Classification of all DO planar polynomials with prime field coefficients over $\mathbb{F}_{3^n}$ for $n \leq 7$

Diana Davidova[1] and Nikolay S. Kaleyski[1]

Department of Informatics, University of Bergen, Norway
{diana.davidova, nikolay.kaleyski}@uib.no

Abstract. We present a simplification of the matrix representation of quadratic APN functions due to Yu et al. Based on this, we adapt a method of Yu et al. for searching for quadratic APN functions with prime field coefficients to the case of planar DO functions. We use this method to find all such functions (up to CCZ-equivalence) over $\mathbb{F}_{3^n}$ for $n \leq 7$. We conclude that the currently known planar DO polynomials cover all possible cases for $n \leq 7$. We find representatives simpler than the known ones for the Zhou-Pott, Dickson, and Lunardon-Marino-Polverino-Trombetti-Bierbrauer families for $n = 6$.

Keywords: planar function · DO polynomial · derivative.

1 Introduction

Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements and $\mathbb{F}_{p^n}^*$ be its multiplicative group for some prime p and some positive integer n. We will identify $\mathbb{F}_{p^n}$ with the vector space $\mathbb{F}_p^n$ over $\mathbb{F}_p$. An (n, m)-**function** is a mapping from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. When $n = m$, any (n, n)-function F has a unique representation as a polynomial in $\mathbb{F}_p[x]$ of the form $F(x) = \sum_{i=0}^{p^n-1} a_i x^i$. This polynomial is called the **univariate representation** of F. We typically identify an (n, n)-function with its univariate representation and use the two interchangeably. Recall that the p-weight of an integer is the weight of its p-ary expansion. The **algebraic degree** of F, denoted $\deg(F)$, is the largest p-weight of any exponent $i \in \{0, 1, 2, \ldots, p^n - 1\}$ in the univariate representation of F with $a_i \neq 0$. If $\deg(F) \leq 1$, we say that F is **affine**; if, in addition, $F(0) = 0$, we say that F is **linear**. As the name implies, any linear function L satisfies $c_1 L(x) + c_2 L(y) = L(c_1 x + c_2 y)$ for any $x, y \in \mathbb{F}_{p^n}$ and $c_1, c_2 \in \mathbb{F}_p$. If $\deg(F) = 2$, we say that F is **quadratic**, and if $F(x) = \sum_{i,j} a_{i,j} x^{p^i+p^j}$, we say that F is a **DO polynomial** (after Dembowski and Ostrom). Thus, any DO polynomial is quadratic but not vice-versa.

The **derivative** of $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ in direction $a \in \mathbb{F}_{p^n}$ is the (n, n)-function $D_a F(x) = F(a+x) - F(x)$. Denoting by $\delta_F(a, b)$ the number of solutions $x \in \mathbb{F}_{p^n}$ to the equation $D_a F(x) = b$, the **differential uniformity** δ_F of F is the maximum value of $\delta_F(a, b)$ across all $a \in \mathbb{F}_{p^n}^*$, $b \in \mathbb{F}_{p^n}$. The differential uniformity is an important cryptographic parameter since it measures the resistance provided by a function to differential cryptanalysis: the lower the value of δ_F, the

stronger the resistance. We say that a function F is **planar**, or **perfect nonlinear (PN)** if it attain the optimal value $\delta_F = 1$. Note that PN functions can also be defined in the more general context of (n, m)-functions with $n \neq m$; however, in this abstract we only consider the case $n = m$ and use the terms "planar" and "PN" interchangeably. Equivalently, a function F is planar if and only if all of its derivatives $D_a F$ for $a \in \mathbb{F}_{p^n}^*$ permute $\mathbb{F}_{p^n}$. It is easy to see that PN functions only exist when the characteristic p is odd, since for $p = 2$ we have $D_a F(x) = D_a F(a + x)$ for any $a, x \in \mathbb{F}_{2^n}$ and any $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. In the case of even characteristic, the lowest possible value of δ_F is 2, and the functions that attains this value are called **almost perfect nonlinear (APN)**.

Due to the large number of (n, n)-functions, PN and APN functions are typically classified up to CCZ-equivalence. Named after Carlet, Charpin and Zinoviev who introduce it in [5], CCZ-equivalence is the most general known relation that preserves the differential uniformity (and hence, PN-ness and APN-ness) of (n, n)-functions. We say that $F, G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are CCZ-equivalent if there exists an affine permutation $A : \mathbb{F}_{p^{2n}} \to \mathbb{F}_{p^{2n}}$ mapping the graph $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_{p^n}\}$ of F to the graph Γ_G of G.

Another notion is that of EA-equivalence (extended affine equivalence). We say that $F, G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are **EA-equivalent** if there are affine permutations A_1, A_2 of $\mathbb{F}_{p^n}$ and an affine function $A : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ such that $A_1 \circ F \circ A_2 + A = G$. If F and G are CCZ-equivalent, then they are EA-equivalent, but the converse is not true in general. However, the converse statement is true for some classes of functions. Most importantly, EA-equivalence implies CCZ-equivalence for planar functions [4], [11] and quadratic APN functions [16]. Note that any quadratic function is equivalent to a DO polynomial (up to addition of an affine function), and so we can use "quadratic" and "DO" interchangeably (up to EA-equivalence).

In general, deciding the CCZ-equivalence of two (n, n)-functions is a hard computational problem. At present, the only practical way to so is via the isomorphism of linear codes [9]. This has a significant time and space complexity, but it works for any pair of functions over any finite field.

Both PN and APN functions have been the subject of intense study in recent years, not only because of their cryptographic significance but also due to their correspondence to important objects in other fields of mathematics and computer science. For instance, there is a one-to-one correspondence between planar DO polynomials and commutative semifields [6]; commutative semifields have been studied since their introduction by Dickson in 1906 [7], and this correspondence has been used to construct new families and instances of semifields that had previously eluded researchers, e.g. [4], [21].

In practice, finding new APN and PN functions CCZ-inequivalent to the known ones is a very hard problem. The number of all (n, n)-functions is too large to allow for an exhaustive search, and so many mathematical constructions and computational methods have been developed, e.g. [8], [10], [19]. The difficulty of finding new instances is particularly prominent in the case of PN functions, where we currently know less than 10 CCZ-inequivalent instances over $\mathbb{F}_{p^n}$ for odd p and $n \leq 7$; for comparison, thousands of CCZ-inequivalent APN functions

have been constructed over $\mathbb{F}_{2^n}$ with $n \leq 8$ using computational methods such as [1] and [19]. Despite this apparent abundance of APN instances, we note that classifying these sporadic instances (coming from computational methods) into general constructions remains an extremely challenging problem. Finding APN functions with other desirable properties, such as being permutations, or having an algebraic degree greater than 2 is quite difficult as well.

A representation of quadratic APN functions in terms of symmetric matrices is presented in [19]. The authors of [19] use this representation to conduct a computational search for APN functions by trying to guess the entries of their associated matrices, and are able to produce more than 400 CCZ-inequivalent APN functions over $\mathbb{F}_{2^7}$, and more than 8 000 CCZ-inequivalent APN functions over $\mathbb{F}_{2^8}$. This is a substantial improvement, since prior to [19], only around 30 CCZ-inequivalent APN functions were known over $\mathbb{F}_{2^8}$. In fact, prior to the publication of [1] (in which more than 20 000 new APN instances over $\mathbb{F}_{2^8}$ are reported), the work from [19] was the largest known corpus of CCZ-inequivalent APN instances. Recently, more than 5 000 new CCZ-inequivalent APN functions were found using the same matrix method [18]. This shows that such a matrix representation is well-worth investigating.

The general matrix method from [19] was later specialized to the case of quadratic APN functions with prime field coefficients, i.e. with a univariate representation $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$ with $a_i \in \mathbb{F}_2$ for $i = 0, 1, 2, \ldots, 2^n - 1$ [17]. This additional assumption allowed additional dependencies among the elements of the corresponding matrix to be derived, which in turn reduced the search space sufficiently to allow a classification of all such functions for for $n \leq 9$. Two new APN functions were discovered over $\mathbb{F}_{2^9}$, and it was verified that the known APN instances over $\mathbb{F}_{2^n}$ with $n \leq 8$ cover all possible cases. In this way, the authors of [17] provided a complete classification of quadratic APN functions with prime field coefficients up to $n = 9$. For comparison, quadratic APN functions have only been classified up to $n = 7$ [10], [12], cubic APN functions up to $n = 6$ [12], and general APN functions only up to $n = 5$ [2]. In the case of quadratic planar functions, a classification of all commutative semifields of order 3^5 is given in [20]; based on the correspondence between commutative semifields and planar DO functions [6], this translates to a classification of all quadratic planar functions over $\mathbb{F}_{3^5}$. To the best of our knowledge, there are no known classifications of planar functions for $n > 5$.

We refer to [13] for a recent survey on APN and PN functions.

In this paper, we present a simpler formulation of the matrix representation from [19], and adapt the approach from [17] to the case of DO planar functions. We derive conditions on matrices corresponding to DO planar functions with prime field coefficients, and use this to find (up to CCZ-equivalence) all such planar functions over $\mathbb{F}_{3^n}$ for $n \leq 7$. We conclude that the known instances cover all possible cases. This is the first computational classification of planar functions of this sort for $n > 5$ to the best of our knowledge.

We note that a similar approach has been considered in [15] in terms of the ANF of the functions. Our approach (based on the univariate representation

rather than the ANF) has the advantage that it allows us to impose additional conditions on the derivative matrix when the coefficients of the function are from the prime field, and to thereby drastically reduce the search space as in [17].

2 Matrix representation of quadratic functions

Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be quadratic for a prime p and a positive integer n. Let $\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$ be a basis of $\mathbb{F}_{p^n}$ as a vector space over $\mathbb{F}_p$. For $a \in \mathbb{F}_{p^n}$, let $\Delta_a F(x) = F(a+x) - F(x) - F(a) = D_a F(x) - F(a)$. The definitions of PN and APN functions can be adapted to use $\Delta_a F$ instead of $D_a F$ since the difference between them is $F(a)$ (for a fixed $a \in \mathbb{F}_{p^n}$). The advantage of using $\Delta_a F$ over $D_a F$ is that, for quadratic F, $\Delta_a F$ is linear while $D_a F$ is merely affine.

Let us denote by $\mathrm{wt}(x)$ the Hamming weight of the coordinate vector of x with respect to the basis $\mathcal{B}$; in other words, if $x = \sum_{i=1}^{n} a_i b_i$ for $a_i \in \mathbb{F}_p$, then $\mathrm{wt}(x) = \#\{i \in \{1, 2, \ldots, n\} : a_i \neq 0\}$. Observe that knowledge of $\Delta_a F$ for all $a \in \mathbb{F}_{p^n}^*$ allows us to uniquely recover F up to EA-equivalence. Indeed, we can assume without loss of generality that $F(b) = 0$ for all $b \in \mathcal{B}$; then $\Delta_{b_i} F(b_i) = F(2b_i) - 2F(b_i)$, so that we also know $F(2b_i)$, and hence the values of F on all x with $\mathrm{wt}(x) = 1$. For any x of weight 2, i.e. $x = b_i + b_j$ for some $1 \leq i < j \leq n$, we consider the identity $\Delta_{b_i} F(b_j) = F(b_i + b_j) - F(b_i) - F(b_j)$. Since we know $\Delta_{b_i} F(b_j)$, and we have already recovered $F(b_i)$ and $F(b_j)$, we can now reconstruct the value of F on $x = b_i + b_j$. Continuing by induction, we can reconstruct all values of F in this way. More formally, we can state the following proposition. To simplify the exposition, we can assume without loss of generality that if $\mathrm{wt}(x) = k$, then $x = b_1 + b_2 + \cdots + b_k$. The proof is straightforward by induction, and is omitted due to space constraints.

Proposition 1. *Let $\{b_1, \ldots, b_n\}$ be a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Let F be a quadratic function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$. Then for any $x \in \mathbb{F}_{p^n}$ of weight k:*

$$F(x) = \Delta_{b_i} F\Big(\sum_{1 \leq j \leq k, j \neq i} b_j\Big) + F\Big(\sum_{1 \leq i \leq k, j \neq i} b_j\Big), \tag{1}$$

where $x = b_1 + \ldots + b_k$, for any $1 \leq i \leq k$.

If F is quadratic, then $\Delta_a F$ is linear, and so it suffices to know $\Delta_a F(b)$ for $b \in \mathcal{B}$ in order to know all values of $\Delta_a F$. Since $\Delta_a F(x)$ is symmetric in a and x, i.e. $\Delta_a F(x) = \Delta_x F(a)$ for any $a, x \in \mathbb{F}_{p^n}$, it suffices to know the values of Δ_b for $b \in \mathcal{B}$ in order to reconstruct $\Delta_a F$ for all $a \in \mathbb{F}_{p^n}$. In this way, knowledge of $\Delta_{b_i} F(b_j)$ for all $b_i, b_j \in \mathcal{B}$ is equivalent to knowledge of F up to EA-equivalence. This motivates the following definition.

Definition 1. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ for some prime p and some positive integer n. The **derivative matrix** of F is the matrix $M_F \in \mathbb{F}_{p^n}^{n \times n}$ given by*

$$M_F = \begin{bmatrix} \Delta_{b_1} F(b_1) & \Delta b_1 F(b_2) & \ldots & \Delta_{b_1} F(b_n) \\ \Delta_{b_2} F(b_1) & \Delta b_2 F(b_2) & \ldots & \Delta_{b_2} F(b_n) \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{b_n} F(b_1) & \Delta b_n F(b_2) & \ldots & \Delta_{b_n} F(b_n) \end{bmatrix}.$$

Clearly, we can obtain M_F from F by evaluating its derivatives on the basis elements. Conversely, given a matrix M_F corresponding to a quadratic (n,n)-function, we can reconstruct the coefficients of its univariate representation as shown in the following proposition. Thus, we can easily convert between the matrix and univariate representation of quadratic functions. The proof of the proposition is straightforward, and we omit it here due to space constraints.

Proposition 2. *Let $\{b_1,\ldots,b_n\}$ be a basis of $\mathbb{F}_p^n$. Let $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ be a DO polynomial, i.e. $F(x)=\sum_{1\le i,j\le n-1, i\le j} a_{ij}x^{p^{i-1}+p^{j-1}}$. Then*

$$M_F = B^T A B, \tag{2}$$

where $B=\begin{pmatrix} b_1^{p^0} & b_2^{p^0} & \ldots & b_n^{p^0} \\ b_1^{p^1} & b_2^{p^1} & \ldots & b_n^{p^1} \\ \vdots & \vdots & \ddots & \vdots \\ b_1^{p^{n-1}} & b_2^{p^{n-1}} & \ldots & b_n^{p^{n-1}} \end{pmatrix}$, $A=\begin{pmatrix} 2a_{11} & a_{12} & \ldots & a_{1n} \\ a_{12} & 2a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \ldots & 2a_{nn} \end{pmatrix}$ *and B^T is the transpose of B.*

We now consider how PN and APN functions can be characterized in terms of the derivative matrix M_F. Following [19], we define the rank of a vector $v\in\mathbb{F}_{p^n}^n$ to be the dimension of the subspace spanned by its elements. In other words, if $v=(v_1,v_2,\ldots,v_n)$ with $v_i\in\mathbb{F}_{p^n}$, the **rank** of v is $r(v)=\log_p\#\{a_1v_1+a_2v_2+\cdots+a_nv_n : a_1,a_2,\ldots,a_n\in\mathbb{F}_p\}$. We now have the following characterization.

Proposition 3. *Let F be an (n,n)-function and M_F be its derivative matrix. Then F is PN if and only if any non-zero linear combination of the rows of M_F has rank n.*

Proof. If F is not PN, then Δ_aF does not permute $\mathbb{F}_{p^n}$ for some $a\in\mathbb{F}_{p^n}^*$, and so there must be distinct $x,y\in\mathbb{F}_{p^n}$ such that $\Delta_aF(x)=\Delta_aF(y)$. Consequently, $\Delta_aF(x-y)=0$, and so $r(\Delta_aF(b_1),\Delta_aF(b_2),\ldots,\Delta_aF(b_n))<n$. By the preceding discussion, if $a=\sum_{i=1}^n a_ib_i$, then the vector $(\Delta_aF(b_1),\ldots,\Delta_aF(b_n))$ is actually the linear combination $\sum_{i=1}^n a_iR_i$, where R_i is the row of M_F corresponding to b_i.

Conversely, suppose that F is PN, and let $a\in\mathbb{F}_{p^n}^*$. Then the p^n linear combinations of $\Delta_aF(b_1),\ldots,\Delta_aF(b_n)$ are precisely the values of Δ_aF on the p^n elements of $\mathbb{F}_{p^n}$. Since Δ_aF is a permutation of $\mathbb{F}_{p^n}$, we have that all these linear combinations are distinct, and thus $(\Delta_aF(b_1),\ldots,\Delta_aF(b_n))$ has full rank.

In the case of APN functions over fields of even characteristic, we can give a similar characterization as follows. The proof resembles that of Proposition 3 3, using the fact that all derivatives of an APN (n,n)-function must take 2^{n-1} distinct values.

Proposition 4. *Let $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ for some positive integer n. Then M_F has only zeros on its main diagonal, and F is APN if and only any linear combination of the rows of M_F has rank $n-1$.*

Generalizing Propositions 3 and 4 to functions of higher differential uniformity is straightforward. Since our focus is exclusively on planar functions, we omit doing this here. In the case of differential uniformity equal to 2, Proposition 4 can be compared with Theorem 1 and Definition 5 of [19]. The condition on the rank of the linear combinations of rows of M_F is the same in both cases; the advantage of our approach is that the matrix M_F has a clear intuitive meaning (containing the values of the first-order derivatives of F on the basis elements), and is consequently easier to analyze and to construct from F in practice. Note that in the case of odd characteristic, the main diagonal of M_F is not necessarily zero since $\Delta_x F(x)$ is not equal to 0 in general.

In particular, from the interpretation of M_F in terms of the derivatives of F, we see that applying a linear permutation $L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ to all elements of M_F gives the derivative matrix of $L(F)$. Compare this with Theorem 3 of [19] which requires a non-trivial proof. We state this as an observation; in practice, we use it to restrict the number of matrices that we consider in our search.

Observation 1 *Let M_F be the derivative matrix of $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, and let $L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a linear function. Then the matrix M'_F defined by $(M'_F)_{i,j} = L((M_F)_{i,j})$ for all i, j is the derivative matrix of $L \circ F$. In particular, if L is a permutation, then M_F and M'_F correspond to EA-equivalent functions.*

3 Functions with prime field coefficients

As in [17], we now consider the case of quadratic functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ with prime field coefficients, i.e. with coefficients in the subfield $\mathbb{F}_p$. Since the Frobenius automorphism $x \mapsto x^p$ fixes $\mathbb{F}_p$, we have $F(x^p) = F(x)^p$ (and, more generally, $F(x^{p^k}) = F(x)^{p^k}$ for any non-negative integer k) for any such function. Consequently, we have $\Delta_{a^{p^k}} F(x^{p^k}) = (\Delta_a F(x))^{p^k}$ for any non-negative integer k. If we construct the matrix M_F corresponding to F with respect to a normal basis, i.e. with respect to a basis $\mathcal{B} = \{b, b^p, b^{p^2}, \ldots, b^{p^{n-1}}\}$ for some suitable $b \in \mathbb{F}_{p^n}^*$, then M_F will be such that $(M_F)_{i+1,j+1} = (M_F)_{i,j}^p$ for any $0 \leq i, j \leq n-1$; here we index the rows and columns from 0 to $n-1$, since $(M_F)_{i+1,j+1} = (M_F)_{i,j}^p$ is true if the indices i, j are considered modulo n; in other words, we have e.g. $(M_F)_{0,1} = (M_F)_{n-1,0}^p$.

This severely restricts the number of elements that we have to guess in order to completely determine M_F. For instance, the matrices M_F^6 and M_F^7 corresponding to a $(6,6)$- and $(7,7)$-function become

$$M_F^6 = \begin{bmatrix} A & B & C & D & C^{p^4} & B^{p^5} \\ B & A^p & B^p & C^p & D^p & C^{p^5} \\ C & B^p & A^{p^2} & B^{p^2} & C^{p^2} & D^{p^2} \\ D^{p^3} & C^p & B^{p^2} & A^{p^3} & B^{p^3} & C^{p^3} \\ C^{p^4} & D^{p^4} & C^{p^2} & B^{p^3} & A^{p^4} & B^{p^4} \\ B^{p^5} & C^{p^5} & D^{p^5} & C^{p^3} & B^{p^4} & A^{p^5} \end{bmatrix}, M_F^7 = \begin{bmatrix} A & B & C & D & D^{p^5} & C^{p^4} & B^{p^6} \\ B & A^p & B^p & C^p & D^p & D^{p^5} & C^{p^6} \\ C & B^p & A^{p^2} & B^{p^2} & C^{p^2} & D^{p^2} & D^{p^6} \\ D & C^p & B^{p^2} & A^{p^3} & B^{p^3} & C^{p^3} & D^{p^3} \\ D^{p^4} & D^p & C^{p^2} & B^{p^3} & A^{p^4} & B^{p^4} & C^{p^4} \\ C^{p^5} & D^{p^5} & D^{p^2} & C^{p^3} & B^{p^4} & A^{p^5} & B^{p^5} \\ B^{p^6} & C^{p^6} & D^{p^6} & D^{p^3} & C^{p^4} & B^{p^5} & A^{p^6} \end{bmatrix},$$

respectively, with $A, B, C, D \in \mathbb{F}_{p^6}$ for M_F^6, and $A, B, C, D \in \mathbb{F}_{p^7}$ for M_F^7. It is easy to see that in the case of even n, we have to guess $n/2+1$ values in order to specify M_F, while for odd n, we have to guess $(n+1)/2$ values. When n is even, we can restrict one of the values to the subfield $\mathbb{F}_{p^{n/2}}$: for instance, in M_F^6, we have $D = D^{p^3}$ due to the fact that M_F^6 is symmetric (since $\Delta_a F(x) = \Delta_x F(a)$), and so we must have $D \in \mathbb{F}_{p^3}$. This naturally generalizes to an arbitrary even dimension n.

Some further necessary conditions can be obtained by observing that the linear combinations of the rows of any submatrix of M_F must also have full rank. Following [19], we say that a matrix $S \in \mathbb{F}_{p^n}^{m \times k}$ is **proper** if any non-zero linear combination of the rows of S has rank k. Thus, M_F is proper if and only if it represents a PN function; and, clearly, if M_F is proper, then the same is true for any submatrix of M_F (since if some linear combination of the rows of a submatrix $S \in \mathbb{F}_p^{m \times k}$ of M_F spans a subspace of dimension less than k, then the same linear combination of the rows of the entire matrix M_F will have rank less than n since appending $n-k$ elements can increase the rank by at most $n-k$).

This submatrix condition is particularly valuable for submatrices that only depend on a subset of the variables needed to specify the matrix. For instance, the submatrix of M_F^6 on the rows with indices $\{0,1\}$ and the columns with indices $\{0,1,2,5\}$ depends on A, B, C, but not on D. Similarly, the submatrix with rows and columns with indices $\{0,1\}$ depends only on A and B. After guessing the value of e.g. A and B, we can check whether all submatrices that depend only on A and B are proper; if not, we can backtrack immediately, thus saving significant computation time.

In this paragraph, we will denote the matrix corresponding to the rows with indices R and columns with indices C by (R, C). For M_F^6, we use the submatrices corresponding to $(\{0,5\},\{0,5\})$, $(\{0,1\},\{0,1\})$ that depend only on A and B; and those corresponding to $\{(0,1,5\},\{0,1,5\})$, $(\{0,2,4\},\{0,2,4\})$, $(\{0,1\},\{0,1,2,5\})$, $(\{0,2\},\{0,1,2,4\})$, $(\{0,5\},\{0,1,4,5\})$, $(\{0,1,4\},\{0,2,5\})$ and $(\{0,1,2\},\{0,1,2\})$ depending only on A, B, C.

In the case of M_F^7, we use $(\{0,6\},\{0,6\})$ and $(\{0,1\},\{0,1\})$ that only depend on A, B, and $(\{0,1,6\},\{0,1,6\})$, $(\{0,5,6\},\{0,5,6\})$, $(\{0,1\},\{0,1,2,6\})$, $(\{0,6\},\{0,1,5,6\})$, $(\{0,1,2\},\{0,1,2\})$ that depend on A, B, C.

We note that the above lists do not exhaust all submatrices that only depend on a subset of values, but according to our empirical observations, verifying whether other submatrices are proper does not detect any contradictions beyond the ones obtained from the submatrices listed above. For dimensions n less than 6, the computation time is so short that we do not have to consider submatrix conditions of this form. As an example of how this improves the efficiency of the search, we note that for $n = 6$, conducting the search for one fixed value of A without the submatrix conditions takes around 7000 seconds as opposed to around 5500 seconds with the submatrix conditions.

4 Computational results

We run our searches on a server with 56 3.2 GHz cores and 500 GB of memory. We perform an exhaustive search over all possible matrices M_F corresponding to quadratic functions with prime field coefficients over $\mathbb{F}_{3^n}$ for $n \leq 7$. In order to facilitate the search, we use Observation 1 to restrict the value of one of the entries of M_F. However, while there is a linear permutation L such that $L(c) = c'$ for any two non-zero $c, c' \in \mathbb{F}_{p^n}$, the composition of such a permutation with a function having prime field coefficients is not necessarily going to have prime field coefficients, and so we cannot simply fix the value of the first variable in M_F to 1. However, we consider all linear permutations with prime field coefficients over $\mathbb{F}_{3^n}$, and use them to restrict the choice of the first variable, A, in M_F. More precisely, we define an equivalence relation $\sim$ on $\mathbb{F}_{p^n}^*$ with $a \sim b$ if there exists a linear permutation $L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ with prime field coefficients such that $L(a) = b$. The number of such linear permutations is sufficiently small for us to partition $\mathbb{F}_{3^n}^*$ into equivalence classes according to $\sim$ for all the dimensions that we consider. Since composing two functions with prime field coefficients gives a function that also has prime field coefficients, it then suffices to consider only one element from each class as the value of the first variable in M_F. For $n = 5$ and $n = 7$, we get 3 equivalence classes; for $n = 4$, we get 7; and for $n = 6$, we get 15.

In the case of $n = 4$, the search takes less than 2 seconds, and yields 24 functions. For $n = 5$, it takes about 17 seconds and yields 616 functions. For $n = 6$, we run 15 parallel processes, one for each equivalence class of the relation $\sim$ described in the previous paragraph; each process (with the submatrix conditions) takes around 5500 seconds (as pointed out above); in total, we get 2928 functions. Finally, in the case of $n = 7$, we conduct the search by running 22 processes in parallel on the server (each process handling all three equivalence classes under $\sim$), with each process handling 100 (out of $3^7 - 1$) possible values for B. Each of the 22 processes takes around 150 000 seconds to finish. Ultimately, we obtain 5093 functions.

The real bottleneck is classifying the functions under CCZ-equivalence. The code isomorphism test can take up to around 5 seconds for $n = 5$, around a minute for $n = 6$, and around an hour for $n = 7$. In order to speed up the classification for $n = 7$, we first compose each function F with all possible linear permutations L with prime field coefficients from the left ($L \circ F$) and from the right ($F \circ L$); if the composition belongs to the list of 5093 functions, we remove it from there. This takes around a day, and leaves us with about 2500 functions. There are around 1400 linear permutations with prime field coefficients over $\mathbb{F}_{3^7}$, so considering $L_1 \circ F \circ L_2$ for all pairs (L_1, L_2) is not feasible; instead, we take pairs of permutations (L_1, L_2) at random and remove $L_1 \circ F \circ L_2$ from the list (if it is in it). After several days of computations, we are able to cut down the number of functions to around 400. Running the code isomorphism test on 40 processes in parallel enables us to classify them. The computation takes about 3 months. The time for classifying the functions for $n < 7$ is negligible compared to the time for $n = 7$. However, we see that classification in higher dimensions

is practically impossible without a faster test, or an efficient invariant to help us distinguish between inequivalent functions.

We omit a list of the known CCZ-classes of planar functions since we see that all functions that we find are CCZ-equivalent to one of the known instances. We refer the reader to [13] for an excellent survey on planar functions which includes all known families and sporadic instances. The families referenced in the last column of Table 1 refer to the names used in [13].

We only find functions that are CCZ-equivalent to known ones. However, in the case of $n = 6$, we find representatives for the Zhou-Pott, the Dickson, and the Lunardon-Marino-Polverino-Trombetti-Bierbrauer (LMPTB) functions that are simpler than the known ones. Comparing with the representatives given in [3] and [14], we see that in the case of Zhou-Pott, our representative has 7 terms with prime field coefficients, while the one in [3] has 11 terms with various coefficients; for the Dickson case, our representative has 5 terms, as opposed to the 6 terms in [14] and the 7 terms in [3]; and for LMPTB, our representative has 5 terms while the one in [3] and [14] has 7 terms.

More importantly, we obtain a complete classification of all quadratic planar functions with prime field coefficients over $\mathbb{F}_{3^n}$ up to $n = 7$. A complete overview is given in Table 1.

Table 1. CCZ-representatives from all quadratic planar functions with prime field coefficients over $\mathbb{F}_{3^n}$ with $4 \leq n \leq 7$

n	F	Family
4	x^2	Finite field
	$x^{36} + 2x^{10} + 2x^4$	Dickson
5	x^2	Finite field
	x^4	Albert
	x^{10}	Albert
	$x^{10} + x^6 + 2x^2$	Coulter-Matthews-Ding-Yuan
	$x^{10} + 2x^6 + 2x^2$	Coulter-Matthews-Ding-Yuan
	$x^{90} + x^2$	sporadic
	$x^{162} + x^{108} - x^{84} + x^2$	sporadic
6	x^2	Finite field
	x^{10}	Albert
	$x^{162} + 2x^{108} + 2x^{90} + x^{82} + 2x^{10} + x^4 + x^2$	Zhou-Pott (*)
	$2x^{270} + 2x^{244} + x^{54} + x^{36} + x^{10} + x^2$	Dickson (*)
	$2x^{486} + x^{270} + 2x^{162} + x^{90} + x^2$	LMPTB (*)
7	x^2	Finite field
	x^4	Albert
	x^{10}	Albert
	x^{28}	Albert
	$x^{10} + x^6 + 2x^2$	Coulter-Matthews-Ding-Yuan
	$x^{10} + 2x^6 + 2x^2$	Coulter-Matthews-Ding-Yuan

References

1. Beierle C, Leander G. New instances of quadratic APN functions. arXiv preprint arXiv:2009.07204. 2020 Sep 15.
2. Brinkmann M, Leander G. On the classification of APN functions up to dimension five. Designs, Codes and Cryptography. 2008 Dec;49(1):273-88.
3. Budaghyan L, Calderini M, Carlet C, Coulter R, Villa I. On isotopic shift construction for planar functions. In2019 IEEE International Symposium on Information Theory (ISIT) 2019 Jul 7 (pp. 2962-2966). IEEE.
4. Budaghyan L, Helleseth T. New commutative semifields defined by new PN multinomials. Cryptography and communications. 2011 Mar;3(1):1-6.
5. Carlet C, Charpin P, Zinoviev V. Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes and Cryptography. 1998 Nov;15(2):125-56.
6. Coulter RS, Henderson M. Commutative presemifields and semifields. Advances in Mathematics. 2008 Jan 15;217(1):282-304.
7. Dickson LE. On commutative linear algebras in which division is always uniquely possible. Transactions of the American Mathematical Society. 1906 Oct 1;7(4):514-22.
8. Edel Y, Pott A. A new almost perfect nonlinear function which is not quadratic. Advances in Mathematics of Communications. 2009;3(1):59.
9. Edel Y, Pott A. On the equivalence of nonlinear functions. InEnhancing cryptographic primitives with techniques from error correcting codes 2009 (pp. 87-103). IOS Press.
10. Kalgin K, Idrisova V. The classification of quadratic APN functions in 7 variables. IACR Cryptol. ePrint Arch.. 2020;2020:1515.
11. Kyureghyan GM, Pott A. Some theorems on planar mappings. InInternational Workshop on the Arithmetic of Finite Fields 2008 Jul 6 (pp. 117-122). Springer, Berlin, Heidelberg.
12. Langevin P, Saygi E, Saygi Z. Classification of APN cubics in dimension 6 over GF(2). http://langevin.univ-tln.fr/project/apn-6/apn-6.html.
13. Pott A. Almost perfect and planar functions. Designs, Codes and Cryptography. 2016 Jan 1;78(1):141-95.
14. Pott A, Zhou Y. Switching construction of planar functions on finite fields. InInternational Workshop on the Arithmetic of Finite Fields 2010 Jun 27 (pp. 135-150). Springer, Berlin, Heidelberg.
15. Sălăgean A. Discrete antiderivatives for functions over $\mathbb{F}_p^n$. Designs, Codes and Cryptography. 2020 Mar;88(3):471-86.
16. Yoshiara S. Equivalences of quadratic APN functions. Journal of Algebraic Combinatorics. 2012 May;35(3):461-75.
17. Yu Y, Kaleyski N, Budaghyan L, Li Y. Classification of quadratic APN functions with coefficients in F2 for dimensions up to 9. Finite Fields and Their Applications. 2020 Dec 1;68:101733.
18. Yu Y, Perrin L. Constructing More Quadratic APN Functions with the QAM Method. IACR Cryptol. ePrint Arch. 2021 Sep 6;2021:574.
19. Yu Y, Wang M, Li Y. A matrix approach for constructing quadratic APN functions. Designs, codes and cryptography. 2014 Nov;73(2):587-600.
20. Weng G, Zeng X. Further results on planar DO functions and commutative semifields. Designs, Codes and Cryptography. 2012 Jun;63(3):413-23.
21. Zha Z, Kyureghyan GM, Wang X. Perfect nonlinear binomials and their semifields. Finite Fields and Their Applications. 2009 Apr 1;15(2):125-33.