

Extended biprojective APN functions

Nadiia Ichanska, Nikolay S. Kaleyski

University of Bergen

Abstract

Almost perfect nonlinear (APN) functions provide optimal resistance to differential cryptanalysis in characteristic two, and constructing new infinite families inequivalent to the known ones remains an important problem in the study of cryptographic functions. We introduce extended biprojective functions, obtained by augmenting biprojective polynomials with truncated trace terms, and establish a new infinite family of quadratic APN functions. To investigate these constructions, we develop an efficient APN test based on the ranks of binary matrices and employ it in exhaustive searches in dimensions up to 28. Using ortho-derivative differential spectra to distinguish CCZ-equivalence classes, we identify APN functions inequivalent to known families and uncover a systematic pattern across dimensions, leading to conjectures on further infinite families of quadratic APN functions.

1 Introduction

Substitution boxes (S-boxes), or vectorial Boolean functions used as the nonlinear components of block ciphers, and their cryptographic properties determine the resistance to various cryptanalytic attacks. In particular, resistance against differential cryptanalysis is measured by differential uniformity, which should be as low as possible. Over a field of characteristic two, the smallest possible differential uniformity is 2, and functions attaining this bound are called almost perfect nonlinear (APN) functions. They provide optimal resistance to differential cryptanalysis, and the construction of new infinite families of such functions remains a central problem in the theory of cryptographic Boolean functions.

In the companion work [27], we constructed an infinite family of APN functions in even dimension $n = 2m$, where m is odd and $3 \nmid m$, by perturbing the Budaghyan–Helleseht–Kaleyski (BHK) family with terms derived from the relative norm. The resulting functions were obtained from a known APN family by the switching construction. In this paper, we study a bivariate analogue of this construction which is no longer restricted to odd m .

Our starting point is the biprojective representation of the BHK family given by Göloğlu [25]. We perturb each of the two coordinates by a trace of the product xy , truncated according to the exponent of that coordinate. We call the resulting functions *extended biprojective functions*. This construction includes the Li–Zhou–Li–Qu family [31] as a particular case and leads to a new infinite family of APN functions.

More precisely, we consider the extended $(2, m - 1)$ -biprojective function $\mathcal{F}_1$ and prove that it is APN for every positive integer m such that $3 \nmid m$ (Theorem 5). When m is odd, we show that $\mathcal{F}_1$ is CCZ-equivalent to the univariate family F_1 constructed in [27] (Theorem 6). Thus, for odd m , the two constructions give the same CCZ-class. For even m , the construction of [27] is not defined, while the bivariate construction remains APN and CCZ-inequivalent to the known constructions.

The family $\mathcal{F}_1$ is closely related to the Li–Zhou–Li–Qu family, which we denote by $\mathcal{F}_0$. In particular, $\mathcal{F}_1$ is a switching neighbour of a function linearly equivalent to $\mathcal{F}_0$, where the switching term is the Boolean function $\text{tr}_1^m(xy)$. Moreover, $\mathcal{F}_0$ can be obtained by adding truncated trace terms to Göloğlu’s $(1, 2)$ -biprojective APN function. We extend this observation to Göloğlu’s $(s, 2s)$ -biprojective functions for every s : the extended Göloğlu function $\mathcal{G}_s$ and its switching neighbour $\mathcal{G}'_s$ generalize $\mathcal{F}_0 = \mathcal{G}_1$ and $\mathcal{F}_1 = \mathcal{G}'_1$ (Proposition 3).

We then investigate the APN property of extended biprojective functions computationally. For this purpose, we develop a faster APN test for quadratic functions of this form. For fixed coefficients, the derivative in a given direction is an $\mathbb{F}_2$ -linear map, and the matrix representing it depends $\mathbb{F}_2$ -linearly on the direction. Taking the directions in Gray-code order, each representing matrix differs from the previous one by a single matrix addition. The APN test then reduces to computing the ranks of binary matrices. The same matrices yield the ortho-derivative differential spectrum, the invariant by which we separate CCZ-classes.

Using this method, we first perform an exhaustive full-field search in dimension eight. The search recovers the Carlet and Li-Zhou-Li-Qu families and produces one additional ortho-derivative differential spectrum, namely that of $\mathcal{F}_1$, which coincides with the ortho-derivative differential spectrum of the univariate family F_1 from [27].

We further perform exhaustive searches in dimensions 10 to 28 with coefficients in the subfield $\mathbb{F}_2$ or $\mathbb{F}_4$. In every dimension up to 22, where the output was fully classified (its spectra computed), the APN functions found outside the Carlet family have exactly the $\varphi(m)$ ortho-derivative differential spectra of the functions $\mathcal{G}_s, \mathcal{G}'_s$ with $1 \leq s \leq (m-1)/2$ and $\gcd(s, m) = 1$. In dimensions 26 and 28, the APN functions found in the searches occur exactly for the exponent pairs corresponding to these constructions. For odd m , constructions $\mathcal{G}_{(m-1)/2}$ and $\mathcal{G}'_{(m-1)/2}$ have the ortho-derivative differential spectra of the conjectured families F_3 and F_2 of [27], which gives these families an alternative bivariate representation. The functions corresponding to $1 < s < (m-1)/2$ are new: they give new CCZ-classes of APN functions in dimensions 14, 16, and 20, and further candidates in dimensions 22 to 28. We conjecture that $\mathcal{G}_s$ and $\mathcal{G}'_s$ are APN whenever $3 \nmid m$ and $\gcd(s, m) = 1$.

To identify the functions we found, we computed the ortho-derivative differential spectra of all known infinite families of quadratic APN functions, to the best of our knowledge, in dimensions 8, 14, 16, and 20. Together with the classification available in dimension 10 [13, 27], this classifies the known families with respect to this invariant in every dimension $n = 2m \leq 20$ with $m \geq 4$ and $3 \nmid m$, that is, in every dimension up to 20 in which the functions $\mathcal{G}_s$ and $\mathcal{G}'_s$ are defined. The comparison also shows several coincidences between the ortho-derivative differential spectra of known families, which are described in Appendix A.2.

The remainder of the paper is organized as follows. Section 2 introduces the notation and recalls the necessary background, including algebraic degree, the bivariate representation, equivalence relations, the ortho-derivative, and the known infinite families of APN functions relevant to this work. Section 3 introduces $\mathcal{F}_1$, proves that it is an infinite APN family, and establishes its equivalence with the family of [27] for odd m . In Section 4, we study structural properties of extended biprojective functions, including necessary conditions for the APN property, normalization of the truncated-trace coefficients, the reduction of degenerate configurations to the Carlet family, and the switching relation between $\mathcal{G}_s$ and $\mathcal{G}'_s$. Section 5 describes the accelerated APN test, the reduction of the search space, and the computation of the ortho-derivative differential spectrum. Section 6 reports the exhaustive full-field searches, and Section 7 reports the subfield searches in dimensions 10 to 28 and the resulting new CCZ-classes. Section 8 collects the results across dimensions and states our conjectures, and Section 9 concludes the paper. Appendix A describes the instances of the known families and the coincidences between them across dimensions, while Appendix B lists the corresponding ortho-derivative differential spectra.

2 Preliminaries

Let m be a positive integer, set $q = 2^m$ and $n = 2m$, and let $\mathbb{F}_q$ and $\mathbb{F}_{q^2} = \mathbb{F}_{2^n}$ denote the finite fields with q and q^2 elements. Fixing an $\mathbb{F}_q$ -basis of $\mathbb{F}_{q^2}$ identifies $\mathbb{F}_{q^2}$ with $\mathbb{F}_q \times \mathbb{F}_q$, and fixing an $\mathbb{F}_2$ -basis of $\mathbb{F}_q$ identifies $\mathbb{F}_q \times \mathbb{F}_q$ with $\mathbb{F}_2^n$. We pass freely between these representations. For $k \geq 1$, the absolute trace $\text{tr}_1^k : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2$ is $\text{tr}_1^k(x) = \sum_{s=0}^{k-1} x^{2^s}$. We refer to [27] and to Carlet's monograph [18] for the general theory of vectorial Boolean functions and their equivalence relations, and recall here only what is needed.

We study mappings $\mathcal{F} : \mathbb{F}_q \times \mathbb{F}_q \rightarrow \mathbb{F}_q \times \mathbb{F}_q$. Every such mapping has a unique **bivariate representation**

$$\mathcal{F}(x, y) = (f(x, y), g(x, y)), \quad (x, y) \in \mathbb{F}_q^2,$$

where $f, g \in \mathbb{F}_q[x, y]$ are reduced modulo $x^q - x$ and $y^q - y$. Equivalently, after identifying $\mathbb{F}_q^2$ with $\mathbb{F}_{2^n}$, a mapping $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ has a unique **univariate representation** $F(x) = \sum_{d=0}^{2^n-1} a_d x^d$, where $a_d \in \mathbb{F}_{2^n}$. For a non-negative integer d , let $\text{wt}_2(d)$ denote the Hamming weight of the binary expansion of d . The **algebraic degree** of $F(x) = \sum_{d=0}^{2^n-1} a_d x^d$ is

$$\deg(F) = \max_{\substack{0 \leq d \leq 2^n-1 \\ a_d \neq 0}} \text{wt}_2(d).$$

The same quantity is visible in the bivariate representation: the monomial $x^{d_1} y^{d_2}$, viewed as a function on $\mathbb{F}_q \times \mathbb{F}_q \cong \mathbb{F}_{2^n}^2$, has algebraic degree $\text{wt}_2(d_1) + \text{wt}_2(d_2)$, so

$$\deg(\mathcal{F}) = \max\{\text{wt}_2(d_1) + \text{wt}_2(d_2) : x^{d_1} y^{d_2} \text{ has a nonzero coefficient in } f \text{ or } g\},$$

the maximum taken over $0 \leq d_1, d_2 \leq q-1$. A function of algebraic degree two is called **quadratic**; in bivariate terms, $\mathcal{F} = (f, g)$ is quadratic exactly when every monomial of f and g satisfies $\text{wt}_2(d_1) + \text{wt}_2(d_2) \leq 2$.

The **differential uniformity** of $\mathcal{F} : \mathbb{F}_q^2 \rightarrow \mathbb{F}_q^2$ is

$$\delta_{\mathcal{F}} = \max_{(a,b) \neq (0,0)} \max_{(u,v) \in \mathbb{F}_q^2} \#\{(x,y) \in \mathbb{F}_q^2 : \mathcal{F}(x+a, y+b) + \mathcal{F}(x,y) = (u,v)\}.$$

Table 1: Known infinite families of APN power functions over $\mathbb{F}_{2^n}$

Family	Exponent	Conditions	Algebraic degree	Source
Gold	$2^i + 1$	$\gcd(i, n) = 1$	2	[24, 33]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	$i + 1$	[29, 30]
Welch	$2^t + 3$	$n = 2t + 1$	3	[21]
Niho	$2^t + 2^{t/2} - 1, t \text{ even}$ $2^t + 2^{(3t+1)/2} - 1, t \text{ odd}$	$n = 2t + 1$	$(t+2)/2$ $t + 1$	[20]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	[3, 33]
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$	[22]

The function $\mathcal{F}$ is **almost perfect nonlinear (APN)** if $\delta_{\mathcal{F}} = 2$, which is the smallest possible differential uniformity in characteristic two.

All functions considered in this paper are quadratic. For a quadratic function $\mathcal{F}$, the derivative in the direction (a, b) is the map

$$D_{(a,b)}\mathcal{F}(x, y) = \mathcal{F}(x+a, y+b) + \mathcal{F}(x, y) + \mathcal{F}(a, b) + \mathcal{F}(0, 0).$$

It is $\mathbb{F}_2$ -linear in (x, y) and its kernel always contains $(0, 0)$ and (a, b) . Consequently, $\mathcal{F}$ is APN if and only if

$$\ker D_{(a,b)}\mathcal{F} = \{(0, 0), (a, b)\} \quad \text{for every } (a, b) \neq (0, 0).$$

Equivalently,

$$\text{rank}_{\mathbb{F}_2} D_{(a,b)}\mathcal{F} = n - 1 \quad \text{for every } (a, b) \neq (0, 0).$$

This criterion will be used throughout the paper.

Functions are typically considered up to **CCZ-equivalence** [19]. Two functions are CCZ-equivalent if there exists an affine permutation of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ mapping the graph of one function $\{x, F(x) : x \in \mathbb{F}_2^n\}$ onto the graph of the other. CCZ-equivalence preserves differential uniformity, and hence the APN property. Two functions F, F' are **linearly equivalent** if $F' = A_1 \circ F \circ A_2$ for some $\mathbb{F}_2$ -linear bijections A_1, A_2 , and **extended-affine (EA) equivalent** if $F' = A_1 \circ F \circ A_2 + A_3$ for some affine bijections A_1, A_2 and an affine map A_3 . Extended-affine (EA) equivalence is a special case of CCZ-equivalence, and for quadratic APN functions the two notions coincide [35]. Thus, to show that a quadratic APN function obtained by a given construction is new, it is sufficient to prove that it is CCZ-inequivalent to the previously known APN functions.

The **switching construction** of Edel and Pott [23] modifies a function by adding a Boolean-valued perturbation in a fixed direction. More precisely, let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, let $\gamma \in \mathbb{F}_2^n$ be nonzero, and let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be a Boolean function. If $F'(x) = F(x) + \gamma f(x)$, then F and F' are called **switching neighbours**, and F' is said to be obtained from F by switching in the direction γ . The functions F and F' need not be CCZ-equivalent, and the switching construction can therefore be used to obtain new APN functions when F' is again APN. When f is quadratic, as in the switchings considered in this paper, F' is quadratic whenever F is quadratic.

To distinguish CCZ-equivalence classes, we use the ortho-derivative [16]. Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a quadratic APN function. For every $a \neq 0$, the image of the linear map $D_a F(x) = F(x+a) + F(x) + F(a) + F(0)$ is a hyperplane of $\mathbb{F}_2^n$. Its orthogonal complement with respect to the nondegenerate pairing $\langle u, v \rangle = \text{tr}_1^n(uv)$ is therefore one-dimensional. The **ortho-derivative** of F is the map $\pi_F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ defined by $\pi_F(0) = 0$ and, for $a \neq 0$ by the unique nonzero element $\pi_F(a)$ satisfying

$$\text{tr}_1^n(\pi_F(a) D_a F(x)) = 0 \quad \text{for all } x \in \mathbb{F}_2^n.$$

For $a \neq 0$ and $b \in \mathbb{F}_2^n$, let $\delta_{\pi_F}(a, b) = \#\{x \in \mathbb{F}_2^n : \pi_F(x+a) + \pi_F(x) = b\}$. The **ortho-derivative differential spectrum** of F is the distribution of these values, that is, the multiplicities $N_k = \#\{(a, b) : a \neq 0, \delta_{\pi_F}(a, b) = k\}$ for $k \geq 0$. It is invariant under CCZ-equivalence of quadratic APN functions [16], so two quadratic APN functions with distinct ortho-derivative differential spectra are CCZ-inequivalent. The converse does not hold in general: equal spectra need not imply CCZ-equivalence. In practice, however, this invariant is highly discriminating and, for the quadratic APN functions considered here, it separates almost all of the relevant CCZ-classes at a small fraction

of the cost of a direct equivalence test. We use this invariant throughout the paper to distinguish the functions obtained in our searches from those originating from the known families.

Tables 1–3 list the known infinite families of APN functions. Table 1 contains the known APN power functions, while Tables 2 and 3 contain the known infinite families of quadratic APN functions in univariate and bivariate form, respectively. The family F_1 of [27], to which $\mathcal{F}_1$ is related, appears as F14 in Table 2. Work [27] also constructs two further families F_2 and F_3 , appearing as F15* and F16* respectively, which enter the comparison in Sections 7 and 8.

Table 2: Known infinite families of quadratic APN polynomials over $\mathbb{F}_{2^n}$ in univariate form

ID	Functions	Conditions	Source
F1- F2	$x^{2^s+1} + u^{2^k-1}x^{2^i k + 2^{m k + s}}$	$n = pk, \gcd(k, 3) = \gcd(s, 3k) = 1, p \in \{3, 4\}, i = sk \bmod p, m = p - i, n \geq 12, u$ primitive in $\mathbb{F}_{2^n}^*$	[9]
F3	$sx^{q+1} + x^{2^i+1} + x^{q(2^i+1)} + cx^{2^i q+1} + c^q x^{2^i+q}$	$q = 2^m, n = 2m, \gcd(i, m) = 1, c \in \mathbb{F}_{2^n}, s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q, X^{2^i+1} + cX^{2^i} + c^q X + 1$ has no solution x s.t. $x^{q+1} = 1$	[8]
F4	$x^3 + a^{-1} \text{Tr}_n(a^3 x^9)$	$a \neq 0$	[10]
F5	$x^3 + a^{-1} \text{Tr}_3^n(a^3 x^9 + a^6 x^{18})$	$3 n, a \neq 0$	[11]
F6	$x^3 + a^{-1} \text{Tr}_3^n(a^6 x^{18} + a^{12} x^{36})$	$3 n, a \neq 0$	[11]
F7- F9	$ux^{2^s+1} + u^{2^k} x^{2^{-k} + 2^{k+s}} + vx^{2^{-k}+1} + wu^{2^k+1} x^{2^s+2^{k+s}}$	$n = 3k, \gcd(k, 3) = \gcd(s, 3k) = 1, v, w \in \mathbb{F}_{2^k}, vw \neq 1, 3 (k+s), u$ primitive in $\mathbb{F}_{2^n}^*$	[6]
F10	$a^2 x^{2^{2m+1}+1} + b^2 x^{2^{m+1}+1} + ax^{2^{2m}+2} + bx^{2^m+2} + (c^2 + c)x^3$	$n = 3m, m$ odd, $L(x) = ax^{2^{2m}} + bx^{2^m} + cx$ satisfies the conditions of Lemma 8 of [7]	[7]
F11	$x^3 + a(x^{2^i+1})^{2^k} + bx^{3 \cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}$	$n = 2m = 10, (a, b, c) = (\beta, 1, 0), i = 3, k = 2, \beta$ primitive in $\mathbb{F}_{2^2}$ $n = 2m, m$ odd, $3 \nmid m, (a, b, c) = (\beta, \beta^2, 1), \beta$ primitive in $\mathbb{F}_{2^2}, i \in \{m-2, m, 2m-1, (m-2)^{-1} \bmod n\}$	[12]
F12	$a \text{tr}_m^n(bx^{2^i+1}) + a^q \text{tr}_m^n(cx^{2^s+1})$	$n = 2m, m$ odd, $q = 2^m, a \notin \mathbb{F}_q, \gcd(i, n) = 1, i, s, b, c$ satisfy the conditions of Theorem 2	[37]
F13	$L(z)^{2^m+1} + vz^{2^m+1}$	$\gcd(s, m) = 1, v \in \mathbb{F}_{2^m}^*, \mu \in \mathbb{F}_{2^{3m}}^*, L(z) = z^{2^{m+s}} + \mu z^{2^s} + z$ permutes $\mathbb{F}_{2^{3m}}$	[31]
F14	$x^3 + \beta x^{2^i+1} + \beta^2 x^{3 \cdot 2^m} + x^{(2^i+1) \cdot 2^m} + \beta \sum_{j=1}^{m-3} N^{2^j}(x) + N^{2^{m-2}}(x) + N^{2^{m-1}}(x)$	$n = 2m, m$ odd, $3 \nmid m, \beta$ primitive in $\mathbb{F}_4, i = m-2, N(x) = x^{2^m+1}$	[27]
F15*	$x^3 + \beta x^{2^i+1} + \beta^2 x^{3 \cdot 2^m} + x^{(2^i+1) \cdot 2^m} + \beta \sum_{j=1}^k N^{2^j}(x) + \sum_{j=k+1}^{m-1} N^{2^j}(x)$	$n = 2m, m$ odd, $3 \nmid m, \beta$ primitive in $\mathbb{F}_4, i = (m-2)^{-1} \bmod n, k = \frac{n-6}{4}, N(x) = x^{2^m+1}$	[27]
F16*	$x^3 + \beta x^{2^i+1} + \beta^2 x^{3 \cdot 2^m} + x^{(2^i+1) \cdot 2^m} + \beta^2 N(x) + \sum_{j=1}^k N^{2^j}(x) + \beta \sum_{j=k+1}^{m-1} N^{2^j}(x)$	$n = 2m, m$ odd, $3 \nmid m, \beta$ primitive in $\mathbb{F}_4, i = (m-2)^{-1} \bmod n, k = \frac{n-6}{4}, N(x) = x^{2^m+1}$	[27]

*Families F15 and F16 are conjectured to be APN and have been computationally verified up to dimension 26.

Table 3: Known infinite families of quadratic APN polynomials over $\mathbb{F}_{2^{2m}}$ in bivariate form

ID	Functions	Conditions	Source
F17	$(xy, x^{2^k+1} + \alpha y^{(2^k+1)2^i})$	$\gcd(k, m) = 1, m \text{ even}, \alpha \text{ not a cube}$	[38]
F18	$(xy, x^{2^{2k}+2^{3k}} + ax^{2^{2k}}y^{2^k} + by^{2^k+1})$	$\gcd(k, m) = 1, x^{2^k+1} + ax + b \text{ has no root in } \mathbb{F}_{2^m}$	[34]
F19	$(xy, x^{2^i+1} + x^{2^{i+m/2}}y^{2^{m/2}} + bxy^{2^i} + cy^{2^i+1})$	$(cx^{2^i+1} + bx^{2^i} + 1)^{2^{m/2}+1} + x^{2^{m/2}+1} \text{ has no roots in } \mathbb{F}_{2^m}$	[14]
F20	$(x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{2i}+1} + x^{2^{2i}}y + y^{2^{2i}+1})$	$\gcd(3i, m) = 1$	[25]
F21	$(x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{3i}}y + xy^{2^{3i}})$	$\gcd(3i, m) = 1, m \text{ odd}$	[25]
F22	$(x^3 + xy^2 + y^3 + xy, x^5 + x^4y + y^5 + xy + x^2y^2)$	$\gcd(3, m) = 1$	[31]
F23	$(x^{q+1} + By^{q+1}, x^r y + \frac{a}{B}xy^r)$	$0 < k < m, q = 2^k, r = 2^{k+m/2}, m \equiv 2 \pmod{4}, \gcd(k, m) = 1, a \in \mathbb{F}_{2^{m/2}}^*, B \in \mathbb{F}_{2^m}, B \text{ not a cube}, B^{q+r} \neq a^{q+1}$	[26]
F24	$(x^{q+1} + xy^q + \alpha y^{q+1}, x^{q^2+1} + \alpha x^{q^2}y + (1 + \alpha)^q xy^{q^2} + \alpha y^{q^2+1})$	$k, m > 0, \gcd(k, m) = 1, q = 2^k, \alpha \in \mathbb{F}_{2^m}, x^{q+1} + x + \alpha \text{ has no roots in } \mathbb{F}_{2^m}$	[15]
F25	$(x^3 + xy + xy^2 + \alpha y^3, x^5 + xy + \alpha x^2y^2 + \alpha x^4y + (1 + \alpha)^2 xy^4 + \alpha y^5)$	$\alpha \in \mathbb{F}_{2^m}, x^3 + x + \alpha \text{ has no roots in } \mathbb{F}_{2^m}$	[15]

2.1 Biprojective and extended biprojective functions

Our construction builds on the biprojective functions introduced in [25]. For $i, j \geq 0$ and coefficient tuples $(a_0, b_0, c_0, d_0), (a_1, b_1, c_1, d_1) \in \mathbb{F}_q^4$, consider the mapping $\mathcal{F} = (f, g)$ defined by

$$\begin{aligned} f(x, y) &= a_0x^{2^i+1} + b_0x^{2^i}y + c_0xy^{2^i} + d_0y^{2^i+1}, \\ g(x, y) &= a_1x^{2^j+1} + b_1x^{2^j}y + c_1xy^{2^j} + d_1y^{2^j+1}. \end{aligned} \tag{1}$$

Such a mapping is called a $(2^i, 2^j)$ -biprojective polynomial [25]. We write it as $[(a_0, b_0, c_0, d_0)_i, (a_1, b_1, c_1, d_1)_j]$ and, for simplicity, refer to it as an (i, j) -**biprojective function**. Two coefficient tuples will occur frequently throughout the paper: we write $T^+ = (1, 0, 1, 1)$ and $T^- = (1, 1, 0, 1)$. The following family is the starting point of our construction.

Theorem 1. [25] *Let $i \geq 1$ with $\gcd(3i, m) = 1$. Then the $(i, 2i)$ -biprojective function*

$$\mathcal{F}_G = [(1, 0, 1, 1)_i, (1, 1, 0, 1)_{2i}] = [T_i^+, T_{2i}^-]$$

is APN on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

For $1 \leq r \leq m-1$, define the **truncated trace polynomial** $t_r(x) = \sum_{k=0}^{r-1} x^{2^k} \in \mathbb{F}_q[x]$.

Definition 2. Let $1 \leq i, j \leq m-1$. An **extended (i, j) -biprojective function** is a mapping $\mathcal{F} = (f, g) : \mathbb{F}_q^2 \rightarrow \mathbb{F}_q^2$ of the form

$$\begin{aligned} f(x, y) &= a_0x^{2^i+1} + b_0x^{2^i}y + c_0xy^{2^i} + d_0y^{2^i+1} + t_i(xy), \\ g(x, y) &= a_1x^{2^j+1} + b_1x^{2^j}y + c_1xy^{2^j} + d_1y^{2^j+1} + t_j(xy), \end{aligned} \tag{2}$$

with $(a_0, b_0, c_0, d_0), (a_1, b_1, c_1, d_1) \in \mathbb{F}_q^4$. We denote this function by $[(a_0, b_0, c_0, d_0)_i^*, (a_1, b_1, c_1, d_1)_j^*]$.

Thus, an extended biprojective function is obtained by adding the truncated trace polynomial $t_i(xy)$ or $t_j(xy)$ to the corresponding biprojective coordinate. Every extended biprojective function is quadratic.

The first known APN family of this form is due to Li, Zhou, Li and Qu [31].

Theorem 3. [31] Let m be a positive integer such that $3 \nmid m$. Then the function $\mathcal{F}_0 : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ given by

$$\mathcal{F}_0(x, y) = (x^3 + xy^2 + y^3 + xy, x^5 + x^4y + y^5 + xy + x^2y^2) \quad (3)$$

is APN.

Since $t_1(xy) = xy$ and $t_2(xy) = xy + x^2y^2$, in the notation above, it is the extended $(1, 2)$ -biprojective function $\mathcal{F}_0 = [(1, 0, 1, 1)_1^*, (1, 1, 0, 1)_2^*] = [T_1^{+*}, T_2^{-*}]$.

Remark 4. (General symmetry) The coordinate swap $\sigma(x, y) = (y, x)$ is $\mathbb{F}_2$ -linear and preserves the extended biprojective form: since $t_\ell(xy) = t_\ell(yx)$, pre-composition with σ fixes the truncated traces and reverses each biprojective tuple $[(a_0, b_0, c_0, d_0)_i^*, (a_1, b_1, c_1, d_1)_j^*] \circ \sigma = [(d_0, c_0, b_0, a_0)_i^*, (d_1, c_1, b_1, a_1)_j^*]$. The two functions are therefore linearly equivalent; in particular, they are APN together and share the same ortho-derivative differential spectrum. For $\mathcal{F}_0 = [(1, 0, 1, 1)_1^*, (1, 1, 0, 1)_2^*]$ this gives $\mathcal{F}_0 \circ \sigma = [(1, 1, 0, 1)_1^*, (1, 0, 1, 1)_2^*]$, which is thus APN whenever $3 \nmid m$.

3 The APN family $\mathcal{F}_1$

Throughout this section, m is a positive integer with $3 \nmid m$ and $q = 2^m$. Take the extended $(1, 2)$ -biprojective function $\mathcal{F}_0 = [(1, 0, 1, 1)_1^*, (1, 1, 0, 1)_2^*]$ of Theorem 3, namely

$$\mathcal{F}_0(x, y) = (x^3 + xy^2 + y^3 + xy, x^5 + x^4y + y^5 + xy + x^2y^2). \quad (4)$$

We use the function

$$\mathcal{F}_l(x, y) = (x^5 + xy^4 + y^5 + xy + x^2y^2, x^{2^{m-1}+1} + xy^{2^{m-1}} + y^{2^{m-1}+1} + x^{2^{m-1}}y^{2^{m-1}}). \quad (5)$$

It is linearly equivalent to $\mathcal{F}_0$: a direct computation, using $z^{2^m} = z$ for $z \in \mathbb{F}_q$, gives $L_1 \circ \mathcal{F}_l \circ L_2 = \mathcal{F}_0$ for the $\mathbb{F}_2$ -linear permutations $L_1(u, v) = (v^2, u)$ and $L_2(x, y) = (y, x)$ of $\mathbb{F}_q^2$.

Corollary 1. Let m be a positive integer such that $3 \nmid m$, and $q = 2^m$. The function $\mathcal{F}_l$ of (5) is APN on $\mathbb{F}_q \times \mathbb{F}_q$ since it is linearly equivalent to $\mathcal{F}_0$.

Let $\delta \in \mathbb{F}_8$ be a root of $z^3 + z^2 + 1$ (irreducible over $\mathbb{F}_2$), and let $\delta_1 = \delta$, $\delta_2 = \delta^2$, $\delta_3 = \delta^4$ be its conjugates. Then $\delta^7 = 1$ and

$$\delta_1 + \delta_2 + \delta_3 = 1, \quad \delta_1\delta_2 + \delta_1\delta_3 + \delta_2\delta_3 = 0, \quad \delta_1\delta_2\delta_3 = 1. \quad (6)$$

Lemma 1. In $\mathbb{F}_8[a, b]$,

$$\begin{aligned} a^3 + a^2b + b^3 &= \prod_{i=1}^3 (a + \delta_i b), \\ a^3 + a^2b + b^3 + a^2 + ab + b^2 + 1 &= \prod_{i=1}^3 (a + \delta_i b + \delta_i^2). \end{aligned}$$

Proof. Write $p(z) = z^3 + z^2 + 1 = \prod_{i=1}^3 (z + \delta_i)$. For the first identity, put $z = a/b$ and multiply by b^3 :

$$\prod_{i=1}^3 (a + \delta_i b) = b^3 p(a/b) = a^3 + a^2b + b^3.$$

For the second, let β_1, β_2 be the two roots of $t^2 + bt + a$ in a splitting field, so that $t^2 + bt + a = (t + \beta_1)(t + \beta_2)$, and $\beta_1 + \beta_2 = b$, $\beta_1\beta_2 = a$. Then, substituting $t = \delta_i$, we get $a + \delta_i b + \delta_i^2 = (\delta_i + \beta_1)(\delta_i + \beta_2)$, and using $p(z) = \prod_i (z + \delta_i)$ brings

$$\prod_{i=1}^3 (a + \delta_i b + \delta_i^2) = \left(\prod_i (\beta_1 + \delta_i) \right) \left(\prod_i (\beta_2 + \delta_i) \right) = p(\beta_1) p(\beta_2).$$

Expanding $p(\beta_1)p(\beta_2) = (\beta_1^3 + \beta_1^2 + 1)(\beta_2^3 + \beta_2^2 + 1)$ and grouping symmetrically,

$$\begin{aligned} p(\beta_1)p(\beta_2) &= (\beta_1\beta_2)^3 + (\beta_1\beta_2)^2(\beta_1 + \beta_2) + (\beta_1^3 + \beta_2^3) + (\beta_1\beta_2)^2 + (\beta_1^2 + \beta_2^2) + 1 \\ &= a^3 + a^2b + (b^3 + ab) + a^2 + b^2 + 1 = a^3 + a^2b + b^3 + a^2 + ab + b^2 + 1, \end{aligned}$$

using $\beta_1 + \beta_2 = b$, $\beta_1\beta_2 = a$, $\beta_1^2 + \beta_2^2 = b^2$ and $\beta_1^3 + \beta_2^3 = b^3 + ab$ in characteristic 2. $\square$

Lemma 2. *Let $3 \nmid m$. Then for every $(a, b) \in \mathbb{F}_{2^m}^2 \setminus \{(0, 0)\}$.*

$$\begin{aligned} a^3 + a^2b + b^3 &\neq 0, \\ a^3 + a^2b + b^3 + a^2 + ab + b^2 + 1 &\neq 0. \end{aligned}$$

Proof. Since $3 \nmid m$, we have $\mathbb{F}_8 \cap \mathbb{F}_{q^2} = \mathbb{F}_2$. Because $z^3 + z^2 + 1$ is irreducible over $\mathbb{F}_2$, its roots $\delta_1, \delta_2, \delta_3$ do not lie in $\mathbb{F}_2$, hence, none of them lies in $\mathbb{F}_q$. The identities of Lemma 1 are identities in $\mathbb{F}_8[a, b]$, so they remain valid after substituting any $a, b \in \mathbb{F}_q$. The two sides are then elements of the compositum $\mathbb{F}_q \cdot \mathbb{F}_8 = \mathbb{F}_{2^{3m}}$, which is the smallest field containing both $\mathbb{F}_q$ and the δ_i . In $\mathbb{F}_{2^{3m}}$, a product vanishes only if one of its factors does. Fix $(a, b) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}$. Suppose $a^3 + a^2b + b^3 = 0$. If $b = 0$, then $a^3 = 0$, so $a = 0$, which is excluded. If $b \neq 0$, then $\prod_{i=1}^3 (a + \delta_i b) = 0$ forces $a + \delta_i b = 0$ for some i , so $\delta_i = a/b \in \mathbb{F}_q$, contradicting $\delta_i \notin \mathbb{F}_q$. Suppose $a^3 + a^2b + b^3 + a^2 + ab + b^2 + 1 = 0$. Then $\prod_{i=1}^3 (a + \delta_i b + \delta_i^2) = 0$ forces $a + \delta_i b + \delta_i^2 = 0$ for some i ; that is, δ_i is a root of $X^2 + bX + a \in \mathbb{F}_q[X]$. A root of a quadratic over $\mathbb{F}_q$ generates an extension of $\mathbb{F}_q$ of degree at most 2, so $\delta_i \in \mathbb{F}_{q^2}$, contradicting $\delta_i \notin \mathbb{F}_q^2$. $\square$

Theorem 5. *Let m be a positive integer with $3 \nmid m$. The extended $(2, m-1)$ -biprojective function $\mathcal{F}_1 = [(1, 0, 1, 1)_2^*, (1, 0, 1, 1)_{m-1}^*]$, that is,*

$$\mathcal{F}_1(x, y) = \left(x^5 + xy^4 + y^5 + t_2(xy), \quad x^{2^{m-1}+1} + xy^{2^{m-1}} + y^{2^{m-1}+1} + t_{m-1}(xy) \right), \quad (7)$$

is APN on $\mathbb{F}_q \times \mathbb{F}_q$.

Proof. For a direction $(a, b) \neq (0, 0)$ consider the $\mathbb{F}_2$ -linear map

$$D_{(a,b)}\mathcal{F}_1(x, y) := \mathcal{F}_1(x + a, y + b) + \mathcal{F}_1(x, y) + \mathcal{F}_1(a, b) + \mathcal{F}_1(0, 0).$$

Since $\mathcal{F}_1$ is quadratic, it is APN if and only if for every $(a, b) \neq (0, 0)$ the kernel

$$\mathcal{K}_{(a,b)} = \{(x, y) \in \mathbb{F}_q^2 : D_{(a,b)}\mathcal{F}_1(x, y) = (0, 0)\}$$

satisfies $|\mathcal{K}_{(a,b)}| = 2$. We have $(x, y) \in \mathcal{K}_{(a,b)}$ if and only if

$$\begin{cases} ax^4 + b^2x^2 + (a^4 + b^4 + b)x + (a + b)y^4 + a^2y^2 + (b^4 + a)y = 0, \\ (a + b)^{2^{m-1}}x + ax^{2^{m-1}} + b^{2^{m-1}}y + (a + b)y^{2^{m-1}} + t_{m-1}(bx + ay) = 0. \end{cases} \quad (8)$$

Put $T := ay + bx$, the linear form in (x, y) attached to the direction (a, b) . The two kernel elements $(0, 0)$ and (a, b) both satisfy $T = 0$, hence $\text{tr}_1^m(T) = 0$ at each of them. At an arbitrary kernel element, however, T need not vanish, so $\text{tr}_1^m(T) \in \{0, 1\}$. We treat the two values separately, and it suffices to show that no kernel element other than $(0, 0)$ and (a, b) occurs.

Case $\text{tr}_1^m(\mathbf{T}) = 0$, where $T = ay + bx$. Since $t_{m-1}(z) = z^{2^{m-1}} + \text{tr}_1^m(z)$, comparing (5) and (7) gives $\mathcal{F}_1 = \mathcal{F}_l + (0, \text{tr}_1^m(xy))$. Therefore, $D_{(a,b)}\mathcal{F}_1(x, y) = D_{(a,b)}\mathcal{F}_l(x, y) + (0, \text{tr}_1^m(T))$. When $\text{tr}_1^m(T) = 0$, the added term vanishes, so a kernel element of $D_{(a,b)}\mathcal{F}_1$ with $\text{tr}_1^m(T) = 0$ is a kernel element of $D_{(a,b)}\mathcal{F}_l$. By Corollary 1, $\mathcal{F}_l$ is APN, so that kernel is $\{(0, 0), (a, b)\}$; hence every kernel element with $\text{tr}_1^m(T) = 0$ lies in $\{(0, 0), (a, b)\}$.

Case $\text{tr}_1^m(\mathbf{T}) = 1$, where $T = ay + bx$. Since $t_{m-1}(bx + ay) = (bx + ay)^{2^{m-1}} + 1$, raising the second equation of (8) to the power of 2 becomes

$$\begin{cases} ax^4 + b^2x^2 + (a^4 + b^4 + b)x + (a + b)y^4 + a^2y^2 + (b^4 + a)y = 0, \\ (a + b)x^2 + (a^2 + b)x + by^2 + (a^2 + b^2 + a)y = 1. \end{cases} \quad (9)$$

For a direction $(a, b) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}$, we denote the first equation of (9) by f , and the left-hand side of the second equation by g , so it reads $g = 1$. Both f and g are $\mathbb{F}_2$ -linear in (x, y) . Denote

$$S := a^2 + ab + b^2, \quad Q := a^3 + a^2b + b^3, \quad \text{hence } a^5 + ab^4 + b^5 = QS.$$

Let $a \neq 0$. From $T = ay + bx$, we get $y = (T + bx)/a$. Substituting y into f and g and clearing denominators yields the identities in $\mathbb{F}_2[a, b, x, T]$:

$$a^2g = Qx(x + a) + P, \quad (10)$$

$$a^4f = QSx(x + a)(x^2 + ax + a^2) + R, \quad (11)$$

where

$$P := bT^2 + a(a^2 + a + b^2)T, \quad R := (a + b)T^4 + a^4T^2 + (a^3b^4 + a^4)T.$$

With $g = 1$, identity (10) gives $Qx(x + a) = P + a^2$, and since $Q \neq 0$ by Lemma 2,

$$\begin{aligned} x(x + a) &= \frac{P + a^2}{Q}, \\ x^2 + ax + a^2 &= x(x + a) + a^2 = \frac{P + a^2 + a^2Q}{Q}. \end{aligned}$$

Substituting both into (11) with $f = 0$ and multiplying by Q gives

$$S(P + a^2)(P + a^2 + a^2Q) = QR.$$

Expanding the left-hand side, $(P + a^2)(P + a^2 + a^2Q) = P^2 + a^2QP + a^4 + a^4Q$, hence

$$SP^2 + a^2QSP + QR = a^4S + a^4SQ = a^4S(Q + 1). \quad (12)$$

On the other hand, a direct expansion in $\mathbb{F}_2[a, b, T]$ yields

$$SP^2 + a^2QSP + QR = a^4(T^4 + (S^2 + S + Q)T^2 + Q(Q + S + 1)T). \quad (13)$$

Consider the linearized polynomial

$$\underline{L(T) = T^4 + (S^2 + S + Q)T^2 + Q(Q + S + 1)T}. \quad (14)$$

Comparing (12) and (13) and dividing by $a^4 \neq 0$ gives the relation

$$L(T) = S(Q + 1). \quad (15)$$

Let $a = 0$ (so $b \neq 0$). Here $S = b^2$, $Q = b^3$, $T = bx$, and (9) reads

$$\begin{cases} b^2x^2 + (b^4 + b)x + by^4 + b^4y = 0, \\ bx^2 + bx + by^2 + b^2y = 1. \end{cases}$$

Squaring the second equation gives $b^2y^4 + b^4y^2 = 1 + b^2x^4 + b^2x^2$; multiplying the first by b gives $b^2y^4 + b^5y = b^3x^2 + (b^5 + b^2)x$. Summing,

$$b^4y^2 + b^5y = b^2x^4 + (b^2 + b^3)x^2 + (b^5 + b^2)x + 1.$$

Since $b^4y^2 + b^5y = b^3(by^2 + b^2y) = b^3(1 + bx^2 + bx)$ by the second equation, rearranging yields

$$b^2x^4 + (b^2 + b^3 + b^4)x^2 + (b^2 + b^4 + b^5)x + (1 + b^3) = 0.$$

Multiplying by b^2 and substituting $T = bx$,

$$T^4 + (b^2 + b^3 + b^4)T^2 + (b^6 + b^5 + b^3)T + (b^2 + b^5) = 0,$$

i.e. $L(T) = b^2(1 + b^3) = S(Q + 1)$, since $b^2 + b^3 + b^4 = S^2 + S + Q$, $b^6 + b^5 + b^3 = Q(Q + S + 1)$ and $b^2 + b^5 = S(Q + 1)$. Thus, (15) holds in both cases.

Put $z = (Q + S + 1)^{-2}$, which is well defined because $Q + S + 1 \neq 0$ by Lemma 2. Let L^* denote the adjoint of L (14) with respect to the trace form $\langle u, v \rangle = \text{tr}_1^m(uv)$, namely

$$L^*(y) = y^{2^{m-2}} + (c_2y)^{2^{m-1}} + c_1y, \quad (16)$$

where $c_2 = S^2 + S + Q$, $c_1 = Q(Q + S + 1)$. Indeed, since $\text{tr}_1^m(u) = \text{tr}_1^m(u^{2^k})$ for all k and $u^{2^m} = u$, we have $\text{tr}_1^m(x^4y) = \text{tr}_1^m((x^4y)^{2^{m-2}}) = \text{tr}_1^m(xy^{2^{m-2}})$, $\text{tr}_1^m(c_2x^2y) = \text{tr}_1^m(x(c_2y)^{2^{m-1}})$, and $\text{tr}_1^m(c_1xy) = \text{tr}_1^m(xc_1y)$; adding these gives $\text{tr}_1^m(L(x)y) = \text{tr}_1^m(xL^*(y))$ for all $x, y \in \mathbb{F}_q$. Raising (16) to the fourth power

$$(L^*(z))^4 = z + c_2^2z^2 + c_1^4z^4.$$

Multiplying by $(Q + S + 1)^8$:

$$(Q + S + 1)^8 (L^*(z))^4 = (Q + S + 1)^6 + c_2^2(Q + S + 1)^4 + Q^4(Q + S + 1)^4 = (Q + S + 1)^4((Q + S + 1)^2 + c_2^2 + Q^4).$$

On the other hand, $(Q + S + 1)^2 = Q^2 + (Q + S + 1) + c_2$; squaring it gives $(Q + S + 1)^4 = Q^4 + (Q + S + 1)^2 + c_2^2$, so the bracketed factor above equals $(Q + S + 1)^4$. Therefore, $(Q + S + 1)^8 (L^*(z))^4 = (Q + S + 1)^4 \cdot (Q + S + 1)^4$ gives $(L^*(z))^4 = 1$, hence $L^*(z) = 1$, since $u \rightarrow u^4$ is bijection of $\mathbb{F}_q$. Consequently, using (15),

$$1 = \text{tr}_1^m(T) = \text{tr}_1^m(T L^*(z)) = \text{tr}_1^m(L(T) z) = \text{tr}_1^m\left(\frac{S(Q + 1)}{(Q + S + 1)^2}\right).$$

Using $S^2 + S(Q + S + 1) = SQ + S = S(Q + 1)$,

$$\frac{S(Q + 1)}{(Q + S + 1)^2} = \left(\frac{S}{Q + S + 1}\right)^2 + \frac{S}{Q + S + 1},$$

which is of the form $w^2 + w$ with $w \in \mathbb{F}_q$; hence its absolute trace is 0. This forces $1 = 0$, a contradiction. Therefore, no kernel element satisfies $\text{tr}_1^m(T) = 1$.

Combining the two cases, $\mathcal{K}_{(a,b)} = \{(0,0), (a,b)\}$, so $|\mathcal{K}_{(a,b)}| = 2$ for every $(a,b) \neq (0,0)$; that is, $\mathcal{F}_1$ is APN. $\square$

For odd m , the family $\mathcal{F}_1$ coincides with the univariate family F_1 of [27], as the next theorem shows. For even m , where the construction of [27] does not apply, it yields new functions (Propositions 5, 8 and 9).

Theorem 6. *Let $m \geq 5$ be odd with $3 \nmid m$. Then the extended $(2, m - 1)$ -biprojective function $\mathcal{F}_1$ of Theorem 5 is EA-equivalent, and hence CCZ-equivalent, to the univariate function F_1 of [27] (F14 in Table 2).*

Proof. By the proof of Theorem 5, $\mathcal{F}_1 = \mathcal{F}_l + (0, \text{tr}_1^m(xy))$, and $L_1 \circ \mathcal{F}_l \circ L_2 = \mathcal{F}_0$ with $L_1(u, v) = (v^2, u)$ and $L_2(x, y) = (y, x)$. Since $L_1(0, h) = (h, 0)$ for every Boolean function h , and $\text{tr}_1^m(xy)$ is symmetric in x and y ,

$$L_1 \circ \mathcal{F}_1 \circ L_2 = \mathcal{F}_0 + (\text{tr}_1^m(xy), 0) =: \mathcal{F}'_0. \quad (17)$$

Since m is odd, $\beta \in \mathbb{F}_4 \setminus \mathbb{F}_2$ does not lie in $\mathbb{F}_q$, and $\bar{\beta} = \beta^2$, where $\bar{X} = X^q$. We use the $\mathbb{F}_q$ -linear identification of $\mathbb{F}_{q^2}$ with $\mathbb{F}_q \times \mathbb{F}_q$ from [27, Lemma 1], which matches the univariate representation of a map $\mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2}$ with its bivariate representation $\mathbb{F}_q^2 \rightarrow \mathbb{F}_q^2$. We write a bivariate function (a map $\mathbb{F}_q^2 \rightarrow \mathbb{F}_q^2$) with a calligraphic letter, $\mathcal{F}$, and a univariate function (a map $\mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$) with a plain letter, F . Let $X \in \mathbb{F}_{q^2}$ correspond to $(x, y) = (X + \bar{X}, \beta X + \beta^2 \bar{X})$, and an output pair (u, v) to $u + \beta v$. By [27, Lemma 1], $\mathcal{F}_0$ then becomes the function F_{l_0} of [27] in the univariate representation. Moreover, $N(X) = X\bar{X} = x^2 + xy + y^2$ and $x + y = \beta^2 X + \beta \bar{X}$, so

$$\text{tr}_1^m(xy) = \text{tr}_1^m(N(X)) + \lambda(X), \quad \lambda(X) = \text{tr}_1^m(\beta^2 X + \beta \bar{X}), \quad (18)$$

where λ is $\mathbb{F}_2$ -linear. Hence the univariate form of $\mathcal{F}'_0$ is $F_{l_0} + \text{tr}_1^m(N(X)) + \lambda$.

On the univariate side, $F_1 = F_l + \beta \text{tr}_1^m(N(X))$ [27], and $M_1 \circ F_l + M_2 = F_{l_0}$ by [27, Theorem 4], where $M_1(X) = \beta X + X^4 + \beta^2 \bar{X} + \beta^2 \bar{X}^4$ is a linear permutation of $\mathbb{F}_{q^2}$ and M_2 is linear (these maps are denoted L_1, L_2 in [27]). The linear equivalence of F_l and F_{l_0} alone does not imply that their switching neighbours are equivalent, but M_1 maps the switching term of F_l onto that of F_{l_0} . Indeed, $\text{tr}_1^m(N(X)) \in \mathbb{F}_2$ and $M_1(\beta) = \beta^2 + \beta^4 + \beta^2 \bar{\beta} + \beta^2 \bar{\beta}^4 = 1$, so

$$M_1 \circ F_1 + M_2 = F_{l_0} + \text{tr}_1^m(N(X)) \quad M_1(\beta) = F_{l_0} + \text{tr}_1^m(N(X)).$$

Therefore, the univariate form of $\mathcal{F}'_0$ is $M_1 \circ F_1 + M_2 + \lambda$. Since M_1 is a linear permutation and $M_2 + \lambda$ is linear, F_1 is EA-equivalent to $\mathcal{F}'_0$ and, by (17), to $\mathcal{F}_1$. $\square$

The parity of m enters only through the univariate representation, which requires $\beta \notin \mathbb{F}_q$. The bivariate function $\mathcal{F}_1$ and the proof of Theorem 5 do not use it, which is why $\mathcal{F}_1$ extends F_1 to even m .

4 Structure of extended biprojective functions

In this section, we establish several properties of extended biprojective functions. These properties explain some of the patterns observed in the computational results of Sections 6–8 and allow us to exclude from the searches several configurations that reduce to known classes. Throughout, $\mathcal{F} = (f, g)$ is an extended (i, j) -biprojective function as in (2), and we write

$$f = f_{\text{bp}} + t_i(xy), \quad g = g_{\text{bp}} + t_j(xy),$$

where f_{bp} and g_{bp} are the biprojective parts, of exponents i and j , respectively.

4.1 Coefficient matrices and projective zero sets

We represent the biprojective parts by their coefficient matrices

$$\Gamma_f = \begin{pmatrix} a_0 & c_0 \\ b_0 & d_0 \end{pmatrix}, \quad \Gamma_g = \begin{pmatrix} a_1 & c_1 \\ b_1 & d_1 \end{pmatrix}, \quad (19)$$

so that $f_{\text{bp}}(x, y) = (x, y) \Gamma_f (x^{2^i}, y^{2^i})^\top$ and $g_{\text{bp}}(x, y) = (x, y) \Gamma_g (x^{2^j}, y^{2^j})^\top$; their determinants are $\det \Gamma_f = a_0 d_0 + b_0 c_0$ and $\det \Gamma_g = a_1 d_1 + b_1 c_1$. The tuples $T^+ = (1, 0, 1, 1)$ and $T^- = (1, 1, 0, 1)$ correspond to the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, respectively. These are transvections, that is, non-identity unipotent elements of the special linear group $SL(2, \mathbb{F}_q)$ —the 2×2 matrices over $\mathbb{F}_q$ of determinant 1—inside the general linear group $GL(2, \mathbb{F}_q)$ of all invertible 2×2 matrices over $\mathbb{F}_q$.

A linear substitution $(x, y) \mapsto (x, y)P$, where $P \in GL(2, \mathbb{F}_q)$, maps f_{bp} to a biprojective form of the same exponent with coefficient matrix $\Gamma'_f = P \Gamma_f (P^{(2^i)})^\top$, where $P^{(2^i)}$ is obtained by raising every entry of P to the power 2^i . Since $\det P^{(2^i)} = (\det P)^{2^i}$, taking determinants gives $\det \Gamma'_f = (\det P)^{2^i+1} \det \Gamma_f$, so the substitution scales the determinant of the coefficient matrix by the factor $(\det P)^{2^i+1}$.

We denote by $V_f, V_g \subseteq \mathbb{P}^1(\mathbb{F}_q)$ the sets of projective zeros of f_{bp} and g_{bp} , respectively. Thus, V_f is the zero set of the dehomogenization $f_{\text{bp}}(x, 1) = a_0 x^{2^i+1} + b_0 x^{2^i} + c_0 x + d_0$ and $g_{\text{bp}}(x, 1)$, with ∞ counted as a zero when the leading coefficient vanishes. These are projective polynomials in the sense of [1, 4]. Hence, if $f_{\text{bp}} \neq 0$, then $|V_f| \in \{0, 1, 2, 2^{\gcd(i, m)} + 1\}$, by [4, 32], and the same holds for $|V_g|$ with exponent j .

4.2 Necessary conditions for APNness

The truncated trace terms vanish from the derivative when it is restricted to the line spanned by the direction of differentiation. This gives several necessary conditions for the APN property.

Lemma 3. *Let $u = (v, w) \neq (0, 0)$. For every $\lambda \in \mathbb{F}_q$,*

$$D_u \mathcal{F}(\lambda u) = \left((\lambda + \lambda^{2^i}) f_{\text{bp}}(u), (\lambda + \lambda^{2^j}) g_{\text{bp}}(u) \right). \quad (20)$$

Proof. Since t_ℓ is $\mathbb{F}_2$ -linear, the derivative of $t_\ell(xy)$ in direction $u = (v, w)$ is $t_\ell(wx + vy)$, whose argument vanishes at $(x, y) = \lambda u$. For the biprojective part, $f_{\text{bp}}(\mu u) = \mu^{2^i+1} f_{\text{bp}}(u)$ for $\mu \in \mathbb{F}_q$ gives $D_u f_{\text{bp}}(\lambda u) = ((\lambda + 1)^{2^i+1} + \lambda^{2^i+1} + 1) f_{\text{bp}}(u) = (\lambda + \lambda^{2^i}) f_{\text{bp}}(u)$. The same applies for g_{bp} . $\square$

Corollary 2. *If an extended (i, j) -biprojective function is APN, then*

$$V_f \cap V_g = \emptyset, \quad V_g \neq \emptyset \Rightarrow \gcd(i, m) = 1, \quad V_f \neq \emptyset \Rightarrow \gcd(j, m) = 1, \quad \gcd(i, j, m) = 1. \quad (21)$$

Proof. The kernel of $\lambda \mapsto \lambda + \lambda^{2^e}$ on $\mathbb{F}_q$ is $\mathbb{F}_{2^{\gcd(e, m)}}$. By Lemma 3, $\ker D_u \mathcal{F}$ therefore contains $\mathbb{F}_{2^{\gcd(i, j, m)}} u$ for every $u \neq (0, 0)$; it contains the whole line $\mathbb{F}_q u$ if the projective point of u lies in $V_f \cap V_g$, the set $\mathbb{F}_{2^{\gcd(i, m)}} u$ if it lies in V_g , and $\mathbb{F}_{2^{\gcd(j, m)}} u$ if it lies in V_f . Since $\mathcal{F}$ is APN if and only if $\ker D_u \mathcal{F} = \{0, u\} = \mathbb{F}_2 u$ for every $u \neq (0, 0)$, each of these sets must equal $\mathbb{F}_2 u$. $\square$

By Lemma 3, the conditions in (21) are the same as for biprojective functions without truncated trace terms: the truncated traces do not affect the derivative on the lines $\mathbb{F}_q u$. These conditions explain several exponent pairs for which our searches cannot produce APN functions. For example, $(2, 2)$ is excluded when $m = 4$. For $(i, j) = (2, m-1)$ with m even, $\gcd(i, m) = 2$ requires $V_g = \emptyset$, while for $(i, j) = (1, 2)$ with m even, $\gcd(j, m) = 2$ requires $V_f = \emptyset$.

4.3 Normalization of the truncated-trace coefficients

Definition (2) fixes the coefficients of both truncated traces to one. More generally, one may consider

$$\mathcal{F} = (f_{\text{bp}} + c_0 t_i(\varepsilon_0 xy), g_{\text{bp}} + c_1 t_j(\varepsilon_1 xy)), \quad c_0, c_1, \varepsilon_0, \varepsilon_1 \in \mathbb{F}_q^*. \quad (22)$$

The next proposition shows that three of these four parameters can be normalized.

Proposition 1. Write $\varepsilon := \varepsilon_1/\varepsilon_0 \in \mathbb{F}_q \setminus \{0\}$. Every function (22) is linearly equivalent to one of the same form and the same exponents i, j whose trace terms are $t_i(xy)$ and $t_j(\varepsilon xy)$ —that is, with $c_0 = c_1 = 1$ and the two trace-argument coefficients equal to 1 and ε . If all coefficients in (22) lie in a subfield $\mathbb{F}_{2^k}$ of $\mathbb{F}_q$, then so do those of the normalized function. Moreover, let $A^{(2)}$ denote the entrywise square of a matrix A , as in Section 4.1, and set $\sigma(z) = z^2$ and $\hat{\sigma}(x, y) = (\sigma(x), \sigma(y))$. Conjugation by $\hat{\sigma}$ maps the normalized function with coefficient matrices Γ_f, Γ_g and trace parameter ε to the normalized function with coefficient matrices $\Gamma_f^{(2)}, \Gamma_g^{(2)}$ and trace parameter ε^2 . Consequently, all functions corresponding to

$$(\Gamma_f, \Gamma_g, \varepsilon), \quad (\Gamma_f^{(2)}, \Gamma_g^{(2)}, \varepsilon^2), \quad (\Gamma_f^{(4)}, \Gamma_g^{(4)}, \varepsilon^4), \quad \dots$$

define linearly equivalent functions.

Proof. Both normalizing steps are linear equivalences $\mathcal{F} \mapsto A \circ \mathcal{F} \circ B$ (Section 2), with A acting on the output and B on the input. The output map $A: (u, v) \mapsto (c_0^{-1}u, c_1^{-1}v)$ removes c_0 and c_1 , rescaling only the biprojective coefficient matrices (which is insignificant, since the search ranges over all of them). The input substitution $B: (x, y) \mapsto (\varepsilon_0^{-1}x, y)$ multiplies xy by ε_0^{-1} , turning $t_i(\varepsilon_0 xy)$ into $t_i(xy)$ and $t_j(\varepsilon_1 xy)$ into $t_j(\varepsilon xy)$. By Section 4.1, applied with $P = \begin{pmatrix} \varepsilon_0^{-1} & 0 \\ 0 & 1 \end{pmatrix}$, it maps each biprojective part to a biprojective part of the same exponent. Both A and B are $\mathbb{F}_2$ -linear bijections with entries in $\mathbb{F}_{2^k}$ whenever those of $\mathcal{F}$ are, so the normalized function keeps its coefficients in $\mathbb{F}_{2^k}$. Finally, the conjugation $\hat{\sigma} \circ \mathcal{F} \circ \hat{\sigma}^{-1}$ is again a linear equivalence; it fixes every biprojective monomial and squares its coefficient (thus $\Gamma_f \mapsto \Gamma_f^{(2)}, \Gamma_g \mapsto \Gamma_g^{(2)}$), while on a truncated trace

$$\sigma\left(t_j(\varepsilon \sigma^{-1}(x) \sigma^{-1}(y))\right) = \sum_{k=0}^{j-1} (\varepsilon^2 xy)^{2^k} = t_j(\varepsilon^2 xy),$$

so it replaces ε by ε^2 . Iterating therefore runs through the orbit of $(\Gamma_f, \Gamma_g, \varepsilon)$ displayed above. $\square$

Thus, up to linear equivalence, the more general construction (22) has only one additional parameter ε ; the extended biprojective functions of (2) correspond to $\varepsilon = 1$. For $\varepsilon \neq 1$, $t_j(\varepsilon xy) + t_j(xy) = t_j((\varepsilon + 1)xy)$ is quadratic, so the parameter ε cannot in general be removed by adding an affine map.

The Frobenius conjugation $\mathcal{F} \mapsto \hat{\sigma} \circ \mathcal{F} \circ \hat{\sigma}^{-1}$ of Proposition 1 squares the trace parameter and the biprojective coefficients at once, sending $(\Gamma_f, \Gamma_g, \varepsilon)$ to $(\Gamma_f^{(2)}, \Gamma_g^{(2)}, \varepsilon^2)$. The scalings (28), in contrast, fix xy and hence ε , while acting on the biprojective coefficients. Together, these equivalences are used to reduce the search space in Section 5.2, where we test one representative from each orbit as in [28]. For coefficients in $\mathbb{F}_2$, the only nonzero value is $\varepsilon = 1$, apart from configurations in which one truncated trace is absent, considered in Section 4.4. For coefficients in $\mathbb{F}_4 = \{0, 1, \beta, \beta^2\}$, which requires m even, the Frobenius orbits in $\mathbb{F}_4^*$ are $\{1\}$ and $\{\beta, \beta^2\}$, so it suffices to add $\varepsilon = \beta$; we test this value in Section 7.2.

4.4 Degenerate and one-sided configurations

To include the cases in which either truncated trace term is absent, consider

$$\mathcal{F} = (f_{\text{bp}} + \varepsilon_0 t_i(xy), g_{\text{bp}} + \varepsilon_1 t_j(xy)), \quad \varepsilon_0, \varepsilon_1 \in \mathbb{F}_2. \quad (23)$$

We call $\mathcal{F}$ *one-sided* if exactly one of $\varepsilon_0, \varepsilon_1$ is zero, and *degenerate* if $\varepsilon_0 = \varepsilon_1 = 1$ while exactly one of the biprojective parts $f_{\text{bp}}, g_{\text{bp}}$ is the zero polynomial. Both cases already occur among the families of Table 3: F17, F18 and F19 have first coordinate $xy = t_1(xy)$, that is, a vanishing first biprojective part together with a truncated trace, and no truncated trace on the second coordinate. Such functions have the shape of the Carlet family $\mathcal{C} = (xy, g_{\text{bp}})$ [17]. Whether a degenerate function can be reduced to this form depends on whether the corresponding truncated trace is a permutation.

Lemma 4. The truncated trace t_ℓ permutes $\mathbb{F}_q$ if and only if $\gcd(\ell, m) = 1$ and ℓ is odd.

Proof. Since t_ℓ is $\mathbb{F}_2$ -linear, it permutes $\mathbb{F}_q$ iff $\ker t_\ell = \{0\}$. From $t_\ell(z)^2 + t_\ell(z) = z^{2^\ell} + z$, any $z \in \ker t_\ell$ satisfies $z^{2^\ell} = z$, so $z \in \mathbb{F}_{2^\ell} \cap \mathbb{F}_q = \mathbb{F}_{2^d}$ with $d = \gcd(\ell, m)$. Thus $\ker t_\ell \subseteq \mathbb{F}_{2^d}$, and it suffices to evaluate t_ℓ on the subfield $\mathbb{F}_{2^d}$. For $z \in \mathbb{F}_{2^d}$ the powers z^{2^k} have period d in k , and $d \mid \ell$, so $t_\ell(z) = \sum_{k=0}^{\ell-1} z^{2^k}$ is ℓ/d repetitions of $\text{tr}_1^d(z) = \sum_{k=0}^{d-1} z^{2^k}$. In characteristic 2 this equals $\text{tr}_1^d(z)$ when ℓ/d is odd and 0 when ℓ/d is even. If ℓ/d is even, t_ℓ vanishes on all of $\mathbb{F}_{2^d}$, so $\ker t_\ell = \mathbb{F}_{2^d} \neq \{0\}$. If ℓ/d is odd, then $t_\ell = \text{tr}_1^d$ on $\mathbb{F}_{2^d}$, and $\ker t_\ell = \{z \in \mathbb{F}_{2^d} : \text{tr}_1^d(z) = 0\}$ has 2^{d-1} elements, trivial iff $d = 1$. Hence t_ℓ permutes $\mathbb{F}_q$ iff $d = \gcd(\ell, m) = 1$ and ℓ is odd. $\square$

Proposition 2. Let $\mathcal{F} = (f_{\text{bp}} + \varepsilon_0 t_i(xy), g_{\text{bp}} + \varepsilon_1 t_j(xy))$, where $\varepsilon_0, \varepsilon_1 \in \mathbb{F}_2$.

- (a) If $\mathcal{F}$ is degenerate with $f_{\text{bp}} = 0$ and t_i permutes $\mathbb{F}_q$, then $\mathcal{F}$ is linearly equivalent to (xy, g_{bp}) . Symmetrically, if $g_{\text{bp}} = 0$ and t_j permutes $\mathbb{F}_q$, then $\mathcal{F}$ is linearly equivalent to (xy, f_{bp}) .
- (b) If $\varepsilon_1 = 0$ and $g_{\text{bp}} = \gamma f_{\text{bp}}^{2^s}$ for some $\gamma \in \mathbb{F}_q^*$ and $s \geq 0$, then $\mathcal{F}$ is linearly equivalent to $(t_i(xy), g_{\text{bp}})$, and hence to (xy, g_{bp}) if t_i permutes $\mathbb{F}_q$. The case $\varepsilon_0 = 0$ is symmetric.

Proof. (a) The map $(u, v) \mapsto (t_i^{-1}(u), v + t_j(t_i^{-1}(u)))$ is an $\mathbb{F}_2$ -linear permutation of $\mathbb{F}_q^2$, and it sends $(t_i(xy), g_{\text{bp}} + t_j(xy))$ to (xy, g_{bp}) . The second statement follows after interchanging the two coordinates. (b) Choose $t \geq 0$ with $s + t \equiv 0 \pmod{m}$. The map $(u, v) \mapsto (u + \gamma^{-2^t} v^{2^t}, v)$ is an $\mathbb{F}_2$ -linear permutation, and it sends $(f_{\text{bp}} + t_i(xy), \gamma f_{\text{bp}}^{2^s})$ to $(t_i(xy), g_{\text{bp}})$, because $\gamma^{-2^t} (\gamma f_{\text{bp}}^{2^s})^{2^t} = f_{\text{bp}}^{2^{s+t}} = f_{\text{bp}}$. If t_i permutes $\mathbb{F}_q$, applying t_i^{-1} to the first coordinate gives (xy, g_{bp}) . $\square$

Consequently, the configurations covered by Proposition 2, when the corresponding truncated trace is a permutation, reduce to the form of the Carlet family and can be excluded from a general search. The remaining degenerate and one-sided configurations are treated computationally in Sections 6.3 and 6.4.

4.5 A switching relation between two series

The proof of Theorem 5 is based on the decomposition $\mathcal{F}_1 = \mathcal{F}_l + (0, \text{tr}_1^m(xy))$, where $\mathcal{F}_l$ is linearly equivalent to $\mathcal{F}_0$. We now show that the same switching relation extends to Göloğlu's $(s, 2s)$ -biprojective functions.

For $s \geq 1$ with $2s \leq m - 1$, define

$$\mathcal{G}_s = [T_s^{+*}, T_{2s}^{-*}], \quad \mathcal{G}'_s = [T_{2s}^{+*}, T_{m-s}^{+*}], \quad (24)$$

that is,

$$\begin{aligned} \mathcal{G}_s(x, y) &= (x^{2^s+1} + xy^{2^s} + y^{2^s+1} + t_s(xy), \quad x^{2^{2s}+1} + x^{2^s}y + y^{2^{2s}+1} + t_{2s}(xy)), \\ \mathcal{G}'_s(x, y) &= (x^{2^{2s}+1} + xy^{2^{2s}} + y^{2^{2s}+1} + t_{2s}(xy), \quad x^{2^{m-s}+1} + xy^{2^{m-s}} + y^{2^{m-s}+1} + t_{m-s}(xy)). \end{aligned}$$

The function $\mathcal{G}_s$ is obtained by adding truncated trace terms to Göloğlu's $(s, 2s)$ -biprojective function of Theorem 1. In particular, $\mathcal{G}_1 = \mathcal{F}_0$ is the family of Theorem 3, and $\mathcal{G}'_1 = \mathcal{F}_1$ is the family of Theorem 5. Since $\gcd(s, 2s, m) = \gcd(2s, m - s, m) = \gcd(s, m)$, Corollary 2 shows that $\mathcal{G}_s$ and $\mathcal{G}'_s$ can be APN only if $\gcd(s, m) = 1$.

Proposition 3. Let $\tau(x, y) = (y, x)$ and $\Pi_s(u, v) = (v, u^{2^{m-s}})$. Then

$$\Pi_s \circ \mathcal{G}_s \circ \tau = \mathcal{G}'_s + (0, \text{tr}_1^m(xy)). \quad (25)$$

In particular, $\mathcal{G}'_s$ is a switching neighbour, by the Boolean function $\text{tr}_1^m(xy)$, of a function linearly equivalent to $\mathcal{G}_s$.

Proof. Because xy is symmetric in x and y ,

$$\mathcal{G}_s(y, x) = (x^{2^s+1} + x^{2^s}y + y^{2^s+1} + t_s(xy), \quad x^{2^{2s}+1} + xy^{2^{2s}} + y^{2^{2s}+1} + t_{2s}(xy)),$$

whose second coordinate is the first coordinate of $\mathcal{G}'_s$. Raise the first coordinate to the power 2^{m-s} and reduce modulo $x^q - x$ and $y^q - y$. The biprojective part becomes $x^{2^m+2^{m-s}} + x^{2^m}y^{2^{m-s}} + y^{2^m+2^{m-s}} = x^{2^{m-s}+1} + xy^{2^{m-s}} + y^{2^{m-s}+1}$, and the truncated trace becomes

$$t_s(z)^{2^{m-s}} = \sum_{k=m-s}^{m-1} z^{2^k} = \text{tr}_1^m(z) + t_{m-s}(z), \quad z = xy.$$

Hence the second coordinate of $\Pi_s \circ \mathcal{G}_s \circ \tau$ is the second coordinate of $\mathcal{G}'_s$ plus $\text{tr}_1^m(xy)$. $\square$

For $s = 1$ the map Π_1 is the inverse of the map L_1 of Section 3, the function $\Pi_1 \circ \mathcal{G}_1 \circ \tau$ is the function $\mathcal{F}_l$ of (5), and (25) is the decomposition used in the proof of Theorem 5. That proof splits the kernel of the derivative according to the value of $\text{tr}_1^m(ay + bx)$; the same argument gives the following criterion for every s .

Corollary 3. Suppose that $\mathcal{G}_s$ is APN, and put $\widehat{\mathcal{G}}_s = \Pi_s \circ \mathcal{G}_s \circ \tau$. Then $\mathcal{G}'_s$ is APN if and only if, for every $(a, b) \neq (0, 0)$, no $(x, y) \in \mathbb{F}_q^2$ with $\text{tr}_1^m(ay + bx) = 1$ satisfies $D_{(a,b)}\widehat{\mathcal{G}}_s(x, y) = (0, 1)$.

Proof. By (25), $D_{(a,b)}\mathcal{G}'_s(x,y) = D_{(a,b)}\widehat{\mathcal{G}}_s(x,y) + (0, \text{tr}_1^m(ay+bx))$. The elements of $\ker D_{(a,b)}\mathcal{G}'_s$ with $\text{tr}_1^m(ay+bx) = 0$ lie in $\ker D_{(a,b)}\widehat{\mathcal{G}}_s = \{(0,0), (a,b)\}$, since $\widehat{\mathcal{G}}_s$ is APN, and both of these points belong to $\ker D_{(a,b)}\mathcal{G}'_s$. The elements with $\text{tr}_1^m(ay+bx) = 1$ are exactly the solutions excluded in the statement. $\square$

For odd m , switching by $(0, \text{tr}_1^m(xy))$ corresponds in univariate form to switching by $\beta \text{tr}_1^m(N(X))$ up to an $\mathbb{F}_2$ -linear term, by (18). This is the switching that relates the families F_l and F_1 in [27]; the conjectured families F_2 and F_3 of [27] are also related by a norm switching, and we return to them in Section 8.

5 Computational method

5.1 An accelerated APN test

Let $\mathcal{F} = (f, g)$ be an extended (i, j) -biprojective function as in (2). By the rank criterion of Section 2, $\mathcal{F}$ is APN if and only if

$$\text{rank}_{\mathbb{F}_2} D_{(a,b)}\mathcal{F} = 2m - 1 \quad \text{for every } (a, b) \neq (0, 0). \quad (26)$$

After fixing an $\mathbb{F}_2$ -basis of $\mathbb{F}_q^2$, the derivative is represented by a $2m \times 2m$ binary matrix. A direct expansion gives

$$\begin{aligned} D_{(a,b)}f(x, y) &= a_0(ax^{2^i} + a^{2^i}x) + b_0(bx^{2^i} + a^{2^i}y) \\ &\quad + c_0(b^{2^i}x + ay^{2^i}) + d_0(by^{2^i} + b^{2^i}y) + \sum_{k=0}^{i-1} (b^{2^k}x^{2^k} + a^{2^k}y^{2^k}), \end{aligned} \quad (27)$$

and analogously for $D_{(a,b)}g$ with (a_1, b_1, c_1, d_1) and exponent j .

For a biprojective function without truncated traces one has $\mathcal{F}(\lambda x, \lambda y) = (\lambda^{2^i+1}f, \lambda^{2^j+1}g)$, so $D_{(a,b)}\mathcal{F}$ and $D_{(\lambda a, \lambda b)}\mathcal{F}$ have equal kernel size and only the $q+1$ projective directions need be tested. The truncated trace destroys this homogeneity, since $(xy)^{2^k}$ is multiplied under $(x, y) \mapsto (\lambda x, \lambda y)$ by $\lambda^{2^{k+1}}$, which depends on k . Thus, in general, all $2^{2m} - 1$ nonzero directions must be tested. The following observation makes this exhaustive test efficient.

Proposition 4. *Fix (i, j) and the coefficient tuples in (2), and let $M(a, b) \in \mathbb{F}_2^{2m \times 2m}$ be the matrix of $D_{(a,b)}\mathcal{F}$ in a fixed $\mathbb{F}_2$ -basis of $\mathbb{F}_q \times \mathbb{F}_q$. Then $(a, b) \mapsto M(a, b)$ is $\mathbb{F}_2$ -linear.*

Proof. By (27), the entries of $M(a, b)$ depend on (a, b) only through the Frobenius powers a^{2^k} and b^{2^k} . These maps are $\mathbb{F}_2$ -linear, and therefore $M(a + a', b + b') = M(a, b) + M(a', b')$. $\square$

Fix an $\mathbb{F}_2$ -basis $e_1, \dots, e_m$ of $\mathbb{F}_q$ and precompute the $2m$ matrices $M(e_k, 0)$ and $M(0, e_k)$. By Proposition 4, the matrix corresponding to any direction is an $\mathbb{F}_2$ -linear combination of these matrices. A *Gray code* is an ordering of all binary vectors of a fixed length in which each vector differs from the previous one in exactly one coordinate, the *flipped coordinate*. Identifying $\mathbb{F}_q^2$ with $\mathbb{F}_2^{2m}$ and listing the nonzero directions in Gray-code order, consecutive directions differ by a single basis vector $(e_k, 0)$ or $(0, e_k)$, so the matrix is updated by adding one precomputed matrix at each step. Algorithm 1 proceeds accordingly. Before the exhaustive sweep, we apply a random pre-filter consisting of r randomly chosen directions. A candidate is rejected as soon as one of these directions has rank different from $2m - 1$. Candidates that pass the filter are then tested exhaustively, so the pre-filter affects only the running time and not the correctness of the test.

Algorithm 1 APN test for an extended (i, j) -biprojective function

Require: dimension m ; exponents i, j ; coefficient tuples; filter size r

Ensure: TRUE iff $\mathcal{F}$ in (2) is APN

```
1: for  $t = 1, \dots, r$  do
2:   sample  $(a, b) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}$  uniformly and build  $M(a, b)$  via (27)
3:   if  $\text{rank } M(a, b) \neq 2m - 1$  then return FALSE
4:   end if
5: end for
6: compute the  $2m$  basis matrices  $M(e_k, 0), M(0, e_k)$ ; set  $M \leftarrow 0$ 
7: for  $c = 1, \dots, 2^{2m} - 1$  in Gray-code order do
8:    $M \leftarrow M + M_k$ , where  $k$  is the flipped coordinate
9:   if  $\text{rank } M \neq 2m - 1$  then return FALSE
10:  end if
11: end for
12: return TRUE
```

The exhaustive part of Algorithm 1 still performs $2^n - 1$ rank computations, where $n = 2m$. Its advantage over the direct test lies in the construction of the derivative matrices. In a direct implementation, $M(a, b)$ is constructed independently for every direction using finite-field arithmetic in (27). In Algorithm 1, all finite-field arithmetic is confined to the one-time computation of the n basis matrices. Each subsequent matrix is obtained by a single bitwise XOR with one of these matrices. The random pre-filter does not change the worst-case complexity, but rejects most non-APN candidates before the exhaustive sweep.

5.2 Reducing the search space

We further reduce the search space using equivalences that preserve the form (2). First, interchanging the two output coordinates together with $(i, j) \mapsto (j, i)$ identifies the corresponding search cases, so it is sufficient to consider $i \leq j$. Second, for $\lambda \in \mathbb{F}_q \setminus \{0\}$ the linear permutation $(x, y) \mapsto (\lambda x, \lambda^{-1}y)$ fixes each truncated trace, since $(\lambda x)(\lambda^{-1}y) = xy$, and acts on the biprojective coefficients by

$$(a_0, b_0, c_0, d_0) \mapsto (\lambda^{2^i+1}a_0, \lambda^{2^i-1}b_0, \lambda^{1-2^i}c_0, \lambda^{-(2^i+1)}d_0), \quad (28)$$

and analogously with j on the second tuple. Third, conjugation by the Frobenius map, as in Proposition 1, squares all coefficients and gives a linearly equivalent function. Hence coefficient tuples in the same orbit under the group generated by (28) and the Frobenius need not be tested separately. After fixing an ordering of $\mathbb{F}_q$, we retain only the lexicographically smallest tuple in each orbit, following the approach of [28].

Each exponent pair (i, j) defines an independent search, so the searches for different pairs can be carried out in parallel. Together with the accelerated APN test, the reductions above make an exhaustive full-field search over all eight biprojective coefficients feasible for $m = 4$.

The structural results of Section 4 provide further reductions. Proposition 1 shows that, when both truncated trace terms are present with nonzero coefficients, their coefficients can be normalized except for the parameter ε . We treat the additional value arising over $\mathbb{F}_4$ separately in Section 7.2. Configurations in which a truncated trace is absent are treated according to Section 4.4. This reduction is important because finding the APN functions is considerably cheaper than classifying them under CCZ-equivalence. Each APN function found must be converted to a truth table and its ortho-derivative differential spectrum computed, which requires $\Theta(2^{2n})$ operations. In the $\mathbb{F}_2$ -coefficient searches, where we retained the degenerate configurations as a check, they account for 36 of the 48 APN functions the search returns in dimension 14, 100 of the 120 in dimension 22, and 144 of the 168 in dimension 26 (all counted as coefficient tuples, not CCZ-classes). Removing these known cases therefore substantially reduces the classification cost without discarding unknown configurations.

5.3 Computing the ortho-derivative differential spectrum

Because the ortho-derivative differential spectrum is the invariant used throughout our comparisons, we compute it using the same derivative matrices $M(a, b)$. For an APN function $\mathcal{F}$ and $(a, b) \neq (0, 0)$, the value $\pi_{\mathcal{F}}(a, b)$ spans the orthogonal complement of the image of $D_{(a,b)}\mathcal{F}$. Hence it is obtained from the one-dimensional left null space $\ker(M(a, b)^\top)$, which is the orthogonal complement of the image under the standard coordinate pairing on $\mathbb{F}_2^n$. This

pairing differs from the trace pairing $\text{tr}_1^n(uv)$ defining $\pi_{\mathcal{F}}$ only by the fixed, invertible Gram matrix of the trace form. Or equivalently, by the change to the trace-dual basis. Being a single invertible $\mathbb{F}_2$ -linear map applied to every value, it does not change the differential spectrum of $\pi_{\mathcal{F}}$. We may therefore take the kernel vector itself as $\pi_{\mathcal{F}}(a, b)$, with no basis conversion. By the Gray-code traversal of Section 5.1, the entire table $\pi_{\mathcal{F}}$ is produced in 2^n kernel computations (Algorithm 2).

Algorithm 2 Ortho-derivative table of an extended (i, j) -biprojective function

Require: m , exponents i, j , coefficient tuples; $\mathcal{F}$ known to be APN

Ensure: table Π with $\Pi[x]$ the encoding of $\pi_{\mathcal{F}}(x)$, $x \in \mathbb{F}_2^n$, $n = 2m$

- 1: compute the n basis matrices $M_1, \dots, M_n$ via (27)
- 2: $M \leftarrow 0$; $x \leftarrow 0$; $\Pi[0] \leftarrow 0$
- 3: **for** $c = 1, \dots, 2^n - 1$ **do**
- 4: $k \leftarrow \nu_2(c) + 1$ $\triangleright$ Gray code: index of the flipped bit
- 5: $M \leftarrow M + M_k$; $x \leftarrow x \oplus 2^{k-1}$
- 6: $\Pi[x] \leftarrow$ the nonzero vector of $\ker(M^T)$
- 7: **end for**
- 8: **return** Π

$\nu_2(c)$ denotes the 2-adic valuation of c , i.e., the 0-indexed position of its least significant set bit.

For $a \neq 0$ and $b \in \mathbb{F}_2^n$, let

$$\delta_{\pi_{\mathcal{F}}}(a, b) = \#\{x \in \mathbb{F}_2^n : \pi_{\mathcal{F}}(x + a) + \pi_{\mathcal{F}}(x) = b\}. \quad (29)$$

For each k , define $N_k = \#\{b : \delta_{\pi_{\mathcal{F}}}(a, b) = k\}$. We record the ortho-derivative differential spectrum in the multiset notation $k \widetilde{N}_k$. For every $a \neq 0$, $\sum_b \delta_{\pi_{\mathcal{F}}}(a, b) = 2^n$ serves as a checksum on each row. Consequently, the global multiplicities satisfy $\sum_k N_k = \sum_k k N_k = 2^n(2^n - 1)$.

Symmetries of the function can reduce the cost of computing the ortho-derivative differential spectrum and, at the same time, impose restrictions on its multiplicities. Let G be a group of linear permutations of $\mathbb{F}_2^n$ arising as the input linear parts of EA-self-equivalences of F : for each $A \in G$ there are an affine permutation L_A with linear part A and a linear permutation B_A of $\mathbb{F}_2^n$ such that $F \circ L_A = B_A \circ F + \ell_A$ for some affine ℓ_A . The group acts on $\mathbb{F}_2^n$ by $a \mapsto Aa$. The orbit of a is $Ga = \{Aa : A \in G\}$, and B_A^* denotes the adjoint of B_A with respect to $\langle u, v \rangle = \text{tr}_1^n(uv)$.

Lemma 5. *Let F be a quadratic APN function on $\mathbb{F}_2^n$, and let G be as above. For every $A \in G$ and every $a \neq 0$, the multisets $\{\delta_{\pi_F}(Aa, b) : b \in \mathbb{F}_2^n\}$ and $\{\delta_{\pi_F}(a, b) : b \in \mathbb{F}_2^n\}$ coincide. Consequently, if G acts freely on $\mathbb{F}_2^n \setminus \{0\}$, meaning no non-identity element of G fixes any nonzero vector, then $|G|$ divides every multiplicity N_k of the ortho-derivative differential spectrum of F , and hence of every quadratic function CCZ-equivalent to F .*

Proof. Fix $A \in G$, with B_A and ℓ_A as above. Applying the derivative D_a in direction a to the identity $F \circ A = B_A \circ F + \ell_A$, and using that A and B_A are linear while $D_a \ell_A = 0$ for the affine map ℓ_A , we obtain $D_{Aa} F(Ax) = B_A(D_a F(x))$ for all $a, x \in \mathbb{F}_2^n$. Since A is a bijection, $\text{im } D_{Aa} F = B_A(\text{im } D_a F)$. Taking orthogonal complements with respect to $\langle \cdot, \cdot \rangle$ gives $\pi_F(Aa) = (B_A^*)^{-1} \pi_F(a)$ for every a . Substituting $x \mapsto Ax$ in (29) and applying this identity yields

$$\delta_{\pi_F}(Aa, b) = \delta_{\pi_F}(a, B_A^* b) \quad \text{for all } b \in \mathbb{F}_2^n.$$

As B_A^* is a bijection, letting b range over $\mathbb{F}_2^n$ shows that the two multisets coincide, proving the first claim. For the second claim, write

$$N_k = \sum_{\mathcal{O}} |\mathcal{O}| \cdot \#\{b \in \mathbb{F}_2^n : \delta_{\pi_F}(a_{\mathcal{O}}, b) = k\},$$

the sum running over the orbits $\mathcal{O}$ of G on $\mathbb{F}_2^n \setminus \{0\}$ with $a_{\mathcal{O}}$ any representative of $\mathcal{O}$. This is well-defined because, by the first claim, $\#\{b : \delta_{\pi_F}(a, b) = k\}$ is constant on each orbit. If G acts freely, every orbit has length $|G|$, so $|G|$ divides N_k . Finally, the ortho-derivative differential spectrum is invariant under CCZ-equivalence of quadratic APN functions, so the same divisibility holds for every quadratic function CCZ-equivalent to F . $\square$

By the first part of Lemma 5, it is sufficient to evaluate (29) for one direction from each orbit of G and weight the resulting distribution by the orbit length. The second part gives a necessary condition for CCZ-equivalence that can be checked directly from the spectrum.

Let $q = 2^m$ and $n = 2m$. Each of the following families admits a group $G \cong \mathbb{F}_q^*$ satisfying the hypotheses of Lemma 5 and acting freely on $\mathbb{F}_2^n \setminus \{0\}$. Consequently, $q - 1$ divides every multiplicity of its ortho-derivative differential spectrum.

- (i) The Gold functions, since $F(\lambda x) = \lambda^{2^i+1}F(x)$.
- (ii) Every bijective APN function (1), since $\mathcal{F}(\lambda x, \lambda y) = (\lambda^{2^i+1}f(x, y), \lambda^{2^j+1}g(x, y))$. This includes the Carlet family and the families F20, F21, F23 and F24. The same applies to families F17 and F18 using the input maps $(x, y) \mapsto (\lambda x, \lambda^{2^{m-i}}y)$ and $(x, y) \mapsto (\lambda x, \lambda^{2^{2k}}y)$, respectively.
- (iii) The families F3, F11 with $(a, b, c) = (\beta, \beta^2, 1)$ and m odd, and F12, via $x \mapsto \lambda x$. Write $\bar{x} = x^q$. For F12 we have $F = aT_1 + a^qT_2$ with $T_1 = \text{tr}_m^n(bx^{2^i+1})$ and $T_2 = \text{tr}_m^n(cx^{2^s+1})$ in $\mathbb{F}_q$. Hence $F(\lambda x) = a\lambda^{2^i+1}T_1 + a^q\lambda^{2^s+1}T_2$ is an $\mathbb{F}_2$ -linear function of $F(x)$, because a and a^q form a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. F3 is treated in the same way with the basis $s, 1$. For F11, the parts $x^3 + \beta^2\bar{x}^3$ and $\beta(x^{2^i+1})^{2^k} + (\bar{x}^{2^i+1})^{2^k}$ lie in the complementary $\mathbb{F}_q$ -subspaces $\{z : \bar{z} = \beta z\}$ and $\{z : \bar{z} = \beta^2 z\}$, and they are multiplied by λ^3 and $\lambda^{(2^i+1)2^k}$, respectively.

The same argument gives smaller symmetry groups for several other families. The families F1–F2 satisfy $F(\lambda x) = \lambda^{2^s+1}F(x)$, $\lambda \in \mathbb{F}_{2^k}^*$, where $n = pk$, while F19 admits the corresponding symmetry under $(x, y) \mapsto (\lambda x, \lambda y)$, $\lambda \in \mathbb{F}_{2^{m/2}}^*$.

Their spectrum multiplicities are therefore divisible by $2^k - 1$ and $2^{m/2} - 1$, respectively. Yet, there are no corresponding symmetries for F4, F14–F16, F22 and F25, and their spectra in Tables 13 and 15 contain multiplicities that are not divisible by $q - 1$. The same holds for every spectrum of $\mathcal{G}_s$ and $\mathcal{G}'_s$ computed in this paper. We use these divisibility conditions in Section 7 to exclude most known families in dimensions 20 and 22, where computing all of their ortho-derivative differential spectra would be computationally expensive.

All computations were carried out in Magma [5]. Since each search is phrased entirely in terms of matrices over $\mathbb{F}_2$ and their ranks, and Magma's linear algebra over $\mathbb{F}_2$ is highly optimized, reducing the APN test to $\mathbb{F}_2$ -rank computations is an efficient way to run it. The results of all searches reported below, together with the ortho-derivative differential spectra, are publicly available in a GitHub repository.

6 Exhaustive full-field searches

We first perform exhaustive searches in which all eight bijective coefficients range over the full field $\mathbb{F}_q$. Both truncated trace terms are present with coefficient one, and for every exponent pair $1 \leq i \leq j \leq m - 1$ we test one representative from each orbit under the reductions of Section 5.2. Degenerate and one-sided configurations are considered separately in Sections 6.3 and 6.4.

6.1 Dimension 8

Let $m = 4$, so $n = 8$ and $q = 16$. The exhaustive search returns 11 350 APN functions. Their ortho-derivative differential spectra depend only on the exponent pair, and only three distinct spectra occur, as shown in Table 4.

Table 4: Exhaustive full-field search over $\mathbb{F}_{16} \times \mathbb{F}_{16}$, by exponent pair.

(i, j)	count	ortho-derivative differential spectrum	identification
$(1, 1), (1, 3), (3, 3)$	11 298	$0\text{---}39600, 2\text{---}19680, 4\text{---}5220, 6\text{---}600, 8\text{---}180$	Carlet
$(1, 2)$	26	$0\text{---}38160, 2\text{---}22104, 4\text{---}4536, 6\text{---}456, 8\text{---}24$	$\mathcal{G}_1 = \mathcal{F}_0$
$(2, 3)$	26	$0\text{---}38256, 2\text{---}22116, 4\text{---}4230, 6\text{---}648, 8\text{---}30$	$\mathcal{G}'_1 = \mathcal{F}_1$
$(2, 2)$	0	—	excluded by Corollary 2

To identify these spectra, we computed the ortho-derivative differential spectra of the Gold and Carlet families, all families of Table 3 defined for $m = 4$, and all univariate families of Table 2 defined in dimension eight. The results are given in Table 5. Families F21 and F23 of Table 3 do not occur in this dimension, since they require m odd and $m \equiv 2 \pmod{4}$, respectively. Among the univariate families of Table 2, only F4 is defined for $n = 8$: F1–F2 require $n \geq 12$, F5–F6 require $3 \mid n$, F7–F10 and F13 require $n = 3m$, and F11–F12 and F14–F16 require $n = 2m$ with m odd. The hexanomials F3 coincide with the Carlet family by [14]. Among the APN power functions of Table 1, only Gold functions are quadratic in dimension eight; moreover, by [36], an APN power function that is CCZ-equivalent to a quadratic function is EA-equivalent to a Gold function.

The comparison identifies all three spectra obtained in the search. The 11 298 functions on the exponent pairs $(1, 1)$, $(1, 3)$ and $(3, 3)$ have the spectrum of the Carlet family. The 26 functions on $(1, 2)$ have the spectrum of

Table 5: Ortho-derivative differential spectra of known APN functions over $\mathbb{F}_{2^8}$

Ortho-derivative differential spectrum	Realized by
$0 \sim 39780, 2 \sim 21930, 6 \sim 3570$	Gold, $k = 1$
$0 \sim 35700, 2 \sim 26520, 4 \sim 3060$	Gold, $k = 3$
$0 \sim 39600, 2 \sim 19680, 4 \sim 5220, 6 \sim 600, 8 \sim 180$	Carlet
$0 \sim 38880, 2 \sim 21165, 4 \sim 4230, 6 \sim 1005$	Taniguchi (F18), $d = 1$
$0 \sim 38580, 2 \sim 21315, 4 \sim 4860, 6 \sim 495, 8 \sim 30$	Taniguchi (F18), $d = g^7$
$0 \sim 36420, 2 \sim 25080, 4 \sim 3780$	Zhou–Pott (F17); Göloğlu (F20); Calderini–Li–Villa (F24)
$0 \sim 39150, 2 \sim 20463, 4 \sim 4920, 6 \sim 675, 8 \sim 54, 10 \sim 12, 12 \sim 6$	Calderini–Budaghyan–Carlet (F19)
$0 \sim 38004, 2 \sim 22614, 4 \sim 4008, 6 \sim 630, 10 \sim 24$	F4, $x^3 + \text{Tr}_n(x^9)$
$0 \sim 38592, 2 \sim 21426, 4 \sim 4590, 6 \sim 654, 8 \sim 18$	F4, $x^3 + a^{-1}\text{Tr}_n(a^3x^9)$
$0 \sim 38160, 2 \sim 22104, 4 \sim 4536, 6 \sim 456, 8 \sim 24$	$\mathcal{F}_0 = \mathcal{G}_1$, Li et al. (F22); Calderini–Li–Villa (F25)
$0 \sim 38256, 2 \sim 22116, 4 \sim 4230, 6 \sim 648, 8 \sim 30$	$\mathcal{F}_1 = \mathcal{G}'_1$ of (7)

$\mathcal{F}_0 = \mathcal{G}_1$, while the 26 functions on $(2, 3)$ have the spectrum of $\mathcal{F}_1 = \mathcal{G}'_1$. The pair $(2, 2)$ produces no APN function, as predicted by Corollary 2, since $\gcd(2, 2, 4) > 1$.

The spectrum of $\mathcal{F}_1$ differs from those of all known families listed in Table 5. We therefore obtain the following.

Proposition 5. *Over $\mathbb{F}_{2^8}$ the function $\mathcal{F}_1$ of (7) is CCZ-inequivalent to the Gold and Carlet families, to F4, and to every family of Table 3 defined for $m = 4$. Moreover, every extended biprojective APN function found in the exhaustive full-field search over $\mathbb{F}_{16} \times \mathbb{F}_{16}$ has the ortho-derivative differential spectrum of a Carlet function, of $\mathcal{F}_0$, or of $\mathcal{F}_1$.*

6.2 The admissible coefficients of $\mathcal{F}_0$ and $\mathcal{F}_1$

The full-field search shows that the spectra of $\mathcal{F}_0$ and $\mathcal{F}_1$ are each realized by several coefficient pairs rather than only by their standard representatives. We now describe the structure observed among these pairs. We focus on the exponent pair $(2, m - 1)$ corresponding to $\mathcal{F}_1$; the pair $(1, 2)$ corresponding to $\mathcal{F}_0$ behaves analogously.

Every APN function found on $(1, 2)$ or $(2, 3)$ satisfies

$$\det \Gamma_f = \det \Gamma_g = 1. \quad (30)$$

This condition is preserved by the equivalences used in our search: the scalings (28) are substitutions $(x, y) \mapsto (x, y)P$ with $\det P = 1$, which leave $\det \Gamma_f$ and $\det \Gamma_g$ unchanged (Section 4.1), while the Frobenius of Proposition 1 squares both determinants and so fixes the value 1. The standard representatives are unipotent: for $\mathcal{F}_1$, $\Gamma_f = \Gamma_g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, while for $\mathcal{F}_0$ the two coefficient matrices are the opposite transvections $\Gamma_f = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\Gamma_g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

For the exponent pair $(2, m - 1)$ the second coordinate has exponent $j = m - 1$, so its biprojective part is $g_{\text{bp}}(x, y) = a_1x^{2^{m-1}+1} + b_1x^{2^{m-1}}y + c_1xy^{2^{m-1}} + d_1y^{2^{m-1}+1}$ (cf. (2)). Squaring g_{bp} and reducing modulo $x^q - x$ and $y^q - y$ gives the cubic form

$$\mathcal{Q}(x, y) = a_1^2x^3 + c_1^2x^2y + b_1^2xy^2 + d_1^2y^3. \quad (31)$$

Its projective zeros are exactly those of g_{bp} , and hence its projective zero set is V_g .

Definition 7. A pair (Γ_f, Γ_g) on the exponent pair $(2, m - 1)$ is *coupled* if $\mathcal{Q}$ divides f_{bp} as a binary form. In this case, the quotient $\mathcal{S} = f_{\text{bp}}/\mathcal{Q}$ is a quadratic form. If, in addition, $\det \Gamma_g = 1$ and $V_g = \emptyset$, we call Γ_g a *partner* of Γ_f .

On $(1, 2)$ the exponent in $\{1, m - 1\}$ is $i = 1$, so the first coordinate f_{bp} is already a cubic form, and the coupling reads $f_{\text{bp}} \mid g_{\text{bp}}$ with a quadratic quotient. In both cases, the cubic comes from the coordinate whose exponent lies in $\{1, m - 1\}$, and it divides the coordinate of exponent 2.

For a coupled pair, every $\mathbb{F}_q$ -rational projective zero of $\mathcal{Q}$ is also a zero of f_{bp} , so $V_g \subseteq V_f$. Corollary 2 therefore implies that an APN coupled pair must satisfy $V_g = \emptyset$. In this case the $\mathbb{F}_q$ -rational projective zeros of f_{bp} are precisely those of $\mathcal{S}$, and hence

$$V_f = \{\text{projective zeros of } \mathcal{S}\}, \quad |V_f| \in \{0, 1, 2\}. \quad (32)$$

For $m = 4$, the exhaustive search gives a particularly simple characterization: a coefficient pair on $(2, 3)$ produces an APN function if and only if $\det \Gamma_f = \det \Gamma_g = 1$, $V_g = \emptyset$, $\mathcal{Q} \mid f_{\text{bp}}$. This computational observation motivates the following conjecture for arbitrary even m .

Conjecture 1. *Let $m \geq 4$ be even with $3 \nmid m$, and let $\mathcal{F}$ be the extended $(2, m-1)$ -biprojective function with coefficient matrices $\Gamma_f, \Gamma_g \in \mathbb{F}_q^{2 \times 2}$. Then $\mathcal{F}$ is APN if and only if*

$$\det \Gamma_f = \det \Gamma_g = 1, \quad V_g = \emptyset, \quad \mathcal{Q} \mid f_{\text{bp}}.$$

In the terminology of Definition 7, the conjectured conditions require $\Gamma_f \in SL(2, \mathbb{F}_q)$ and Γ_g to be a partner of Γ_f . The next proposition determines exactly when such a partner exists.

Proposition 6. *Let m be even and $\Gamma_f \in SL(2, \mathbb{F}_q)$. Then Γ_f has a partner if and only if $|V_f| = 2$, and it is unique. More precisely, suppose $f_{\text{bp}} = \ell_1 \ell_2 \mathcal{C}$ with linear forms ℓ_1, ℓ_2 and an irreducible cubic form $\mathcal{C} = \gamma_3 x^3 + \gamma_2 x^2 y + \gamma_1 x y^2 + \gamma_0 y^3$, then the partner of Γ_f is*

$$\Gamma_g = \frac{1}{\kappa} \begin{pmatrix} \gamma_3^{1/2} & \gamma_2^{1/2} \\ \gamma_1^{1/2} & \gamma_0^{1/2} \end{pmatrix}, \quad \kappa = (\gamma_0 \gamma_3 + \gamma_1 \gamma_2)^{1/4}.$$

Proof. Since $\det \Gamma_f \neq 0$, the partial derivatives $a_0 x^4 + c_0 y^4$ and $b_0 x^4 + d_0 y^4$ of f_{bp} have no common projective zero, so f_{bp} has five distinct projective zeros over $\mathbb{F}_q$. Fixing one zero v_0 and substituting $sv_0 + w$ turns f_{bp} into a polynomial $Bs^4 + As + E$; its four roots are distinct, so $A, B \neq 0$, and they form a coset of the $\mathbb{F}_4$ -line $\{s : Bs^4 + As = 0\}$. Therefore, the five zeros are the image of $\mathbb{P}^1(\mathbb{F}_4)$ under a projective linear map. As $\mathbb{F}_4 \subseteq \mathbb{F}_q$, the Frobenius $z \mapsto z^q$ acts on the five zeros through the projective linear group $PGL(2, \mathbb{F}_4) \cong A_5$ – the quotient of $GL(2, \mathbb{F}_4)$ by its scalar matrices, acting on $\mathbb{P}^1(\mathbb{F}_4)$ by projective transformation, which is isomorphic to A_5 . Thus it acts by an even permutation of the five points. Its orbits have sizes $1^5, 2^2 1, 3 1^2$ or 5 , and they are the sets of zeros of the irreducible factors of f_{bp} over $\mathbb{F}_q$. Hence f_{bp} has an irreducible cubic factor if and only if $|V_f| = 2$, and this factor $\mathcal{C}$ is then unique up to a scalar.

Let Γ_g be a partner of Γ_f . The conditions $V_g = \emptyset$ and $\mathcal{Q} \mid f_{\text{bp}}$ say that $\mathcal{Q}$ is an irreducible cubic factor of f_{bp} , so $\mathcal{Q} = \mu \mathcal{C}$ with $\mu \in \mathbb{F}_q^*$. By (31), Γ_g is obtained from $\mathcal{Q}$ by taking square roots of the coefficients, so $\Gamma_g = \mu^{1/2} \Gamma_{\mathcal{C}}$, where $\Gamma_{\mathcal{C}}$ denotes the matrix in the statement without the factor $1/\kappa$. Its determinant is κ^2 , and $\kappa \neq 0$: if the rows (a, c) and (b, d) of a matrix are linearly dependent, its cubic form $x^2(a^2 x + c^2 y) + y^2(b^2 x + d^2 y)$ is $x^2(a^2 x + c^2 y)$ when $(b, d) = (0, 0)$ and $(tx + y)^2(b^2 x + d^2 y)$ when $(a, c) = t(b, d)$, so it has a projective zero, whereas $\mathcal{C}$ has none. Therefore $\det \Gamma_g = \mu \kappa^2$, and the condition $\det \Gamma_g = 1$ gives $\mu^{1/2} = \kappa^{-1}$, so Γ_g is the matrix in the statement. Conversely, if $|V_f| = 2$, this matrix has determinant one and cubic form $\kappa^{-2} \mathcal{C}$, which divides f_{bp} and has no projective zero over $\mathbb{F}_q$; hence it is a partner of Γ_f . $\square$

Combining Conjecture 1 with Proposition 6 shows which matrices Γ_f can be completed to an APN function.

Corollary 4. *Let $m \geq 4$ be even with $3 \nmid m$, assume Conjecture 1, and let $\Gamma_f \in \mathbb{F}_q^{2 \times 2}$. There exists $\Gamma_g \in \mathbb{F}_q^{2 \times 2}$ such that the extended $(2, m-1)$ -biprojective function with coefficient matrices Γ_f and Γ_g is APN if and only if $\Gamma_f \in SL(2, \mathbb{F}_q)$ and $|V_f| = 2$. In this case Γ_g is unique and is given by Proposition 6.*

For $m = 4$, Conjecture 1 is verified by the exhaustive full-field search. Exactly $1360 = |SL(2, \mathbb{F}_{16})|/3$ matrices $\Gamma_f \in SL(2, \mathbb{F}_{16})$ satisfy $|V_f| = 2$, and all 1360 pairs of Proposition 6 occur in the search; the same holds on $(1, 2)$, with the roles of the two coordinates exchanged. For $m = 8$ and $m = 10$, we additionally tested all 2^{16} pairs of coefficient matrices with entries in $\mathbb{F}_4$. In each dimension, exactly 20 pairs satisfy the conditions of Conjecture 1, and these are precisely the 20 APN pairs obtained in the search. Thus, the conjecture is verified on this restricted coefficient set in dimensions 16 and 20.

Table 6 illustrates the role of the coupling condition for $m = 4$. All four pairs satisfy $\det \Gamma_f = \det \Gamma_g = 1$, $|V_f| = 2$, $V_g = \emptyset$. The first three pairs are coupled and APN, whereas the last pair is not coupled and is not APN. In particular, for $(a_0, b_0, c_0, d_0) = (g^2, g^7, g, 1)$, there are 1360 determinant-one matrices Γ_g with $V_g = \emptyset$, but only its partner $(a_1, b_1, c_1, d_1) = (g^5, g^5, g^7, g^6)$ is coupled. Thus the coupling condition in Conjecture 1 cannot be omitted.

The admissible set is a proper subset of $SL(2, \mathbb{F}_q) \times SL(2, \mathbb{F}_q)$, and it is not concentrated on the unipotent class of the literature representatives: of the 1360 admissible Γ_f on $(2, 3)$ only 60 have trace $a_0 + d_0 = 0$ (90 on $(1, 2)$), and the identity matrix, although of determinant one, admits no partner, since $|V_f| = 5$ for it (Proposition 6). Over $\mathbb{F}_4$ only $20 = |SL(2, \mathbb{F}_4)|/3$ matrices Γ_f satisfy $|V_f| = 2$; each of them has its partner over $\mathbb{F}_4$ (Proposition 6), and the two transvection pairs $\Gamma_f = \Gamma_g = T^+$ and $\Gamma_f = \Gamma_g = T^-$ are two of these 20 pairs. Over $\mathbb{F}_{16}$ the admissible matrices are sixty-eight times as many and include matrices with coefficients outside $\mathbb{F}_4$, such as the second row of Table 6, yet all of them have the same ortho-derivative differential spectrum as $\mathcal{F}_1$ (on $(1, 2)$, the same spectrum as $\mathcal{F}_0$).

Table 6: Determinant-one coefficient pairs on the exponent pair $(2, 3)$ for $m = 4$, all with $|V_f| = 2$ and $V_g = \emptyset$. The tuples are those of (2), of exponents 2 and 3; g is a root of the primitive polynomial $x^4 + x + 1$ over $\mathbb{F}_2$.

$(a_0, b_0, c_0, d_0)_2^*$	$(a_1, b_1, c_1, d_1)_3^*$	$\mathcal{Q} \mid f_{\text{bp}}$	APN	remark
$(1, 0, 1, 1)$	$(1, 0, 1, 1)$	yes	yes	$\mathcal{F}_1, \Gamma_f = \Gamma_g = T^+$
$(0, g, g^{14}, 0)$	$(g^8, 0, 0, g^7)$	yes	yes	entries outside $\mathbb{F}_4$
$(g^2, g^7, g, 1)$	(g^5, g^5, g^7, g^6)	yes	yes	partner of Γ_f
$(g^2, g^7, g, 1)$	$(1, 0, 1, 1)$	no	no	not coupled

Remark 8 (Parity). Proposition 6 is specific to even m , but the coupling is not. For the representative $\Gamma_f = \Gamma_g = T^+$ one has $f_{\text{bp}}(x, 1) = x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$ and $\mathcal{Q}(x, 1) = x^3 + x^2 + 1$, so the pair is coupled with $\mathcal{S} = x^2 + xy + y^2$, which splits over $\mathbb{F}_q$ exactly when m is even. Hence $|V_f| = 2$ for even m , while for odd m the pattern degenerates to $|V_f| = |V_g| = 0$, which holds for about a third of $SL(2, \mathbb{F}_q)$ and no longer singles out the admissible pairs. We expect the determinant condition together with the coupling to describe the admissible pairs for every m ; the full-field search in dimension ten (Section 6.4) is designed to test this in the smallest odd case.

6.3 Degenerate and one-sided configurations

Over $\mathbb{F}_{16} \times \mathbb{F}_{16}$, the degenerate search returns 2112 APN functions and the one-sided search returns 33 275. All occur on the exponent pairs $(1, 1)$, $(1, 3)$ and $(3, 3)$ and have the ortho-derivative differential spectrum of the Carlet family. In every case, the remaining bijective tuple has nonzero leading coefficient and no projective zero, precisely the admissible parameter set of the Carlet family.

This is explained by the results of Section 4.4. On these exponent pairs, both exponents are odd and coprime to 4, so the corresponding truncated traces permute $\mathbb{F}_{16}$ by Lemma 4. Proposition 2(a) therefore applies to the degenerate configurations. Moreover, every one-sided APN function found with both bijective tuples nonzero satisfies $g_{\text{bp}} = \gamma f_{\text{bp}}^{2^s}$ for suitable γ and s , so Proposition 2(b) applies as well. In either case, the function reduces to the Carlet form (xy, g_{bp}) . These configurations therefore do not generalize the Carlet family; they coincide with it exactly. Indeed, the admissible tuples here – those with nonzero leading coefficient and no projective zero – are precisely Carlet’s parameter set. There are $(2^m + 1)2^m(2^m - 1)^2/3$ of them by [2, Lemma 4], and by [26, Theorem 5.1(d)] they all give CCZ-equivalent functions for fixed q .

The Carlet family is not confined to degenerate configurations. The 11 298 Carlet functions of Table 4 have both bijective parts nonzero, with $\det \Gamma_f, \det \Gamma_g \neq 0$ and $|V_f| = |V_g| = 0$. On their exponent pairs, both truncated traces permute $\mathbb{F}_{16}$, and their ortho-derivative differential spectrum is that of the Carlet family. We do not have a proof that every APN function on such a pair is a Carlet function, but the same holds in every dimension we examined (Section 7).

6.4 Dimension 10

Let $m = 5$, so that $n = 10$ and $q = 32$. This is the smallest odd value of m with $3 \nmid m$ for which the construction of [27] is defined, and the smallest dimension in which $\mathcal{F}_1$ coincides with the univariate family F_1 of [27] under CCZ-equivalence (Theorem 6).

The degenerate and one-sided configurations not covered by Proposition 2 were searched over $\mathbb{F}_{32} \times \mathbb{F}_{32}$: the exponent pairs whose trace-carrying side fails Lemma 4 and, in the one-sided case, the pairs for which the Gold exponents $2^i + 1$ and $2^j + 1$ do not lie in a common cyclotomic coset modulo $2^m - 1$, which is necessary for the hypothesis of Proposition 2(b). Both searches return no APN function. Hence, in dimension ten as in dimension eight, the degenerate and one-sided configurations produce only functions of Carlet type.

7 Searches with subfield coefficients

For $m \geq 5$, we restrict the bijective coefficients to a proper subfield: to $\mathbb{F}_2$ when m is odd, which for prime m is the only proper subfield, and to $\mathbb{F}_4 = \{0, 1, \beta, \beta^2\}$ when m is even, where $\beta = g^{(2^m - 1)/3}$ for a primitive element g of $\mathbb{F}_{2^m}$. For every exponent pair $1 \leq i \leq j \leq m - 1$, we search all coefficient tuples in the chosen subfield, with both truncated trace terms present with coefficient one. Coefficient pairs that differ only by interchanging the two coordinates are counted as one class. We label each class by the function $\mathcal{G}_s$ or $\mathcal{G}'_s$ of (24) with the corresponding

exponent pair and coefficient tuples. As observed in Section 8, every class found outside the Carlet family admits such a label.

7.1 Coefficients in $\mathbb{F}_2$: dimensions 10, 14, 22 and 26

Over $\mathbb{F}_2$, the orbit reduction of Section 5.2 has no effect: the only scaling $(x, y) \mapsto (\lambda x, \lambda^{-1}y)$ that keeps every coefficient in $\mathbb{F}_2$ is $\lambda = 1$, and the Frobenius fixes $\mathbb{F}_2$ pointwise. These searches therefore enumerate every $\mathbb{F}_2$ -coefficient tuple. We retain the degenerate configurations as a check on Proposition 2. In all four dimensions, the only coefficient tuples that occur in APN functions with both biprojective parts nonzero are the transvections T^+ and T^- , in accordance with the determinant condition (30). Each class is represented by two equivalent coefficient pairs: $[T^+, T^-]$, $[T^-, T^+]$ or $[T^+, T^+]$, $[T^-, T^-]$.

Dimension 10. Let $m = 5$. The search returns 24 APN functions. Sixteen are degenerate and are equivalent to the $\varphi(5)/2 = 2$ Carlet classes. The remaining eight form exactly four classes, one for each of $\mathcal{G}_s, \mathcal{G}'_s$ with $s \in \{1, 2\}$ (Table 7); the pair $(2, 4)$ induces two of them, with the coefficients $[T^+, T^+]$ and $[T^+, T^-]$. Their ortho-derivative differential spectra coincide with those of F_l, F_1, F_3 and F_2 in [27, Table IV], respectively. No class beyond those of [27] occurs.

Table 7: Output of the exhaustive $\mathbb{F}_2$ -coefficient search over $\mathbb{F}_{2^5} \times \mathbb{F}_{2^5}$ with both biprojective parts nonzero: four classes, each occurring as the two orderings of one transvection pair.

(i, j)	coefficients	function	ortho-derivative differential spectrum	identification
(1, 2)	$[T^+, T^-]$	$\mathcal{G}_1 = \mathcal{F}_0$	$0 \sim 634041, 2 \sim 320166, 4 \sim 78420, 6 \sim 13020,$ $8 \sim 1830, 10 \sim 60, 12 \sim 15$	F_l of [27]
(2, 4)	$[T^+, T^+]$	$\mathcal{G}'_1 = \mathcal{F}_1$	$0 \sim 636591, 2 \sim 316371, 4 \sim 78720, 6 \sim 13740,$ $8 \sim 1935, 10 \sim 165, 12 \sim 30$	F_1 of [27]
(2, 4)	$[T^+, T^-]$	$\mathcal{G}_2$	$0 \sim 631911, 2 \sim 323421, 4 \sim 78495, 6 \sim 11775,$ $8 \sim 1725, 10 \sim 210, 12 \sim 15$	F_3 of [27]
(3, 4)	$[T^+, T^+]$	$\mathcal{G}'_2$	$0 \sim 632286, 2 \sim 322566, 4 \sim 78540, 6 \sim 12675,$ $8 \sim 1320, 10 \sim 165$	F_2 of [27]

Dimension 14. Let $m = 7$. The search returns 48 APN functions. Of these, 36 are degenerate and realize the $\varphi(7)/2 = 3$ Carlet classes, twelve instances each; their spectra are those of the Carlet family for $k \in \{1, 6\}, \{2, 5\}$ and $\{3, 4\}$, in agreement with the identification of the Carlet parameters k and $m - k$ in [26, Theorem 5.1(d)]. The remaining twelve functions form six classes, one for each of $\mathcal{G}_s, \mathcal{G}'_s$ with $s \in \{1, 2, 3\}$ (Table 8).

Table 8: Output of the exhaustive $\mathbb{F}_2$ -coefficient search over $\mathbb{F}_{2^7} \times \mathbb{F}_{2^7}$ with both biprojective parts nonzero: six classes, each occurring as the two orderings of one transvection pair.

(i, j)	coefficients	function	identification
(1, 2)	$[T^+, T^-]$	$\mathcal{G}_1 = \mathcal{F}_0$	Li–Zhou–Li–Qu (F22)
(2, 6)	$[T^+, T^+]$	$\mathcal{G}'_1 = \mathcal{F}_1$	spectrum of F_1 of [27] (F14)
(2, 4)	$[T^+, T^-]$	$\mathcal{G}_2$	new (Proposition 7)
(4, 5)	$[T^+, T^+]$	$\mathcal{G}'_2$	new (Proposition 7)
(3, 6)	$[T^+, T^-]$	$\mathcal{G}_3$	spectrum of F_3 of [27] (F16*)
(4, 6)	$[T^+, T^+]$	$\mathcal{G}'_3$	spectrum of F_2 of [27] (F15*)

We compare these six classes with every known family defined for $n = 14$. Among the power functions of Table 1, only the Gold functions are quadratic, and by [36], a power APN function CCZ-equivalent to a quadratic function is EA-equivalent to a Gold function. Among the univariate families of Table 2, F1–F2 require $n = pk$ with $p \in \{3, 4\}$, which excludes $n = 14$; F5–F6 require $3 \mid n$; and F7–F10 and F13 require $n = 3m$. The hexanomials F3 coincide with the Carlet family by [14]. This leaves F4, F11 of [12], F12 of [37], and the functions F_1, F_2, F_3 of [27]. The families F11 and F12 carry free parameters, so for each we first reduce to a complete set of representatives up to

than six. Since the substitution $x \mapsto \lambda x$ replaces the parameter a of F4 by $a\lambda^3$ up to an output scaling, and the Frobenius replaces a by a^2 , the classes of F4 are represented by $a = 1$ and $a = g$. None of these spectra coincides with any of the ten, with the two exceptions predicted by Conjecture 2(c): those of F_2 and F_3 coincide with the spectra of $\mathcal{G}'_5$ and $\mathcal{G}_5$ respectively. In particular, all of them differ from the spectra of the six candidates. We note that the computed spectra of the Gold functions, of F11 and of F12, have all their multiplicities divisible by 2047, as Lemma 5 requires, which corroborates the argument of the preceding paragraph.

Up to linear equivalence, F25 is an extended (1, 2)-biprojective function with trace parameter $\varepsilon = \alpha$ in the sense of Proposition 1, since $xy + \alpha x^2 y^2 = \alpha^{-1} t_2(\alpha xy)$; for $\alpha = 1$ it is F22 itself. For $\alpha \notin \mathbb{F}_2$ we know no symmetry of its members that would reduce the computation, and Lemma 5 does not apply to F25, the perturbation carried by its functions destroying the diagonal scaling on which the lemma rests. Of the 683 admissible values of α , one is $\alpha = 1$ and the remaining 682 fall into 62 classes under the Frobenius, each requiring about 2^{44} operations. We computed $\alpha = 1$, which is F22 itself, and one further Frobenius class, which again gives the spectrum of F22; owing to the cost, we did not test the remaining 61 classes. For $m \in \{4, 7, 8, 10\}$ we checked that every admissible value of α gives the spectrum of F22 — at $m = 10$ this is a complete sweep of all 36 Frobenius classes — which suggests that F25 yields no class beyond F22. Therefore, the six candidates are CCZ-inequivalent to every known family defined for $n = 22$, except possibly to members of F25 (Proposition 10).

Dimension 26. Let $m = 13$. The search returns 168 APN functions, of which 144 are degenerate; as the ortho-derivative differential spectra were not computed in this dimension, we do not classify the degenerate functions further. The remaining 24 functions lie on exactly twelve exponent pairs, those of $\mathcal{G}_s$ and $\mathcal{G}'_s$ for $s \in \{1, \dots, 6\}$ (Table 12), each as the two orderings of the transvection pair of that function. Besides $\mathcal{G}_1, \mathcal{G}'_1$ and the member $s = 6 = (m - 1)/2$, the eight functions with $s \in \{2, \dots, 5\}$ are candidates for new CCZ-classes.

7.2 Coefficients in $\mathbb{F}_4$: dimensions 16, 20 and 28

For even m we take coefficients in $\mathbb{F}_4$ and exclude the degenerate configurations using Proposition 2. Here the admissible tuples are no longer only T^+ and T^- : each class outside the Carlet family contains several coefficient tuples, all satisfying the determinant condition (30), for instance $[(1, 0, \beta, 1), (\beta, 1, 0, \beta^2)]$ on the pair (3, 6) for $m = 8$. These classes thus exhibit the same widening of the coefficient set as $\mathcal{F}_1$ in Section 6.2. As in Section 6, each search tests one coefficient tuple from each orbit of Section 5.2, and the numbers of APN functions reported below count these tuples.

Dimension 16. Let $m = 8$. The search returns 132 APN functions, all with both biprojective parts nonzero, in six ortho-derivative differential spectra (Table 10). The two spectra with 56 instances each lie on the pairs (1, 1), (1, 7), (7, 7) and (3, 3), (3, 5), (5, 5), where both truncated traces permute $\mathbb{F}_{2^8}$, and they are the Carlet classes for $k \in \{1, 7\}$ and $k \in \{3, 5\}$. These instances are nondegenerate, showing that the presence of two nonzero biprojective parts does not by itself distinguish a function from the Carlet family. The four remaining spectra, with 5 instances each, are those of $\mathcal{G}_1 = \mathcal{F}_0$ on (1, 2), $\mathcal{G}'_1 = \mathcal{F}_1$ on (2, 7), $\mathcal{G}_3$ on (3, 6) and $\mathcal{G}'_3$ on (5, 6); the value $s = 2$, with the pairs (2, 4) and (4, 6), is excluded by $\gcd(s, m) = 2$.

Table 10: Exhaustive $\mathbb{F}_4$ -coefficient search over $\mathbb{F}_{2^8} \times \mathbb{F}_{2^8}$, degenerate configurations excluded, grouped by ortho-derivative differential spectrum. Coefficient tuples are written $[(a_0, b_0, c_0, d_0), (a_1, b_1, c_1, d_1)]$, with the exponents added where a row lists several pairs; one representative is shown per spectrum.

(i, j)	#	representative	identification
(1, 1), (1, 7), (7, 7)	56	$[(1, 0, 0, \beta)_1^*, (\beta, 0, 0, 1)_7^*]$	Carlet, $k \in \{1, 7\}$
(3, 3), (3, 5), (5, 5)	56	$[(1, 0, 0, \beta)_3^*, (\beta, 0, 0, 1)_5^*]$	Carlet, $k \in \{3, 5\}$
(1, 2)	5	$[(1, 0, 1, 1), (1, 1, 0, 1)]$	$\mathcal{G}_1 = \mathcal{F}_0$ (F22)
(2, 7)	5	$[(0, \beta, \beta^2, 0), (\beta^2, 0, 0, \beta)]$	$\mathcal{G}'_1 = \mathcal{F}_1$
(3, 6)	5	$[(1, 0, 1, 1), (1, 1, 0, 1)]$	$\mathcal{G}_3$, new (Proposition 8)
(5, 6)	5	$[(1, 0, 1, 1), (1, 0, 1, 1)]$	$\mathcal{G}'_3$, new (Proposition 8)

Of the univariate families, only F4 is defined for $n = 16$: F1–F2 require $n = pk$ with $p \in \{3, 4\}$, and $n = 16$ forces $p = 4$, $k = 4$ and $i = sk \bmod p = 0$, so that the two exponents collapse and the function is a scalar multiple of a Gold function; F5–F6 require $3 \mid n$; F7–F10 and F13 require $n = 3m$; F11, F12 and F14–F16 require m odd; and the hexanomials F3 coincide with the Carlet family. Of the power functions, only the Gold function is quadratic. Of the

bivariate families of Table 3, F21 and F23 do not occur for $m = 8$, since they require m odd and $m \equiv 2 \pmod{4}$, respectively. F19 does not occur either: an exhaustive check for $m = 8$, and likewise for $m = 10$, finds no triple (i, b, c) satisfying the no-root condition of Table 3. The spectra of all remaining known families in this dimension are listed in Table 15 of Appendix B; none of them equals the spectrum of $\mathcal{F}_1$, $\mathcal{G}_3$ or $\mathcal{G}'_3$ (Proposition 8).

Dimension 20. Let $m = 10$. The search returns 84 APN functions in six ortho-derivative differential spectra (Table 11). Two spectra with 32 instances each lie on the pairs $(1, 1), (9, 9)$ and $(3, 3), (7, 7)$, where both truncated traces permute $\mathbb{F}_{2^{10}}$, and they are the $\varphi(10)/2 = 2$ Carlet classes. The four spectra with 5 instances each are those of $\mathcal{G}_1$ on $(1, 2)$, $\mathcal{G}'_1 = \mathcal{F}_1$ on $(2, 9)$, $\mathcal{G}_3$ on $(3, 6)$ and $\mathcal{G}'_3$ on $(6, 7)$; the values $s = 2$ and $s = 4$ are excluded by $\gcd(s, 10) = 2$.

In Table 16, we compare these spectra with those of the known families computed over $\mathbb{F}_{2^{20}}$: the Gold functions, F4, the Carlet family, F17, F18, F20, F22, F23, F24 and F25. Three coincidences appear among them. The spectra of F17 for $k = 1$ and $k = 3$ equal those of the Carlet family with the same k , as [26, Theorem B.3] requires for m even; F24 realizes one spectrum per k , independent of α , equal to that of F20 with the same k ; and F25 has the spectrum of F22, which is that of $\mathcal{G}_1 = \mathcal{F}_0$ on $(1, 2)$. The spectra of $\mathcal{F}_1$, $\mathcal{G}_3$ and $\mathcal{G}'_3$ coincide with none of them and are pairwise distinct.

To the rest of the known functions in this dimension, we can apply Lemma 5, since all multiplicities in the spectra of F1–F2, which here have $n = 4k$ with $k = 5$, are divisible by $2^5 - 1 = 31$, and those of the Carlet family and of F17, F18, F20, F23 and F24 are divisible by $q - 1 = 1023 = 3 \cdot 11 \cdot 31$, for every value of their parameters. In contrast, each of the spectra of $\mathcal{F}_1$, $\mathcal{G}_3$ and $\mathcal{G}'_3$ has multiplicities not divisible by 31. This matters in particular for F18, which admits 36 classes of its parameter per k , and for F17, which admits about 69. The table lists a sample of each, and the lemma disposes of the rest. Finally, F19 and F21 do not occur for $m = 10$, the first having no admissible parameters and the second requiring m odd.

The one family requiring a complete parameter sweep is F25, whose functions carry a perturbation destroying the diagonal scaling on which Lemma 5 rests; none of the 13 multiplicities of its spectrum is divisible by 1023. For $m = 10$, we therefore computed it completely: of the 341 admissible values of α , which fall into 36 classes under the Frobenius, all 36 were computed and give the spectrum of F22.

Hence $\mathcal{F}_1$, $\mathcal{G}_3$ and $\mathcal{G}'_3$ are CCZ-inequivalent to each other and to every known family defined for $n = 20$ (Proposition 9).

Table 11: Exhaustive $\mathbb{F}_4$ -coefficient search over $\mathbb{F}_{2^{10}} \times \mathbb{F}_{2^{10}}$, degenerate configurations excluded; one representative is shown per class.

(i, j)	#	representative	identification
$(1, 1), (9, 9)$	32	$[(1, 0, 0, \beta)_1^*, (\beta, 0, 0, \beta^2)_1^*]$	Carlet, $k \in \{1, 9\}$
$(3, 3), (7, 7)$	32	$[(1, 0, 0, \beta)_3^*, (\beta, 0, 0, \beta^2)_3^*]$	Carlet, $k \in \{3, 7\}$
$(1, 2)$	5	$[(1, 0, 1, 1)_1^*, (1, 1, 0, 1)_2^*]$	$\mathcal{G}_1 = \mathcal{F}_0$
$(2, 9)$	5	$[(0, \beta, \beta^2, 0)_2^*, (\beta^2, 0, 0, \beta)_9^*]$	$\mathcal{G}'_1 = \mathcal{F}_1$
$(3, 6)$	5	$[(1, 0, 1, 1)_3^*, (1, 1, 0, 1)_6^*]$	$\mathcal{G}_3$, new (Proposition 9)
$(6, 7)$	5	$[(0, \beta, \beta^2, 0)_6^*, (\beta^2, 0, 0, \beta)_7^*]$	$\mathcal{G}'_3$, new (Proposition 9)

Dimension 28. Let $m = 14$. The search returns 126 APN functions; ortho-derivative differential spectra were not computed. Ninety-six of them lie, sixteen each, on the six pairs $(1, 1), (13, 13), (3, 3), (11, 11), (5, 5)$ and $(9, 9)$, on which both truncated traces permute; by analogy with all smaller dimensions we expect them to form the $\varphi(14)/2 = 3$ Carlet classes. The remaining 30 functions lie, five each, on the six pairs of $\mathcal{G}_s, \mathcal{G}'_s$ with $s \in \{1, 3, 5\}$, namely $(1, 2), (2, 13), (3, 6), (6, 11), (5, 10), (9, 10)$.

Varying the trace coefficient. By Proposition 1, for coefficients in $\mathbb{F}_4$ the only Frobenius orbit of nonzero trace ratios not represented by $\varepsilon = 1$ is represented by $\varepsilon = \beta$. We tested this case in dimensions 8 and 16, enumerating one representative from each orbit under the scaling and Frobenius reductions. In dimension 8, every APN function obtained with $\varepsilon = \beta$ has a spectrum already obtained for $\varepsilon = 1$. In dimension 16, the APN functions with $\varepsilon = \beta$ realize only three of the six spectra in Table 10: the two Carlet spectra and that of $\mathcal{G}_1 = \mathcal{F}_0$. The spectra of $\mathcal{F}_1$, $\mathcal{G}_3$ and $\mathcal{G}'_3$ occur only for $\varepsilon = 1$. Thus, in the dimensions tested, allowing a free trace coefficient produces no additional ortho-derivative differential spectrum.

7.3 New CCZ-classes

In each case, the APN property is certified by the exhaustive test of Section 5.1 (Algorithm 1). The listed functions have pairwise distinct ortho-derivative differential spectra, which also differ from those of every family of Tables 1–3 over $\mathbb{F}_{2^n}$ (Appendix B) for $n = 14, 16, 20$ and 22 . Since this is a CCZ-invariant of quadratic APN functions, the stated inequivalences follow.

Proposition 7 (New instances in dimension 14). *Over $\mathbb{F}_{2^{14}}$ the extended bijective functions*

$$\mathcal{G}_2 = [T_2^{+*}, T_4^{-*}] = (x^5 + xy^4 + y^5 + t_2(xy), x^{17} + x^{16}y + y^{17} + t_4(xy)), \quad (33)$$

$$\mathcal{G}'_2 = [T_4^{+*}, T_5^{+*}] = (x^{17} + xy^{16} + y^{17} + t_4(xy), x^{33} + xy^{32} + y^{33} + t_5(xy)) \quad (34)$$

are APN, CCZ-inequivalent to each other, and CCZ-inequivalent to every family of Tables 1–3 defined for $n = 14$, including $\mathcal{F}_1$ and the functions F_2, F_3 of [27].

Proposition 8 (New instances in dimension 16). *Over $\mathbb{F}_{2^{16}}$ the extended bijective function*

$$\mathcal{G}_3 = [T_3^{+*}, T_6^{-*}] = (x^9 + xy^8 + y^9 + t_3(xy), x^{65} + x^{64}y + y^{65} + t_6(xy)) \quad (35)$$

and the function $\mathcal{G}'_3 = [T_6^{+*}, T_5^{+*}]$, which up to the order of its coordinates is

$$[T_5^{+*}, T_6^{+*}] = (x^{33} + xy^{32} + y^{33} + t_5(xy), x^{65} + xy^{64} + y^{65} + t_6(xy)), \quad (36)$$

are APN, CCZ-inequivalent to each other, and CCZ-inequivalent to every family of Tables 1–3 defined for $n = 16$. The same holds for $\mathcal{F}_1 = \mathcal{G}'_1$ over $\mathbb{F}_{2^{16}}$.

Proposition 9 (New instances in dimension 20). *Over $\mathbb{F}_{2^{20}}$ the extended bijective functions*

$$\mathcal{G}_3 = [T_3^{+*}, T_6^{-*}] = (x^9 + xy^8 + y^9 + t_3(xy), x^{65} + x^{64}y + y^{65} + t_6(xy)),$$

$$\mathcal{G}'_3 = [T_6^{+*}, T_7^{+*}] = (x^{65} + xy^{64} + y^{65} + t_6(xy), x^{129} + xy^{128} + y^{129} + t_7(xy))$$

are APN and CCZ-inequivalent to each other and to $\mathcal{F}_1$. Moreover, each of $\mathcal{F}_1, \mathcal{G}_3$ and $\mathcal{G}'_3$ is CCZ-inequivalent to every family of Tables 1–3 defined for $n = 20$.

Proposition 10 (New instances in dimension 22). *Over $\mathbb{F}_{2^{22}}$ the ten extended bijective functions $\mathcal{G}_s, \mathcal{G}'_s$ with $1 \leq s \leq 5$ are APN and pairwise CCZ-inequivalent. The six functions with $s \in \{2, 3, 4\}$,*

$$\mathcal{G}_2 = [T_2^{+*}, T_4^{-*}],$$

$$\mathcal{G}_3 = [T_3^{+*}, T_6^{-*}],$$

$$\mathcal{G}_4 = [T_4^{+*}, T_8^{-*}],$$

$$\mathcal{G}'_2 = [T_4^{+*}, T_9^{+*}],$$

$$\mathcal{G}'_3 = [T_6^{+*}, T_8^{+*}],$$

$$\mathcal{G}'_4 = [T_7^{+*}, T_8^{+*}],$$

are CCZ-inequivalent to every family of Tables 1–3 defined for $n = 22$, with the single exception of the members of F25 whose parameter α lies in one of the 61 Frobenius classes we did not test. We expect no such member to give a spectrum other than that of F22, in which case the six functions are CCZ-inequivalent to every known family defined for $n = 22$.

Remark 9. We tested the parameter α in both families of [15] over $\mathbb{F}_{2^{22}}$, computing all ten instances of F24 fixed in Section A.1 and two of F25. The two families stand differently. F24 is a bijective polynomial pair, both of whose components are homogeneous of degree $q + 1$, respectively $q^2 + 1$, so the diagonal scaling $(x, y) \mapsto (ax, ay)$ is an EL-automorphism for every $a \in \mathbb{F}_{2^m}^\times$ and Lemma 5 applies to every instance of F24, whatever the values of k and α . For F24 the exclusion is therefore proved and not merely tested; the ten computed spectra confirm it, all of their multiplicities being divisible by 2047. For F25 the lemma does not apply, the term xy breaking the homogeneity of the first component. There we computed $\alpha = 1$, which is F22 itself, and one Frobenius class of $\alpha \notin \mathbb{F}_2$, which gives the spectrum of F22 as well. Together with the complete sweeps for $m \in \{4, 7, 8, 10\}$, where every admissible α gives the spectrum of F22, we do not expect F25 to yield a spectrum beyond that of F22, although 61 Frobenius classes of α remain untested for $m = 11$.

The spectra on which Propositions 7–10 rely are listed in Tables 13, 14, 15, 16 and 17 of Appendix B. For $n = 20$, the table contains instances of every family defined in that dimension except F1–F2, for which Lemma 5 applies with $G \cong \mathbb{F}_{2^5} \setminus \{0\}$, so that all multiplicities are divisible by 31; the same lemma covers the instances of the Carlet family and of F17, F18, F20, F22, F23 and F24 that the table does not list, with the divisor $q - 1 = 1023$. For $n = 22$, the

table is complemented by the lemma analogously, leaving only the comparison with F25 unresolved; see Remark 9 above.

All new instances in Propositions 7–10 come from the switching series of Section 4.5. They are the functions $\mathcal{G}_s, \mathcal{G}'_s$ with $s \in S_m$, $s \neq 1$ and $2s \neq m - 1$, together with $\mathcal{G}'_1 = \mathcal{F}_1$ when m is even. Their coefficient tuples are independent of the dimension: $[T^+, T^-]$ on $(s, 2s)$ for $\mathcal{G}_s$, and $[T^+, T^+]$ on $\{2s, m - s\}$ for $\mathcal{G}'_s$. In Section 8 we show that, apart from functions of Carlet type, the searches in all dimensions up to 28 return exactly these series (Observation 10). This leads us to conjecture that, for each fixed s , the functions $\mathcal{G}_s$ and $\mathcal{G}'_s$ form infinite families of APN functions whose members with $m = 2s + 1$ are the functions F_3 and F_2 of [27] (Conjecture 2).

8 The switching series across dimensions

For $m \geq 4$ let

$$S_m = \left\{ s : 1 \leq s \leq \frac{m-1}{2}, \gcd(s, m) = 1 \right\}.$$

The map $s \mapsto m - s$ pairs the units modulo m , with exactly one element of each pair smaller than $m/2$. Hence $|S_m| = \varphi(m)/2$. For $s \in S_m$, the functions $\mathcal{G}_s$ and $\mathcal{G}'_s$ of Section 4.5 have exponent pairs $(s, 2s)$ and $\{2s, m - s\}$, respectively. Table 12 lists these pairs for every value of m considered in our searches. Recall that $\mathcal{G}_s$ has coefficient pair $[T^+, T^-]$, while $\mathcal{G}'_s$ has coefficient pair $[T^+, T^+]$.

Table 12: Exponent pairs of $\mathcal{G}_s$ and $\mathcal{G}'_s$ for $s \in S_m$.

m	S_m	$\mathcal{G}_s$: $(s, 2s)$	$\mathcal{G}'_s$: $\{2s, m - s\}$
4	$\{1\}$	(1, 2)	(2, 3)
5	$\{1, 2\}$	(1, 2) , (2, 4)	(2, 4) , (3, 4)
7	$\{1, 2, 3\}$	(1, 2) , (2, 4) , (3, 6)	(2, 6) , (4, 5) , (4, 6)
8	$\{1, 3\}$	(1, 2) , (3, 6)	(2, 7) , (5, 6)
10	$\{1, 3\}$	(1, 2) , (3, 6)	(2, 9) , (6, 7)
11	$\{1, \dots, 5\}$	(1, 2) , (2, 4) , (3, 6) , (4, 8) , (5, 10)	(2, 10) , (4, 9) , (6, 8) , (7, 8) , (6, 10)
13	$\{1, \dots, 6\}$	(1, 2) , (2, 4) , (3, 6) , (4, 8) , (5, 10) , (6, 12)	(2, 12) , (4, 11) , (6, 10) , (8, 9) , (8, 10) , (7, 12)
14	$\{1, 3, 5\}$	(1, 2) , (3, 6) , (5, 10)	(2, 13) , (6, 11) , (9, 10)

The entries in boldface correspond to $\mathcal{G}_1 = \mathcal{F}_0$ and $\mathcal{G}'_1 = \mathcal{F}_1$ for every m , and, for odd m , to $\mathcal{G}_{(m-1)/2}$ and $\mathcal{G}'_{(m-1)/2}$. The latter are the bivariate candidates for the families F_3 and F_2 of [27], respectively; see Conjecture 2(c). In every search, all APN functions outside the Carlet family occur on the exponent pairs listed in Table 12.

Observation 10. Let $m \in \{4, 5, 7, 8, 10, 11, 13, 14\}$, that is, $4 \leq m \leq 14$ and $3 \nmid m$.

- (i) In every search of Sections 6 and 7, each exponent pair of Table 12 carries APN functions with the coefficients of $\mathcal{G}_s$ or $\mathcal{G}'_s$. Every APN function found with both biprojective parts nonzero lies either on a pair of Table 12 or on a pair (i, j) with i, j odd and coprime to m , on which both truncated traces permute $\mathbb{F}_q$.
- (ii) In the dimensions where the spectra were computed ($n \leq 22$), the functions on the exponent pairs of Table 12 have the spectra of the corresponding $\mathcal{G}_s$ and $\mathcal{G}'_s$. For each fixed m , these $\varphi(m)$ spectra are pairwise distinct.
- (iii) In the dimensions where the spectra were computed ($n \leq 22$), the functions of Carlet type found in the searches realize exactly $\varphi(m)/2$ distinct spectra, namely those of the Carlet family.

Thus, outside the Carlet family, the output of every search consists of the $\varphi(m)/2$ switching pairs $(\mathcal{G}_s, \mathcal{G}'_s)$, $s \in S_m$, introduced in Section 4.5. The same pairs recur across dimensions with the same coefficient tuples. For example, $\mathcal{G}_3$ occurs on $(3, 6)$ with coefficient pair $[T^+, T^-]$ for $m = 7, 8, 10, 11, 13, 14$. We therefore fix s and regard $\mathcal{G}_s$ and $\mathcal{G}'_s$ as two infinite families, defined for every m with $s \in S_m$, that is, for $m \geq 2s + 1$ with $\gcd(s, m) = 1$ and $3 \nmid m$. For $s = 1$ they are the Li–Zhou–Li–Qu family $\mathcal{F}_0$ and the family $\mathcal{F}_1$, which for odd m is F_1 of [27] (Theorem 6). For $s \geq 2$, the smallest admissible value of m is the odd value $m = 2s + 1$. There $\mathcal{G}_s$ and $\mathcal{G}'_s$ lie on the pairs $(s, m - 1)$ and $(m - 1, s + 1)$, and for $m = 5, 7$ and 11 they have the spectra of F_3 and F_2 of [27]. For all larger m , of either parity, the same two families give new CCZ-classes in every dimension in which we compared them with the known families (Propositions 7–10). For instance, $\mathcal{G}_3$ and $\mathcal{G}'_3$ have the spectra of F_3 and F_2 for $m = 7$, and they give new classes for $m = 8$ and $m = 10$. Thus F_3 and F_2 , which exist only for odd m , are the members with

$m = 2s + 1$ of the families $\mathcal{G}_s$ and $\mathcal{G}'_s$, and the new classes in even dimensions belong to the same families. This leads us to the following conjecture.

Conjecture 2. *Let $s \geq 1$, and let $m \geq 2s + 1$ with $\gcd(s, m) = 1$ and $3 \nmid m$.*

- (a) *The functions $\mathcal{G}_s$ and $\mathcal{G}'_s$ are APN on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.*
- (b) *For fixed m , the $\varphi(m)$ functions $\mathcal{G}_s, \mathcal{G}'_s$ with $s \in S_m$ are pairwise CCZ-inequivalent.*
- (c) *If $m = 2s + 1$, then $\mathcal{G}_s$ and $\mathcal{G}'_s$ are CCZ-equivalent to the functions F_3 and F_2 of [27] (F_{16}^* and F_{15}^* in Table 2), respectively:*

$$F_3 \sim \mathcal{G}_s = [T_s^{+*}, T_{m-1}^{-*}], \quad (37)$$

$$F_2 \sim \mathcal{G}'_s = [T_{m-1}^{+*}, T_{s+1}^{+*}], \quad (38)$$

where $\sim$ denotes CCZ-equivalence.

- (d) *If $s \geq 2$ and $m > 2s + 1$, then $\mathcal{G}_s$ and $\mathcal{G}'_s$ are CCZ-inequivalent to the Carlet family and to every member of the families of Tables 1–3. The same holds for $\mathcal{G}'_1 = \mathcal{F}_1$ when m is even.*

We summarize the evidence for the conjecture. Part (a) is proved for $s = 1$: $\mathcal{G}_1 = \mathcal{F}_0$ is APN by [31], and $\mathcal{G}'_1 = \mathcal{F}_1$ is APN by Theorem 5. Observation 10, together with the direct verification of $\mathcal{G}_s$ and $\mathcal{G}'_s$ for $m = 14$, verifies part (a) for every $m \leq 14$ with $3 \nmid m$. Part (b) is verified by the distinct ortho-derivative differential spectra for every $m \leq 11$ with $3 \nmid m$. For part (c), the ortho-derivative differential spectra agree for $m = 5$ (Table 7 and [27, Table IV]), $m = 7$ (Table 13), and $m = 11$ (Table 17). For $m = 13$, the functions $\mathcal{G}_6$ and $\mathcal{G}'_6$ are again found in the search with the same transvection coefficient pairs, although their spectra were not computed. Part (d) is established for $m = 7, 8$, and 10 by Propositions 7, 8, and 9, respectively. For $m = 11$, it is up to the unresolved members of $\mathcal{F}_{25}$ (see Proposition 10). For $\mathcal{G}'_1 = \mathcal{F}_1$, the corresponding statement holds for $m = 4, 8$ and 10 by Propositions 5, 8, and 9, respectively. The condition $\gcd(s, m) = 1$ is necessary by Corollary 2. Moreover, for $m \in \{6, 9\}$, none of the functions $\mathcal{G}_s, \mathcal{G}'_s$ with $1 \leq s \leq (m - 1)/2$ is APN.

By Corollary 3, once $\mathcal{G}_s$ is known to be APN, the APN property of $\mathcal{G}'_s$ is equivalent to the absence of solutions of $D_{(a,b)}\widehat{\mathcal{G}}_s(x, y) = (0, 1)$ with $\text{tr}_1^m(ay + bx) = 1$; this is exactly how Theorem 5 is proved for $s = 1$.

Remark 11. The coupling of Section 6.2 requires a coordinate of exponent 1 or $m - 1$, whose bijective part reduces to a cubic form. Among the functions $\mathcal{G}_s, \mathcal{G}'_s$, such a coordinate exists only for $s = 1$ and, when m is odd, for $s = (m - 1)/2$. For $1 < s < (m - 1)/2$ neither $\mathcal{G}_s$ nor $\mathcal{G}'_s$ has such an exponent, so a description of their admissible coefficients, as found over $\mathbb{F}_4$ in Section 7.2, requires a different mechanism.

9 Conclusions and open problems

We have shown that the extended $(2, m - 1)$ -bijective function $\mathcal{F}_1$ is APN whenever $3 \nmid m$. For odd m it is EA-equivalent to the family $\mathcal{F}_1$ of [27], and for even m it is new, as the ortho-derivative comparisons in dimensions 8, 16 and 20 confirm. The function $\mathcal{F}_1$ is a $\text{tr}_1^m(xy)$ -switching neighbour of a function linearly equivalent to the Li–Zhou–Li–Qu family. More generally, the same switching construction relates each extended Göğlü function $\mathcal{G}_s$ to the corresponding function $\mathcal{G}'_s$.

Our computational searches in dimensions 8 to 28 show a consistent pattern. Apart from functions of Carlet type, all APN functions found belong to the switching series $\mathcal{G}_s, \mathcal{G}'_s$. This accounts for all functions classified by their ortho-derivative differential spectra up to dimension 22, and for all non-Carlet exponent pairs found in dimensions 26 and 28. The degenerate and one-sided configurations examined in the searches produce only functions of Carlet type. The constructions $\mathcal{G}_s, \mathcal{G}'_s$ with $1 < s < (m - 1)/2$ give new CCZ-classes of APN functions in dimensions 14, 16 and 20, and further candidates for new classes in dimensions 22 to 28. For $m = 5, 7$ and 11 , the functions with $s = (m - 1)/2$ have the ortho-derivative differential spectra of the conjectured families F_2 and F_3 of [27]. Along the way, we have classified the known infinite families of quadratic APN functions by their ortho-derivative differential spectra in all dimensions up to 20 where our constructions are defined.

The main open problems are summarized by Conjectures 1 and 2. First, it remains to prove that the extended Göğlü functions $\mathcal{G}_s$ are APN whenever $3 \nmid m$ and $\gcd(s, m) = 1$, extending the result of [31] for $s = 1$. By Corollary 3, once the APN property of $\mathcal{G}_s$ is established, that of $\mathcal{G}'_s$ reduces to the corresponding switching condition, as in the proof of Theorem 5. For $s = (m - 1)/2$, proving this together with an explicit equivalence would settle the conjecture of [27] for F_2 and F_3 . Second, the pairwise CCZ-inequivalence of the functions $\mathcal{G}_s, \mathcal{G}'_s$ and their

inequivalence to the known families, as stated in Conjecture 2(b) and (d), remain to be established in general, beyond the dimensions in which the ortho-derivative differential spectra can be computed. Finally, it remains to determine the admissible coefficient pairs on the exponent pair $(2, m - 1)$, as predicted by Conjecture 1, and to explain the second recurring pattern in our searches: every APN function found on an exponent pair for which both truncated traces permute $\mathbb{F}_q$ is of Carlet type.

References

- [1] Shreeram S. Abhyankar. Projective polynomials. *Proceedings of the American Mathematical Society*, 125(6):1643–1650, 1997.
- [2] Daniele Bartoli, Jürgen Bierbrauer, Gohar Kyureghyan, Massimo Giulietti, Stefano Marcugini, and Fernanda Pambianco. A family of semifields in characteristic 2. *Journal of Algebraic Combinatorics*, 45(2):455–473, 2017.
- [3] Thomas Beth and Cunsheng Ding. On almost perfect nonlinear permutations. In *Workshop on the Theory and Application of Cryptographic Techniques*, pages 65–76. Springer, 1993.
- [4] Antonia W. Bluher. On $x^{q+1} + ax + b$. *Finite Fields and Their Applications*, 10(3):285–305, 2004.
- [5] Wieb Bosma, John Cannon, and Catherine Playoust. *The Magma algebra system. The user language*, 1997.
- [6] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. A few more quadratic APN functions. *Cryptography and Communications*, 3(1):43–53, 2011.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Constructing new APN functions from known ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.
- [11] Lilya Budaghyan, Claude Carlet, and Gregor Leander. On a construction of quadratic APN functions. In *2009 IEEE Information Theory Workshop*, pages 374–378. IEEE, 2009.
- [12] Lilya Budaghyan, Tor Helleseth, and Nikolay Kaleyski. A new family of APN quadrinomials. *IEEE Transactions on Information Theory*, 66(11):7081–7087, 2020.
- [13] Lilya Budaghyan, Ivana Ivkovic, and Nikolay Kaleyski. Triplicate functions. *Cryptography and Communications*, 15(1):35–83, 2023.
- [14] 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*, (546=25):79–105, 2021.
- [15] Marco Calderini, Kangquan Li, and Irene Villa. Extending two families of bivariate APN functions. *Finite Fields and Their Applications*, 88:102190, 2023.
- [16] Anne Canteaut, Alain Couvreur, and Léo Perrin. Recovering or testing extended-affine equivalence. *IEEE Transactions on Information Theory*, 68(9):6187 – 6206, 2022.
- [17] 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.
- [18] Claude Carlet. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021.
- [19] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

- [20] Hans Dobbertin. Almost perfect nonlinear power functions on $\text{GF}(2^n)$: the Niho case. *Information & Computation*, 151(1):57–72, 1999.
- [21] Hans Dobbertin. Almost perfect nonlinear power functions on $\text{GF}(2^n)$: the Welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.
- [22] Hans Dobbertin. Almost perfect nonlinear power functions on $\text{GF}(2^n)$: A new case for n divisible by 5. *International Conference on Finite Fields and Applications*, pages 113–121, 2001.
- [23] Yves Edel and Alexander Pott. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications*, 3(1):59–81, 2009.
- [24] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE Transactions on Information Theory*, 14(1):154–156, 1968.
- [25] Faruk Göloğlu. Biprojective almost perfect nonlinear functions. *IEEE Transactions on Information Theory*, 68(7):4750–4760, 2022.
- [26] Faruk Göloğlu and Lukas Kölsch. Equivalences of biprojective almost perfect nonlinear functions. *arXiv preprint arXiv:2111.04197*, 2021.
- [27] Tor Helleseht, Nadiia Ichanska, and Nikolay S. Kaleyski. New infinite families of APN functions from the switching construction in even dimension. IACR Cryptology ePrint Archive, Paper 2026/2401, 2026.
- [28] Nadiia Ichanska, Simon Berg, Nikolay Kaleyski, and Yuyin Yu. Pushing the QAM method for finding APN functions further. *Cryptography and Communications*, 18:727–762, 2026.
- [29] Heeralal Janwa and Richard M Wilson. Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 180–194. Springer, 1993.
- [30] Tadao Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes. *Information & Computation*, 18(4):369–394, 1971.
- [31] 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.
- [32] Gary McGuire and John Sheekey. A characterization of the number of roots of linearized and projective polynomials in the field of coefficients. *Finite Fields and Their Applications*, 57:68–91, 2019.
- [33] Kaisa Nyberg. Differentially uniform mappings for cryptography. *Lecture Notes in Computer Science*, 765:55–64, 1994.
- [34] Hiroaki Taniguchi. On some quadratic APN functions. *Designs, Codes and Cryptography*, 87(9):1973–1983, 2019.
- [35] Satoshi Yoshiara. Equivalences of quadratic APN functions. *Journal of Algebraic Combinatorics*, 35(3):461–475, 2012.
- [36] Satoshi Yoshiara. Equivalences of power APN functions with power or quadratic APN functions. *Journal of Algebraic Combinatorics*, 44(3):561–585, 2016.
- [37] 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.
- [38] Yue Zhou and Alexander Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43–60, 2013.

Appendix A The known families in dimensions up to 20

To identify the output of the searches, we computed the ortho-derivative differential spectra of the known infinite families of quadratic APN functions of Tables 1–3 in dimensions $n = 8, 14, 16$ and 20 . The spectra are listed in Table 5 for $n = 8$ and in Appendix B for the other dimensions. For $n = 10$, the corresponding classification is available in [13]; see also [27, Table IV]. These are all dimensions $n = 2m \leq 20$ with $m \geq 4$ and $3 \nmid m$, that is, all dimensions up to 20 in which the functions $\mathcal{G}_s$ and $\mathcal{G}'_s$ are defined. Section A.1 fixes the instances of the families that appear in the tables, and Section A.2 collects the coincidences between families that the tables reveal.

A.1 Instances and parameters

Most families of Tables 2 and 3 depend on parameters. The rows of Table 5 and of the tables in Appendix B refer to the following instances. Here g denotes a primitive element of the field in question; for $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ it is a root of the Conway polynomial $x^4 + x + 1$ and $x^8 + x^4 + x^3 + x^2 + 1$, respectively.

- Gold functions: x^{2^i+1} with $\gcd(i, n) = 1$; the exponents i and $n - i$ give the same class.
- F4: the substitution $x \mapsto \lambda x$ replaces a by $a\lambda^3$ up to an output scaling, and the Frobenius replaces a by a^2 . Hence $a = 1$ and $a = g$ represent all instances.
- F11: [12, Corollary 1] with $k = 0$ and $i \in \{m - 2, (m - 2)^{-1} \bmod n, m, n - 1\}$.
- F12: the instances of [37, Theorem 3.3(iii)] and of [37, Corollary 1(1),(2)]; the remaining items of [37, Theorem 3.3] are shown there to be equivalent to F11, to F10 or to x^3 , or to be empty.
- F14–F16: the parameters of Table 2.
- Carlet family: $(xy, x^{2^k+1} + xy^{2^k} + y^{2^k+1})$ with $\gcd(k, m) = 1$, labelled by k ; the values k and $m - k$ give the same class.
- F17 (Zhou–Pott): $\alpha = g$. In the tables, we write j for the exponent i of Table 3.
- F18 (Taniguchi): if $a \neq 0$, the substitution $y \mapsto \nu y$ with $\nu^{2^k} = a^{-1}$, followed by a scaling of the first coordinate, replaces the parameters (a, b) by $(1, d)$ with $d = b\nu^{2^k+1}$. We therefore use the functions

$$T_{k,d}(x, y) = (xy, x^{2^k+2^{3k}} + x^{2^k} y^{2^k} + d y^{2^k+1}),$$

where $d \in \mathbb{F}_q$ is such that $X^{2^k+1} + X + d$ has no root in $\mathbb{F}_q$; the tables list k and d . For $a = 0$, the function is of Zhou–Pott type after a Frobenius on the second coordinate, and for odd m this case does not occur.

- F19: for $m = 4$, all admissible parameters (i, b, c) give the same spectrum.
- F20 and F21: the tables write k for the parameter i of Table 3.
- F24: for $m \in \{4, 7, 8\}$, every admissible value of α gives the spectrum of F20 with the same k , and the tables therefore list F24 together with F20. For $m = 10$, the instances listed give the same spectrum as F20, and the remaining ones are covered by Lemma 5.
- F25: for $m \in \{4, 7, 8, 10\}$, every admissible value of α gives the spectrum of F22, and the tables therefore list F25 together with F22. For $m = 10$ this is a complete sweep: of the 341 admissible values of α , which fall into 36 classes under the Frobenius, all 36 were computed. The family F25 is the only one to which Lemma 5 does not apply. Its functions carry a perturbation that destroys the diagonal scaling, so this sweep cannot be replaced by a divisibility argument.

For a family with parameters, the instances listed need not represent all of its CCZ-classes; for instance, for $m = 8$ the tables contain two Taniguchi functions for each k . For the comparison with the functions $\mathcal{G}_s$ and $\mathcal{G}'_s$, this does not matter. The remaining instances of the Carlet family and of F1–F2, F11, F12, F17, F18, F20, F21, F23 and F24 are covered by Lemma 5, whose divisibility condition holds for all values of the parameters, and F4, F19 and, for $m \in \{4, 7, 8, 10\}$, F25 are covered completely.

A.2 Coinciding spectra

For each family we list one row per spectrum; rows with several labels collect families whose instances have the same spectrum. Since the spectrum is a CCZ-invariant, these tables separate the known families into sets of pairwise CCZ-inequivalent instances, and they single out the pairs of instances that are candidates for CCZ-equivalence.

Besides the identifications used in Sections 6 and 7, the tables exhibit the following coincidences of spectra.

- (i) For $n = 8$, the families F17, F20 and F24 share one spectrum, and F22, F25 and $\mathcal{F}_0$ share another.
- (ii) For $n = 14$, F11 with $i = 13$, $i = 7$, $i = 5$ and $i = 3$ has the spectrum of the Gold function x^3 , of the Carlet family with $k \in \{1, 6\}$, and of F20 and F24 with $k \in \{1, 6\}$ and $k \in \{3, 4\}$, respectively; F20 and F24 also agree for $k \in \{2, 5\}$; F12 from [37, Theorem 3.3(iii)] has the spectrum of F21 with $k \in \{1, 6\}$; the two instances of F12 from [37, Corollary 1] have the spectra of two Taniguchi functions with $k \in \{1, 6\}$; and F22, F25 and $\mathcal{F}_0$ agree.
- (iii) For $n = 16$, F20 and F24 agree for $k \in \{1, 7\}$ and for $k \in \{3, 5\}$, and F22, F25 and $\mathcal{F}_0$ agree.
- (iv) For $n = 20$, F17 with $k = 1$ and with $k = 3$ has the spectrum of the Carlet family with the same k ; F20 and F24 agree for $k = 1$ and for $k = 3$, the spectrum of F24 being independent of α ; and F22, F25 and $\mathcal{F}_0$ agree.

Apart from these coincidences, all spectra in each of the tables are pairwise distinct. In particular, the Taniguchi family alone realizes at least 21 CCZ-classes over $\mathbb{F}_{2^{14}}$. The coincidences between F20 and F24 and between F22 and F25 are to be expected, since the families F24 and F25 of [15] extend F20 and F22 and coincide with them for $\alpha = 1$; by Section A.1, they persist for every admissible α when $m \in \{4, 7, 8\}$, and for F25 also when $m = 10$. The remaining coincidences identify candidates for CCZ-equivalence between families from different constructions.

Appendix B Ortho-derivative differential spectra

This appendix lists the ortho-derivative differential spectra used in Sections 7 and 8, with one subsection for each of the dimensions 14, 16, 20 and 22; the instances of the known families are those of Appendix A.1. The spectra of the known families over $\mathbb{F}_{2^8}$ are given in Table 5; for the known families over $\mathbb{F}_{2^{10}}$ we refer to [13], and for F_l, F_1, F_2, F_3 over $\mathbb{F}_{2^{10}}$ to [27, Table IV]. Spectra are written in the multiset notation of Section 5.3.

B.1 Dimension 14

Table 13: Ortho-derivative differential spectra over $\mathbb{F}_{2^{14}}$ of the known families and of $\mathcal{G}'_1 = \mathcal{F}_1, \mathcal{G}_2, \mathcal{G}'_2, \mathcal{G}_3, \mathcal{G}'_3$. The 21 spectra of the Taniguchi family (F18) are listed in Table 14.

Family	Spectrum
Gold, $i \in \{1, 13\}$ $F_{11}, i = 13$	$0^{156916374}, 2^{100149279}, 6^{11353419}$
Gold, $i \in \{3, 11\}$	$0^{161700210}, 2^{83176491}, 4^{19954494}, 6^{3325749}, 8^{229362}, 14^{32766}$
Gold, $i \in \{5, 9\}$	$0^{157801056}, 2^{89713308}, 4^{18922365}, 6^{1376172}, 8^{573405}, 14^{32766}$
$F_4, a = 1$	$0^{162452562}, 2^{82368621}, 4^{19531995}, 6^{3544653}, 8^{467880}, 10^{49035}, 12^{4011}, 14^{315}$
$F_4, a = g, g^2$	$0^{162533559}, 2^{82165614}, 4^{19691826}, 6^{3507630}, 8^{468888}, 10^{47754}, 12^{3570}, 14^{210}, 16^{21}$
$F_{11}, i = 3$ Göloğlu (F_{20}), $F_{24}; k \in \{3, 4\}$	$0^{162876738}, 2^{81200244}, 4^{20517231}, 6^{3381756}, 8^{394716}, 10^{42672}, 12^{5334}, 28^{381}$
$F_{11}, i = 5$ Göloğlu (F_{20}), $F_{24}; k \in \{1, 6\}$	$0^{162999801}, 2^{81077562}, 4^{20389215}, 6^{3501771}, 8^{405384}, 10^{45339}$
Göloğlu (F_{20}), $k \in \{2, 5\}$ $F_{24}, k \in \{2, 5\}$	$0^{163143819}, 2^{80797527}, 4^{20501229}, 6^{3533775}, 8^{405384}, 10^{37338}$
$F_{11}, i = 7$ Carlet, $k \in \{1, 6\}$	$0^{162298380}, 2^{82099023}, 4^{20351877}, 6^{3315081}, 8^{312039}, 10^{42672}$
Carlet, $k \in \{2, 5\}$	$0^{162471735}, 2^{81880329}, 4^{20383881}, 6^{3221736}, 8^{410718}, 10^{50673}$
Carlet, $k \in \{3, 4\}$	$0^{162541077}, 2^{81805653}, 4^{20306538}, 6^{3328416}, 8^{381381}, 10^{56007}$
F_{12} , Thm. 3.3(iii) Göloğlu (F_{21}), $k \in \{1, 6\}$	$0^{162935793}, 2^{81402936}, 4^{20021169}, 6^{3549777}, 8^{440055}, 10^{61341}, 12^{8001}$
Göloğlu (F_{21}), $k \in \{2, 5\}$	$0^{162858450}, 2^{81344262}, 4^{20298537}, 6^{3461766}, 8^{402717}, 10^{48006}, 12^{5334}$
Göloğlu (F_{21}), $k \in \{3, 4\}$	$0^{162151695}, 2^{82445733}, 4^{20189190}, 6^{3181731}, 8^{413385}, 10^{37338}$
F_{12} , Cor. 1(1) Taniguchi (F_{18}), $k \in \{1, 6\}$	$0^{162746436}, 2^{81533619}, 4^{20263739}, 6^{3403981}, 8^{424942}, 10^{41656}, 12^{4445}, 14^{254}$
F_{12} , Cor. 1(2) Taniguchi (F_{18}), $k \in \{1, 6\}$	$0^{162729291}, 2^{81505552}, 4^{20355814}, 6^{3374390}, 8^{406400}, 10^{42799}, 12^{4318}, 14^{381}, 16^{127}$
$F_{14}, i = 5$ $\mathcal{F}_1 = \mathcal{G}'_1$	$0^{162757251}, 2^{81482043}, 4^{20330352}, 6^{3383247}, 8^{418698}, 10^{43092}, 12^{3927}, 14^{462}$
$F_{15}^* = F_2, k=2, i=3$ $\mathcal{G}'_3$ on $(4, 6)$	$0^{162740661}, 2^{81504996}, 4^{20332305}, 6^{3374469}, 8^{421239}, 10^{41118}, 12^{4032}, 14^{231}, 16^{21}$
$F_{16}^* = F_3, k=2, i=3$ $\mathcal{G}_3$ on $(3, 6)$	$0^{162773841}, 2^{81444264}, 4^{20350848}, 6^{3386166}, 8^{418824}, 10^{41349}, 12^{3444}, 14^{315}, 16^{21}$
Li–Zhou–Li–Qu (F_{22}), F_{25} ; $\mathcal{G}_1 = \mathcal{F}_0$	$0^{162832473}, 2^{81353292}, 4^{20365863}, 6^{3395658}, 8^{425880}, 10^{41832}, 12^{3717}, 14^{315}, 16^{21}, 18^{21}$
Taniguchi (F_{18})	21 classes over $\mathbb{F}_{2^{14}}$; see Table 14
$\mathcal{G}_2$ on $(2, 4)$ new	$0^{162774324}, 2^{81454008}, 4^{20334237}, 6^{3388854}, 8^{421890}, 10^{42021}, 12^{3360}, 14^{357}, 16^{21}$
$\mathcal{G}'_2$ on $(4, 5)$ new	$0^{162739461}, 2^{81507516}, 4^{20331108}, 6^{3373860}, 8^{421155}, 10^{42462}, 12^{3276}, 14^{234}$

For each of the three classes $k \in \{1, 6\}, \{2, 5\}$ and $\{3, 4\}$, the Taniguchi functions with the admissible parameters d have seven distinct spectra, 21 in all (Table 14). None of them coincides with the spectrum of $\mathcal{F}_1, \mathcal{G}_2, \mathcal{G}'_2, \mathcal{G}_3$ or $\mathcal{G}'_3$, and two of them coincide with the spectra of the two instances of F12 from [37, Corollary 1] (Appendix A).

Table 14: Ortho-derivative differential spectra of the Taniguchi family (F18) over $\mathbb{F}_{2^{14}}$; the seven spectra in each k -class arise as d ranges over the admissible parameters. None coincides with the spectrum of $\mathcal{F}_1$, $\mathcal{G}_2$, $\mathcal{G}'_2$, $\mathcal{G}_3$ or $\mathcal{G}'_3$.

k -class	Ortho-derivative differential spectrum
{1, 6}	$0^{162642423}, 2^{81656301}, 4^{20341209}, 6^{3302635}, 8^{424053}, 10^{48006}, 12^{4445}$
	$0^{162746436}, 2^{81533619}, 4^{20263739}, 6^{3403981}, 8^{424942}, 10^{41656}, 12^{4445}, 14^{254}$
	$0^{162686365}, 2^{81582895}, 4^{20329525}, 6^{3363468}, 8^{410718}, 10^{42545}, 12^{3302}, 14^{254}$
	$0^{162832034}, 2^{81355946}, 4^{20352258}, 6^{3411093}, 8^{426720}, 10^{37338}, 12^{3556}, 14^{127}$
	$0^{162732085}, 2^{81538064}, 4^{20290790}, 6^{3390646}, 8^{423164}, 10^{40894}, 12^{3175}, 14^{254}$
	$0^{162776789}, 2^{81475326}, 4^{20299553}, 6^{3386963}, 8^{432308}, 10^{44323}, 12^{3302}, 14^{508}$
	$0^{162729291}, 2^{81505552}, 4^{20355814}, 6^{3374390}, 8^{406400}, 10^{42799}, 12^{4318}, 14^{381}, 16^{127}$
{2, 5}	$0^{163035107}, 2^{81026889}, 4^{20424775}, 6^{3457321}, 8^{419608}, 10^{49784}, 12^{5334}, 14^{254}$
	$0^{162854640}, 2^{81323942}, 4^{20361275}, 6^{3406902}, 8^{424307}, 10^{43180}, 12^{4572}, 14^{254}$
	$0^{162851211}, 2^{81299431}, 4^{20402042}, 6^{3408426}, 8^{412877}, 10^{42164}, 12^{2286}, 14^{381}, 16^{254}$
	$0^{162688524}, 2^{81623408}, 4^{20257008}, 6^{3382137}, 8^{418973}, 10^{44577}, 12^{4191}, 14^{254}$
	$0^{162742626}, 2^{81482438}, 4^{20372070}, 6^{3352546}, 8^{424688}, 10^{41910}, 12^{2540}, 14^{254}$
	$0^{162697922}, 2^{81581117}, 4^{20310856}, 6^{3357372}, 8^{427863}, 10^{40640}, 12^{3175}, 14^{127}$
	$0^{162833558}, 2^{81357470}, 4^{20346797}, 6^{3416300}, 8^{418973}, 10^{42418}, 12^{3302}, 14^{254}$
{3, 4}	$0^{162600513}, 2^{81650078}, 4^{20428331}, 6^{3304413}, 8^{394716}, 10^{35560}, 12^{5334}, 14^{127}$
	$0^{162751897}, 2^{81510251}, 4^{20294981}, 6^{3388868}, 8^{427228}, 10^{41275}, 12^{4572}$
	$0^{162837876}, 2^{81356454}, 4^{20330287}, 6^{3431159}, 8^{421259}, 10^{38608}, 12^{3175}, 14^{127}, 16^{127}$
	$0^{162732593}, 2^{81483200}, 4^{20406233}, 6^{3327908}, 8^{419735}, 10^{45847}, 12^{2921}, 14^{635}$
	$0^{162816794}, 2^{81397856}, 4^{20318857}, 6^{3418713}, 8^{420116}, 10^{43307}, 12^{3175}, 14^{254}$
	$0^{162761295}, 2^{81494376}, 4^{20288250}, 6^{3412744}, 8^{415036}, 10^{44196}, 12^{2921}, 14^{254}$
	$0^{162908361}, 2^{81258410}, 4^{20337526}, 6^{3437001}, 8^{427609}, 10^{46736}, 12^{3048}, 14^{381}$

B.2 Dimension 16

Table 15: Ortho-derivative differential spectra over $\mathbb{F}_{2^{16}}$ of the known families and of $\mathcal{F}_1$, $\mathcal{G}_3$, $\mathcal{G}'_3$.

Realized by	Ortho-derivative differential spectrum
Gold, $k = 1$	$0 \sim 2497932060, 2 \sim 1621729110, 6 \sim 175240590$
Gold, $k = 3$	$0 \sim 2604885180, 2 \sim 1308078600, 4 \sim 319286520, 6 \sim 52952280,$ $8 \sim 8126340, 12 \sim 1572840$
Gold, $k = 5$	$0 \sim 2626642800, 2 \sim 1261941960, 4 \sim 344451960, 6 \sim 53476560,$ $8 \sim 6291360, 10 \sim 1572840, 12 \sim 524280$
Gold, $k = 7$	$0 \sim 2602788060, 2 \sim 1305850410, 4 \sim 322432200, 6 \sim 58588290,$ $8 \sim 5242800$
$F4, a = 1$	$0 \sim 2599953228, 2 \sim 1315784334, 4 \sim 314915208, 6 \sim 56032542,$ $8 \sim 7413144, 10 \sim 738672, 12 \sim 60240, 14 \sim 4008, 16 \sim 384$
$F4, a = g, g^2$	$0 \sim 2599261020, 2 \sim 1317360126, 4 \sim 313840572, 6 \sim 56215086,$ $8 \sim 7426728, 10 \sim 736440, 12 \sim 57564, 14 \sim 3960, 16 \sim 240, 18 \sim 24$
Carlet, $k \in \{1, 7\}$	$0 \sim 2603769300, 2 \sim 1304836530, 4 \sim 324300330, 6 \sim 54702600,$ $8 \sim 6604500, 10 \sim 645660, 12 \sim 41310, 14 \sim 1020, 18 \sim 510$
Carlet, $k \in \{3, 5\}$	$0 \sim 2603938620, 2 \sim 1304498910, 4 \sim 324658350, 6 \sim 54304800,$ $8 \sim 6878370, 10 \sim 538560, 12 \sim 80580, 16 \sim 3060, 20 \sim 510$
Taniguchi ($F18$), $k \in \{1, 7\},$ $d = 1$	$0 \sim 2605263600, 2 \sim 1302224310, 4 \sim 325578390, 6 \sim 54167865,$ $8 \sim 6853890, 10 \sim 741540, 12 \sim 62730, 14 \sim 9180, 18 \sim 255$
Taniguchi ($F18$), $k \in \{1, 7\},$ $d = g$	$0 \sim 2605257735, 2 \sim 1302118740, 4 \sim 325576095, 6 \sim 54443775,$ $8 \sim 6751125, 10 \sim 686715, 12 \sim 62985, 14 \sim 4080, 16 \sim 510$
Taniguchi ($F18$), $k \in \{3, 5\},$ $d = 1$	$0 \sim 2605572150, 2 \sim 1302037905, 4 \sim 324929670, 6 \sim 54745695,$ $8 \sim 6846750, 10 \sim 695640, 12 \sim 66300, 14 \sim 7650$
Taniguchi ($F18$), $k \in \{3, 5\},$ $d = g^7$	$0 \sim 2604115590, 2 \sim 1303828770, 4 \sim 325474350, 6 \sim 54054135,$ $8 \sim 6701655, 10 \sim 664020, 12 \sim 58650, 14 \sim 4335, 16 \sim 255$
Zhou-Pott ($F17$), $k \in \{1, 7\},$ $j \in \{2, 6\}$	$0 \sim 2605739175, 2 \sim 1301553150, 4 \sim 325295595, 6 \sim 54730650,$ $8 \sim 6867405, 10 \sim 657135, 12 \sim 54315, 14 \sim 2805, 18 \sim 1530$
Zhou-Pott ($F17$), $k \in \{1, 7\},$ $j = 4$	$0 \sim 2607521880, 2 \sim 1298189700, 4 \sim 327260880, 6 \sim 53937090,$ $8 \sim 7153260, 10 \sim 729810, 12 \sim 97920, 14 \sim 11220$
Zhou-Pott ($F17$), $k \in \{3, 5\},$ $j \in \{2, 6\}$	$0 \sim 2604709740, 2 \sim 1302903375, 4 \sim 325786725, 6 \sim 53886600,$ $8 \sim 6857715, 10 \sim 676260, 12 \sim 67320, 14 \sim 14025$
Zhou-Pott ($F17$), $k \in \{3, 5\},$ $j = 4$	$0 \sim 2604784200, 2 \sim 1302025920, 4 \sim 326870220, 6 \sim 53888640,$ $8 \sim 6706500, 10 \sim 568140, 12 \sim 55080, 14 \sim 3060$
Göloğlu ($F20$), $F24; k \in \{1, 7\}$	$0 \sim 2605796040, 2 \sim 1303191015, 4 \sim 322738200, 6 \sim 54973920,$ $8 \sim 7284840, 10 \sim 802485, 12 \sim 96900, 14 \sim 18360$
Göloğlu ($F20$), $F24; k \in \{3, 5\}$	$0 \sim 2610206520, 2 \sim 1294015860, 4 \sim 327499560, 6 \sim 55346730,$ $8 \sim 6895200, 10 \sim 855270, 12 \sim 58140, 14 \sim 15300,$ $16 \sim 3060, 18 \sim 3060, 20 \sim 3060$
F25; F22, $\mathcal{G}_1 = \mathcal{F}_0$	$0 \sim 2604835344, 2 \sim 1302709182, 4 \sim 325645338, 6 \sim 54196980,$ $8 \sim 6779634, 10 \sim 675174, 12 \sim 55416, 14 \sim 4356, 16 \sim 336$
$\mathcal{F}_1 = \mathcal{G}'_1$ new	$0 \sim 2605007706, 2 \sim 1302464844, 4 \sim 325663068, 6 \sim 54214656,$ $8 \sim 6808422, 10 \sim 680772, 12 \sim 57942, 14 \sim 4104, 16 \sim 210, 18 \sim 36$
$\mathcal{G}_3$ on $(3, 6)$ new	$0 \sim 2604870078, 2 \sim 1302676290, 4 \sim 325614576, 6 \sim 54219522,$ $8 \sim 6785574, 10 \sim 674754, 12 \sim 56316, 14 \sim 4290, 16 \sim 360$
$\mathcal{G}'_3$ on $(5, 6)$ new	$0 \sim 2604676980, 2 \sim 1302955653, 4 \sim 325589292, 6 \sim 54195840,$ $8 \sim 6755190, 10 \sim 669108, 12 \sim 55356, 14 \sim 4080, 16 \sim 222, 18 \sim 39$

B.3 Dimension 20

Table 16 lists the spectra of all known functions over $\mathbb{F}_{2^{20}}$ and of the six classes returned by the exhaustive $\mathbb{F}_4$ -coefficient search: the two Carlet classes, $\mathcal{G}_1 = \mathcal{F}_0$, $\mathcal{G}'_1 = \mathcal{F}_1$, $\mathcal{G}_3$ and $\mathcal{G}'_3$. The families F19 and F21 do not occur for $m = 10$: F21 requires m odd, and F19 has no admissible parameters (Section 7.2).

Table 16: Ortho-derivative differential spectra over $\mathbb{F}_{2^{20}}$ of the known families and of the functions found by the search.

Family / function	Ortho-derivative differential spectrum
Gold, $i = 1$	$0 \sim 641065200600, 2 \sim 412790423100, 6 \sim 45654955500$
Gold, $i = 3$	$0 \sim 665586126975, 2 \sim 335542951425, 4 \sim 82942282500,$ $6 \sim 13605260625, 8 \sim 1698691500, 10 \sim 104857500,$ $12 \sim 19922925, 14 \sim 10485750$
Gold, $i = 7$	$0 \sim 665051353725, 2 \sim 336176290725, 4 \sim 82931796750,$ $6 \sim 13856918625, 8 \sim 1357904625, 10 \sim 115343250,$ $12 \sim 10485750, 14 \sim 10485750$
Gold, $i = 9$	$0 \sim 666713345100, 2 \sim 332862793725, 4 \sim 84672431250,$ $6 \sim 13731089625, 8 \sim 1300233000, 10 \sim 230686500$
F4, $a = 1$	$0 \sim 665686234905, 2 \sim 336759251700, 4 \sim 80539428600,$ $6 \sim 14408951430, 8 \sim 1910339715, 10 \sim 190357020,$ $12 \sim 14988720, 14 \sim 969870, 16 \sim 54180,$ $18 \sim 3000, 20 \sim 60$
F4, $a = g$	$0 \sim 665656739610, 2 \sim 336843600798, 4 \sim 80462660130,$ $6 \sim 14427410100, 8 \sim 1913726820, 10 \sim 190502790,$ $12 \sim 14914602, 14 \sim 968130, 16 \sim 53625,$ $18 \sim 2460, 20 \sim 135$
Carlet, $k \in \{1, 9\}$; F17, $k = 1$	$0 \sim 666948512340, 2 \sim 333396137844, 4 \sim 83300578020,$ $6 \sim 13915418880, 8 \sim 1755483345, 10 \sim 178308900,$ $12 \sim 14960352, 14 \sim 1007655, 16 \sim 122760,$ $18 \sim 30690, 20 \sim 15345, 22 \sim 3069$
Carlet, $k \in \{3, 7\}$; F17, $k = 3$	$0 \sim 667015518840, 2 \sim 333221628366, 4 \sim 83432084670,$ $6 \sim 13906713150, 8 \sim 1740839100, 10 \sim 178191255,$ $12 \sim 14273919, 14 \sim 1242945, 16 \sim 86955$
F18, $k \in \{1, 9\}$, $d = 1$	$0 \sim 666883506828, 2 \sim 333478867854, 4 \sim 83311114920,$ $6 \sim 13904104500, 8 \sim 1740475935, 10 \sim 176563662,$ $12 \sim 14620716, 14 \sim 1196910, 16 \sim 102300,$ $18 \sim 20460, 20 \sim 5115$
F18, $k \in \{1, 9\}$, $d = g^7$	$0 \sim 666903075795, 2 \sim 333424152699, 4 \sim 83355365808,$ $6 \sim 13897943994, 8 \sim 1740384888, 10 \sim 174016392,$ $12 \sim 14584911, 14 \sim 999471, 16 \sim 51150,$ $18 \sim 4092$
F18, $k \in \{1, 9\}$, $d = g^9$	$0 \sim 666870138264, 2 \sim 333471828591, 4 \sim 83353196025,$ $6 \sim 13890324690, 8 \sim 1736091357, 10 \sim 173416914,$ $12 \sim 14500002, 14 \sim 1021977, 16 \sim 61380$
F18, $k \in \{1, 9\}$, $d = g^{13}$	$0 \sim 666865826319, 2 \sim 333483870324, 4 \sim 83344611009,$ $6 \sim 13889825466, 8 \sim 1736397234, 10 \sim 174392856,$ $12 \sim 14510232, 14 \sim 1070058, 16 \sim 65472,$ $18 \sim 10230$
F18, $k \in \{3, 7\}$, $d = 1$	$0 \sim 666961952514, 2 \sim 333315458949, 4 \sim 83397665835,$ $6 \sim 13905178650, 8 \sim 1739928630, 10 \sim 174464466,$ $12 \sim 14682096, 14 \sim 1166220, 16 \sim 66495,$ $18 \sim 15345$
F18, $k \in \{3, 7\}$, $d = g$	$0 \sim 666903588318, 2 \sim 333416765616, 4 \sim 83365578417,$ $6 \sim 13897781337, 8 \sim 1737367038, 10 \sim 173608215,$ $12 \sim 14791557, 14 \sim 1033230, 16 \sim 58311,$ $18 \sim 6138, 20 \sim 1023$
F20, $k = 1$; F24, $k = 1$ (all α)	$0 \sim 667038234555, 2 \sim 333263354490, 4 \sim 83308833630,$ $6 \sim 13940185710, 8 \sim 1763779875, 10 \sim 179858745,$ $12 \sim 15104595, 14 \sim 1150875, 16 \sim 76725$
F20, $k = 3$; F24, $k = 3$ (all α)	$0 \sim 667257171900, 2 \sim 332957030439, 4 \sim 83348730630,$ $6 \sim 13957837575, 8 \sim 1772035485, 10 \sim 179582535,$ $12 \sim 28605126, 14 \sim 7483245, 16 \sim 1764675,$ $18 \sim 276210, 20 \sim 61380$
F23, $k = 1$, $a = 1$	$0 \sim 666928554633, 2 \sim 333380781591, 4 \sim 83366570727,$ $6 \sim 13905125454, 8 \sim 1738695915, 10 \sim 175080312,$ $12 \sim 14672889, 14 \sim 1021977, 16 \sim 67518,$ $18 \sim 8184$

Table 16 (continued)

Family / function	Ortho-derivative differential spectrum
F23, $k = 1$, $a = g^{99}$	$0 \sim 666890907210, 2 \sim 333438441963, 4 \sim 83362894065,$ $6 \sim 13888601958, 8 \sim 1740503556, 10 \sim 173352465,$ $12 \sim 14742453, 14 \sim 1071081, 16 \sim 55242,$ $18 \sim 9207$
F23, $k = 3$, $a = 1$	$0 \sim 666907162680, 2 \sim 333417359979, 4 \sim 83355753525,$ $6 \sim 13901008902, 8 \sim 1739917377, 10 \sim 173743251,$ $12 \sim 14519439, 14 \sim 1029138, 16 \sim 74679,$ $18 \sim 10230$
F23, $k = 3$, $a = g^{99}$	$0 \sim 666902696262, 2 \sim 333426959811, 4 \sim 83349043668,$ $6 \sim 13904405262, 8 \sim 1737431487, 10 \sim 174245544,$ $12 \sim 14598210, 14 \sim 1115070, 16 \sim 76725,$ $18 \sim 7161$
F22; F25 (all 36 classes of α); $\mathcal{G}_1 = \mathcal{F}_0$ on $(1, 2)$	$0 \sim 666885312324, 2 \sim 333445521030, 4 \sim 83360909835,$ $6 \sim 13893331275, 8 \sim 1736348475, 10 \sim 173564046,$ $12 \sim 14478210, 14 \sim 1044945, 16 \sim 64935,$ $18 \sim 3735, 20 \sim 330, 22 \sim 45,$ $24 \sim 15$
$\mathcal{G}'_1 = \mathcal{F}_1$ on $(2, 9)$ new	$0 \sim 666884734815, 2 \sim 333445786293, 4 \sim 83362204170,$ $6 \sim 13892337555, 8 \sim 1736277015, 10 \sim 173647500,$ $12 \sim 14479992, 14 \sim 1042395, 16 \sim 65610,$ $18 \sim 3465, 20 \sim 345, 22 \sim 30,$ $24 \sim 15$
$\mathcal{G}_3$ on $(3, 6)$ new	$0 \sim 666884823390, 2 \sim 333447042585, 4 \sim 83359773915,$ $6 \sim 13893172185, 8 \sim 1736440275, 10 \sim 173716185,$ $12 \sim 14509320, 14 \sim 1030815, 16 \sim 66255,$ $18 \sim 3840, 20 \sim 405, 22 \sim 30$
$\mathcal{G}'_3$ on $(6, 7)$ new	$0 \sim 666884909850, 2 \sim 333448071702, 4 \sim 83357676420,$ $6 \sim 13893981225, 8 \sim 1736565705, 10 \sim 173781750,$ $12 \sim 14475645, 14 \sim 1043775, 16 \sim 69030,$ $18 \sim 3795, 20 \sim 225, 22 \sim 63,$ $24 \sim 15$

B.4 Dimension 22

Table 17 lists, besides the ten functions found over $\mathbb{F}_{2^{22}}$, the spectra of the known families computed directly in this dimension: the Gold functions, $F4$, $F11$ and $F12$. The remaining families are covered by Lemma 5, with the exception of $F25$: of its 63 Frobenius classes of α we tested two, both coinciding with $F22$. We leave the other 61 untested (Remark 9).

Table 17: Ortho-derivative differential spectra over $\mathbb{F}_{2^{22}}$ of the ten functions $\mathcal{G}_s, \mathcal{G}'_s$ found (Table 9) and of the known families computed directly.

Family / function	Ortho-derivative differential spectrum
Gold, $i = 1$	$0 \sim 10261689445134, 2 \sim 6597693144939, 6 \sim 732799260039$
Gold, $i = 3$	$0 \sim 10667005915539, 2 \sim 5336298460719, 4 \sim 1339182227658,$ $6 \sim 220121215743, 8 \sim 27174889137, 10 \sim 2030042652,$ $12 \sim 369098664$
Gold, $i = 5$	$0 \sim 10656255916950, 2 \sim 5358813479223, 4 \sim 1326586735749,$ $6 \sim 221874434397, 8 \sim 25421670483, 10 \sim 2722102647,$ $12 \sim 369098664, 14 \sim 138411999$
Gold, $i = 7$	$0 \sim 10670420078181, 2 \sim 5333299534074, 4 \sim 1335675790350,$ $6 \sim 223627653051, 8 \sim 25744631814, 10 \sim 2906651979,$ $12 \sim 507510663$
Gold, $i = 9$	$0 \sim 10680293467443, 2 \sim 5320058119503, 4 \sim 1336460125011,$ $6 \sim 222751043724, 8 \sim 28605146460, 10 \sim 3644849307,$ $12 \sim 369098664$
$F11$ (BHK), $i = 9, k = 0$	$0 \sim 10670778773991, 2 \sim 5333976124890, 4 \sim 1334292683625,$ $6 \sim 222310070796, 8 \sim 27792170175, 10 \sim 2781412425,$ $12 \sim 232172787, 14 \sim 17157954, 16 \sim 1215918,$ $18 \sim 67551$
$F11$ (BHK), $i = 5, k = 0$	$0 \sim 10669805093877, 2 \sim 5335616330721, 4 \sim 1333858128042,$ $6 \sim 222121535955, 8 \sim 27774877119, 10 \sim 2760336513,$ $12 \sim 227917074, 14 \sim 16077138, 16 \sim 1486122,$ $18 \sim 67551$
$F12$, Thm. 3.3(iii) (both a)	$0 \sim 10669809687345, 2 \sim 5335614439293, 4 \sim 1333827527439,$ $6 \sim 222185101446, 8 \sim 27724821828, 10 \sim 2772563244,$ $12 \sim 230754216, 14 \sim 16144689, 16 \sim 810612$
$F12$, Cor. 1(1) (both a)	$0 \sim 10670137950406, 2 \sim 5335195369265, 4 \sim 1333753763794,$ $6 \sim 222289402237, 8 \sim 27775202592, 10 \sim 2780824936,$ $12 \sim 231605768, 14 \sim 16652345, 16 \sim 1027594,$ $18 \sim 47081, 20 \sim 4094$
$F12$, Cor. 1(2) (both a)	$0 \sim 10670071584619, 2 \sim 5335318279333, 4 \sim 1333706302052,$ $6 \sim 222280039259, 8 \sim 27776760359, 10 \sim 2779175054,$ $12 \sim 232119565, 14 \sim 16502914, 16 \sim 1017359,$ $18 \sim 65504, 20 \sim 4094$
$F4$, $a = 1$	$0 \sim 10651092447276, 2 \sim 5388612686661, 4 \sim 1287507539373,$ $6 \sim 230995981986, 8 \sim 30663848655, 10 \sim 3053562600,$ $12 \sim 239426220, 14 \sim 15457893, 16 \sim 854172,$ $18 \sim 42735, 20 \sim 2442, 22 \sim 99$
$F4$, $a = g, g^2$	$0 \sim 10651322098104, 2 \sim 5387945879091, 4 \sim 1288119302481,$ $6 \sim 230852476371, 8 \sim 30634568085, 10 \sim 3051797958,$ $12 \sim 239304087, 14 \sim 15512970, 16 \sim 866547,$ $18 \sim 42240, 20 \sim 2046, 22 \sim 132$
$\mathcal{G}_1 = \mathcal{F}_0$ on $(1, 2)$ (F22)	$0 \sim 10670185288560, 2 \sim 5335118953830, 4 \sim 1333769713749,$ $6 \sim 222294643857, 8 \sim 27785634987, 10 \sim 2778383454,$ $12 \sim 231626604, 14 \sim 16508250, 16 \sim 1036827,$ $18 \sim 57156, 20 \sim 2673, 22 \sim 165$
$\mathcal{G}'_1 = \mathcal{F}_1$ on $(2, 10)$	$0 \sim 10670187555561, 2 \sim 5335112796921, 4 \sim 1333777590123,$ $6 \sim 222289040457, 8 \sim 27786570636, 10 \sim 2779045269,$ $12 \sim 231602283, 14 \sim 16551117, 16 \sim 1036794,$ $18 \sim 57816, 20 \sim 3069, 22 \sim 66$
$\mathcal{G}_2$ on $(2, 4)$ new candidate	$0 \sim 10670176343745, 2 \sim 5335130041995, 4 \sim 1333773936165,$ $6 \sim 222288419133, 8 \sim 27785575191, 10 \sim 2778540666,$ $12 \sim 231369897, 14 \sim 16523331, 16 \sim 1036332,$ $18 \sim 60786, 20 \sim 2772, 22 \sim 99$

Table 17 (continued)

Family / function	Ortho-derivative differential spectrum
$\mathcal{G}'_2$ on (4, 9) new candidate	$0 \sim 10670183730366, 2 \sim 5335118369136, 4 \sim 1333776835644,$ $6 \sim 222289029006, 8 \sim 27785677425, 10 \sim 2778950592,$ $12 \sim 231629211, 14 \sim 16534914, 16 \sim 1032372,$ $18 \sim 58212, 20 \sim 3168, 22 \sim 66$
$\mathcal{G}_3$ on (3, 6) new candidate	$0 \sim 10670178310644, 2 \sim 5335128999393, 4 \sim 1333772575344,$ $6 \sim 222287399763, 8 \sim 27786284592, 10 \sim 2779049031,$ $12 \sim 231585519, 14 \sim 16552173, 16 \sim 1032405,$ $18 \sim 58014, 20 \sim 3102, 22 \sim 132$
$\mathcal{G}'_3$ on (6, 8) new candidate	$0 \sim 10670174996784, 2 \sim 5335133339289, 4 \sim 1333773688863,$ $6 \sim 222285409467, 8 \sim 27786210441, 10 \sim 2778903699,$ $12 \sim 231656799, 14 \sim 16543395, 16 \sim 1040292,$ $18 \sim 58443, 20 \sim 2541, 22 \sim 99$
$\mathcal{G}_4$ on (4, 8) new candidate	$0 \sim 10670186698716, 2 \sim 5335119026529, 4 \sim 1333766276172,$ $6 \sim 222295595049, 8 \sim 27786713790, 10 \sim 2778296235,$ $12 \sim 231636009, 14 \sim 16515807, 16 \sim 1031184,$ $18 \sim 57849, 20 \sim 2607, 22 \sim 165$
$\mathcal{G}'_4$ on (7, 8) new candidate	$0 \sim 10670191521072, 2 \sim 5335108749834, 4 \sim 1333774205907,$ $6 \sim 222291778071, 8 \sim 27787571988, 10 \sim 2778788067,$ $12 \sim 231596211, 14 \sim 16552272, 16 \sim 1025904,$ $18 \sim 57519, 20 \sim 3102, 22 \sim 165$
$\mathcal{G}_5$ on (5, 10) $F16^* = F_3, k=4, i=5$	$0 \sim 10670196815061, 2 \sim 5335100989191, 4 \sim 1333775961936,$ $6 \sim 222290486649, 8 \sim 27789427908, 10 \sim 2778957258,$ $12 \sim 231588951, 14 \sim 16531878, 16 \sim 1028181,$ $18 \sim 59400, 20 \sim 3465, 22 \sim 234$
$\mathcal{G}'_5$ on (6, 10) $F15^* = F_2, k=4, i=5$	$0 \sim 10670179425054, 2 \sim 5335123827138, 4 \sim 1333777181022,$ $6 \sim 222288789888, 8 \sim 27784735539, 10 \sim 2778695865,$ $12 \sim 231584991, 14 \sim 16515081, 16 \sim 1033758,$ $18 \sim 58707, 20 \sim 2970, 22 \sim 99$

The families not listed are covered by Lemma 5. For the Carlet family and for F18, F20, F21 and F24, the discussion following the lemma exhibits in each case a group G of order $q - 1 = 2047$ inside the EL-automorphism group, acting freely on $\mathbb{F}_2^{22} \setminus \{0\}$, so that every multiplicity of their spectra is divisible by 2047 for all values of the parameters. Of the twelve multiplicities of each of the ten spectra found, not one is divisible by 2047, so no instance of any of those families, for any value of its parameters, can realize any of them. This is why a complete sweep of the parameter spaces of F18 and F24, which at $m = 11$ would run to several hundred spectra at about 2^{44} operations each, is unnecessary.

The exceptions are F4 and F25, to which Lemma 5 does not apply. Indeed, none of the twelve multiplicities of either F4 spectrum is divisible by 2047. F4 has been computed completely, since by Section A.1 the values $a = 1$ and $a = g$ represent all its instances. For F25, we tested $\alpha = 1$, which is F22, and one further Frobenius class, both giving the spectrum of F22, while the remaining 61 Frobenius classes are left untested (Remark 9).