □

The previous theorems thus provide an answer to the problem left open by Beierle, Brinkmann & Leander [BBL21]: a quadratic APN function F for which $\mathrm{Aut}(F)$ is non-trivial does not necessarily admit a CCZ-equivalent function G for which $\mathrm{Aut}_{\mathrm{Lin}}(G)$ is non-trivial.

However, the results reported above indicate that all of the investigated quadratic APN in dimensions 6 and 8 *for which* $\mathrm{Aut}_{\mathrm{EL}}(F)$ *is not trivial* do admit a quadratic representative G for which $\mathrm{Aut}_{\mathrm{EL}}(G) = \mathrm{Aut}_{\mathrm{Lin}}(G)$, that is, for which $\mathrm{Aut}_{\mathrm{EL}}(G)$ is entirely made of linear self-equivalences. For the vast majority of them, this is obvious since these APN functions were obtained in [BL22] and admit a linear self-equivalence of prime order by construction. We can computationally verify that they do not admit any other EL-automorphisms than the linear automorphisms present by design. Yet, there exist 46 classes for which this is not the case. Among them, $\mathrm{Aut}_{\mathrm{EL}}(F)$ is cyclic in 35 cases. While in that case the block-diagonalization of a generator is sufficient to provide a representative such that $\mathrm{Aut}_{\mathrm{EL}}(G) = \mathrm{Aut}_{\mathrm{Lin}}(G)$, there is *a priori* no known reason for this to happen. The cases of non-cyclic groups are even more intriguing. Their orders are $9, 9, 9, 12, 24, 24, 60, 180, 180, 2040, 2040$. Obviously, the two 2040 correspond to the non-cyclic automorphism groups of $x \mapsto x^3$ and $x \mapsto x^9$ which are generated by $\mathrm{diag}(M_\alpha, M_{\alpha^3})$ with α a primitive element of $\mathbb{F}_{2^n}^*$ and $\mathrm{diag}(\sigma, \sigma)$ where σ is the Frobenius mapping. The following restricted variant of Problem 2 then remains open.

Problem 3. *Let F be a quadratic APN function such that $\mathrm{Aut}_{\mathrm{EL}}(F) \neq \{\mathrm{Id}\}$. Does there always exist an EA-equivalent (and thus quadratic) function G such that $\mathrm{Aut}_{\mathrm{EL}}(G) = \mathrm{Aut}_{\mathrm{Lin}}(G)$.*

Concerning the very few $\frac{n}{2}$-twistable functions, we observe the following remarkable fact. In dimension 6, there exist exactly three $\frac{n}{2}$-twistable quadratic EA-equivalence classes. But, as reported by Item **(iii)** of Theorem 5, only one of them leads to the block-diagonalization of some automorphisms of $\mathrm{Aut}_{\Delta}(F)$, for a representative outside of the quadratic EA-equivalence class. This corresponds to the only case among the three where $\mathrm{Aut}_{\mathrm{EL}}(F)$ is also non-trivial. The same happens in dimension 8: we report four $\frac{n}{2}$-twistable quadratic EA-equivalence classes. Among them, two admit a non-trivial group $\mathrm{Aut}_{\mathrm{EL}}(F)$ and some elements of $\mathrm{Aut}_{\Delta}(F)$ can be become block-diagonal automorphism (outside of the EA-equivalence class), while the two others admit a trivial group $\mathrm{Aut}_{\mathrm{EL}}(F)$ and no element of $\mathrm{Aut}_{\Delta}(F)$ can be block-diagonalized. Whether this is a pure coincidence remains an open question. The case of the Kim mapping seems very specific. Indeed, the CCZ-equivalence class of the Kim mapping consists of 13 EA-equivalence classes, among which only two are obtained from the Kim mapping by a 3-twist [CP19, Cal20]. These two EA-equivalence classes both contain bijections. Therefore, any function G CCZ-equivalent to κ and having an automorphism in $\mathrm{Aut}_{\mathrm{Aff}}(G)$ conjugate to some $\mathcal{D} \in \mathrm{Aut}_{\Delta}(\kappa)$ is EA-equivalent to a bijection.

5 Open problems and conclusions

In this study, we have shown that, despite the diversity of the representations of the known infinite families of APN functions, their symmetries can be systematically understood through the lens of automorphism groups, which allows most of these families to be viewed as very specific instances of linear self-equivalences. We have also clarified that these symmetries, both within infinite families of APN functions and among some sporadic examples, are byproducts of the techniques used to construct these functions, rather than fundamental properties of (quadratic) APN functions themselves. However, even before these structures were explicitly identified, they had already led to many interesting results on APN functions. This observation clearly motivates further investigation in the following directions.

Quadratic APN cyclotomic mappings. While the case of quadratic APN cyclotomic mappings with respect to a subfield has been often studied in former works, it still deserves attention. First, it is clear that the exponent d of an APN cyclotomic mapping with respect to $\mathbb{F}_{2^k}$ must be such that $x \mapsto x^d$ is APN over $\mathbb{F}_{2^k}$ since if V is an invariant space of F, the restriction of F to V must be APN. Furthermore, as seen in Proposition 2, a quadratic cyclotomic mapping of exponent d with respect to a subfield must satisfy $\mathrm{wt}(d) \leq 2$. Together, with the previous observation, it implies that we can restrict ourselves to the APN Gold exponents.

For even n, 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 $x^{2^{\frac{n}{2}-1}+1}$ [CL21, LLHQ21] when $\frac{n}{2} > 3$, 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] (using the terminology detailed in Proposition 3), who has shown that a quadratic cyclotomic mapping with respect to $\mathbb{F}_{2^{\frac{n}{2}}}$ is APN if and only if it is equivalent to some specific Gold mappings (depending on the parities of $\frac{n}{2}$ and s where $d = 2^s + 1$) *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 Table 1 contain functions that are equivalent to cyclotomic mappings but not to Gold mappings. This is the case for instance of the two families from [LK23], that were recently generalized in [GK26], see (GK26) in Table 1, and which consist of quadratic cyclotomic mappings with respect to $\mathbb{F}_{2^{\frac{n}{3}}}$, and of Family (CBC21) which consists of quadratic cyclotomic mappings with respect to $\mathbb{F}_{2^{\frac{n}{4}}}$, for n divisible by 3 or 4, respectively.

Multivariate projective mappings for high ℓ. More generally, these constructions raise the question of searching for more quadratic APN cyclotomic mappings with respect to subfields $\mathbb{F}_{2^k}$ where $k < \frac{n}{2}$, but also quadratic APN ℓ-projective mappings for $\ell > 2$. Another interesting direction would be to try to define an infinite family by fixing the size of the subfield $\mathbb{F}_{2^k}$ and letting the number of branches ℓ tend to infinity.

Non-quadratic projective mappings. Among all open problems around APN functions, and due to the high number of quadratic examples, finding APN functions that are not CCZ-equivalent to a quadratic function is now yet-another Big APN problem. This tends to suggest that considering cyclotomic mappings with respect to subfields with exponents d corresponding to *non-quadratic* APN monomial functions is a direction worth investigating. Even though the properties of quadratic APN functions are inherently easier to study due to the affine nature of their derivatives, one may ask whether the structure induced by linear self-equivalence could serve as a practical tool for providing new results on non-quadratic APN 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.

[Bau24] Jules Baudrin. *Algebraic properties of symmetric ciphers and of their non-linear components*. PhD thesis, Sorbonne Université, December 2024. https://theses.hal.science/tel-05020635v2/file/140560_BAUDRIN_2024_archivage.pdf.

[BBF+25] Jules Baudrin, Christof Beierle, Patrick Felke, Gregor Leander, Patrick Neumann, Léo Perrin, and Lukas Stennes. Commutative cryptanalysis as a

generalization of differential cryptanalysis. *Designs, Codes and Cryptography*, 93(8):3243–3281, 2025.

[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.

[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.

[BCLP22] Christof Beierle, Claude Carlet, Gregor Leander, and Léo Perrin. A further study of quadratic APN permutations in dimension nine. *Finite Fields and Their Applications*, 81:102049, 2022.

[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.

[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.

[BLL+25] Christof Beierle, Philippe Langevin, Gregor Leander, Alexandr Polujan, and Shahram Rasoolzadeh. Millions of inequivalent quadratic APN functions in eight variables (version 1). https://doi.org/10.5281/zenodo.16752428, 2025.

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

[Cal20] Marco Calderini. On the EA-classes of known APN functions in small dimensions. *Cryptogr. Commun.*, 12:821–840, 2020.

[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.

[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.

[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.

[DF04] David Steven Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & sons, Hoboken, NJ, Third edition, 2004.

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

[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.

[GK25] Faruk Göloğlu and Lukas Kölsch. Equivalences of biprojective almost perfect nonlinear functions. *arXiv preprint arXiv:2111.04197*, 2025.

[GK26] Faruk Göloğlu and Lukas Kölsch. Triprojective almost perfect nonlinear permutations and functions, 2026.

[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.

[HK71] Kenneth Hoffman and Ray A. Kunze. *Linear Algebra*. Prentice-Hall Inc., Englewood Cliffs, New Jersey, second edition, 1971.

[Hou18] Xiang-dong Hou. *Lectures on Finite Fields*. Graduate Studies in Mathematics. American Mathematical Society, 2018.

[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.

[KZ22] Christian Kaspers and Yue Zhou. A lower bound on the number of inequivalent APN functions. *J. Comb. Theory A*, 186:105554, 2022.

[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.

[PRKv26] Enes Pasalic, René Rodríguez, Sadmir Kudin, and Ajla Šehović. On images, preimages and different notions related to APN mappings. In *Workshop on Coding and Cryptography - WCC 2026*, 2026.

[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.

[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.

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 4 and 5. In Table 3, we provide precise references where these results were found. We also detail below the conditions for Family (ZKLPT22) which do not fit in the tables.

Table 3: References for the known infinite families.

ID	Reference	ID	Reference
(BCL08a)	[BCL08, Corollary 1]	**(ZP13)**	[ZP13, Corollary 2]
(BCL08b)	[BCL08, Theorem 2]	**(T19)**	[Tan19, Theorem 3]
(BCV20)	[BCV20, Lemma 3.17]	**(CBC21)**	[CBC21, Theorem 6.2]
(BBMM11)	[BBMM11, Theorem 2.1]	**(G22b)**	[Göl22, Theorem III.2, $\mathcal{F}_2$]
(G22a)	[Göl22, Theorem III.2, $\mathcal{F}_1$]	**(GK21)**	[GK25, Theorem 1]
(BHK20)	[BHK20, Corollary 1]	**(CLV22a)**	[CLV22, Theorem 3]
(LZLQ22a)	[LZLQ22, Theorem 6]	**(CLV22b)**	[CLV22, Theorem 4]
(LZLQ22b)	[LZLQ22, Theorem 5]	**(GK26)**	[GK26, Theorem 1.3]
(BCL09a)	[BCL09a, Corollary 1] [BCL09b, Corollaries 3 & 4]	**(BCCCV20)**	[BCC+20, Theorem VI.3] [BCC+20, Equation 16]

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 $\frac{c^{2^i}}{b} \notin \mathbb{F}_{2^k}$.*

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:** $sk \equiv i \bmod 3, i \in \{1,2\}$, $\mathrm{ord}(a) = \frac{2^n-1}{2^k-1}$	[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:** $sk \equiv i \bmod 4, i \in \{1,3\}$, $\mathrm{ord}(a) = \frac{2^n-1}{2^k-1}$	[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]
(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]
(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]
(BCL09a)	$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$	$a \neq 0$	[BCL09a]

Table 4: 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
(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 $b^{2^s+2^{s+\frac{k}{2}}} \neq a^{2^s+1}$	[GK25]
(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]
(GK26)	$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{2^s}z + bx^{2^s}y + cx^{2^s}z \\ ay^{2^s+1} + z^{2^s}x + bz^{2^s}y + cx^{2^s}y \\ z^{2^s+1} + x^{2^s}y \end{pmatrix}$	**Field:** $n = 3k$. **Exponent:** $\gcd(s,k) = 1$. **Others:** $a \neq 0$ s.t. $aX2^{2s} + 2^s + 1 + bX^{2^s+1} + cX + 1$ has no root in $\mathbb{F}_{2^k}$	[GK26]

Table 5: Known infinite families of multivariate quadratic APN functions over $\mathbb{F}_{2^n}$.