Testing CCZ-equivalence to permutations via projections of Walsh zero spaces, with applications to APN functions

Emanuele Bellini (ORCID: 0000-0002-2349-0247)[1*]

[1*]Technology Innovation Institute, Abu Dhabi, United Arab Emirates.

Corresponding author(s). E-mail(s): emanuele.bellini@tii.ae;

Abstract

Whether almost perfect nonlinear (APN) permutations exist in even dimension $n \geq 8$ is a long-standing open question, the big APN problem. The only example known in even dimension, on six bits, was found from a quadratic APN function that is not itself a permutation, by Carlet–Charpin–Zinoviev (CCZ) equivalence. It is therefore natural to test APN functions for CCZ-equivalence to a permutation. This amounts to finding two complementary n-dimensional subspaces among the zeros of the Walsh transform, which lie in $\mathbb{F}_2^{2n}$. A known necessary condition only uses their projections to $\mathbb{F}_2^n$ and cannot decide every case. We give an exact test for functions whose Walsh supports are affine, including all quadratic functions. It reconstructs the subspaces from their projections, through searches for subspaces of $\mathbb{F}_2^n$ and for constrained bilinear maps. On the benchmarked functions in dimension twelve, it lists them **39** to **55** times faster than the generic search of the commonly used sboxU library. We then study the functions $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$, which Göloğlu and Pavlů proved not to be CCZ-equivalent to permutations when **4** divides n. With their result, our computations show that this holds for every even $n \leq 24$. In dimension **18** the necessary condition is satisfied, and the new test decides the case. We conjecture this for every even dimension. We also compile **25** classes of quadratic APN functions in dimension ten from published instances, with equivalence certificates. No function in these classes or in their switching closure is CCZ-equivalent to a permutation. All code and data are public.

Keywords: APN permutation, big APN problem, CCZ-equivalence, Walsh zero space, switching construction, vectorial Boolean function

MSC Classification: 94A60 , 06E30 , 11T71 , 94D10

1 Introduction

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is *almost perfect nonlinear* (APN) if, for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^n$, the equation $F(x + a) + F(x) = b$ has at most two solutions. APN functions offer the best possible resistance to differential cryptanalysis [1]. They are also related to optimal objects in coding theory, sequence design and finite geometry; see [2] for an account. Many block ciphers, for instance substitution–permutation networks, need invertible S-boxes. In odd dimension APN permutations are plentiful: the Gold functions x^{2^i+1} with $\gcd(i, n) = 1$ [1, 3], the Kasami [4], Welch [5] and Niho [6] functions, and the inverse function are APN permutations of $\mathbb{F}_{2^n}$ for odd n. In even dimension the situation is completely different. There is no APN permutation of $\mathbb{F}_2^4$ [7]. No APN power function and no quadratic APN function is a permutation in even dimension (see [2]). The only APN permutation known in even dimension is the six-bit permutation found by Browning, Dillon, McQuistan and Wolfe [8]. Whether APN permutations exist for some even $n \geq 8$ is known as the *big APN problem*.

Dillon's permutation was not found by a search among permutations. It was obtained as a function CCZ-equivalent [9] to the quadratic APN function $x^3 + x^{10} + ux^{24}$ over $\mathbb{F}_{2^6}$, which is not itself a permutation. Two lines of attack on the big APN problem have therefore been pursued. The first constructs permutations with a prescribed structure, such as the butterfly structure that underlies Dillon's permutation [10–12]. The second searches for APN functions that are not permutations but are CCZ-equivalent to one. This second approach relies on a characterization due to Canteaut and Perrin [13]. A function F is CCZ-equivalent to a permutation if and only if the set of zeros of its Walsh transform contains two n-dimensional subspaces with trivial intersection.

1.1 Related work

Constructions of permutations.

Perrin, Udovenko and Biryukov [10] decomposed Dillon's permutation as an open butterfly on $\mathbb{F}_{2^3}^2$. Canteaut, Duval and Perrin [11] generalized the construction to all dimensions $4k + 2$, obtaining differential uniformity four for $k > 1$. Canteaut, Perrin and Tian [12] proved that a generalized butterfly is APN only on six bits. Beierle, Brinkmann and Leander [14] classified APN permutations with nontrivial linear self-equivalences in small dimension.

CCZ-equivalence to permutations.

Göloğlu and Langevin [15] proved that Gold functions are not CCZ-equivalent to permutations in any even dimension. They proved the same for Kasami functions in every dimension divisible by four. These results rest on a necessary condition: if F is CCZ-equivalent to a permutation, its non-bent components contain two subspaces whose sum is the whole space. This condition follows directly from an observation of Browning et al. [8]. Göloğlu and Pavlů [16] turned it into an algorithm, a depth-first search for the largest subspace contained in the set of non-bent components. With it they showed that no member of the families of APN functions known at that time is CCZ-equivalent to a permutation of $\mathbb{F}_2^n$ for even $n \leq 12$, apart from the known case $n = 6$.

They also checked random members of these families up to $n = 18$, and introduced the number of subspaces of the set of non-bent components as an EA-invariant. Moreover, they proved that $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$ is not CCZ-equivalent to a permutation when $4 \mid n$. As reported in [16], Canteaut and Perrin independently designed a similar algorithm. Budaghyan, Ivkovic and Kaleyski [17] extended the result for $4 \mid n$ to all quadratic 3-to-1 APN functions. Bénéteau, Goluboff, Kölsch and Vaghasiya [18] showed that a quadratic function that is CCZ-equivalent to a permutation has at least $3(2^{n/2} - 1)$ non-bent components.

When the non-bent components do contain subspaces spanning $\mathbb{F}_2^n$, the necessary condition is satisfied and therefore inconclusive. One then has to search for Walsh zero spaces in $\mathbb{F}_2^{2n}$. Chase and Lisoněk [19] constructed Walsh zero spaces for Gold functions in odd dimension. Bonnetain, Perrin and Tian [20] described generic algorithms for finding vector spaces of a given dimension in a set; the test of [13] is one of them. These algorithms, together with a test for CCZ-equivalence to a permutation, are implemented in the library sboxU of Perrin et al. [21]. Most of the works cited below used sboxU to check their functions.

Quadratic APN functions and switching.

Edel and Pott [22] introduced the switching construction. With it they found, in dimension six, the only known APN function that is CCZ-inequivalent to both power and quadratic functions.

In dimension eight the only known APN function that is not quadratic is the Kasami function x^{57}. The known quadratic APN functions form at least 3,808,491 CCZ-classes [23, Theorem 5.1]. Each item below gives the number of classes first found in the given source. The counts of the first four items are those of [24, Section 4].

- 22: the quadratic functions in the list of Edel and Pott [22], which collects the earlier constructions and includes the Gold functions x^3 and x^9.
- 8,157: Yu, Wang and Li [25], with a matrix method.
- 10: Weng, Tan and Gong [26].
- 2: the family of Taniguchi [27].
- 12,921: Beierle and Leander [24]. They found 12,733 classes by a recursive tree search among functions with prescribed linear self-equivalences, and 188 by switching.
- 5,412: Yu and Perrin [28], with the same matrix method.
- 6,368: Beierle, Leander and Perrin [29], by extending quadratic APN functions in dimension seven.
- 3,775,599: Beierle, Langevin, Leander, Polujan and Rasoolzadeh [23, 30], by extending vectorial bent functions.

The first seven items give the 32,892 classes known before [23]. Beierle et al. estimate the total number of classes at about six million. In a recent preprint, Kuznetsov [31] reports four further classes, which are not included in the count above. In [24] and [23], none of the new functions is CCZ-equivalent to a permutation. For the known infinite families, see [16]. We do not repeat these tests in dimension eight.

In dimension ten the known APN functions that are not quadratic are the Kasami function x^{57} and the Dobbertin function x^{339} [32]. Section 8.4 shows that the quadratic

APN instances we considered form exactly 25 CCZ-classes. For some families we took all parameters and for others random samples, and for [33] we used the instances of the preprint version (Section 8.4). We use the names F3, F4, F12 and F13 of the families in [34, Table 3]. Each item below gives a set of classes and the sources whose functions lie in them.

- 2 classes: the Gold functions x^3 and x^9. The class of x^3 also contains members of the relative-trace family of Zheng, Kan, Li, Peng and Tang [33].
- 2 classes: the family F3 of Budaghyan and Carlet [35]. They also contain Carlet's bivariate family (see [36, Table 2.1]) and members of the family of [33].
- 2 classes: the family F4, $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$, of Budaghyan, Carlet and Leander [37].
- 6 classes: the family F12 of Taniguchi [27].
- 5 classes: the family F13 of Budaghyan, Helleseth and Kaleyski [38], with parameters in $\mathbb{F}_4$. They also contain the two biprojective families of Göloğlu [39] and the first family of Calderini, Li and Villa [40]. Two of the five instances of Beierle and Leander [24] lie in them. So do two instances and some members of the family of [33], and the second instance of Budaghyan, Ivkovic and Kaleyski [17, Table 2].
- 3 classes: the other three instances of [24]. One of them also contains the third instance of [33].
- 5 classes: the other five instances of [17, Table 2], obtained by adding five to seven terms with coefficients in $\mathbb{F}_4$ to x^3, x^9 or x^{33}. The class of the first one also contains the function of Li, Zhou, Li and Qu [41]. It also contains the second family of [40].

Budaghyan, Ivkovic and Kaleyski checked with sboxU that none of their functions is CCZ-equivalent to a permutation. Göloğlu and Kölsch [36] determined the equivalences between the biprojective families. Yu, Li, Ichanska and Kaleyski [42] classified the quadratic APN functions in dimension ten with coefficients in $\mathbb{F}_2$. There are three classes, those of x^3, x^9 and $x^3+\mathrm{Tr}(x^9)$, the last one in F4. Yu, Kaleyski, Budaghyan and Li [43] did the same for $n \leq 9$. The same classification is the case $(n, m) = (10, 1)$ of the QAM search of Ichanska, Berg, Kaleyski and Yu [44]. Their search for $(n, m) = (10, 2)$ is only partial, and the new APN function it reports is in dimension eight, so it adds no class in dimension ten.

Budaghyan, Calderini and Villa [45] determined the equivalences between the known families in small dimension. Kaleyski [34] surveyed the invariants for telling classes apart. Kalgin and Idrisova [46] classified the quadratic APN functions in seven variables. This classification is reproduced in the data of Beierle et al. [47], which list the EA-classes of quadratic (n, m)-APN functions for small $n \leq m$. Recently, Göloğlu and Kölsch [48] gave a large family of APN permutations in every odd dimension divisible by three. They also gave quadratic APN functions in even dimension that are not bijective. Their functions are defined on $\mathbb{F}_{2^m}^3$, so none of them has dimension ten.

1.2 Our contribution

We study the big APN problem computationally, with an emphasis on exact methods whose results can be checked independently. Our main contributions are the projection test and its application to the family $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$ up to dimension 24. The other contributions concern dimensions eight to ten.

1. We consider functions whose Walsh supports are affine subspaces. These include all quadratic functions. We parametrize the n-dimensional subspaces of their Walsh zeros by three objects: a subspace B of the components with Walsh zeros, a subspace P of $\mathbb{F}_2^n$ of the same dimension, and a bilinear map $B \times P \to \mathbb{F}_2$ (Theorem 8). The resulting test for CCZ-equivalence to a permutation, which we call the projection test, searches for B and P in $\mathbb{F}_2^n$ instead of searching for subspaces of $\mathbb{F}_2^{2n}$. It complements the necessary condition of [15, 16] (Proposition 7): it decides exactly the cases in which that condition is satisfied and therefore inconclusive. An example is the Gold functions in dimension ten, whose non-bent components contain eleven 5-dimensional subspaces that pairwise span $\mathbb{F}_2^{10}$. We compared it with the generic search of the sboxU library. Listing all Walsh zero spaces is 5 to 18 times faster in dimension ten, and 39 to 55 times faster in dimension twelve (Section 8.3).
2. The family $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$ in dimensions $n = 2m$ with m odd is not covered by the theorem of [16]. For these dimensions we show that the non-bent components contain a line of the Desarguesian spread whenever a is a cube (Proposition 11). So their dimension alone cannot exclude a permutation. We decide these cases for $n \in \{6, 10, 14, 18, 22\}$ by computation, and conclude that no member of the family is CCZ-equivalent to a permutation for even $n \leq 24$ (Corollary 12). In dimension 18 the necessary condition is satisfied, and the case is decided by Theorem 8. Dimension 22 needs a subspace search that exploits the symmetries of the family. We state a conjecture that would settle the family in all even dimensions (Conjecture 14). The case $n = 22$, computed after the conjecture was formed, agrees with it.
3. We compile 25 classes of quadratic APN functions in dimension ten from the published instances we could examine, and test them. With an explicit EA-equivalence test we show that the published instances we could obtain lie in these 25 classes. These are the instances of the preprint version of [33], those of the bivariate families of [39–41], and the second instance of [17, Table 2] as printed there. In particular, the function of [41] is EA-equivalent to the first instance of [17, Table 2]. No class is CCZ-equivalent to a permutation. For the families considered in [16] this confirms their result independently, and our values of the largest subspace dimension agree with theirs. The classes found after that work were tested in [24] and [17], so our test is an independent confirmation for them as well. Of the 25 classes, 18 are excluded by the dimension bound, 4 by the spanning condition, and 3 need Theorem 8.
4. We compute the quadratic switching closure of the source functions listed in Table 5, in dimensions six, eight, nine and ten, with a certified equivalence for every neighbour, and we test every quadratic class found. In dimensions eight to ten the resulting quadratic classes have no non-quadratic switching neighbours. In dimension ten the 25 classes are closed under switching. In dimensions nine and ten this extends the computations of [24], which were performed in dimensions seven and eight.
5. We search for new quadratic APN functions in dimension ten by symmetry-restricted sampling of univariate polynomials and by the tree search of [24] with a large randomized campaign. Every function found is tested individually, and none is CCZ-equivalent to a permutation. A search over bilinear forms in dimensions six to eight shows that unstructured search does not scale.

6. We explain why the inverse function is not APN in even dimension. The sets of four points on which it is affine, and which therefore violate the APN condition, are exactly the two-dimensional subspaces $a\mathbb{F}_4$, $a \neq 0$ (Proposition 3). We then show for $n = 8$ that swapping two entries of the lookup table of the inverse function I never brings it closer to the APN property, measured by the cost (1). Here a swap exchanges the outputs $I(i)$ and $I(j)$ of two inputs $i \neq j$. We also enumerate three structured families of permutations: butterflies whose keyed permutations are built from power maps, cyclotomic maps and switched inverse functions. None of them contains a permutation of $\mathbb{F}_2^8$ closer to the APN property than the inverse function. The butterflies of this kind contain none of $\mathbb{F}_2^{10}$ either (Sections 3 and 4).

We find no APN permutation in dimension eight or ten. We believe that the tools, in particular the projection test, are useful for future searches. We make all code and data available at https://github.com/peacker/ccz-projection-test-apn, together with a script that compares every number reported here with the stored results.

1.3 Outline

Section 2 recalls definitions. Section 3 studies the inverse function and local search around it, and Section 4 structured families of permutations. Section 5 recalls exact switching and describes how we compute the switching closure. Section 6 contains the parametrization of Walsh zero spaces and the resulting test for CCZ-equivalence to a permutation, and Section 7 applies it to the family $x^3+a^{-1}\mathrm{Tr}(a^3x^9)$. Section 8 reports the experiments, and Section 9 concludes with open questions.

2 Preliminaries

We identify $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ whenever a field structure is needed. The components of F are then also written $x \mapsto \mathrm{Tr}(\beta F(x))$ with $\beta \in \mathbb{F}_{2^n}$. The field coordinate β and the bit coordinate b of the same component are related by the dual basis of the trace form; the repository contains this conversion. In our computations $\mathbb{F}_{2^n}$ is represented in a polynomial basis modulo a fixed primitive polynomial, listed in the accompanying repository. For $x, y \in \mathbb{F}_2^n$ we write $x \cdot y$ for the usual scalar product, and Tr denotes the absolute trace of $\mathbb{F}_{2^n}$. An (n, n)-*function* is a map $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$; its *components* are the Boolean functions $F_b(x) = b \cdot F(x)$, $b \neq 0$.

Differential properties.

For $a, b \in \mathbb{F}_2^n$ let $\delta_F(a, b) = \#\{x \in \mathbb{F}_2^n : F(x + a) + F(x) = b\}$. The values $\delta_F(a, b)$ are even, and F is APN if $\delta_F(a, b) \leq 2$ for all $a \neq 0$ and all b. To measure how far F is from being APN we use

$$\mathrm{cost}(F) = \sum_{a \neq 0} \sum_{b} \binom{\delta_F(a,b)/2}{2}, \tag{1}$$

which vanishes exactly when F is APN. An entry $\delta_F(a, b) = 4$ contributes 1, and an entry 6 contributes 3. A 2-*flat* is an affine subspace of dimension two, $\{x, x + a, x +$

$b, x+a+b\}$ with a, b linearly independent. We say that F is *affine on* a 2-flat if $F(x)+F(x+a)+F(x+b)+F(x+a+b)=0$. We write $\mathrm{A}(F)$ for the number of 2-flats on which F is affine. A function is APN if and only if it is affine on no 2-flat.

Walsh transform.

The Walsh transform of F is $\mathcal{W}_F(a,b) = \sum_{x\in\mathbb{F}_2^n}(-1)^{a\cdot x+b\cdot F(x)}$ for $a, b \in \mathbb{F}_2^n$. The *Walsh zeros* of F form the set $\mathcal{Z}_F = \{(a,b) \neq (0,0) : \mathcal{W}_F(a,b) = 0\}$, which always contains $\{(a,0) : a \neq 0\}$. For $b \neq 0$ the *Walsh support* of the component F_b is $S_b = \{a : \mathcal{W}_F(a,b) \neq 0\}$. The component is *bent* if $|\mathcal{W}_F(a,b)| = 2^{n/2}$ for all a. We write $\mathcal{N}_F = \{b \neq 0 : S_b \neq \mathbb{F}_2^n\}$ for the set of components that have a Walsh zero. A bent component has no Walsh zero. For plateaued components, in particular for quadratic ones, the converse holds, so for quadratic F the set $\mathcal{N}_F$ is the set of non-bent components. This is not true in general. For example, the Boolean function on $\mathbb{F}_2^3$ that is 1 at exactly one point has no Walsh zero but is not bent. All our proofs use only the definition of $\mathcal{N}_F$. In general statements we call its elements the components with Walsh zeros. For quadratic functions, where they are exactly the non-bent components, we also use that name. If F is quadratic, the component F_b has a linear space $L_b = \{y : F_b(x+y)+F_b(x)+F_b(y)+F_b(0) = 0 \text{ for all } x\}$, and S_b is a coset of $L_b^\perp$, so that $|\mathcal{W}_F(a,b)| \in \{0, 2^{(n+\dim L_b)/2}\}$; see [2].

Equivalences.

Two functions F, G are *CCZ-equivalent* if an affine permutation of $\mathbb{F}_2^{2n}$ maps the graph $\{(x, F(x))\}$ of F onto the graph of G [9]. They are *EA-equivalent* if $G = A_1 \circ F \circ A_2 + A_3$ with A_1, A_2 affine permutations and A_3 affine. CCZ-equivalence preserves the differential spectrum and the extended Walsh spectrum, hence the APN property. For quadratic APN functions CCZ-equivalence coincides with EA-equivalence [49]. The following characterization is the basis of our tests.

Proposition 1 ([13]) *F is CCZ-equivalent to a permutation if and only if $\mathcal{Z}_F \cup \{0\}$ contains two n-dimensional linear subspaces U, V with $U \cap V = \{0\}$.*

Given such $U = \langle u_1, \ldots, u_n\rangle$ and $V = \langle v_1, \ldots, v_n\rangle$, a permutation in the CCZ-class of F is $G = G_2 \circ G_1^{-1}$ with $G_1(x) = (u_i \cdot (x, F(x)))_i$ and $G_2(x) = (v_j \cdot (x, F(x)))_j$. Indeed, the linear map with rows $u_1, \ldots, u_n, v_1, \ldots, v_n$ maps the graph of F onto a set whose Walsh transform vanishes on both coordinate axes, so that both projections of this set are bijective. Following [19] we call an n-dimensional subspace of $\mathcal{Z}_F \cup \{0\}$ a *Walsh zero space* of F.

Invariants.

To tell CCZ-classes of quadratic APN functions apart we use the ortho-derivative. For $a \neq 0$, the image of $x \mapsto F(x+a)+F(x)+F(a)+F(0)$ is a hyperplane, and $\pi_F(a)$ is the nonzero vector orthogonal to it. The differential spectrum and the extended Walsh spectrum of π_F are EA-invariants of F [34, 50], hence CCZ-invariants for quadratic APN functions [49]. These invariants are not complete. Two functions with different

invariants are inequivalent, but equal invariants do not prove equivalence. We say that a function lies in a class only when we have proved the equivalence by an explicit certificate (Section 8.4). Otherwise we only say that it has the invariant of that class. All CCZ-equivalence tests are applied to every function individually (Section 8). Our conclusions therefore do not depend on the completeness of the invariant.

3 The inverse function and local search

The cost (1) has a simple geometric meaning.

Lemma 2 *For every (n,n)-function F, $\mathrm{cost}(F) = 3\,\mathrm{A}(F)$.*

Proof Fix $a \neq 0$ and b. The solutions of $F(x+a)+F(x) = b$ come in $\delta_F(a,b)/2$ pairs $\{x, x+a\}$, and every unordered pair of distinct such pairs $\{x, x+a\}$, $\{y, y+a\}$ determines the 2-flat $\{x, x+a, y, y+a\}$, on which F is affine. Conversely, let F be affine on a 2-flat E with direction space $\{0, a, a', a+a'\}$. For each of the three nonzero directions c of E, the two pairs of E in direction c have the same derivative value. Hence every 2-flat on which F is affine is counted exactly three times in (1), once for each nonzero direction. □

Let $I(x) = x^{2^n-2}$ be the inverse function, with $I(0) = 0$. For even n the field $\mathbb{F}_{2^n}$ contains $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, and $\mathbb{F}_{2^n}$ is a vector space over $\mathbb{F}_4$; we call the sets $a\mathbb{F}_4$, $a \neq 0$, the $\mathbb{F}_4$-*lines through the origin*. There are $(2^n-1)/3$ of them. The following proposition is a geometric restatement of Nyberg's computation of the differential spectrum of I [1].

Proposition 3 *Let n be even. The 2-flats on which I is affine are exactly the $\mathbb{F}_4$-lines through the origin. In particular $\mathrm{A}(I) = (2^n-1)/3$ and $\mathrm{cost}(I) = 2^n - 1$.*

Proof For $a \neq 0$ the equation $I(x) + I(x+a) = b$ has at most four solutions, and four solutions only for $b = a^{-1}$ [1]. The four solutions are $x \in a\mathbb{F}_4$: this is clear for $x \in \{0, a\}$, and for $x = a\omega$ we get $(a\omega)^{-1} + (a\omega^2)^{-1} = a^{-1}(\omega^2 + \omega) = a^{-1}$, using $\omega + 1 = \omega^2$, and symmetrically for $x = a\omega^2$. So the 2-flats on which I is affine are the sets $a\mathbb{F}_4$, each of which is a 2-dimensional linear subspace with nonzero directions $a, a\omega, a\omega^2$; by Lemma 2 there are $\mathrm{cost}(I)/3 = (2^n-1)/3$ of them. □

Proposition 3 says that the inverse function is close to APN in a very regular way: it fails the APN condition only on the subspaces $a\mathbb{F}_4$, and all of them contain the point 0. A modification of I that produces an APN permutation must destroy all these flats simultaneously without creating new ones. Changing the value $I(0) = 0$ to any other value already destroys all of them, since each of these flats contains 0. The result is no longer a permutation, so other values must change as well, and the question is how many new flats are created.

Local search.

For $n = 8$ we measured how cost changes when two entries of the lookup table are swapped, i.e. under the moves $S \mapsto S \circ (i\ j)$, which exchange the outputs $S(i)$ and $S(j)$. With an incremental update of the difference table, one move is evaluated in $O(2^n)$ operations. All $\binom{256}{2} = 32{,}640$ transpositions of I can then be scanned in a few milliseconds. The result is that no swap of two entries improves I. No transposition decreases the cost. The 255 transpositions that leave it unchanged are exactly those involving the position 0. Every other transposition increases the cost by at least 222. None of the 255 permutations reached by the cost-preserving transpositions can be improved by a further transposition. We also ran simulated annealing started at I, with plain transpositions or with moves that preserve the involution property of I; recall that Dillon's permutation is CCZ-equivalent to an involution. It never found a permutation of cost below 255 (Section 8.2). For comparison, simulated annealing started from random permutations of $\mathbb{F}_2^8$ does not get below costs between 4,776 and 4,926.

4 Structured families of permutations

We considered three families of permutations that contain, or are related to, the known APN permutations. We searched them exhaustively in dimension eight, and the first family also in dimension ten. All results are negative and are collected in Table 1.

Butterflies with power-based keyed permutations.

Let $n = 2k$ and let R_z, $z \in \mathbb{F}_{2^k}$, be a family of permutations of $\mathbb{F}_{2^k}$. The *open butterfly* [10]

$$H(x, y) = \big(R_t(y),\, t\big), \qquad t = R_y^{-1}(x),$$

is a permutation of $\mathbb{F}_{2^k}^2$ for every such family. Dillon's permutation is an open butterfly with $k = 3$ and $R_z(x) = (x + \alpha z)^3 + z^3$ [10]. The generalized butterflies of [11, 12] use $R_z(x) = (x + \alpha z)^e + z^e$ with $e = 2^i + 1$, which requires k odd. For $n = 8$ the exponent 3 is not available, since x^3 is not a permutation of $\mathbb{F}_{16}$. We therefore allowed

$$R_z(x) = (x + \alpha z)^e + \beta z^f.$$

Here e runs over one representative of each cyclotomic class of exponents coprime to $2^k - 1$. Further, f runs over $0, \ldots, 2^k - 2$ (with z^0 read as 1 for $z \neq 0$ and as 0 for $z = 0$), and α, β run over all of $\mathbb{F}_{2^k}$, including 0. Every such tuple gives a permutation, and we count tuples, not distinct lookup tables. For $k = 3$ six tuples give APN permutations; we did not check how many of them are equivalent. For $k = 4$ and $k = 5$ the smallest costs are 8,280 and 71,424, compared with 255 and 1,023 for the inverse function.

Cyclotomic maps.

For $\ell \mid 2^n - 1$ and $s = (2^n - 1)/\ell$, a cyclotomic map is $S(x) = x^r\, h(x^s)$ with h defined on the ℓ-th roots of unity. In other words, it is a power function multiplied by a constant that depends on the coset of x in $\mathbb{F}_{2^n}^*$ modulo the subgroup of index ℓ. Both x^3, which is APN but not a permutation for even n, and I belong to such families. For $n = 8$

Table 1 Structured families of permutations (Section 4). Butterflies use $R_z(x) = (x + \alpha z)^e + \beta z^f$, switched inverses $I + \gamma \mathrm{Tr}(\delta x^d)$. "Exp. classes" is the number of cyclotomic classes of e, r or d; "Perms." counts parameter tuples that give a permutation, without merging equal or equivalent tables; for the switched inverse the second-smallest cost is also given. The cost of I is $2^n - 1$; a cost of 0 means APN.

Family	n	Exp. classes	Perms.	APN	Min. cost
Butterflies	6	2	896	6	0
	8	2	7,680	0	8,280
	10	6	190,464	0	71,424
Cyclotomic $x^r h(x^{85})$	8	24	346,800	0	255
Switched inverse	8	35	33,660	0	255; 4,155

and $\ell = 3$, each $\mathbb{F}_4$-line $a\mathbb{F}_4^*$ of Proposition 3 meets each of the three cosets in exactly one point, because $\omega = \alpha^{85}$ and 85 is not divisible by three. For $n = 8$ and $\ell = 3$ we took one representative r of each cyclotomic class with $\gcd(r, 85) = 1$, 24 classes in all, and all h with $h(1) = 1$. We kept the maps that are permutations. None of them has cost below 255, and the nontrivial choices of h applied to the inverse function have cost at least 4,080.

Switched inverse functions.

Finally we considered $S(x) = I(x) + \gamma \mathrm{Tr}(\delta x^d)$ for all exponents d, up to cyclotomic equivalence, and all $\gamma, \delta \in \mathbb{F}_{2^8}^*$. Such a switching modifies I on a large set at once. Among the 33,660 parameter tuples that give a permutation, 32,385 give cost 255, the cost of I. Every other one has cost at least 4,155.

These experiments indicate that, in contrast with dimension six, the natural structured generalizations of the known constructions do not come close to the APN property in dimensions eight and ten. The inverse function has the smallest cost we observed for a permutation. The modifications of it that we tried either keep its cost or have a much larger one. This motivates the approach of the following sections, which searches for APN functions that are not permutations and tests them for CCZ-equivalence to a permutation.

5 Exact switching and switching neighbourhoods

Two functions F, G are *switching neighbours* if $G = F + uf$ for a Boolean function f and a nonzero $u \in \mathbb{F}_2^n$ [22]. If F is APN, all its APN switching neighbours can be found by linear algebra.

Proposition 4 ([22]) *Let F be APN and $u \neq 0$. Then $F + uf$ is APN if and only if*

$$f(x) + f(x + a) + f(y) + f(y + a) = 0$$

for all $a \neq 0$ and all x, y such that $F(x) + F(x + a) + F(y) + F(y + a) = u$.

Sketch $F+uf$ fails to be APN iff there are $a \neq 0$ and two distinct pairs $\{x, x+a\}$, $\{y, y+a\}$ with equal derivatives, i.e. $D_aF(x) + D_aF(y) = u\,(D_af(x) + D_af(y))$. Since F is APN the left-hand side is nonzero, so this happens iff $D_aF(x) + D_aF(y) = u$ and $D_af(x) + D_af(y) = 1$. □

The conditions are linear in the truth table of f. So the set $K(F, u)$ of all f with $F + uf$ APN is a subspace of the space of Boolean functions. We compute it exactly by Gaussian elimination over $\mathbb{F}_2$. In dimension ten the system has 2^{10} unknowns and up to a few hundred thousand equations; with rows packed into machine words it is solved in about a quarter of a second.

$K(F, u)$ always contains the affine Boolean functions, and it contains the components $f = b \cdot F$ with $b \cdot u = 0$, for which $F + uf = L \circ F$ with the invertible linear map $L(y) = y + u\,(b \cdot y)$. We call the span $T(F, u)$ of these functions the *trivial* part of $K(F, u)$. If $f \in K(F, u)$ and $t \in T(F, u)$, then $F + u(f + t)$ is EA-equivalent to $F + uf$: for $G = F + uf$ and $b \cdot u = 0$ we have $b \cdot F = b \cdot G$, so $G + u(b \cdot F) = L \circ G$. Hence the switching neighbours of F in direction u are, up to EA-equivalence, given by the $2^q - 1$ nonzero classes of the quotient $K(F, u)/T(F, u)$, where $q = \dim K(F, u) - \dim T(F, u)$.

Lemma 5 *Let F be quadratic and $f \in K(F, u)$. Then $F + uf$ has algebraic degree at least three if and only if the algebraic normal form of f contains a monomial of degree at least three. Consequently, let $K_{\leq 2}$ be the subspace of the elements of $K(F, u)$ of degree at most two, and let $r = \dim K(F, u) - \dim K_{\leq 2}$. Then r is the rank of the degree-≥ 3 parts of the algebraic normal forms of a basis of $K(F, u)$, and F has $2^{\dim K(F,u)} - 2^{\dim K_{\leq 2}}$ switching neighbours of degree at least three in direction u. In particular such neighbours exist if and only if $r > 0$.*

Proof The coordinate functions of $F + uf$ are $F_i + u_i f$; those of F have degree at most two, and u has a nonzero coordinate. The map that sends f to the degree-≥ 3 part of its algebraic normal form is linear on $K(F, u)$, with kernel $K_{\leq 2}$ and image of dimension r. □

Switching closure.

Starting from a list of APN functions, we compute $K(F, u)$ for every source F and every $u \neq 0$. For a power function x^d it suffices to take u modulo the $\gcd(d, 2^n - 1)$-th powers, because of the equivalence $x \mapsto cx$. For each u we record whether non-quadratic solutions exist (Lemma 5). We then form one function $G = F + uf$ for each nonzero class of $K(F, u)/T(F, u)$. In our computations $q \leq 5$ in dimension six and $q \leq 2$ in dimensions eight to ten, so this is cheap. Each quadratic G is compared with the stored functions that have the same ortho-derivative spectra, with the EA-equivalence test of Section 8.4. This test is exhaustive and returns an explicit certificate, which is checked separately. If G is equivalent to a stored function, it is discarded. Otherwise it becomes a new class, is stored, and is in turn switched. EA-equivalent functions have EA-equivalent switching neighbours: if $G = L_1 \circ F \circ L_2 + A$, then $L_1 \circ (F + uf) \circ L_2 + A = G + L_1(u)\,(f \circ L_2)$. So it suffices to switch one function per class. The procedure ends when every stored class has been switched. Non-quadratic neighbours are recorded but not switched further. The result is therefore the exact set of quadratic APN classes reachable from the sources by switching paths whose intermediate functions remain

quadratic, and the classes in it are pairwise inequivalent. In dimensions eight to ten no quadratic class in the closure has a non-quadratic neighbour, so there the closure is also closed under unrestricted switching. In dimension six it is not, but the known classification shows that all thirteen quadratic classes are reached. Every new class is tested for CCZ-equivalence to a permutation with the test of Section 6.

In dimension six we started this procedure from three sources: x^3, the functions $x^3+a^{-1}\mathrm{Tr}(a^3x^9)$ with $a \in \mathbb{F}_4^*$, and $x^3+\alpha(x^{17}+x^{18}+x^{20}+x^{24})$, where α is a primitive element. It reaches all thirteen classes of quadratic APN functions. Five of them have switching neighbours of degree three. Among them is the last source, whose switching gives the non-quadratic APN function of Edel and Pott [22]. Exactly one of the thirteen classes, the class of the Kim function, is found to be CCZ-equivalent to a permutation by the test of Section 6. The procedure thus rediscovers both known exceptional phenomena of dimension six, which serves as a check of the implementation. The results in dimensions eight, nine and ten are reported in Section 8.6.

6 The projection test for CCZ-equivalence to a permutation

By Proposition 1, deciding whether F is CCZ-equivalent to a permutation amounts to finding all Walsh zero spaces of F, i.e. all n-dimensional subspaces of $\mathcal{Z}_F \cup \{0\} \subseteq \mathbb{F}_2^{2n}$, and testing them for a pair with trivial intersection. For a quadratic APN function in even dimension, $\mathcal{Z}_F$ contains about a quarter of $\mathbb{F}_2^{2n}$. In dimension ten this is 262,911 vectors for x^3. A generic search [20] has to find all 10-dimensional subspaces of this set. In this section we assume that the Walsh supports are affine. We show that a Walsh zero space is then described by three objects: a subspace B of $\mathcal{N}_F \cup \{0\}$, a subspace P of $\mathbb{F}_2^n$ of the same dimension m, and a bilinear map Ψ with m^2 binary entries. The searches for B and P take place in $\mathbb{F}_2^n$. We do not claim an improvement of the worst-case complexity of the generic search; the gain is practical, and we measure it in Section 8.3. Throughout, $\pi : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$, $\pi(a,b) = b$, denotes the projection onto the second coordinate, and for a Walsh zero space U we write $U_0 = \{a : (a,0) \in U\}$.

6.1 Projections onto the components with Walsh zeros

Lemma 6 *Let U be a Walsh zero space of an (n,n)-function F. Then $\pi(U) \subseteq \mathcal{N}_F \cup \{0\}$, and $\dim U_0 = n - \dim \pi(U)$.*

Proof If $b \neq 0$ is not in $\mathcal{N}_F$, then $S_b = \mathbb{F}_2^n$, so $\mathcal{W}_F(a,b) \neq 0$ for every a and no vector (a,b) can lie in U. The second statement is the rank–nullity theorem for $\pi|_U$, whose kernel is $U_0 \times \{0\}$. □

Proposition 7 ([15, 16]) *If F is CCZ-equivalent to a permutation, then $\mathcal{N}_F \cup \{0\}$ contains two linear subspaces B_1, B_2 with $B_1 + B_2 = \mathbb{F}_2^n$. In particular, if M denotes the largest dimension of a linear subspace contained in $\mathcal{N}_F \cup \{0\}$, then $M \geq n/2$, and every Walsh zero space U that belongs to a pair with trivial intersection satisfies $n - M \leq \dim \pi(U) \leq M$.*

Proof We recall the short argument for completeness. If $U \cap V = \{0\}$ for two Walsh zero spaces, then $U + V = \mathbb{F}_2^{2n}$, hence $\pi(U) + \pi(V) = \mathbb{F}_2^n$, and both projections lie in $\mathcal{N}_F \cup \{0\}$ by Lemma 6. Then $\dim \pi(U) + \dim \pi(V) \geq n$ with both dimensions at most M. □

Proposition 7 is Condition 2 and Corollary 1 of [16]. The condition was used in [15] for Gold and Kasami functions. The number of subspaces of $\mathcal{N}_F \cup \{0\}$ is an EA-invariant [16, 34]. For quadratic F, Bénéteau, Goluboff, Kölsch and Vaghasiya [18, Corollary V.6] show two further necessary conditions: $|\mathcal{N}_F| \geq 3(2^{n/2} - 1)$, and every $(n/2)$-dimensional subspace meets $\mathcal{N}_F$ in at least three points. In dimension ten the quadratic APN functions considered below have 341 non-bent components, so the bound on $|\mathcal{N}_F|$ does not exclude them. Budaghyan, Ivkovic and Kaleyski [17, Theorem 7] prove $M \leq n/2 - 1$ for every quadratic 3-to-1 APN function when $4 \mid n$. Hence no such function is CCZ-equivalent to a permutation. By [17, Proposition 8], this applies for $4 \mid n$ to all APN monomials and to several infinite families, among them $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$. The case $n \equiv 2 \pmod 4$, which contains dimension ten, is left open there.

Computing M settles every function with $M < n/2$. The computation is inconclusive when $\mathcal{N}_F \cup \{0\}$ contains subspaces spanning $\mathbb{F}_2^n$. In that case one has to decide whether these subspaces are projections of Walsh zero spaces that intersect trivially. The rest of this section shows how to do so.

6.2 Walsh zero spaces of functions with affine supports

We now assume that for every $b \in \mathcal{N}_F$ the Walsh support is an affine subspace $S_b = s_b + D_b$, with D_b a linear subspace. We set $L_b = D_b^\perp$. This holds for every quadratic function, with L_b the linear space of the component F_b (Section 2). Note that $y \cdot s_b$ does not depend on the choice of $s_b \in S_b$ when $y \in L_b$.

Theorem 8 *Let F have affine Walsh supports. Let $B \subseteq \mathcal{N}_F \cup \{0\}$ and $P \subseteq \mathbb{F}_2^n$ be linear subspaces of the same dimension m, and let $\Psi : B \times P \to \mathbb{F}_2$ be a bilinear map. Let $\varphi : B \to \mathbb{F}_2^n$ be a linear map with $y \cdot \varphi(b) = \Psi(b, y)$ for all $b \in B$ and $y \in P$, and set*

$$U(B, P, \Psi) = \{(a, b) : b \in B,\ a \in \varphi(b) + P^\perp\}.$$

Then:

1. *$U(B, P, \Psi)$ is an n-dimensional subspace of $\mathbb{F}_2^{2n}$ that does not depend on the choice of φ, with $\pi(U) = B$ and $U_0 = P^\perp$;*
2. *every n-dimensional subspace U with $\pi(U) \subseteq \mathcal{N}_F \cup \{0\}$ equals $U(B, P, \Psi)$ for exactly one triple, namely $B = \pi(U)$, $P = U_0^\perp$ and $\Psi(b, y) = y \cdot a$ for any $(a, b) \in U$;*
3. *$U(B, P, \Psi)$ is a Walsh zero space of F if and only if for every $b \in B \setminus \{0\}$ there exists $y \in P \cap L_b$ with $\Psi(b, y) \neq y \cdot s_b$.*

Proof (1) A map φ exists because $P^\perp$ has codimension m and $\mathbb{F}_2^n / P^\perp$ is dual to P. Two choices of φ differ by a linear map $B \to P^\perp$, which does not change the set $U(B, P, \Psi)$. The set is the image of the injective linear map $(b, c) \mapsto (\varphi(b) + c, b)$ on $B \times P^\perp$, so it has dimension $m + (n - m) = n$. Its projection is B and its kernel is $P^\perp$.

(2) Let U be given and $B = \pi(U)$, $m = \dim B$. By the rank–nullity theorem for $\pi|_U$, whose kernel is $U_0 \times \{0\}$, we have $\dim U_0 = n - m$, so $P = U_0^\perp$ has dimension m. For $b \in B$ the fibre $\{a : (a, b) \in U\}$ is a coset of $U_0 = P^\perp$. So $y \cdot a$ is the same for all a in the fibre when $y \in P$, and Ψ is well defined and bilinear. The fibres of U and of $U(B, P, \Psi)$ over each b are the same coset of $P^\perp$, hence the two sets coincide. Conversely B, P and Ψ are determined by U, which proves uniqueness.

(3) The fibre over $b = 0$ is $P^\perp$, and $(a, 0) \in \mathcal{Z}_F$ for all $a \neq 0$. For $b \in B \setminus \{0\}$ the fibre $\varphi(b) + P^\perp$ consists of Walsh zeros if and only if it is disjoint from $S_b = s_b + D_b$. Two cosets $x + X$ and $z + Y$ are disjoint if and only if $x + z \notin X + Y$, and $P^\perp + D_b = (P \cap L_b)^\perp$. Hence the fibre consists of Walsh zeros if and only if there exists $y \in P \cap L_b$ with $y \cdot (\varphi(b) + s_b) = 1$, that is, $\Psi(b, y) \neq y \cdot s_b$. □

In particular a Walsh zero space with projection B requires a subspace P of dimension $\dim B$ that meets L_b nontrivially for every $b \in B \setminus \{0\}$. For quadratic APN functions in even dimension the non-bent components typically have $\dim L_b = 2$, so this is a strong condition.

Relation to previous work.

Parts (1) and (2) of Theorem 8 are linear algebra: a subspace of $\mathbb{F}_2^{2n}$ is determined by its projection, its kernel and a linear map between them. The new ingredient is part (3). For affine supports the condition that a fibre consists of Walsh zeros involves only $P \cap L_b$ and s_b. So the possible subspaces P are cut out by the spaces L_b, and Ψ by equations that are linear in the typical case. The characterization of Canteaut and Perrin [13] and the generic search of Bonnetain, Perrin and Tian [20] work with the set $\mathcal{Z}_F$ in $\mathbb{F}_2^{2n}$. Chase and Lisoněk [19] construct Walsh zero spaces of Gold functions explicitly. The necessary condition of [15, 16] uses only the projections. Our test starts from these projections and decides exactly which of them lift to Walsh zero spaces.

6.3 The algorithm

Theorem 8 and Proposition 7 give Algorithm 1, which we call the *projection test*, since it reconstructs the Walsh zero spaces from their projections. All searches take place in $\mathbb{F}_2^n$ or in $B \times P$, never in $\mathbb{F}_2^{2n}$.

Proposition 9 *Let F have affine Walsh supports. Algorithm 1 returns a permutation if and only if F is CCZ-equivalent to a permutation, and every permutation it returns is CCZ-equivalent to F.*

Proof If U, V are Walsh zero spaces with $U \cap V = \{0\}$, then $M \geq n/2$ and $n - M \leq \dim \pi(U), \dim \pi(V) \leq M$ by Proposition 7. By Theorem 8(2) and (3), U equals $U(\pi(U), P, \Psi)$ for a subspace P and a map Ψ that the loops enumerate, and likewise for V. So both lie in $\mathcal{U}$, and the algorithm returns a permutation. Conversely, every element of $\mathcal{U}$ is a Walsh zero space by Theorem 8(3). A pair with trivial intersection gives a permutation CCZ-equivalent to F by Proposition 1. □

The subspaces B are found with a standard vector space search in the set $\mathcal{N}_F \cup \{0\} \subseteq \mathbb{F}_2^n$, where every subspace is generated once through its reduced echelon basis.

Algorithm 1 Projection test: CCZ-equivalence to a permutation for functions with affine Walsh supports

for each $b \neq 0$ with $S_b \neq \mathbb{F}_2^n$ compute s_b and a basis of L_b (from $\mathcal{W}_F$, or from the bilinear form if F is quadratic)
$M \leftarrow$ largest dimension of a subspace of $\mathcal{N}_F \cup \{0\}$
if $M < n/2$ **then return** *not CCZ-equivalent to a permutation*
end if
$\mathcal{U} \leftarrow \emptyset$
for all subspaces $B \subseteq \mathcal{N}_F \cup \{0\}$ with $n - M \leq \dim B \leq M$ **do**
    for all subspaces P, $\dim P = \dim B$, with $P \cap L_b \neq \{0\}$ for all $b \in B \setminus \{0\}$ **do**
        enumerate the bilinear maps Ψ satisfying condition (3) of Theorem 8
        add every $U(B, P, \Psi)$ to $\mathcal{U}$
    end for
end for
if $U, V \in \mathcal{U}$ with $U \cap V = \{0\}$ exist **then return** the permutation $G_2 \circ G_1^{-1}$ of Section 2
else return *not CCZ-equivalent to a permutation*
end if

The subspaces P are built by a depth-first search. At each step it takes the first b whose L_b is not yet met by the current partial basis, and adds one of the nonzero vectors of L_b. Once all L_b are met, it completes the basis in all possible ways. Every admissible P contains a nonzero vector of the L_b chosen at each step, so no P is missed. Every partial and complete subspace is recorded by its reduced echelon basis and visited only once, so every P is produced exactly once.

Let $b_1, \ldots, b_m$ be a basis of B and $p_1, \ldots, p_m$ a basis of P. We store Ψ as the binary $m \times m$ matrix $(\Psi(b_i, p_k))$. If $P \cap L_b = \{0, y\}$, condition (3) is the linear equation $\Psi(b, y) = 1 + y \cdot s_b$ in these m^2 entries. If $\dim(P \cap L_b) \geq 2$, condition (3) says that the equations $\Psi(b, y) = y \cdot s_b$, $y \in P \cap L_b$, do not all hold. This is not a linear condition. We solve the linear equations first and check the other conditions on each element of their solution space. If that space is too large to list, we use a depth-first search instead. It chooses the linear forms $\Psi(b_i, \cdot)$ one at a time and checks condition (3) for every b in the span of the basis vectors already treated. An additional mode enumerates all dimensions $0 \leq \dim B \leq M$; the algorithm then returns the complete list of Walsh zero spaces. We used this mode to compare the algorithm with independent implementations of the generic search (Section 8.3).

Quadratic functions.

For a quadratic F the data of Theorem 8 can be obtained without the Walsh transform. The space L_b is the radical of the alternating form $b \cdot B(x, y)$, an $n \times n$ binary matrix. The vector s_b is any solution of the linear system $s \cdot y = F_b(y) + F_b(0)$, $y \in L_b$. We also split the vector space search in $\mathcal{N}_F$ over several threads at its first level. With these improvements the whole test takes about five seconds for the Gold function in dimension 14. In dimension 18 it takes a few minutes, and the dominant cost is the search for 9-dimensional subspaces in a set of 87,381 elements.

Cost.

The running time is governed by the number of subspaces B in the admissible range, the number of subspaces P for each B, and the size of the solution spaces for Ψ. These numbers depend on the function, and we know no useful worst-case bound for them. The preprocessing stores the sets $\mathcal{N}_F$ and L_b, that is, $O(n2^n)$ words. The search for P also stores the reduced echelon bases of all partial and complete subspaces it visits, and the algorithm stores the Walsh zero spaces it finds. Neither of these is bounded by $O(n2^n)$ in general. Both were small for the functions of Section 8. Section 8.3 reports the running times for the functions we tested.

Scope.

Theorem 8 only needs the Walsh supports to be affine. All functions on which we used it are quadratic, so we have not evaluated the test on other functions with affine supports. For functions whose Walsh supports are not affine, such as the Kasami function x^{57} in dimension ten, Proposition 7 still applies but Theorem 8 does not. For such functions one has to fall back to the generic search.

7 The family $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$

In this section $n = 2m$ and $q = 2^m$. We write $C = \{x^3 : x \in \mathbb{F}_{2^n}^*\}$ for the subgroup of cubes, which has index three since n is even. Let α be a primitive element of $\mathbb{F}_{2^n}$. We study

$$F_a(x) = x^3 + a^{-1}\mathrm{Tr}(a^3x^9), \qquad a \in \mathbb{F}_{2^n}^*,$$

the family of Budaghyan, Carlet and Leander [37] (family F4 above). Göloğlu and Pavlů proved that F_a is not CCZ-equivalent to a permutation when m is even [16, Theorem 3]. Their proof shows that $\mathcal{N}_{F_a} \cup \{0\}$ contains no m-dimensional subspace, using that for even m the set $C \cup \{0\}$ contains no subspace of dimension m [15, Lemma 13]. We study the case of odd m, where this fails.

Lemma 10 *For $c \in \mathbb{F}_{2^n}^*$ we have $F_a(cx) = c^3F_{ac^3}(x)$ and $F_a(x)^2 = F_{a^2}(x^2)$. Hence F_a and $F_{a'}$ are linearly equivalent whenever $a' \in aC$ or $a' = a^2$, and every member of the family is linearly equivalent to F_1 or to F_α.*

Proof $c^3F_{ac^3}(x) = c^3x^3+c^3(ac^3)^{-1}\mathrm{Tr}(a^3c^9x^9) = F_a(cx)$, and $F_a(x)^2 = x^6+a^{-2}\mathrm{Tr}(a^6x^{18}) = F_{a^2}(x^2)$ since $\mathrm{Tr}(y)^2 = \mathrm{Tr}(y)$. The cosets of C in $\mathbb{F}_{2^n}^*$ are C, αC and $\alpha^2 C$, and $a \mapsto a^2$ maps αC onto $\alpha^2 C$. □

The components of F_a are $\mathrm{Tr}(\beta F_a(x)) = \mathrm{Tr}(\beta x^3) + \mathrm{Tr}(\beta a^{-1})\mathrm{Tr}(a^3x^9)$. On the hyperplane $H_a = \{\beta : \mathrm{Tr}(\beta a^{-1}) = 0\}$ they coincide with the components of x^3, which are bent exactly when $\beta \notin C$ [16, Lemma 1]. For odd m we have $\gcd(3, q-1) = 1$, so $\mathbb{F}_q^* \subseteq C$, and $C \cup \{0\}$ is the union of the $(q+1)/3$ lines $c\mathbb{F}_q$, $c \in C$, of the Desarguesian spread $\{c\mathbb{F}_q : c \in \mathbb{F}_{2^n}^*\}$ of $\mathbb{F}_{2^n}$.

Proposition 11 *Let m be odd and $a \in C$. Then the m-dimensional subspace $a\mathbb{F}_q$ is contained in $\mathcal{N}_{F_a} \cup \{0\}$. In particular the necessary condition of Proposition 7 does not exclude F_a by dimension alone.*

Proof Let $\beta = at$ with $t \in \mathbb{F}_q^*$. Then $\beta \in C$ because $a \in C$ and $t \in \mathbb{F}_q^* \subseteq C$, and $\mathrm{Tr}(\beta a^{-1}) = \mathrm{Tr}(t) = \mathrm{Tr}_{\mathbb{F}_q}(t + t^q) = 0$, so $\beta \in H_a$. The component $\mathrm{Tr}(\beta F_a)$ is therefore the component $\mathrm{Tr}(\beta x^3)$ of the Gold function, which is not bent since $\beta \in C$. □

Here $\mathcal{N}_{F_a}$ is taken with respect to the trace form, i.e. in the field coordinates β of the components $x \mapsto \mathrm{Tr}(\beta F(x))$. The computations below are carried out in bit coordinates and translated to field coordinates through the dual basis of the trace form.

7.1 Computations for $n \in \{6, 10, 14, 18, 22\}$

By Lemma 10 it suffices to consider $a \in \{1, \alpha\}$, where $1 \in C$ and $\alpha \notin C$. For $n \leq 18$ we nevertheless computed $a = \alpha^2$ as well, with the same results as for $a = \alpha$. Table 2 lists, for each case, the m-dimensional subspaces of $\mathcal{N}_{F_a} \cup \{0\}$. In every case there is none of dimension $m + 1$. So $M \leq m$, with equality whenever an m-dimensional subspace exists. By Proposition 7 a permutation then requires two m-dimensional subspaces B_1, B_2 with $B_1 \cap B_2 = \{0\}$. If there is at most one m-dimensional subspace, this excludes a permutation. For $n = 22$ this follows from the uniqueness of the m-dimensional subspace, since a subspace of dimension $m+1$ contains $2^{m+1}-1$ subspaces of dimension m. For $n = 18$ the set $\mathcal{N}_{F_a}$ has 87,381 elements. The search for subspaces of dimension nine and ten was split over 128 threads and took about five minutes per value of a.

For $n = 22$ the set $\mathcal{N}_{F_a}$ has 1,398,101 elements, and the plain search is no longer feasible. We therefore used the symmetries of the family. The two identities of Lemma 10 give $F_a(ax^4) = a^3 F_a(x)^4$, and moreover $F_1(x^2) = F_1(x)^2$. So, in bit coordinates, $\mathcal{N}_{F_a}$ is invariant under the transpose of the linear map $y \mapsto a^3 y^4$, which has order 11. For $a = 1$, $\mathcal{N}_{F_1}$ is also invariant under the transpose of $y \mapsto y^2$, which has order 22. The subspaces are then searched only through the smallest element of each orbit, removing the orbits already treated, and the results are closed under the group. These searches are independent, so they can be distributed over several machines. For $a = 1$ the search over the 63,644 orbit representatives took about 63 hours on 128 threads. For $a = \alpha$ the 127,101 representatives were split over up to three servers with 200 threads each, and every finished representative was saved. This search took about three days.

The orbit-pruned search works as follows. Let T be the linear map that generates the group $G = \langle T \rangle$, and let $Z = \mathcal{N}_{F_a}$ in bit coordinates, so that $T(Z) = Z$.

1. List the smallest elements $r_1 < r_2 < \cdots < r_k$ of the G-orbits in Z, as integers.
2. For each i, let Z_i be Z minus the orbits of $r_1, \ldots, r_{i-1}$. Find all d-dimensional subspaces V with $r_i \in V \subseteq Z_i \cup \{0\}$. Their images in the quotient $\mathbb{F}_2^n / \langle r_i \rangle$ are the $(d-1)$-dimensional subspaces contained in $Q_i = \{0\} \cup \{w + \langle r_i \rangle : w \in Z_i,\ w + r_i \in Z_i\}$, which we find with the plain search.

Table 2 Number (#) of m-dimensional subspaces of $\mathcal{N}_{F_a} \cup \{0\}$ for $F_a(x) = x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$, $n = 2m$, m odd. "Lines" means that every such subspace is a line $c\mathbb{F}_q$ of the Desarguesian spread; "$a\mathbb{F}_q$" that one of them is $a\mathbb{F}_q$. The necessary condition of Proposition 7 (column "condition") is inconclusive when two of the subspaces intersect trivially. In every case F_a is not CCZ-equivalent to a permutation.

n	m	a	#	lines	$a\mathbb{F}_q$	condition	decided by
6	3	$1 \in C$	3	yes	yes	inconcl.	Thm. 8
6	3	$\alpha, \alpha^2 \notin C$	0	–	–	excludes	Prop. 7
10	5	$1 \in C$	1	yes	yes	excludes	Prop. 7
10	5	$\alpha, \alpha^2 \notin C$	1	yes	no	excludes	Prop. 7
14	7	$1 \in C$	1	yes	yes	excludes	Prop. 7
14	7	$\alpha, \alpha^2 \notin C$	1	yes	no	excludes	Prop. 7
18	9	$1 \in C$	3	yes	yes	inconcl.	Thm. 8
18	9	$\alpha, \alpha^2 \notin C$	0	–	–	excludes	Prop. 7
22	11	$1 \in C$	1	yes	yes	excludes	Prop. 7
22	11	$\alpha, \alpha^2 \notin C$	1	yes	no	excludes	Prop. 7

3. Return the union of the G-orbits of all subspaces found, deduplicated by reduced echelon bases.

No subspace is missed. Let $V \subseteq Z \cup \{0\}$ have dimension d, and let i be the smallest index such that V meets the orbit of r_i, say in $g(r_i)$ with $g \in G$. Then $g^{-1}(V)$ contains r_i, and it meets no orbit of r_j with $j < i$, because these orbits are G-invariant. So $g^{-1}(V)$ is found in step 2 for this i, and V in step 3. Subspaces with a nontrivial stabilizer need no special treatment. They may be found several times, and step 3 removes the duplicates. The steps for different i are independent. For $a = \alpha$ they were run in twelve lanes (i modulo 12), each with a checkpoint file of finished indices. A final check confirms that every index from 1 to 127,101 is present. We also checked the implementation against the plain search with the same groups for $n = 14$ (dimensions 5 to 8, with up to 5,348 subspaces) and for $n = 18$ (dimensions 9 and 10), for $a \in \{1, \alpha, \alpha^2\}$. The two lists of subspaces coincide in every case (Section 8.5).

We also timed a sample of 800 representatives for each value of a on the same server, at the same relative positions in the two lists of representatives. A single search costs the same for both values: the ratio of the mean CPU times is 0.97. The total cost is therefore proportional to the number of representatives. It is about 13,000 thread-hours for $a = 1$ and 25,000 for $a = \alpha$, measured as CPU time of the hardware threads of a fully loaded server. The factor of two comes from the symmetry group, whose order is 11 instead of 22.

For $n = 18$ and $a = 1$ the three subspaces intersect pairwise trivially, so they span $\mathbb{F}_2^{18}$ in pairs and the necessary condition is satisfied. Algorithm 1 shows that none of them is the projection of a Walsh zero space. Once the subspaces are known, this takes two seconds. The failure occurs in the last step. For each of the three subspaces B, every L_b with $b \in B \setminus \{0\}$ has dimension two, and there are exactly three admissible subspaces P. Each of them meets every L_b in a single nonzero vector. So condition (3) of Theorem 8 is a system of 511 linear equations in the 81 entries of Ψ, and this system has no solution. For each of the nine systems the repository contains a witness

of infeasibility: a set of 7 to 23 of the equations whose left-hand sides sum to zero and whose right-hand sides sum to one. It also contains the bases of the three subspaces. The same happens for $n = 6$ and $a = 1$: each of the three candidate projections has three admissible P, and each resulting system of 7 equations in the 9 entries of Ψ has no solution. Together with the theorem of Göloğlu and Pavlů this gives the following statement. It is a computer-assisted result for $n \in \{6, 10, 14, 18, 22\}$.

Corollary 12 *For every even $n \leq 24$ and every $a \in \mathbb{F}_{2^n}^*$, the function $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$ is not CCZ-equivalent to a permutation.*

Proof For $n \in \{4, 8, 12, 16, 20, 24\}$ this is [16, Theorem 3]; for $n = 2$ there is no APN permutation of $\mathbb{F}_2^2$. For $n \in \{6, 10, 14, 18, 22\}$ it follows from Lemma 10 and Table 2. □

For $n = 10$ and $n = 14$ the necessary condition suffices. These cases are therefore within reach of the method of [16], which reports computations for $n \leq 12$ and random members of the known families up to $n = 18$. For $n = 18$ and $a \in C$, on the other hand, the necessary condition is inconclusive and no theorem applies. To our knowledge this case is new, and it is decided by Theorem 8.

Subspaces of the cubes.

Behind Table 2 is the structure of the large subspaces of $C \cup \{0\}$. For $m = 5$ and $m = 7$, every subspace of $C \cup \{0\}$ of dimension m or $m-1$ lies in a single spread line. There are 11 and 341 such subspaces for $n = 10$, and 43 and 5,461 for $n = 14$. For $m = 3$, in contrast, only 21 of the 28 two-dimensional subspaces do. If this holds for all odd $m \geq 5$, the proof of [16, Theorem 3] can be followed with $V = W \cap H_a$ contained in one spread line. For $\dim V = m$ one obtains exactly the line of Proposition 11. For $\dim V = m-1$ the character-sum argument of [16] no longer gives a contradiction, by the following lemma. Here $V^\perp$ is taken with respect to the trace form.

Lemma 13 *Let m be odd, $c \in C$, and let V be an $(m-1)$-dimensional subspace of the spread line $c\mathbb{F}_q$. Then $|V^\perp \cap C| = (4q-5)/3$.*

Proof Write $V = cH$ with H a hyperplane of $\mathbb{F}_q$, and let T be the trace from $\mathbb{F}_{2^n}$ to $\mathbb{F}_q$. For $\beta \in \mathbb{F}_{2^n}$ and $h \in \mathbb{F}_q$ we have $\mathrm{Tr}(\beta ch) = \mathrm{Tr}_{\mathbb{F}_q}(hT(\beta c))$. So $\beta \in V^\perp$ if and only if $T(\beta c) \in \{0, s\}$, where $\{0, s\}$ is the orthogonal of H in $\mathbb{F}_q$. Put $\gamma = \beta c$; since $c \in C$, $\beta \in C$ if and only if $\gamma \in C$. The kernel of T is $\mathbb{F}_q$, and $\mathbb{F}_q^* \subseteq C$, which gives $q-1$ elements with $T(\gamma) = 0$. Multiplication by $t \in \mathbb{F}_q^*$ preserves C and multiplies T by t. So all nonzero values of T are taken equally often on C, namely $(|C| - (q-1))/(q-1) = (q+1)/3 - 1 = (q-2)/3$ times. The total is $q - 1 + (q-2)/3 = (4q-5)/3$. □

The data suggest the following.

Conjecture 14 *Let $m \geq 5$ be odd and $n = 2m$. If $3 \nmid m$, then $\mathcal{N}_{F_a} \cup \{0\}$ contains exactly one subspace of dimension m, a line of the Desarguesian spread, equal to $a\mathbb{F}_q$ if and only if*

$a \in C$. If $3 \mid m$, it contains three such subspaces if $a \in C$ and none otherwise, and none of them is the projection of a Walsh zero space of F_a. In particular F_a is not CCZ-equivalent to a permutation for any even n.

The case $3 \mid m$ of the conjecture rests on a single value in its range, $m = 9$. The case $m = 3$ lies outside the range but behaves in the same way. The case $3 \nmid m$ rests on $m = 5, 7, 11$. The case $m = 11$ ($n = 22$) was computed after the conjecture was formed, and agrees with it for both $a \in C$ and $a \notin C$. Lemma 13 was also checked numerically for $n = 10$ and $n = 14$.

8 Experiments

8.1 Setup and reproducibility

The core routines are written in C and called from Python. They compute difference tables and the cost (1), and implement incremental local search, vector space search, switching kernels, and an APN test for quadratic functions from their bilinear form. The test of Section 6, the invariants and the experiment drivers are written in Python with NumPy. Unless stated otherwise, experiments were run on a laptop with an Apple M5 Pro processor (18 cores, 24 GB of memory). The randomized tree-search campaign of Section 8.7 and experiments E7, E10 and E12 were run on servers. Each server has two AMD EPYC 7763 processors (128 physical cores, 256 hardware threads and 1 TB of memory), and we ran at low priority, in containers limited to 200 CPUs. The number of worker processes is given with each experiment.

The accompanying repository (https://github.com/peacker/ccz-projection-test-apn) contains one script per experiment (E1–E12 below) and the data files they produce. Running a script recomputes its results. A separate script compares every number reported in this section with the stored results; it does not recompute them. The repository gives the field representations (primitive polynomials) and the bit order. The random seeds are fixed in the scripts.

The checks validate different things.

- APN property: every APN function found by our search programs (dimensions six to ten) was checked by computing its full difference table, independently of the method that produced it. In larger dimensions only the functions of known families are used.
- Permutations: every permutation produced by the CCZ test was checked to be a bijection and APN.
- Equivalences: every EA-equivalence we claim comes with an explicit certificate (L_1, L_2), and a separate routine checks that L_1, L_2 are invertible and that $G + L_1 \circ F \circ L_2$ is affine.
- Walsh zero spaces: the projection test and sboxU return the same lists for the 14 functions of Table 3.
- Completeness of exhaustive searches: this cannot be checked from the output. We rely on cross-checks with independent implementations. sboxU checks the Walsh

zero spaces, and the plain search checks the symmetry-reduced search (E10). The known classification in dimension six checks the switching closure (E5).

The code, the experiments and a first draft of the manuscript were prepared with the assistance of a large language model (Claude, Anthropic). The author takes full responsibility for the content. The checks listed above are run by the scripts of the repository.

8.2 The inverse function and structured permutations (E1, E2)

For $n \in \{4, 6, 8, 10\}$ we verified Proposition 3 directly. For every $a \neq 0$ the difference table of I has exactly one entry equal to 4, and its four solutions form the line $a\mathbb{F}_4$. For $n = 8$ we scanned all 32,640 transpositions of I. None of them decreases the cost. Exactly 255 leave it unchanged: those involving position 0, each of which replaces 6 entries equal to 4 by two entries equal to 6. All others increase the cost by at least 222. The 255 permutations reached by the cost-preserving moves cannot be improved by a further transposition either. We ran simulated annealing from I for $2 \cdot 10^7$ moves per run, without restarts. The temperature decreases geometrically from T_0 to T_1, with $(T_0, T_1) \in \{(2, 0.1), (20, 0.5), (60, 1)\}$, and a move that increases the cost by d is accepted with probability $e^{-d/T}$. We used plain transpositions and involution-preserving moves, with three seeds per setting. An involution-preserving move picks two points $x \neq y$; if they form a 2-cycle it splits it into two fixed points, and otherwise it makes $\{x, y\}$ a 2-cycle and pairs their former partners. No run found a permutation of cost below 255. With the same budget and $(T_0, T_1) = (8, 0.2)$, 18 annealing runs started from random permutations end at costs between 4,776 and 4,926. The seeds are fixed in the script.

The families of Section 4 were enumerated exhaustively, with the results of Table 1. The butterfly enumeration for $n = 10$ (190,464 permutations) takes about three minutes.

8.3 The projection test compared with a generic search (E3, E12)

We compared the projection test (Algorithm 1) with the library sboxU [21]. sboxU implements the generic vector space search of [20], and was used to test CCZ-equivalence to permutations in [17, 23, 24]. Both programs ran on the same otherwise idle server (two AMD EPYC 7763 processors), with sboxU at commit `bedb6d1`. Library loading is not included in the times. We measured two tasks. The first is listing all Walsh zero spaces, with one thread for both programs: the mode of Algorithm 1 that enumerates every dimension $0 \leq \dim B \leq M$, and the function `get_WalshZeroesSpaces` of sboxU. The second is deciding whether the class contains a permutation: Algorithm 1 with one thread, and the function `enumerate_permutations_in_ccz_class` of sboxU with all available threads.

Table 3 shows the results. Each time is a single run, so the benchmark is illustrative and we make no statistical claim about the ratios. The two programs find the same Walsh zero spaces for every function, and both find permutations in the class of the Kim function. For $n \leq 8$ both take a fraction of a second, and sboxU is faster for

Table 3 The projection test (Alg. 1) and the generic search of sboxU [21] on the same machine (E12). "Spaces" is the number of Walsh zero spaces and "perm." whether the CCZ-class contains a permutation; times are in seconds. "List": all Walsh zero spaces, one thread for both; "decide": Alg. 1 with one thread, sboxU (`enumerate_permutations_in_ccz_class`) with all threads. "By" is a sufficient reason for the answer: M the dimension bound, 1 a single candidate projection (with $M = n/2$), Ψ the lifting step of Theorem 8, perm. a permutation found.

n	Function	Spaces	perm.	List		Decide		
				Alg. 1	sboxU	Alg. 1	sboxU	by
6	x^3	190	no	0.030	0.004	0.007	0.022	Ψ
6	Kim function	222	yes	0.036	0.006	0.009	0.034	perm.
8	x^3	256	no	0.10	0.11	0.025	0.064	M
8	$x^3 + \mathrm{Tr}(x^9)$	256	no	0.11	0.12	0.025	0.065	M
8	x^9	256	no	0.10	0.12	0.024	0.064	M
10	x^3	1,024	no	3.37	19.9	0.24	5.47	Ψ
10	$x^3 + \mathrm{Tr}(x^9)$	1,744	no	3.37	17.5	0.15	6.90	1
10	x^9	1,024	no	3.46	19.8	0.24	5.54	Ψ
10	$x^3 + \alpha^{-1}\mathrm{Tr}(\alpha^3 x^9)$	1,624	no	3.21	17.6	0.15	6.56	1
10	Beierle–Leander #3	1,644	no	2.78	24.3	0.16	7.59	Ψ
10	F3 (one class)	1,024	no	2.26	40.8	0.14	8.63	M
10	F12 (one class)	1,024	no	2.55	34.5	0.14	7.15	M
12	x^3	12,286	no	81.6	3,200	0.63	744	M
12	$x^3 + \mathrm{Tr}(x^9)$	8,038	no	64.1	3,507	0.82	727	M

$n = 6$. From $n = 10$ on the projection test is faster. Listing all Walsh zero spaces is the cleanest comparison of the two enumeration methods. The projection test takes 5 to 18 times less time in dimension ten, and 39 to 55 times less in dimension twelve.

For deciding, the column "by" of Table 3 gives a sufficient reason for the answer. For M and Ψ it is also the step at which our implementation stops. For the two functions marked 1, a single candidate projection already excludes a permutation, because $M = n/2$; our implementation does not use this shortcut and still runs the lifting step. In dimension twelve both functions have $M = 4 < 6$, so the dimension bound of Proposition 7 settles them before any projection is examined. The large ratio in that row therefore measures this bound, which sboxU does not apply, and not Theorem 8. A generic search preceded by the same bound would also be fast there. In dimension ten three of the functions need the lifting step of Theorem 8: x^3, x^9 and the Beierle–Leander function. For them deciding takes 0.16 to 0.24 seconds, against 5.5 to 7.6 seconds for sboxU, that is, 23 to 47 times less.

Three further points limit this comparison. First, sboxU used all threads and the projection test one. Second, the function of sboxU computes all permutations in the class, not only whether one exists; here, however, there are none except for the Kim function. Third, the projection test applies only to functions with affine Walsh supports. For the Edel–Pott function in dimension six and the Kasami function in dimension eight, whose supports are not affine, we used our own generic search (E3). It finds 25 and 1 Walsh zero spaces, respectively.

8.4 Known quadratic APN classes in dimension ten (E4, E11)

We instantiated the families F3, F4, F12 and F13 of [34, Table 3] in dimension ten, together with the Gold functions. For F4 we took $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$ with $a \in \mathbb{F}_4^*$ and with a primitive a. For F3 and F12 we took 300 random parameter choices each. For F13 we took all functions of the shape $x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^5} + c(x^{2^{i+5}+2^5})^{2^k}$ with $a, b, c \in \mathbb{F}_4$ and all i, k; these 5,760 functions include the family of [38]. Of the 6,366 functions, 1,266 are APN. They have 17 distinct ortho-derivative invariants. We added the five functions of [24, 51]. Two of them have the same invariants as F13-type functions found above (with $M = 5$), so this gives twenty invariants. The two coincidences are in fact EA-equivalences (E11, see below).

Every distinct APN instance is certified EA-equivalent to the representative of its group by the explicit EA-equivalence test described below. So the twenty groups are exactly twenty classes. None of them is CCZ-equivalent to a permutation. For 13 of them the set of non-bent components contains no subspace of dimension 5. For these, the dimension bound of Proposition 7 already excludes a permutation. Our values of M for the families F3, F4, F12 and the Budaghyan–Helleseth–Kaleyski functions agree with those reported in [16, Table 3] (families 6, 7, 12 and 10 there). For the remaining seven classes, the non-bent components contain between one and eleven subspaces of dimension 5. Algorithm 1 shows that none of them is the projection of a Walsh zero space. For four of these classes there is a single candidate, so the spanning condition of Proposition 7 already excludes a permutation. For the other three the necessary condition is satisfied: the two Gold classes and the class with two candidate projections. There the candidate projections intersect pairwise trivially and therefore span $\mathbb{F}_2^{10}$, so Proposition 7 is inconclusive and the projection test is needed. For the Gold functions the conclusion also follows from the theorem of [15]. For the other class it was obtained in [24] with sboxU. Algorithm 1 decides these cases in 0.15 to 0.25 seconds, while sboxU takes 5 to 8 seconds on the same machine (Section 8.3).

To make the conclusion independent of the invariant, we applied the test to every distinct APN function of the experiment, 402 functions in total. None is CCZ-equivalent to a permutation, and 256 of them are already excluded by the dimension bound of Proposition 7 ($M < 5$). For the families known at the time, this confirms the result of Göloğlu and Pavlů [16] by an independent computation. The F13-type classes with parameters in $\mathbb{F}_4$ that have $M = 5$ contain instances of [24], which were tested there.

Experiment E11 treats the sources of quadratic APN functions in dimension ten that the list above does not cover. We group their APN instances by the ortho-derivative invariant. Then we prove every coincidence by an explicit EA-equivalence $G = L_1 \circ F \circ L_2 + A$. In that case the ortho-derivatives satisfy $\pi_G = (L_1^\top)^{-1} \circ \pi_F \circ L_2$, so the equivalence can be recovered through the ortho-derivative, as in [50]. We use a plain depth-first search over the images of a basis under L_2, pruned by point invariants of π_F and π_G. A candidate is accepted only if $G + L_1 \circ F \circ L_2$ is affine, which we verify directly. (A general algorithm for this problem is given by Kaleyski and Sunde [52].) By [49], EA- and CCZ-equivalence coincide for quadratic APN functions. The search is exhaustive. It tries every image of a basis under L_2 that is compatible with the relation $\pi_G = (L_1^\top)^{-1} \circ \pi_F \circ L_2$, and the point invariants it uses for pruning are

preserved by that relation, so no equivalence is lost. It takes at most a few seconds per pair. The certificates of E4, E5 and E11 are stored in the repository, together with a short script that checks them without the search. Each of the 373 APN instances of E11 is certified to be EA-equivalent to the representative of its class.

- Zheng et al. [33]. We used the three instances given explicitly in the preprint version of their paper (arXiv:2101.11535v1, Table III): the function of their family F15 and the two sporadic instances. We took them for every primitive element of $\mathbb{F}_{2^{10}}$ up to Frobenius. We also took 200 random members of the family of their Theorem 3.3. The first two instances are APN for every primitive element, the third only for two of the 60 primitive elements up to Frobenius. All of them are EA-equivalent to known functions. The first two lie in the F13-type classes that contain the fourth and the second instance of [24], respectively. The third is equivalent to the third instance of [24]. The APN members of the family lie in the classes of x^3, F3 and F13. We could not access a list of the instances of the journal version, whose abstract mentions two instances of an infinite family.
- Göloğlu's biprojective families $\mathcal{F}_1$ and $\mathcal{F}_2$ [39] for all q, and the first family of Calderini, Li and Villa [40, Theorem 3] for all parameters. $\mathcal{F}_1$ and the latter family give two of the F13-type classes. $\mathcal{F}_2$ gives the two F13-type classes that contain the second and fourth instance of [24]. These are the $\varphi(5)/2 = 2$ classes of each of $\mathcal{F}_1$ and $\mathcal{F}_2$ counted in [36, Theorem 5.1]. Random members of Carlet's family give the two classes of F3.
- Budaghyan, Ivkovic and Kaleyski [17, Table 2]. All six functions, instantiated with either primitive element of $\mathbb{F}_4$, are APN. Their ortho-derivatives have exactly the differential spectra printed there. Five of them lie outside the twenty classes above and have pairwise different invariants, so they are five further classes. The second function of their table, as printed, is EA-equivalent to the function $x^3 + \beta x^{36}$, β primitive in $\mathbb{F}_4$, of Edel, Kyureghyan and Pott [53]. This is the F13-type class with $(a, b, c) = (\beta, 0, 0)$, $i = 3$, $k = 2$ above.
- The function of Li, Zhou, Li and Qu ([41]; Theorem 5 of the preprint arXiv:2105.08464v1), and all eleven APN members of the second family of Calderini, Li and Villa [40, Theorem 4], which contains it. They are EA-equivalent to the first function of [17, Table 2].
- Yu et al. [42]. The representative $x^{513} + x^{192} + x^{96} + x^{48} + x^{33} + x^{18} + x^{12}$ of the class of $x^3 + \mathrm{Tr}(x^9)$ given there is EA-equivalent to $x^3 + \mathrm{Tr}(x^9)$, as stated in [42]. The other two classes of that classification are those of x^3 and x^9.

For each of the five further classes, the non-bent components contain no subspace of dimension five ($M = 4$). So Proposition 7 excludes a permutation. This agrees with the check made with sboxU in [17], and for these classes our test is an independent confirmation. In total, the instances we examined give 25 classes of quadratic APN functions in dimension ten (Table 4). None of them is CCZ-equivalent to a permutation.

The count 25 is exact for the instances we considered, but it is not a classification of the families. For F4 we took representatives of all parameters up to the equivalences of Lemma 10. We took all parameters for F13 with parameters in $\mathbb{F}_4$, for the biprojective families of Göloğlu and for the two families of Calderini, Li and Villa. We also took

Table 4 The 25 classes of quadratic APN functions in dimension ten represented by the instances examined in E4 and E11. M is the largest dimension of a subspace of $\mathcal{N}_F \cup \{0\}$ (there are 341 non-bent components in every case). The last column says what excludes a permutation: "$M < 5$" is the dimension bound of Proposition 7; "one projection" means that $\mathcal{N}_F \cup \{0\}$ contains a single 5-dimensional subspace, so the spanning condition of Proposition 7 fails; "Thm. 8" means that the candidate projections span $\mathbb{F}_2^{10}$ in pairs and the projection test is needed. No class is CCZ-equivalent to a permutation.

Family	Classes	M	Reason
Gold x^3, x^9	2	5	Thm. 8 (11 projections)
F4: $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$ [37]	2	5	one projection
F3 [35]	2	4	$M < 5$
F12 [27]	6	3, 4	$M < 5$
F13-type, parameters in $\mathbb{F}_4$ [38]	5	3, 4, 5	$M < 5$ (3), one projection (2)
Beierle–Leander [24]	3	3, 4, 5	$M < 5$ (2), Thm. 8 (1; 2 projections)
Budaghyan et al. [17], [41]	5	4	$M < 5$
Total	25		$M < 5$: 18; one projection: 4; Thm. 8: 3

all published sporadic instances we could obtain. For F3 and F12 we took 300 random parameter choices each, for Carlet's family 50, and for the family of Zheng et al. 200. For Zheng et al. we used the instances of the preprint version. A class of these sampled families that our samples missed would be a known class that we did not test.

8.5 The family $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$ (E9, E10)

The computations of Section 7 are experiments E9 and E10. E9 covers $n \in \{6, 10, 14\}$ and the subspaces of the cubes, on the laptop. E10 covers $n = 18$ and $n = 22$, on the servers. For each n and each a, they list the subspaces of $\mathcal{N}_{F_a} \cup \{0\}$ of dimensions m and $m+1$, translate them to field coordinates through the dual basis of the trace form, and run Algorithm 1. For $n = 18$ the computation of $\mathcal{N}_{F_a}$ takes about one minute and the parallel subspace search about five minutes. The final step of Algorithm 1 takes two seconds. The same subspace search on a single core took four hours. The results are those of Table 2. For $n = 22$, E10 uses the symmetry reduction of Section 7. For $a = 1$ it ran in one go, in about 63 hours on 128 threads; computing $\mathcal{N}_{F_1}$ takes 20 minutes. For $a = \alpha$ the orbit representatives were split into 12 lanes that ran on up to three servers. Every finished representative was saved with its index and the subspaces found, so the work could be moved between servers and survive reboots. The repository contains these lane files, the merged result, and a check that every index from 1 to 127,101 is present. A list of SHA-256 hashes of all result files fixes their content.

Two further computations support these results. First, we compared the symmetry-reduced search with the plain search, with the same groups (E10, symmetry check). For $n = 14$ we used dimensions 5 to 8 and found up to 5,348 subspaces, in about a minute on the laptop. For $n = 18$ we used dimensions 9 and 10; the plain search takes about three minutes per case on 128 threads. The two lists coincide in all 18 cases. Second, for $n = 18$ and $a = 1$ we recorded where Theorem 8 fails for each of the three candidate projections (Section 7). This takes about one second per projection.

Table 5 Exact switching closure (E5). "Classes" is the number of pairwise EA-inequivalent quadratic classes in the closure; "Neighb." is the number of functions formed, one per nonzero class of a quotient $K(F,u)/T(F,u)$; "Certified" is the number of explicit EA-equivalences proved, between a neighbour or a source and a stored class; "deg ≥ 3" indicates whether a class of the closure has a switching neighbour of degree at least three (for non-quadratic sources such as the Kasami function, the quotient is trivial in all our cases); "Perm." gives the classes that are CCZ-equivalent to a permutation.

n	Sources	Classes	Neighb.	Certified	deg ≥ 3	Perm.
6	x^3, F4, Edel–Pott	13	1,259	1,186	yes (5)	1 (Kim)
8	powers, F4	17	96	83	no	none
9	powers, F4	6	14	12	no	(odd n)
10	powers, 25 classes	25	13	18	no	none

8.6 Switching closure (E5)

Table 5 summarizes the switching computations of Section 5. In each dimension we computed the switching closure of the sources over switching paths whose intermediate functions remain quadratic, as described in Section 5. Every nonzero class of every quotient $K(F,u)/T(F,u)$ was formed. Every quadratic neighbour that is not a new class was certified EA-equivalent to a stored class. In dimensions eight, nine and ten no quadratic class in the computed closure has a switching neighbour of degree three or more. Among the power functions only the Gold functions have nontrivial switchings, x^3 in all three dimensions and x^9 in dimension eight. The Kasami, Welch, Niho, Dobbertin and inverse functions have none in these dimensions. In dimension eight the closure has 17 classes, none of which is CCZ-equivalent to a permutation. This is consistent with [24], where switching was applied to all quadratic APN functions known in dimension eight. In dimension ten the closure of the 25 classes contains no other class. Only x^3, the two F4 classes and four of the five classes of [17] have nontrivial switching neighbours. The classes of F3, F12, F13 and of [24] have none.

8.7 Searching for new quadratic APN functions in dimension ten (E6–E8)

Since all 25 classes examined here are excluded, an APN permutation CCZ-equivalent to a quadratic function would have to come from a class outside this tested set. We tried three generators. The first (E6) is a feasibility test in dimensions six to eight. It shows that unstructured search does not scale, so we did not run it in dimension ten. The other two (E7, E8) run in dimension ten.

Search over bilinear forms (E6).

A quadratic function is APN if and only if its alternating bilinear form $B(x,y) = F(x+y)+F(x)+F(y)+F(0)$ satisfies $B(x,y) \neq 0$ for all linearly independent x, y. We build B on $\langle e_1, \ldots, e_k \rangle$ for increasing k. The extension by e_{k+1} amounts to choosing a linear map $L(x) = B(x, e_{k+1})$ with $L(x) \notin B(x, \langle e_1, \ldots, e_k \rangle)$ for all nonzero x. We explore these choices by a randomized depth-first search. In dimension six the search

reaches all thirteen classes from 3,000 restarts, in three seconds; their 13 invariants are pairwise distinct, so every class is reached. In dimension seven it finds 237 solutions with 194 distinct invariants, hence at least 194 classes, where 488 classes are known [46]. In dimension eight it finds no solution in 36 runs of $3 \cdot 10^7$ nodes. Unstructured search is therefore not a viable generator beyond dimension seven. This is consistent with the use of self-equivalences in [24].

Symmetry-restricted univariate families (E7).

We sampled quadratic polynomials $\sum_e c_e x^e$, $e = 2^i + 2^j$, in 522 families:

- coefficients in $\mathbb{F}_2$ (Frobenius-invariant functions), with four densities;
- coefficients in the subfields $\mathbb{F}_4$ and $\mathbb{F}_{32}$;
- sparse polynomials with two to five terms;
- polynomials whose exponents lie in a single residue class modulo m, for each divisor $m \leq 341$ of 1023 (functions with $F(\zeta x) = \zeta^d F(x)$ for ζ of order m).

For quadratic functions the APN property is decided from the $n \times n$ bilinear matrix in about $40\,\mu$s, and faster for the many candidates rejected early. Of the 522 families, 372 residue families contain no exponent $2^i + 2^j$, so they have no candidates; the other 150 families sample. Each of them got a maximum budget of 2,560 batches of 2,000 candidates, with a fixed seed. Before each batch a family stops if it has already found 2,000 APN functions, counted with repetitions; so it ends with fewer than 4,000, and all of them are kept. 56 families stopped in this way, and 94 used their full budget. In total we tested 535,492,000 candidates, out of a maximum of $150 \cdot 2{,}560 \cdot 2{,}000 = 768{,}000{,}000$. They gave 166,157 APN functions counted with repetitions, and 105,595 distinct ones; for instance, a family with a single exponent contains at most 1,023 distinct functions. The repository records these numbers for every family, and lists every distinct function with its test result. Every distinct APN function found was tested individually with Algorithm 1. None is CCZ-equivalent to a permutation. Their invariants are those of 11 of the twenty classes of E4, and no other invariant occurs. The run took 15 minutes on 64 server threads.

Tree search with prescribed self-equivalences (E8).

We ran the deterministic tree search of Beierle and Leander [54] for each of the 195 classes of linear self-equivalences of $\mathbb{F}_2^{10}$ considered in [24], with a time limit of five minutes per class. The search terminated for 69 classes. Solutions were found in six classes, giving 686 APN functions with nine distinct invariants, all among those of the twenty classes of E4. The test applied to each of the 686 functions finds no CCZ-equivalent permutation. For the 126 classes in which the search did not terminate, we then ran the randomized version of the tree search for 24 hours on 128 threads. That is about one CPU-day per class (6,144 runs of 30 minutes). Solutions were again found only in the six classes above. Together with the deterministic runs we obtained 4,638 distinct APN functions with 16 distinct invariants, all among those of the twenty classes of E4. None of the 4,638 functions is CCZ-equivalent to a permutation. In particular, no solution was found in the two classes for which [24] reports that solutions must exist but were not found after 16 CPU-days each.

9 Conclusions and future work

We gave a parametrization of the Walsh zero spaces of functions with affine Walsh supports. It turns the test for CCZ-equivalence to a permutation into searches for subspaces of $\mathbb{F}_2^n$ and for bilinear maps between them. This projection test decides the cases in which the necessary condition of [15, 16] is inconclusive. For listing all Walsh zero spaces it is 39 to 55 times faster than the generic search of sboxU in dimension twelve, on the functions we measured. With it we settled the family $x^3+a^{-1}\mathrm{Tr}(a^3x^9)$ in all even dimensions up to 24, by computation for $n \in \{6, 10, 14, 18, 22\}$. This includes a case in dimension 18 that the known necessary condition leaves open.

In dimension ten we checked the 25 classes of quadratic APN functions represented by the published instances we examined. Five of them, from [17], are not in the earlier lists; for these our test confirms the result obtained there with sboxU. We computed the quadratic switching closure of the source functions listed in Table 5 in dimensions eight to ten, and tested every function found by two generators of quadratic APN functions in dimension ten. No APN permutation was found. For $n = 8$, the inverse function fails the APN condition exactly on the two-dimensional subspaces $a\mathbb{F}_4$, and swapping two entries of its lookup table never brings it closer to the APN property. The butterflies with power-based keyed permutations, the cyclotomic maps and the switched inverse functions that we enumerated contain no permutation of $\mathbb{F}_2^8$ closer to the APN property than the inverse function.

Several directions remain open.

- *Conjecture 14.* It holds in all computed cases, up to $n = 22$. A proof would settle the family $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$ in all even dimensions. It needs two ingredients. The first is a description of the subspaces of dimension $m - 1$ and m of the cubes for odd m. The second is an analysis of the case $\dim(W \cap H_a) = m - 1$, where the argument of [16] no longer applies.
- *Non-affine Walsh supports.* Theorem 8 requires affine supports. Plateaued functions need not have affine supports. Proposition 7 still applies to plateaued and general functions, so an extension of the projection test to them would be useful. Natural test cases are the Kasami function in dimension ten, which is not covered by [15] since $10 \not\equiv 0 \pmod 4$, and the Dobbertin function x^{339}.
- *New quadratic APN functions in dimension ten.* The bottleneck of the CCZ approach in dimension ten is the small number of known quadratic APN classes. The complete classification of the functions with coefficients in $\mathbb{F}_2$ [42] gives no new class. New classes therefore have to come from larger coefficient fields or other structures. On the functions we tested, the test costs a fraction of a second per function. So any generator that produces many new classes can be combined with it directly, for instance the constructions of Beierle et al. [23] adapted to dimension ten.
- *Dimension twelve.* The two functions we measured in dimension twelve are decided in under a second, by the dimension bound, and listing all their Walsh zero spaces takes about a minute (Section 8.3). Testing all known quadratic APN classes in dimension twelve, and their switching closure, seems a plausible next step. The functions of Göloğlu and Kölsch [48] in dimension twelve would be natural test cases.

- *Two-step switching.* The switching graph of quadratic APN functions in dimension ten is small. Switching simultaneously in two directions, $F + u_1 f_1 + u_2 f_2$, leads to quadratic rather than linear systems and is a natural next step.
- *Program search.* Romera-Paredes et al. recently used large language models to search for programs that construct combinatorial objects [55]. A candidate construction of a permutation, given as a program that works in every dimension, can be scored exactly by cost. The big APN problem is therefore a natural target for such methods.

Statements and Declarations

- **Funding:** No dedicated funding was received for conducting this study.

- **Competing interests:** The author has no competing interests to declare that are relevant to the content of this article.
- **Data and code availability:** All scripts, the C and Python sources, the generated data and the expected results are publicly available at https://github.com/peacker/ccz-projection-test-apn (release v1.0, commit `0ac04cd`). The repository contains one script per experiment, which recomputes its results, and a script that compares every number reported in this paper with the stored results.
- **Use of AI tools:** The code, the experiments and a first draft of the manuscript were prepared with the assistance of a large language model (Claude, Anthropic). Section 8 lists the checks applied to the results and what each of them validates. The author takes full responsibility for the content.

References

[1] Nyberg, K.: Differentially uniform mappings for cryptography. In: Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. Lecture Notes in Computer Science, vol. 765, pp. 55–64. Springer, Berlin, Heidelberg (1993). https://doi.org/10.1007/3-540-48285-7_6

[2] Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2021). https://doi.org/10.1017/9781108606806

[3] Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). IEEE Trans. Inf. Theory **14**(1), 154–156 (1968) https://doi.org/10.1109/TIT.1968.1054106

[4] Kasami, T.: The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. Inf. Control. **18**(4), 369–394 (1971) https://doi.org/10.1016/S0019-9958(71)90473-6

[5] Dobbertin, H.: Almost perfect nonlinear power functions on GF(2^n): The Welch case. IEEE Trans. Inf. Theory **45**(4), 1271–1275 (1999) https://doi.org/10.1109/18.761283

[6] Dobbertin, H.: Almost perfect nonlinear power functions on GF(2^n): The Niho case. Inf. Comput. **151**(1-2), 57–72 (1999) https://doi.org/10.1006/inco.1998.2764

[7] Hou, X.: Affinity of permutations of $\mathbb{F}_2^n$. Discret. Appl. Math. **154**(2), 313–325 (2006) https://doi.org/10.1016/j.dam.2005.03.022

[8] Browning, K.A., Dillon, J.F., McQuistan, M.T., Wolfe, A.J.: An APN permutation in dimension six. In: Finite Fields: Theory and Applications. Contemporary Mathematics, vol. 518, pp. 33–42. American Mathematical Society, Providence, RI (2010). https://doi.org/10.1090/conm/518/10194

[9] Carlet, C., Charpin, P., Zinoviev, V.A.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**(2), 125–156 (1998) https://doi.org/10.1023/A:1008344232130

[10] Perrin, L., Udovenko, A., Biryukov, A.: Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. In: Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9815, pp. 93–122. Springer, Berlin, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53008-5_4

[11] Canteaut, A., Duval, S., Perrin, L.: A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}. IEEE Trans. Inf. Theory **63**(11), 7575–7591 (2017) https://doi.org/10.1109/TIT.2017.2676807

[12] Canteaut, A., Perrin, L., Tian, S.: If a generalised butterfly is APN then it operates on 6 bits. Cryptogr. Commun. **11**(6), 1147–1164 (2019) https://doi.org/10.1007/s12095-019-00361-x

[13] Canteaut, A., Perrin, L.: On CCZ-equivalence, extended-affine equivalence, and function twisting. Finite Fields Their Appl. **56**, 209–246 (2019) https://doi.org/10.1016/j.ffa.2018.11.008

[14] Beierle, C., Brinkmann, M., Leander, G.: Linearly self-equivalent APN permutations in small dimension. IEEE Trans. Inf. Theory **67**(7), 4863–4875 (2021) https://doi.org/10.1109/TIT.2021.3071533

[15] Göloğlu, F., Langevin, P.: Almost perfect nonlinear families which are not equivalent to permutations. Finite Fields Their Appl. **67**, 101707 (2020) https://doi.org/10.1016/j.ffa.2020.101707

[16] Göloğlu, F., Pavlů, J.: On CCZ-inequivalence of some families of almost perfect nonlinear functions to permutations. Cryptogr. Commun. **13**(3), 377–391 (2021) https://doi.org/10.1007/s12095-021-00476-0

[17] Budaghyan, L., Ivkovic, I., Kaleyski, N.S.: Triplicate functions. Cryptogr. Commun. **15**(1), 35–83 (2023) https://doi.org/10.1007/s12095-022-00587-2

[18] Bénéteau, S.H., Goluboff, N., Kölsch, L., Vaghasiya, D.: On the Walsh spectra of quadratic APN functions. IEEE Trans. Inf. Theory **72**(7), 5207–5216 (2026) https://doi.org/10.1109/TIT.2026.3695003 . Preprint: arXiv:2510.12008

[19] Chase, B., Lisoněk, P.: Construction of APN permutations via Walsh zero spaces. Cryptogr. Commun. **14**(6), 1345–1357 (2022) https://doi.org/10.1007/s12095-022-00580-9

[20] Bonnetain, X., Perrin, L., Tian, S.: Anomalies and vector space search: Tools for s-box analysis. In: Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I. Lecture Notes in Computer Science, vol. 11921, pp. 196–223. Springer, Berlin, Heidelberg (2019). https://doi.org/10.1007/978-3-030-34578-5_8

[21] Perrin, L., Alich, J., Baudrin, J., Boeuf, A., Bonnetain, X., Couvreur, A., Fruchon, M., Joly, M., Galissant, P., Stennes, L.: sboxU: black-box analysis of discrete functions. Software, https://github.com/lpp-crypto/sboxU. Commit bedb6d1 (2026)

[22] Edel, Y., Pott, A.: A new almost perfect nonlinear function which is not quadratic. Adv. Math. Commun. **3**(1), 59–81 (2009) https://doi.org/10.3934/amc.2009.3.59

[23] Beierle, C., Langevin, P., Leander, G., Polujan, A.A., Rasoolzadeh, S.: Millions of inequivalent quadratic APN functions in eight variables. CoRR **abs/2508.04644** (2025) https://doi.org/10.48550/arXiv.2508.04644 . Version 2, August 2026

[24] Beierle, C., Leander, G.: New instances of quadratic APN functions. IEEE Trans. Inf. Theory **68**(1), 670–678 (2022) https://doi.org/10.1109/TIT.2021.3120698

[25] Yu, Y., Wang, M., Li, Y.: A matrix approach for constructing quadratic APN functions. Des. Codes Cryptogr. **73**(2), 587–600 (2014) https://doi.org/10.1007/s10623-014-9955-3

[26] Weng, G., Tan, Y., Gong, G.: On quadratic APN functions and their related algebraic objects. In: International Workshop on Coding and Cryptography (WCC 2013), Bergen, Norway, pp. 48–57 (2013)

[27] Taniguchi, H.: On some quadratic APN functions. Des. Codes Cryptogr. **87**(9), 1973–1983 (2019) https://doi.org/10.1007/s10623-018-00598-2

[28] Yu, Y., Perrin, L.: Constructing more quadratic APN functions with the QAM method. Cryptogr. Commun. **14**(6), 1359–1369 (2022) https://doi.org/10.1007/s12095-022-00598-z

[29] Beierle, C., Leander, G., Perrin, L.: Trims and extensions of quadratic APN functions. Des. Codes Cryptogr. **90**(4), 1009–1036 (2022) https://doi.org/10.1007/s10623-022-01024-4

[30] Beierle, C., Langevin, P., Leander, G., Polujan, A., Rasoolzadeh, S.: Millions of inequivalent quadratic APN functions in eight variables. Dataset, Zenodo (2025). https://doi.org/10.5281/zenodo.16752428

[31] Kuznetsov, O.: Quadratic APN functions in dimension 8 via Gröbner basis search in a self-equivalence subspace. CoRR **abs/2606.11967** (2026) https://doi.org/10.48550/arXiv.2606.11967

[32] Dobbertin, H.: Almost perfect nonlinear power functions on GF(2^n): A new case for n divisible by 5. In: Finite Fields and Applications, Fifth International Conference on Finite Fields and Applications Fq5, Augsburg, Germany, August 2-6, 1999, pp. 113–121. Springer, Berlin, Heidelberg (2001). https://doi.org/10.1007/978-3-642-56755-1_11

[33] Zheng, L., Kan, H., Li, Y., Peng, J., Tang, D.: Constructing new APN functions through relative trace functions. IEEE Trans. Inf. Theory **68**(11), 7528–7537 (2022) https://doi.org/10.1109/TIT.2022.3186899 . Preprint: arXiv:2101.11535

[34] Kaleyski, N.S.: Invariants for EA- and CCZ-equivalence of APN and AB functions. Cryptogr. Commun. **13**(6), 995–1023 (2021) https://doi.org/10.1007/s12095-021-00541-8

[35] Budaghyan, L., Carlet, C.: Classes of quadratic APN trinomials and hexanomials and related structures. IEEE Trans. Inf. Theory **54**(5), 2354–2357 (2008) https://doi.org/10.1109/TIT.2008.920246

[36] Göloğlu, F., Kölsch, L.: Equivalences of biprojective almost perfect nonlinear functions. Comb. Theory **5**(3) (2025) https://doi.org/10.5070/C65365555 . Preprint: arXiv:2111.04197

[37] Budaghyan, L., Carlet, C., Leander, G.: Constructing new APN functions from known ones. Finite Fields Their Appl. **15**(2), 150–159 (2009) https://doi.org/10.1016/j.ffa.2008.10.001

[38] Budaghyan, L., Helleseth, T., Kaleyski, N.S.: A new family of APN quadrinomials. IEEE Trans. Inf. Theory **66**(11), 7081–7087 (2020) https://doi.org/10.1109/TIT.2020.3007513

[39] Göloğlu, F.: Biprojective almost perfect nonlinear functions. IEEE Trans. Inf. Theory **68**(7), 4750–4760 (2022) https://doi.org/10.1109/TIT.2022.3157798

[40] Calderini, M., Li, K., Villa, I.: Extending two families of bivariate APN functions. Finite Fields Their Appl. **88**, 102190 (2023) https://doi.org/10.1016/j.ffa.2023.

102190 . Preprint: arXiv:2204.07462

[41] Li, K., Zhou, Y., Li, C., Qu, L.: Two new families of quadratic APN functions. IEEE Trans. Inf. Theory **68**(7), 4761–4769 (2022) https://doi.org/10.1109/TIT.2022.3157810 . Preprint: arXiv:2105.08464

[42] Yu, Y., Li, J., Ichanska, N., Kaleyski, N.S.: Classification of quadratic APN functions with coefficients in $\mathbb{F}_2$ in dimension 10. Appl. Algebra Eng. Commun. Comput. (2025) https://doi.org/10.1007/s00200-025-00711-8 . Online first. Preprint: Cryptology ePrint Archive, Paper 2024/1778

[43] Yu, Y., Kaleyski, N.S., Budaghyan, L., Li, Y.: Classification of quadratic APN functions with coefficients in $\mathbb{F}_2$ for dimensions up to 9. Finite Fields Their Appl. **68**, 101733 (2020) https://doi.org/10.1016/j.ffa.2020.101733

[44] Ichanska, N., Berg, S., Kaleyski, N.S., Yu, Y.: Pushing the QAM method for finding APN functions further. Cryptogr. Commun. **18**(3), 727–762 (2026) https://doi.org/10.1007/s12095-025-00851-1 . Preprint: Cryptology ePrint Archive, Paper 2024/1838

[45] Budaghyan, L., Calderini, M., Villa, I.: On equivalence between known families of quadratic APN functions. Finite Fields Their Appl. **66**, 101704 (2020) https://doi.org/10.1016/j.ffa.2020.101704

[46] Kalgin, K., Idrisova, V.: The classification of quadratic APN functions in 7 variables and combinatorial approaches to search for APN functions. Cryptogr. Commun. **15**(2), 239–256 (2023) https://doi.org/10.1007/s12095-022-00588-1

[47] Beierle, C., Langevin, P., Leander, G., Polujan, A., Rasoolzadeh, S.: Classification of quadratic APN functions up to EA-equivalence. Dataset, Zenodo (2026). https://doi.org/10.5281/zenodo.22010376

[48] Göloğlu, F., Kölsch, L.: Triprojective almost perfect nonlinear permutations and functions. CoRR **abs/2605.17545** (2026)

[49] Yoshiara, S.: Equivalences of quadratic APN functions. J. Algebraic Combin. **35**(3), 461–475 (2012) https://doi.org/10.1007/s10801-011-0309-1

[50] Canteaut, A., Couvreur, A., Perrin, L.: Recovering or testing extended-affine equivalence. IEEE Trans. Inf. Theory **68**(9), 6187–6206 (2022) https://doi.org/10.1109/TIT.2022.3166692

[51] Beierle, C., Leander, G.: New Instances of Quadratic APN Functions in Small Dimension. Dataset, Zenodo, version 2.1 (2021). https://doi.org/10.5281/zenodo.4738942

[52] Kaleyski, N.S., Sunde, J.: Efficiently deciding and recovering CCZ and EA equivalence for arbitrary vectorial Boolean functions using the partition refinement framework. Cryptology ePrint Archive, Paper 2026/940 (2026). https://eprint.iacr.org/2026/940

[53] Edel, Y., Kyureghyan, G.M., Pott, A.: A new APN function which is not equivalent to a power mapping. IEEE Trans. Inf. Theory **52**(2), 744–747 (2006) https://doi.org/10.1109/TIT.2005.862128

[54] Beierle, C.: quadratic_apn: Tree Search for Quadratic APN Functions, v1.0. Software, Zenodo (2020). https://doi.org/10.5281/zenodo.4305864

[55] Romera-Paredes, B., Barekatain, M., Novikov, A., Balog, M., Kumar, M.P., Dupont, E., Ruiz, F.J.R., Ellenberg, J.S., Wang, P., Fawzi, O., Kohli, P., Fawzi, A.: Mathematical discoveries from program search with large language models. Nat. **625**(7995), 468–475 (2024) https://doi.org/10.1038/s41586-023-06924-6