ARITHMETIZATION-ORIENTED APN FUNCTIONS

LILYA BUDAGHYAN AND MOHIT PAL

Abstract. Recently, many cryptographic primitives such as homomorphic encryption (HE), multi-party computation (MPC) and zero-knowledge (ZK) protocols have been proposed in the literature which operate on prime field $\mathbb{F}_p$ for some large prime p. Primitives that are designed using such operations are called *arithmetization-oriented* primitives. As the concept of arithmetization-oriented primitives is new, a rigorous cryptanalysis of such primitives is yet to be done. In this paper, we investigate arithmetization-oriented APN functions. More precisely, we investigate APN permutations in the CCZ-classes of known families of APN power functions over prime field $\mathbb{F}_p$. Moreover, we present a new class of APN binomials over $\mathbb{F}_q$ obtained by modifying the planar function x^2 over $\mathbb{F}_q$. We also present a class of binomials having differential uniformity at most 5 defined via the quadratic character over finite fields of odd characteristic. We give sufficient conditions for which this family of binomials is permutation. Computationally it is confirmed that the latter family contains new APN functions for some small parameters. We conjecture it to contain an infinite subfamily of APN functions.

1. Introduction

Zero-knowledge (ZK) proof systems were introduced by Goldwasser et al. [13] in 1989. In this system, a prover P convinces a verifier V that a certain statement z is true while keeping some elements of a computation secret. With a ZK protocol, V can verify that the result of this computation is correct without even knowing some of the details of the computation, e.g., its intermediate values or any potentially secret inputs.

Cryptographic hash functions are often used as part of the ZK protocol, e.g., by compressing multiple public inputs to a single hash. Modern cryptographic hash functions such as SHA2, SHA3 and BLAKE are designed over finite fields of even characteristic, while ZK protocols often operate over prime field $\mathbb{F}_p$ for some large prime p. Therefore, efficient hash functions which are designed over $\mathbb{F}_p$, for some large prime p, were needed. In view of this, many cryptographic hash functions such as MiMCHash [1], Rescue-Prime [2, 24], Reinforced Concrete [3], Anemoi [5], Poseidon [14] and Grendel [23], to name a few, have been proposed in the literature which operate on prime field $\mathbb{F}_p$ for some large prime p. These cryptographic primitives are called *arithmetization-oriented* primitives. Except for Anemoi [5] and Grendel [23], all of these primitives use low-degree non-linear functions such as power maps. The non-linear function of Grendel [23] is defined via the Legendre symbol whereas Anemoi [5] is defined via the so-called *Flystel* structure. As the concept of arithmetization-oriented primitives is new, a rigorous cryptanalysis of such primitives is yet to be done.

One of the main design requirements of an arithmetization-oriented hash function is that it should be efficient in verification. Thus, in order for a function F to be arithmetization-oriented, it is necessary that verifying whether $y = F(x)$ can be done using few multiplications in a specific field. One way to achieve this is to use a function F such that $F(x)$ can be

2020 *Mathematics Subject Classification.* 12E20, 11T06, 94A06.

Key words and phrases. Finite fields, Arithmetization-oriented primitives, Differential uniformity, CCZ-equivalence.

evaluated using a small number of multiplications. Cryptographic hash functions MiMC-Hash [1] and Poseidon [14] work in this way, i.e., they use power map x^d, $d \in \{3, 5\}$ as a round function which can be evaluated easily. However, using a low degree round function may imply vulnerability to some algebraic attacks [9]. As a consequence, these algorithms have to use a high number of rounds. To overcome this, the designers of Rescue-Prime [2, 24] adopted a different strategy which was based on the fact that for a permutation F checking $y = F(x)$ is equivalent to checking $x = F^{-1}(y)$. The authors chose $\alpha \in \mathbb{F}_p$, where $\gcd(\alpha, p-1) = 1$, in such a way that the evaluation of x^α is efficient and its compositional inverse $x^{\frac{1}{\alpha}}$ has very high algebraic degree. It allows them to use x^α for evaluation and both x^α and $x^{\frac{1}{\alpha}}$ in their round function. As a consequence, much fewer rounds were needed to prevent algebraic attacks. The designers of Anemoi [5] observed that the idea of using a low degree permutation for the verification purpose (for cheap verification) and its compositional inverse (which is of high algebraic degree) as a round function can be generalised using the so-called CCZ-equivalence [10]. The idea was to use a low degree function for the verification and some permutation of high algebraic degree in its CCZ-class as a round function. In view of this, finding permutations with good cryptographic properties (including a high algebraic degree) that are CCZ-equivalent to functions with a low number of multiplications is an intriguing problem.

In this paper we shall focus on a cryptographic property of functions over finite fields called differential uniformity. Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer. We denote by $\mathbb{F}_q^*$ the multiplicative cyclic group of nonzero elements of the finite field $\mathbb{F}_q$. The ring of polynomials in indeterminate x over $\mathbb{F}_q$ is denoted by $\mathbb{F}_q[x]$. Let F be a function from the finite field $\mathbb{F}_q$ to itself. Using Lagrange's interpolation formula, F can be uniquely represented by a polynomial in $\mathbb{F}_q[x]$ of degree at most $q-1$. Therefore, throughout this paper we shall use the term function and polynomial for F, interchangeably. A polynomial $F(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial over $\mathbb{F}_q$ if the induced mapping $x \mapsto F(x)$ is a bijection of $\mathbb{F}_q$. A function F is called differentially δ-uniform if for every $a \in \mathbb{F}_q^*$ and every $b \in \mathbb{F}_q$, the equation $F(x+a) - F(x) = b$ admits at most δ solutions. When used as a substitution box in a block cipher, the differential uniformity of a function F quantifies its resistance against the differential attack (see [20]). Lower the differential uniformity, higher is the immunity of the function against differential attacks. The lowest possible differential uniformity of a function is 1 and in this case we say that the function is perfect nonlinear. Perfect nonlinear functions are commonly known as planar functions, and were first introduced by Dembowski and Ostrom [11] in connection to the study of projective planes. It is well-known that planar functions can never be a permutation. Therefore, the minimum differential uniformity that a permutation function can have over finite fields of odd characteristic is 2 and such functions are known as almost perfect nonlinear (APN). To the best of our knowledge, a systematic study of APN functions in odd characteristic starts with the seminal work of Helleseth, Rong and Sandberg [15], where the authors gave several infinite classes of APN power maps. These infinite classes of APN power functions were based on the computational results over fields of small orders popularly known as Helleseth-Rong-Sandberg (HRS) tables. The entries in the HRS tables which were not explained in the infinite class of families were the basis of investigation of many infinite families of APN power mappings in characteristic 3 and 5 (see [12, 16, 28, 29]). It is worth mentioning here that all the infinite families of APN power mappings obtained in [12, 16, 28, 29] are in the case of characteristic 3 or 5. Thus, over fields of characteristic $p \geq 7$, the only known infinite classes of APN power maps are due to Helleseth, Rong and Sandberg [15] (see Table 1).

In [5], the authors gave the following definition of arithmetization-oriented function in terms of CCZ-equivalence: *A subfunction is arithmetization-oriented if it is CCZ-equivalent to a function that can be verified efficiently.* In this paper, we shall study arithmetization-oriented APN functions, i.e., those APN functions over prime fields which are CCZ-equivalent to a function with a low number of multiplications. More precisely, we investigate APN permutations in the CCZ-classes of known families of APN power functions over prime field $\mathbb{F}_p$. Moreover, we present a new class of APN binomials over $\mathbb{F}_q$ obtained by modifying the planar function x^2 over $\mathbb{F}_q$. We also present a class of binomials having differential uniformity at most 5 defined via the quadratic character over finite fields of odd characteristic. Sufficient conditions for which this family of binomials is permutation have also been obtained. Computationally it is confirmed that the latter family contains new APN functions for some small parameters. We conjecture it to contain an infinite subfamily of APN functions

The paper is organised in the following way. In Section 2, we give a brief survey of APN functions over finite fields of odd characteristic. In Section 3, we study different equivalence relations over prime fields and investigate arithmetization-oriented functions in the CCZ-classes of known families of APN power maps. We present some new classes of APN functions and differentially low uniform functions over finite field $\mathbb{F}_q$, in Section 4. Finally, we summarize the paper with an open problem in Section 5.

2. Known classes of APN functions in odd characteristic

In the study of the differential uniformity of functions over finite fields, we often classify them with respect to some equivalence relations which preserve the differential uniformity of the functions. It is then sufficient to consider the differential uniformity of a single representative from each equivalence class. Two functions $F, G : \mathbb{F}_q \to \mathbb{F}_q$ are called linear (affine) equivalent if there exist linear (affine) permutations $A_1, A_2 : \mathbb{F}_q \to \mathbb{F}_q$ such that $G = A_2 \circ F \circ A_1$. We say that F and G are extended affine (EA) equivalent if there exist affine permutations $A_1, A_2 : \mathbb{F}_q \to \mathbb{F}_q$ and an affine function $A : \mathbb{F}_q \to \mathbb{F}_q$ such that $G = A_2 \circ F \circ A_1 + A$. The most general equivalence relation, known so far, which preserves the differential uniformity is the Carlet-Charpin-Zinoviev (CCZ) equivalence [10]. Two functions F and G are called CCZ-equivalent if there exists an affine permutation $\mathcal{A} : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q \times \mathbb{F}_q$ which maps the graph $\mathcal{G}_F := (x, F(x))$ to the graph $\mathcal{G}_G := (x, G(x))$. Thus, we can classify functions over finite fields in CCZ-equivalence classes and then each CCZ-equivalence class can be further classified into EA-equivalent classes. Thus, the CCZ-class of a function F always contains the EA-class of the function F. It is well-known [8] that if F is a permutation then CCZ-class also contains the EA-class of F^{-1}, the compositional inverse of the function F. This property of CCZ-equivalence motivated the designers of Anemoi [5] to use CCZ-equivalence in the design of arithmetization-oriented functions.

In this section, we give a brief survey of known classes of APN functions, upto CCZ-equivalence, over finite fields of odd characteristic. The simplest kind of functions over finite fields are the monomials x^d, where d is a positive integer. The Table 1 gives the known classes of APN power functions x^d over finite fields $\mathbb{F}_{p^n}$ of odd characteristic.

We say a class of APN functions F over $\mathbb{F}_{p^n}$ or an infinite family of APN functions if either it is APN over $\mathbb{F}_{p^n}$ for infinitely many values of n, or it is APN over $\mathbb{F}_{p^n}$ for infinitely many primes p. In arithmetization-oriented primitives we are mainly interested in functions which are APN for infinitely many primes p. One may note, from Table 1, that the infinite families of APN power maps $C_i, 1 \leq i \leq 6$, given by Helleseth, Rong and Sandberg [15], are the only families of APN power maps which are APN for infinitely many extensions n and infinitely many primes p.

	d	p	Conditions	Ref
C_1	3	$p \neq 3$		[15, Theorem 3]
C_2	p^n-2		$p^n \equiv 2 \pmod 3$	[15, Theorem 3]
C_3	$\frac{p^n-3}{2}$		$p \equiv 3,7 \pmod{20}$, $p^n>7, p^n \neq 27, n$ odd	[15, Theorem 3]
C_4	$\frac{p^n+1}{4}+\frac{p^n-1}{2}$		$p^n \equiv 3 \pmod 8$	[15, Theorem 4]
C_5	$\frac{p^n+1}{4}$		$p^n \equiv 7 \pmod 8$, $p^n>7$	[15, Theorem 4]
C_6	p^m+2		$p^m \equiv 1 \pmod 3, n=2m$	[15, Theorem 8]
C_7	p^n-3	$p=3$	$n>1$ is odd	[15, Theorem 7]
C_8	$\frac{3^{\frac{n+1}{2}}-1}{2}$	$p=3$	$n \equiv 3 \pmod 4$, $n>3$	[12, Theorem 2.1]
C_9	$\frac{3^{\frac{n+1}{2}}-1}{2}+\frac{3^n-1}{2}$	$p=3$	$n \equiv 1 \pmod 4$, $n>1$	[12, Theorem 2.1]
C_{10}	$\frac{3^{n+1}-1}{8}$	$p=3$	$n \equiv 3 \pmod 4$	[12, Theorem 2.2]
C_{11}	$\frac{3^{n+1}-1}{8}+\frac{3^n-1}{4}$	$p=3$	$n \equiv 1 \pmod 4$	[12, Theorem 2.2]
C_{12}	$\frac{3^{n+1}-1}{3^{\frac{n+1}{2^\ell}}+1}$	$p=3$	$n \equiv -1 \pmod{2^\ell}$	[16] [28, Theorem 4.1]
C_{13}	$\frac{5^k+1}{2}$	$p=5$	$\gcd(2n,k)=1$	[15, Corollary 1]
C_{14}	$\frac{5^n-1}{4}+\frac{5^{\frac{n+1}{2}}-1}{2}$	$p=5$	n odd	[12] [28, Theorem 4.5]
C_{15}	$\frac{5^{n+1}-1}{2(5^{\frac{n+1}{2^\ell}}+1)}+\frac{5^n-1}{4}$	$p=5$	$\ell \geq 2$, $n \equiv -1 \pmod{2^\ell}$	[28] [16, Theorem 1.9]

Table 1. Known classes of APN power maps x^d over $\mathbb{F}_{p^n}$, $p>2$.

Until 2007, only known classes of APN functions over finite fields of odd characteristic were power maps. The first infinite class of non-monomial APN functions was a class of APN binomials in characteristic 3 introduced by Ness and Helleseth [19]. More precisely, the authors showed that the binomials

$$F(x) = x^{p^n-2} + ux^{\frac{p^n-3}{2}} \in \mathbb{F}_{p^n}[x], \tag{2.1}$$

where $p=3$, $n \geq 3$ is odd and $u \in \mathbb{F}_{3^n}$ such that $\chi(u+1)=\chi(u-1)=\chi(u)$, is APN. Here, $\chi : \mathbb{F}_q \to \{0,1,-1\}$ is the quadratic character of the finite field $\mathbb{F}_q$ defined as follows:

$$\chi(a) = \begin{cases} 0 & \text{if } a=0; \\ 1 & \text{if } x^2=a \text{ has a solution } x \in \mathbb{F}_q; \\ -1 & \text{if } x^2=a \text{ has no solution } x \in \mathbb{F}_q. \end{cases}$$

The binomial F is known as Ness-Helleseth function. Later, Zeng et al. [26] showed that the Ness-Helleseth function F is APN for all $p^n \equiv 3 \pmod 4$, $p^n>7$ and $u \in \mathbb{F}_{p^n}$ satisfies either of the following conditions:

$$\begin{cases} \chi(u+1)=\chi(u-1)=-\chi(5u+3); \text{ or} \\ \chi(u+1)=\chi(u-1)=-\chi(5u-3). \end{cases}$$

The authors also showed that the Ness-Helleseth function is CCZ-inequivalent to all other known APN power functions when $p \geq 7$.

In 2014, by using the idea of some known construction methods of quadratic APN functions over finite fields of even characteristic [4, 7], Zha et al. [27] gave a general construction of APN polynomials of the form

$$F(x) = c_{30}x^3 + c_{03}x^{3q} + \sum_{i=0}^{2}\sum_{j=0}^{2} c_{ij}x^{i+qj} \in \mathbb{F}_{q^2}[x]. \tag{2.2}$$

After APN power maps C_1 and C_6 in Table 1, this was the third class of APN functions over finite field $\mathbb{F}_{p^n}$, with n even. The authors also showed that similar to C_1 and C_6 in Table 1, F is also not a permutation. Some non-monomial APN functions in odd characteristic constructed via switching method can be found in [25].

3. CCZ-equivalence and Arithmetization-oriented APN functions

In this section, we study EA-equivalence and CCZ-equivalence over prime fields. We know that over finite field $\mathbb{F}_p$, affine functions are of the form $ax + b$, $a \neq 0$ which are always permutations. Therefore, over prime fields, two functions F and G are EA-equivalent if and only if there exist affine functions $A_1 = a_1x + b_1$, $A_2 = a_2x + b_2$ and $A_3 = a_3x + b_3$ such that

$$G = (a_1x + b_1) \circ F(a_2x + b_2) + a_3x + b_3 = a_1F(a_2x + b_2) + a_3x + b_1 + b_3,$$

where $a_1, a_2 \in \mathbb{F}_p^*$. If $a_3 = 0 = b_3$ then F and G are called affine equivalent. If $a_3 = b_1 = b_2 = b_3 = 0$ then F and G are called linear equivalent.

We shall now recall the definition of CCZ-equivalence. Two functions F and G from $\mathbb{F}_{p^n}$ to itself are said to be CCZ-equivalent if there exists an affine permutation $\mathcal{A}$ of $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ such that

$$\mathcal{A}(\{(x, F(x)), x \in \mathbb{F}_{p^n}\}) = \{(x, G(x)), x \in \mathbb{F}_{p^n}\}. \tag{3.1}$$

Let $\mathcal{L}$ be the linear part of the affine permutation $\mathcal{A}$. Then [6, Lemma 3.1] shows that the affine permutation $\mathcal{A}$ simply adds constants to input and output of the CCZ-equivalent function obtained by applying $\mathcal{L}$. Thus CCZ-equivalent functions obtained by applying affine permutation $\mathcal{A}$ and linear permutation $\mathcal{L}$ are in the same affine class. Therefore, in what follows, we shall always consider $\mathcal{A}$ to be a linear function and shall denote it by $\mathcal{L}$. Recall that, any linear function $\mathcal{L} : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ can be described in the following way:

$$\mathcal{L} = \begin{bmatrix} L_1 & L_2 \\ L_3 & L_4 \end{bmatrix}, \tag{3.2}$$

where L_i are linear maps over $\mathbb{F}_{p^n}$ for $1 \leq i \leq 4$, and

$$\mathcal{L}(x, y) = \begin{bmatrix} L_1 & L_2 \\ L_3 & L_4 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = (L_1(x) + L_2(y), L_3(x) + L_4(y)).$$

In general, given a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and a linear permutation $\mathcal{L}$ of $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, there does not always exist a function G such that Equation (3.1) holds. Let F_1, F_2 be mappings from $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ defined as follows:

$$F_1(x) \mapsto L_1(x) + L_2(F(x)),$$
$$F_2(x) \mapsto L_3(x) + L_4(F(x)).$$

Then it is necessary for G to be well-defined that the mapping F_1 is a permutation. We can then define the function $G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ as

$$G = F_2 \circ F_1^{-1}(x) = L_3(F_1^{-1}(x)) + (L_4 \circ F)(F_1^{-1}(x)).$$

It is easy to observe that when $L_2 = 0$, then F_1 is a permutation if and only if the linear function L_1 is a permutation. Let L_1^{-1} be the compositional inverse of L_1 then L_1^{-1} is also linear and the function G is given by

$$G = (L_4 \circ F + L_3) \circ L_1^{-1} = L_4 \circ F \circ L_1^{-1} + L_3 \circ L_1^{-1}.$$

Thus, G is EA-equivalent to F. Also, one may note that when $L_1 = 0$ then F_1 is a permutation if and only if both L_2 and F are permutations of $\mathbb{F}_{p^n}$. Let L_2 and F are permutations of $\mathbb{F}_{p^n}$ and L_2^{-1} and F^{-1} are their compositional inverses, respectively. Then $F_1^{-1} = F^{-1} \circ L_2^{-1}$, where

L_2^{-1}, being the compositional inverse of a linear function, is a linear function. Therefore, G is given by

$$G = (L_4 \circ F + L_3) \circ (F^{-1} \circ L_2^{-1}) = L_4 \circ L_2^{-1} + L_3 \circ F^{-1} \circ L_2^{-1}.$$

Thus, G is EA-equivalent to F^{-1}. From here we see that CCZ-class of a function F always contains EA-class of F and EA-class of F^{-1} (if inverse exist).

Another important property of CCZ-equivalence is that it does not preserves the algebraic degree of the function. This was the motivation for the designers of Anemoi [5] to use CCZ-equivalence to construct arithmetization-oriented functions. Let G be a function with a low number of multiplications and it is CCZ-equivalent to a function F whose evaluation involves large number of multiplications than G, i.e., there exists linear function $\mathcal{L}$ such that $\mathcal{L}(\{(x, F(x)), x \in \mathbb{F}_{p^n}\}) = \{(x, G(x)), x \in \mathbb{F}_{p^n}\}$. Then verifying $y = F(x)$ is equivalent to verifying that $L_1(x) + L_2(y) = G(L_3(x) + L_4(y))$ which only involves linear functions and G. Arithmetization-oriented primitives designed in the recent years such as MiMCHash [1], Rescue–Prime [2, 24], Reinforced Concrete [3] and Poseidon [14] use low-degree non-linear functions as power maps $x \mapsto x^d$ with $d \in \{3, 5\}$. The non-linear function of Grendel [23] is defined as $x^d \cdot \chi(x)$, where χ is the quadratic character of the finite field $\mathbb{F}_p$ (the authors used the term Legendre symbol for quadratic characters over prime fields). The non-linear function of Anemoi [5] is defined via the flystel structure which is inspired from the butterfly structure [21] and a Feistel network. It gives a pair of functions called open flystel and closed flystel which are CCZ-equivalent to each other. The open flystel is a permutation whereas the closed flystel is not necessarily a permutation. In order to provide more choices for the non-linear functions of arithmetization-oriented primitives, we investigate functions over prime fields with following properties:

(i) Optimal differential uniformity,
(ii) Simple algebraic structure,
(iii) CCZ-equivalent to a permutation with high algebraic degree.

We call such functions *arithmetization-oriented APN functions*. In the remaining of this section, we investigate permutations in the CCZ-classes of known classes of APN power functions over prime field $\mathbb{F}_p$.

It is easy to observe that the linear maps over $\mathbb{F}_p$ are of the form $x \mapsto \alpha x$ for some $\alpha \in \mathbb{F}_p$. Therefore, any linear permutation $\mathcal{L} : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p \times \mathbb{F}_p$ can be represented as

$$\mathcal{L} = \begin{bmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{bmatrix},$$

where $\alpha_i \in \mathbb{F}_p$ for $1 \leq i \leq 4$ and $\alpha_1\alpha_4 - \alpha_3\alpha_2 \in \mathbb{F}_p^*$. Let $F(x) = x^d$, $d > 1$ be a power map over $\mathbb{F}_p$. Since the trivial cases $\alpha_1\alpha_2 = 0$ has already been considered, we shall always assume that $\alpha_1\alpha_2 \neq 0$. Notice that when $F(x) = x^d$ then $F_1(x) = \alpha_2 x^d + \alpha_1 x$ is a binomial. Also, if F_1 permutes $\mathbb{F}_p$ then so does $\alpha_2^{-1}F_1$. Therefore, without loss of generality, we may assume that $\alpha_2 = 1$. Thus, finding functions CCZ-equivalent to x^d but EA-inequivalent to both x^d and its inverse (if $x^{\frac{1}{d}}$ exists) over $\mathbb{F}_p$ is equivalent to finding permutation binomials of the form $x^d + ax \in \mathbb{F}_p[x]$ with $a \neq 0$. We now recall the following lemma concerning the non-existence of certain types of permutation binomials.

Lemma 3.1. [18, Theorem 1.3] *If $x^m + ax^n$ permutes the prime field $\mathbb{F}_p$, where $m > n > 0$ and $a \in \mathbb{F}_p^*$. Then* $\gcd(m - n, p - 1) > \sqrt{p} - 1$.

The following theorem gives a condition on the exponent d for which the CCZ-class of the power map x^d contains at most two EA-classes, namely, the EA-classes of x^d and the EA-class of its compositional inverse (if it exists).

Theorem 3.2. *Let $F(x) = x^d$, $1 < d < p$ be a power map over prime field $\mathbb{F}_p$. If $\gcd(d-1, p-1) \leq \sqrt{p}-1$ then for F, CCZ-equivalence class coincides with the EA-equivalence classes of F and F^{-1} (if F^{-1} exists).*

Proof. Result directly follow from the previous discussions and Lemma 3.1. □

We shall now use Theorem 3.2 to investigate permutations in the CCZ-classes of known classes of APN power maps over $\mathbb{F}_p$. We consider $p > 7$ to avoid some extra conditions in certain cases and the cases for $p = 3, 5, 7$ can be easily verified using SageMath [22]. The following table gives, up to CCZ-equivalence, the known classes of APN power maps over prime fields $\mathbb{F}_p,\ p > 7$.

	d	Conditions	Ref
D1	3	$p \neq 3$	[15, Theorem 3]
D2	$p-2$	$p \equiv 2 \pmod 3$	[15, Theorem 3]
D3	$\frac{p-3}{2}$	$p \equiv 3, 7 \pmod{20}$	[15, Theorem 3]
D4	$\frac{3p-1}{4}$	$p \equiv 3 \pmod 8$	[15, Theorem 4]
D5	$\frac{p+1}{4}$	$p \equiv 7 \pmod 8$	[15, Theorem 4]

Table 2. APN power maps x^d over $\mathbb{F}_p,\ p > 7$.

The following theorem shows that for all the APN power maps in Table 2, CCZ-equivalence class coincides with EA-equivalence class, if x^d is not a permutation; and contains exactly two EA-classes, namely, EA-class of x^d and EA-class of its compositional inverse, if x^d is a permutation.

Theorem 3.3. *Let $F(x) = x^d$ be an APN power map given in the Table 2. Then, the CCZ-class of x^d*

(i) coincides with the EA-class of x^d if $\gcd(d, p-1) > 1$,

(ii) consists of exactly two EA-classes, namely, EA-class of x^d and EA-class of $x^{\frac{1}{d}}$, if $\gcd(d, p-1) = 1$.

Proof. From Theorem 3.2, we know that if $\gcd(d-1, p-1) \leq \sqrt{p}-1$ then for the power map x^d, CCZ-equivalence class is consists of EA-equivalence class of x^d and EA-equivalence class of $x^{\frac{1}{d}}$, (if it exists). Now, we show that in all the five classes given in Table 2, $\gcd(d-1, p-1) \leq \sqrt{p}-1$.

Case 1. $d = 3$. In this case $\gcd(d-1, p-1) = \gcd(2, p-1) = 2 < \sqrt{p}-1$ for all $p > 7$.

Case 2. $d = p-2$ and $p \equiv 2 \pmod 3$. In this case

$$\gcd(d-1, p-1) = \gcd(p-3, p-1) = \gcd(2, p-1) = 2 < \sqrt{p}-1,$$

for all $p > 7$.

Case 3. $d = \dfrac{p-3}{2}$ and $p \equiv 3$ or $7 \pmod{20}$. It is easy to observe that since $p \equiv 3$ or $7 \pmod{20}$, we have $p \equiv 3 \pmod 4$ and hence $p-5 \equiv 2 \pmod 4$ and $p-1 \equiv 2 \pmod 4$ which further implies that $\gcd(p-5, p-1) = \gcd(4, p-1) = 2$. Therefore,

$$\gcd(d-1, p-1) = \gcd\left(\frac{p-5}{2}, p-1\right) = 1 < \sqrt{p}-1,$$

for all $p > 7$ and the second last equality holds as $\frac{p-5}{2}$ is odd.

Case 4. $d = \frac{3p-1}{4}$ and $p \equiv 3 \pmod 8$. Notice that, since $p \equiv 3 \pmod 8$, we have $p-1 \equiv 2 \pmod 8$ and $3p-5 \equiv 4 \pmod 8$. Hence, $\gcd(3p-5, p-1) = \gcd(2(p-2), p-1) = 2$. Therefore,

$$\gcd(d-1, p-1) = \gcd\left(\frac{3p-5}{4}, p-1\right) = 1 < \sqrt{p} - 1,$$

for all $p > 7$ and the second last equality holds as $\frac{3p-5}{4}$ is odd.

Case 5. $d = \frac{p+1}{4}$ and $p \equiv 7 \pmod 8$. One may note that, since $p \equiv 7 \pmod 8$, we have $p-1 \equiv 6 \pmod 8$ and $p-3 \equiv 4 \pmod 8$. Hence, $\gcd(p-3, p-1) = \gcd(2, p-1) = 2$. Therefore,

$$\gcd(d-1, p-1) = \gcd\left(\frac{p-3}{4}, p-1\right) = 1 < \sqrt{p} - 1,$$

for all $p > 7$ and the second last equality holds as $\frac{p-3}{4}$ is odd. □

A well-known strategy for finding APN permutations is to start with any non-permutation APN function and then finding a permutation in its CCZ-class. The following theorem gives a list of all APN permutations that can be obtained from the CCZ-classes of APN power maps given in Table 2.

Theorem 3.4. *Let $F(x) = x^d$ be an APN power map given in Table* (2) *and let G be a function CCZ-equivalent to F. Then G is a permutation if and only if $p \equiv 2 \pmod 3$ and either*

(i) G is affine equivalent to x^3; or
(ii) G is affine equivalent to $x^{\frac{2p-1}{3}}$; or
(iii) G is affine equivalent to x^{p-2}.

Proof. Let $\gcd(d, p-1) > 1$, where d is an exponent given in the Table 2. Then, from Theorem 3.3, CCZ-class of x^d is same as the EA-class of x^d. Let G be a function which is EA-equivalent to x^d then G will be of the form $G(x) = a'(ax+b)^d + b'x + c$, where $aa' \neq 0$. Also, notice that $G(x)$ is a permutation polynomial if and only if its multiplicatively equivalent polynomial $G'(x) = x^d + b''x$ is a permutation polynomial for some $b'' \in \mathbb{F}_p$. From Theorem 3.3, we have seen that for all the exponents d in Table 2, $\gcd(d-1, p-1) \leq \sqrt{p} - 1$ therefore, from Lemma 3.1, G' is never a permutation for any exponent d in Table 2. Thus, when $\gcd(d, p-1) > 1$ then there is no permutation function in the CCZ-classes of APN power maps given in the Table 2.

Let $\gcd(d, p-1) = 1$, where d is an exponent given in the Table 2. Then, from Theorem 3.3, CCZ-class consists of EA-classes of x^d and $x^{\frac{1}{d}}$. One may note that, in this case, any function that is affine equivalent to x^d or $x^{\frac{1}{d}}$ will also be a permutation. Also, it is easy to verify that if $p \equiv 1 \pmod 3$ then for all the exponents d in the Table 2, $\gcd(d, p-1) > 1$ and if $p \equiv 2 \pmod 3$ then $d \in \{3, p-2\}$ are the only exponents such that $\gcd(d, p-1) = 1$. Note that, the compositional inverse of x^3 is given by $x^{\frac{2p-1}{3}}$ and the function x^{p-2} is self-inverse. We now show that any function G that is EA-equivalent but not affine-equivalent to x^d, where $d \in \{3, \frac{2p-1}{3}, p-2\}$ is not a permutation. This is equivalent to show that for $d \in \{3, \frac{2p-1}{3}, p-2\}$, there is no permutation binomial $x^d + b''x$ with $b'' \neq 0$. From Lemma 3.1, $x^d + b''x$ is not a permutation for all $d \in \{3, \frac{2p-1}{3}, p-2\}$. This completes the proof. □

Remark 3.5. *Any APN permutation over prime field $\mathbb{F}_p$, $p > 7$, that is not affine equivalent to $x^3, x^{\frac{2p-1}{3}}$ or x^{p-2}, is CCZ-inequivalent to all the known APN power functions in odd characteristic.*

4. Some new APN and differentially low-uniform functions over $\mathbb{F}_q$

In this section, we present some new infinite classes of APN and differentially low-uniform binomials over finite fields of odd characteristic. In [19], Ness and Helleseth introduced a family of APN binomials

$$f(x) = x^{p^n-2} + ux^{\frac{p^n-3}{2}} \in \mathbb{F}_{p^n}[x], \tag{4.1}$$

where $p = 3$, $n \geq 3$ is odd and the element $u \in \mathbb{F}_{p^n}^*$ satisfies $\chi(u+1) = \chi(u-1) = \chi(u)$. Later, Zeng et al [26] showed that F is APN over $\mathbb{F}_{p^n}$, where $p^n \equiv 3 \pmod 4$, $p^n \geq 7$ and the element $u \in \mathbb{F}_{p^n}^*$ satisfies

$$\begin{cases} \chi(u+1) &= \chi(u-1) = -\chi(5u+3); \text{ or} \\ \chi(u+1) &= \chi(u-1) = -\chi(5u-3). \end{cases}$$

We performed computer search for all the APN binomials of the form $x^{d_2} + ux^{d_1}$ over prime field $\mathbb{F}_p$ for $5 \leq p \leq 97$. In the Table 3, we have listed all the values of $D = (d_2, d_1)$ for which binomial $x^{d_2} + ux^{d_1}$ is APN over prime field $\mathbb{F}_p$ for some $u \in \mathbb{F}_p^*$. Here, $D_1 = (3, 2)$, $D_2 = (p-1, 2)$, $D_3 = \left(p^n - 2, \frac{p^n-3}{2}\right)$, $D_4 = \left(\frac{p^n+3}{2}, 2\right)$ and $D = (d_2, d_1)$. We give necessary and sufficient conditions on $u \in \mathbb{F}_p^*$ for which binomials corresponding to D_1 and D_2 are APN in Remark 4.1 and Theorem 4.2, respectively. One may note that the class of APN binomials corresponding to D_3 is the generalised Ness-Helleseth function. For the class of binomials corresponding to D_4, we have proved in Theorem 4.4 that its differential uniformity is ≤ 5. We leave open the problem of explicitly finding conditions on u and p for which the binomial corresponding to D_4 is APN.

The first class of APN binomials, corresponding to D_1, is turned out to be EA-equivalent to x^3 as can be seen in the following remark.

Remark 4.1. *Let $p > 3$ be an odd prime. Then the binomial $F(x) = x^3 + ux^2$, $u \in \mathbb{F}_{p^n}^*$ is APN over $\mathbb{F}_{p^n}$.*

Proof. We know that the function x^3 is APN over $\mathbb{F}_{p^n}$ for all $p > 3$. Also, notice that

$$x^3 + ux^2 = \left(x + \frac{u}{3}\right)^3 - \frac{u^2 x}{3} - \frac{u^3}{27}.$$

Therefore, F is EA-equivalent to x^3 for all $u \in \mathbb{F}_{p^n}^*$ and hence is APN. □

The following theorem give necessary and sufficient conditions on $u \in \mathbb{F}_{p^n}^*$, p and n for which binomials corresponding to D_2 is APN over $\mathbb{F}_{p^n}$.

Theorem 4.2. *Let p be an odd prime and n be a positive integer. Then the binomial $F(x) = x^{p^n-1} + ux^2$, $u \in \mathbb{F}_{p^n}^*$ over $\mathbb{F}_{p^n}$ is APN if*

$$\begin{cases} \chi(u) = -1 \text{ and } p^n \equiv 1 \pmod 4; \text{ or} \\ \chi(u) = 1 \text{ and } p^n \equiv 3 \pmod 4, \end{cases}$$

and differentially 3-uniform, otherwise.

p	D_1	D_2	D_3	D_4	D
5	(3,2)	(4,2)	*	*	*
7	(3,2)	(6,2)	(5,2)	*	(6,3), (5,4), (6,4)
11	(3,2)	(10,2)	(9,4)	(7,2)	(8,3)
13	(3,2)	(12,2)	*	(8,2)	(10,2), (9,3), (7,4), (10,4), (8,5), (8,6), (10,6), (12,9)
17	(3,2)	(16,2)	(15,7)	(10,2)	(13,5), (14,6), (14, 10)
19	(3,2)	((18,2)	(17,8)	(11,2)	(12,3),(15,3),(10, 4),(13,4),(16,4),(14,5),(15,6),(10,7),(16,7), (16,10)
23	(3,2)	(22,2)	(21,10)	(13,2)	(14,3), (15,4), (16,5), (17,6), (18,7), (19, 8), (20,9)
29	(3,2)	(28,2)	*	(16,2)	(18,4), (24,10), (25,11), (26,12)
31	(3,2)	(30,2)	(29,14)	(17,2)	(19,4), (21,6), (22,7), (23,8), (24,9), (26,11), (28,13), (29,16)
37	(3,2)	(36,2)	*	*	(26,14), (32,14)
41	(3,2)	(40,2)	*	*	(34,14), (38,18)
43	(3,2)	(42,2)	(41,20)	*	(26,5), (33,12), (34,13), (36,15), (39,18)
47	(3,2)	(46,2)	(45,22)	*	(32,9), (39,16), (41,18)
53	(3,2)	(52,2)	*	(28,2)	(34,8), (38,12), (46,20),
59	(3,2)	(58,2)	(57,28)	*	*
61	(3,2)	(60,2)	*	*	(52,22)
67	(3,2)	(66,2)	(65, 32)	*	(46,13), (61,28)
71	(3,2)	(70,2)	(69,34)	*	*
73	(3,2)	(72,2)	*	*	*
79	(3,2)	(78,2)	(77,38)	*	*
83	(3,2)	(82,2)	(81,40)	*	*
89	(3,2)	(88,2)	*	*	(86,42)
97	(3,2)	(96,2)	*	*	*

Table 3. Exponents (d_2, d_1) for which $x^{d_2} + ux^{d_1}$ is APN over $\mathbb{F}_p$ for some $u \neq 0$.

Proof. Recall that the differential uniformity of F is given by the maximum number of solutions of the following equation

$$(x+a)^{p^n-1} + u(x+a)^2 - x^{p^n-1} - ux^2 = b \tag{4.2}$$

where $a, b \in \mathbb{F}_{p^n}$ and $a \neq 0$. We shall now consider three cases, namely, $x = 0$, $x = -a$ and $x \notin \{0, -a\}$.

Case 1. Let $x = 0$. In this case Equation (4.2) reduces to

$$1 + ua^2 = b.$$

Case 2. Let $x = -a$. In this case Equation (4.2) reduces to

$$-(1 + ua^2) = b.$$

Case 3. Let $x \notin \{0, -a\}$. In this case Equation (4.2) reduces to

$$(x+a)^2 - x^2 = bu^{-1} \implies x = \frac{b - ua^2}{2au}.$$

It is easy to observe that $x = 0$ and $x = -a$ both will be a solution of Equation (4.2) if and only if $b = 0$ and $a^2 = -\frac{1}{u}$. We know that

$$\chi(-1) = \begin{cases} -1 & \text{if } p^n \equiv 3 \pmod 4, \\ 1 & \text{if } p^n \equiv 1 \pmod 4, \end{cases}$$

and for any non-zero $u \in \mathbb{F}_{p^n}$, $\chi\left(\frac{1}{u}\right) = \chi(u)$. Thus, $x = 0, -a$ both will be a solution of Equation (4.2) if and only if $b = 0$, $1 + ua^2 = 0$ and

$$\begin{cases} \chi(u) = -1 \text{ and } p^n \equiv 3 \pmod 4; \text{ or} \\ \chi(u) = 1 \text{ and } p^n \equiv 1 \pmod 4. \end{cases}$$

This completes the proof. □

We now prove that the above family of APN binomials is CCZ-inequivalent to all the known APN functions over finite fields of odd characteristic. The following lemma will be used in proving inequivalence.

Lemma 4.3. [17, Theorem 7.4] *A polynomial $F(x) \in \mathbb{F}_{p^n}[x]$ is a permutation polynomial over $\mathbb{F}_{p^n}$ if and only if the following two conditions hold:*

(i) F has exactly one root in $\mathbb{F}_{p^n}$;
(ii) for each integer t with $1 \leq t \leq p^n - 2$ and $t \not\equiv 0 \pmod p$, the reduction of $F(x)^t \pmod{x^{p^n} - x}$ has degree $< p^n - 1$.

It is easy to observe that the APN binomial $F(x) = x^{p^n-1} + ux^2$ can never be a permutation. Recall that, in order to show that CCZ-equivalence is more general than EA-equivalence we need to show the existence of the permutations of the form

$$F_1 = L_1(F(x)) + L_2(x),$$

where L_1, L_2 are linearized polynomials over $\mathbb{F}_{p^n}$ and are not zero polynomials. From Lemma 4.3, we know that F_1 can never be a permutation as its degree is $p^n - 1$. Thus, for the APN binomial $F(x) = x^{p^n-1} + ux^2$, CCZ-equivalence coincides with the EA-equivalence. Since, EA-equivalence preserves the algebraic degree and there is no APN function whose algebraic degree is equal to the algebraic degree of $F(x)$, we conclude that $F(x)$ is CCZ-inequivalent to all the known classes of APN functions over finite finite fields of odd characteristic.

The following theorem shows that the binomial corresponding to D_3 has differential uniformity ≤ 5.

Theorem 4.4. *Let $p \equiv 3 \pmod 4$ be a prime number and n is an odd positive integer. Then the differential uniformity of the binomial $F(x) = x^{\frac{p^n+3}{2}} + ux^2$, $u \in \mathbb{F}_{p^n} \backslash \{0, 1, -1\}$ is less than or equal to 5.*

Proof. Recall that the differential uniformity of F is given by the maximum number of solutions of the following equation

$$\begin{aligned} & (x+a)^{\frac{p^n+3}{2}} + u(x+a)^2 - x^{\frac{p^n+3}{2}} - ux^2 = b \\ \implies & \chi(x+a)(x+a)^2 - \chi(x)x^2 + u((x+a)^2 - x^2) = b \\ \implies & (\chi(x+a) - \chi(x))x^2 + (u + \chi(x+a))(2ax + a^2) = b. \end{aligned} \tag{4.3}$$

where $a, b \in \mathbb{F}_{p^n}$, $a \neq 0$. We shall now consider three cases, namely, $x = 0$, $x = -a$ and $x \notin \{0, -a\}$.

Case 1. Let $x = 0$. In this case Equation (4.3) reduces to

$$(u + \chi(a))a^2 = b.$$

Case 2. Let $x = -a$. In this case Equation (4.3) reduces to

$$-(u - \chi(a))a^2 = b.$$

Case 3. Let $x \notin \{0, -a\}$. In this case $\chi(x+a), \chi(x) \in \{1, -1\}$ and we shall consider four subcases.

Subcase 3.1. Let $\chi(x+a) = 1 = \chi(x)$. In this case Equation (4.3) reduces to $(u+1)(2ax + a^2) = b$, which has a unique solution

$$x = \frac{b - (u+1)a^2}{2a(u+1)}.$$

Notice that this x will be a solution of Equation (4.3) if and only if

$$\chi\left(\frac{b - (u+1)a^2}{2a(u+1)}\right) = 1 = \chi\left(\frac{b + (u+1)a^2}{2a(u+1)}\right).$$

Subcase 3.2. Let $\chi(x+a) = -1 = \chi(x)$. In this case Equation (4.3) reduces to $(u-1)(2ax + a^2) = b$, which has a unique solution

$$x = \frac{b - (u-1)a^2}{2a(u-1)}.$$

This solution x will be a solution of Equation (4.3) if and only if

$$\chi\left(\frac{b - (u-1)a^2}{2a(u-1)}\right) = -1 = \chi\left(\frac{b + (u-1)a^2}{2a(u-1)}\right).$$

Subcase 3.3. Let $\chi(x+a) = -1$ and $\chi(x) = 1$. In this case Equation (4.3) reduces to

$$\begin{aligned} &-2x^2 + (u-1)(2ax + a^2) = b \\ \implies &x^2 - a(u-1)x + \frac{b - (u-1)a^2}{2} = 0. \end{aligned} \tag{4.4}$$

Let x_1, x_2 be the two solutions of Equation (4.4), then

$$x_1 x_2 = \frac{b - (u-1)a^2}{2}.$$

One may note that both x_1 and x_2 can be a solution of Equation (4.3) only if

$$\chi(x_1 x_2) = \chi\left(\frac{b - (u-1)a^2}{2}\right) = 1.$$

It is easy to observe that both $x_1 + a$ and $x_2 + a$ will be a solution of the equation

$$x^2 - a(u+1)x + \frac{b + (u+1)a^2}{2} = 0,$$

and hence

$$(x_1 + a)(x_2 + a) = \frac{b + (u+1)a^2}{2}.$$

Again, both x_1 and x_2 can be solution of Equation (4.3) only if

$$\chi((x_1 + a)(x_2 + a)) = \chi\left(\frac{b + (u+1)a^2}{2}\right) = 1.$$

From here we conclude that we can have

$$\begin{cases} \text{at most two solutions if} & \chi\left(\frac{b-(u-1)a^2}{2}\right) = 1 = \chi\left(\frac{b+(u+1)a^2}{2}\right), \\ \text{at most 1 solution} & \text{otherwise,} \end{cases}$$

of Equation (4.3) from this subcase.

Subcase 3.4. Let $\chi(x+a)=1$ and $\chi(x)=-1$. In this case Equation (4.3) reduces to

$$\begin{aligned} &2x^2+(u+1)(2ax+a^2)=b \\ \implies &x^2+a(u+1)x+\frac{-b+(u+1)a^2}{2}=0. \end{aligned} \tag{4.5}$$

Let x_1, x_2 be the two solutions of Equation (4.5), then

$$x_1x_2=\frac{-b+(u+1)a^2}{2}.$$

One may note that both x_1 and x_2 can be a solution of Equation (4.3) only if

$$\chi\left(\frac{b-(u+1)a^2}{2}\right)=-1.$$

It is easy to observe that x_1+a and x_2+a will be a solution of the equation

$$x^2+a(u-1)x+\frac{-b-(u-1)a^2}{2}=0,$$

and hence

$$(x_1+a)(x_2+a)=\frac{-b-(u-1)a^2}{2}.$$

Again, both x_1 and x_2 can be solution of Equation (4.3) only if

$$\chi\left(\frac{b+(u-1)a^2}{2}\right)=-1$$

From here we conclude that we can have

$$\begin{cases} \text{at most two solutions if} & \chi\left(\frac{b-(u+1)a^2}{2}\right)=-1=\chi\left(\frac{b+(u-1)a^2}{2}\right), \\ \text{at most 1 solution} & \text{otherwise,} \end{cases}$$

of Equation (4.3) from this subcase.

We shall now consider different possibilities for the number of solutions of Equation (4.3). Let $(u+\chi(a))a^2=b$. Then $x=0$ will be a solution of Equation (4.3) from Case 1. Notice that, in this case, $x=-a$ can not be a solution of Equation (4.3), as $u\neq 0$. Now consider the solution from Subcase 3.1 which is given by

$$x=\frac{(\chi(a)-1)a}{2(u+1)}=\begin{cases} 0 & \text{if } \chi(a)=1, \\ \frac{-a}{(u+1)} & \text{if } \chi(a)=-1. \end{cases}$$

Thus, we have a solution $x=-\dfrac{a}{u+1}$ of Equation (4.3) from the Subcase 3.1 if and only if $\chi(a)=-1$, $\chi(u+1)=1$ and $\chi(u)=-1$. Now consider the solution from the Subcase 3.2, which reduces to

$$x=\frac{(\chi(a)+1)a}{2(u-1)}=\begin{cases} \frac{a}{(u-1)} & \text{if } \chi(a)=1 \\ 0 & \text{if } \chi(a)=-1. \end{cases}$$

Thus, we have a solution $x=\dfrac{a}{u-1}$ of Equation (4.3) from the Subcase 3.2 if and only if $\chi(a)=1$, $\chi(u-1)=-1$ and $\chi(u)=1$. Now consider the solutions from Subcase 3.3, i.e, the solution of equation

$$x^2-a(u-1)x+\frac{(\chi(a)+1)a^2}{2}=0 \tag{4.6}$$

We shall now consider two different cases, namely, $\chi(a) = 1$ and $\chi(a) = -1$. Let $\chi(a) = 1$ then Equation (4.6) reduces to

$$x^2 - a(u-1)x + a^2 = 0$$

Let x_1, x_2 be the solutions of the above equation. Since $\chi(x_1x_2) = \chi(a^2) = 1$ therefore either both or none from x_1, x_2 will be a solution of Equation (4.3). It is easy to observe that $x_1 + a$ and $x_2 + a$ will be a solution of the equation

$$x^2 - a(u+1)x + (u+1)a^2 = 0.$$

Consider $\chi((x_1+a)(x_2+a)) = \chi((u+1)a^2) = \chi(u+1)$. From here, we conclude the following

$$\begin{cases} \text{at most two solutions if} & \chi(u+1) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\chi(a) = -1$ then we have only one solution $x = a(u-1)$ of Equation (4.6) as $x \neq 0$. Notice that $x = a(u-1)$ will also be a solution of Equation (4.3) if and only if $\chi(u-1) = -1$ and $\chi(u) = 1$. We shall now consider the solutions from Subcase 3.4 which, in this case, reduces to

$$x^2 + a(u+1)x + \frac{(1-\chi(a))a^2}{2} = 0. \tag{4.7}$$

Again, we shall consider two cases, namely, $\chi(a) = 1$ and $\chi(a) = -1$, respectively. Let $\chi(a) = 1$ then we have only one solution $x = -a(u+1)$ of Equation (4.7), as $x \neq 0$. It is easy to see that this solution will also be a solution of Equation (4.3) if and only if $\chi(u+1) = 1$ and $\chi(u) = -1$. Let $\chi(a) = -1$ then Equation (4.7) reduces to

$$x^2 + a(u+1)x + a^2 = 0.$$

Let x_1, x_2 be the solutions of the above equation. Since $\chi(x_1x_2) = \chi(a^2) = 1$ either both or none from x_1, x_2 will be a solution of Equation (4.3). It is easy to observe that $x_1 + a$ and $x_2 + a$ will be a solution of the equation

$$x^2 + a(u-1)x - (u-1)a^2 = 0.$$

Consider $\chi((x_1 + a)(x_2 + 1)) = \chi(-(u-1)a^2) = -\chi(u-1)$. From here, we conclude the following

$$\begin{cases} \text{at most two solutions if} & \chi(u-1) = -1, \\ 0 & \text{otherwise.} \end{cases}$$

We summarize the above discussion in the first two rows of Table 4.

Let $(\chi(a) - u)a^2 = b$. Then $x = -a$ will be a solution of Equation (4.3) from Case 2. We have already seen that $x = 0$ can not be a solution of Equation (4.3), as $u \neq 0$. Now consider the solution from Subcase 3.1 which is given by

$$x = \frac{(\chi(a) - 2u - 1)a}{2(u+1)} = \begin{cases} \frac{-ua}{(u+1)} & \text{if } \chi(a) = 1, \\ -a & \text{if } \chi(a) = -1. \end{cases}$$

Thus, we have a solution $x = -\dfrac{ua}{u+1}$ of Equation (4.3) from the Subcase 3.1 if and only if $\chi(a) = 1$, $\chi(u+1) = 1$ and $\chi(u) = -1$. Now consider the solution from the Subcase 3.2, which reduces to

$$x = \frac{(\chi(a) - 2u + 1)a}{2(u-1)} = \begin{cases} -a & \text{if } \chi(a) = 1 \\ \frac{-ua}{(u-1)} & \text{if } \chi(a) = -1. \end{cases}$$

Thus, we have a solution $x = \dfrac{-ua}{u-1}$ of Equation (4.3) from the Subcase 3.2 if and only if $\chi(a) = -1$, $\chi(u-1) = -1$ and $\chi(u) = 1$. Now consider the solutions from Subcase 3.3, i.e, the solution of equation

$$x^2 - a(u-1)x + \frac{(\chi(a) - 2u + 1)a^2}{2} = 0 \tag{4.8}$$

We shall now consider two different cases, namely, $\chi(a) = 1$ and $\chi(a) = -1$. Let $\chi(a) = 1$ then Equation (4.8) reduces to

$$x^2 - a(u-1)x - (u-1)a^2 = 0.$$

Let x_1, x_2 be the solutions of the above equation. Since $\chi(x_1x_2) = \chi(-(u-1)a^2) = -\chi(u-1)$, we infer the following

$$\begin{cases} \text{at most two solutions if} & \chi(u-1) = -1, \\ \text{at most one solutions if} & \chi(u-1) = 1, \end{cases}$$

of Equation (4.3). It is easy to observe that x_1+a and x_2+a will be a solution of the equation

$$x^2 - a(u+1)x + a^2 = 0.$$

Consider $\chi((x_1+a)(x_2+a)) = \chi(a^2) = 1$. Therefore, either both x_1, x_2 or none will be a solution of Equation (4.3). Let $\chi(a) = -1$ then Equation (4.8) reduces to

$$x^2 - a(u-1)x - ua^2 = 0.$$

Let x_1, x_2 be the solution of the above equation, then $x_1 + a, x_2 + a$ will be the solutions of the following equation

$$x^2 - a(u+1)x = 0.$$

Since $x_1, x_2 \neq -a$, $x \neq 0$ in the above solution. Therefore, we have $x_1 + a = a(u+1)$. One may note that this x_1 will be a solution of Equation (4.3) if and only if $\chi(a(u+1)) = -1 \implies \chi(u+1) = 1$ and $\chi(au) = 1 \implies \chi(u) = -1$. We shall now consider the solutions from Subcase 3.4 which, in this case, reduces to

$$x^2 + a(u+1)x + \frac{(-\chi(a) + 2u + 1)a^2}{2} = 0. \tag{4.9}$$

Again, we shall consider two cases, namely, $\chi(a) = 1$ and $\chi(a) = -1$, respectively. Let $\chi(a) = 1$ then Equation (4.9) reduces to

$$x^2 + a(u+1)x + ua^2 = 0.$$

Let x_1, x_2 be the solution of the above equation. Then $x_1 + a, x_2 + a$ will be the solution of the following equation

$$x^2 + a(u-1)x = 0.$$

Since $x_1, x_2 \neq -a$, we have only one solution $x_1 + a = -a(u-1)$. It is easy to see that x_1 is a solution of Equation (4.3) if and only if $\chi(-a(u-1)) = 1 \implies \chi(u-1) = -1$ and $\chi(-au) = -1 \implies \chi(u) = 1$. Let $\chi(a) = -1$ then Equation (4.9) reduces to

$$x^2 + a(u+1)x + (u+1)a^2 = 0.$$

Let x_1, x_2 be the solutions of the above equation. Since $\chi(x_1x_2) = \chi((u+1)a^2) = \chi(u+1)$, we have

$$\begin{cases} \text{at most two solutions if} & \chi(u+1) = 1, \\ \text{at most one solutions if} & \chi(u+1) = -1. \end{cases}$$

of Equation (4.3). It is easy to observe that x_1+a and x_2+a will be a solution of the equation

$$x^2 + a(u-1)x + a^2 = 0.$$

Since $\chi((x_1+a)(x_2+1)) = \chi(a^2) = 1$, either both or none from x_1, x_2 will be a solution of Equation (4.3). We summarize the above discussion in the third and fourth row of Table 4.

Let $\{(a,b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n} \mid b \neq \pm(u \pm 1)a^2\}$ then we do not have solutions from Case 1 and Case 2. Now suppose we have a solution from Subcase 3.1 then we have

$$\chi\left(\frac{b-(u+1)a^2}{2a(u+1)}\right) = 1 = \chi\left(\frac{b+(u+1)a^2}{2a(u+1)}\right). \tag{4.10}$$

If we have a solution from Subcase 3.2, then we have

$$\chi\left(\frac{b-(u-1)a^2}{2a(u-1)}\right) = -1 = \chi\left(\frac{b+(u-1)a^2}{2a(u-1)}\right). \tag{4.11}$$

We now show that for any fixed $(a,b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}$, if we have a solution from Subcase 3.1 and Subcase 3.2, simultaneously then we can not have at most 2 solutions from Subcase 3.3 and at most 2 solutions from Subcase 3.4, simultaneously. Assume that for any fixed $(a,b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}$, we have solutions from Subcase 3.1 and Subcase 3.2, simultaneously, i.e., both Equation (4.10) and Equation (4.11) hold. Now, we have at most two solution from the Subcase 3.3 only if

$$\begin{aligned}
&\chi\left(\frac{b-(u-1)a^2}{2}\right) = 1 = \chi\left(\frac{b+(u+1)a^2}{2}\right) \\
\implies &\chi\left(\frac{b-(u-1)a^2}{2a(u-1)}\right)\chi(a(u-1)) = 1 = \chi\left(\frac{b+(u+1)a^2}{2a(u+1)}\right)\chi(a(u+1)) \\
\implies &-\chi(a(u-1)) = 1 = \chi(a(u+1))
\end{aligned} \tag{4.12}$$

Similarly, we have at most two solution from the Subcase 3.4 only if

$$\begin{aligned}
&\chi\left(\frac{b-(u+1)a^2}{2}\right) = -1 = \chi\left(\frac{b+(u-1)a^2}{2}\right) \\
\implies &\chi\left(\frac{b-(u+1)a^2}{2a(u+1)}\right)\chi(a(u+1)) = -1 = \chi\left(\frac{b+(u-1)a^2}{2a(u-1)}\right)\chi(a(u-1)) \\
\implies &\chi(a(u+1)) = -1 = -\chi(a(u-1))
\end{aligned} \tag{4.13}$$

It is easy to observe that for any fixed u and a, Equation (4.12) and Equation (4.13) can not hold simultaneously. We summarize the above discussion in the last four rows of Table 4. □

(a,b)	$\chi(a)$	C1	C2	subcase 3.1	subcase 3.2	subcase 3.3	subcase 3.4
$(u+\chi(a))a^2=b$	1	1	0	0	$\begin{cases}1 \text{ if } \chi(u-1)=-1=\chi(-u),\\ 0 \text{ otherwise.}\end{cases}$	$\begin{cases}\text{at most 2 if } \chi(u+1)=1,\\ 0 \text{ otherwise.}\end{cases}$	$\begin{cases}1 \text{ if } \chi(u+1)=1=\chi(-u),\\ 0 \text{ otherwise.}\end{cases}$
$(u+\chi(a))a^2=b$	-1	1	0	$\begin{cases}1 \text{ if } \chi(u+1)=1=\chi(-u),\\ 0 \text{ otherwise.}\end{cases}$	0	$\begin{cases}1 \text{ if } \chi(u-1)=-1=\chi(-u),\\ 0 \text{ otherwise.}\end{cases}$	$\begin{cases}\text{at most 2 if } \chi(u-1)=-1,\\ 0 \text{ otherwise.}\end{cases}$
$-(u-\chi(a))a^2=b$	1	0	1	$\begin{cases}1 \text{ if } \chi(u+1)=1=\chi(-u),\\ 0 \text{ otherwise.}\end{cases}$	0	$\begin{cases}\text{at most 2 if } \chi(u-1)=-1,\\ 0 \text{ otherwise.}\end{cases}$	$\begin{cases}1 \text{ if } \chi(u-1)=-1=\chi(-u),\\ 0 \text{ otherwise.}\end{cases}$
$-(u-\chi(a))a^2=b$	-1	0	1	0	$\begin{cases}1 \text{ if } \chi(u-1)=-1=\chi(-u),\\ 0 \text{ otherwise.}\end{cases}$	$\begin{cases}1 \text{ if } \chi(u+1)=1=\chi(-u),\\ 0 \text{ otherwise.}\end{cases}$	$\begin{cases}\text{at most 2 if } \chi(u+1)=1,\\ 0 \text{ otherwise..}\end{cases}$
$\frac{b}{a^2}-\chi(a)\notin\{u,-u\}$	±1	0	0	1	1	1	at most 2
$\frac{b}{a^2}-\chi(a)\notin\{u,-u\}$	±1	0	0	1	1	at most 2	1
$\frac{b}{a^2}-\chi(a)\notin\{u,-u\}$	±1	0	0	1	0	at most 2	at most 2
$\frac{b}{a^2}-\chi(a)\notin\{u,-u\}$	±1	0	0	0	1	at most 2	at most 2

Table 4. Number of solutions from different cases and subcases related to Theorem 4.4.

Remark 4.5. *We have verified computationally over prime fields $\mathbb{F}_p$, $5 \leq p \leq 97$ that if the binomial $F(x) = x^{\frac{p^n+3}{2}} + ux^2$, $u \in \mathbb{F}_{p^n} \backslash \{0, 1, -1\}$ is APN then it is CCZ-inequivalent to all the known APN power functions and Ness-Helleseth binomials.*

Based on computational results over fields of small orders we propose the following conjecture.

Conjecture 4.6. *The family of binomials given in Theorem 4.4 contains an infinite subfamily of APN functions.*

The motivation behind the construction of differentially low-uniform permutations involving quadratic characters stems from the fact that such functions have been used in the nonlinear layers of some arithmetization-oriented hash functions such as Grendel [23]. The benefit of using quadratic characters is that it corresponds to a high-degree power map, i.e., $\chi(x) = x^{\frac{q-1}{2}}$, which significantly increase the algebraic degree of the function and there is an efficient algorithm for computing it which makes the evaluation easy. The following theorem give sufficient conditions on parameters u, p and n for which the family of binomials given in Theorem 4.4 is permutation.

Theorem 4.7. *Let $p^n \equiv 3 \pmod 4$ and $u \in \mathbb{F}_{p^n} \backslash \{0, 1, -1\}$ such that $\chi(u^2 - 1) = -1$ then the binomial $F(x) = x^{\frac{p^n+3}{2}} + ux^2 \in \mathbb{F}_{p^n}[x]$ is a permutation polynomial over $\mathbb{F}_{p^n}$.*

Proof. Notice that $F(x) = x^{\frac{p^n+3}{2}} + ux^2 = x^2(\chi(x) + u)$. Let $b \in \mathbb{F}_{p^n}$ such that $F(b) = b^2(\chi(b) + u) = 0$ then $b = 0$ as $u \in \mathbb{F}_{p^n} \backslash \{0, 1, -1\}$. Now, let $b, c \in \mathbb{F}_{p^n}^*$ such that $F(b) = F(c)$ then we have following three cases:

Case 1. $\chi(b) = \chi(c)$. In this case we have

$$F(b) = F(c) \implies b^2(\chi(b) + u) = c^2(\chi(c) + u) \implies b^2 = c^2 \implies b = \pm c.$$

Since $p^n \equiv 3 \pmod 4, \chi(-1) = -1$ and hence $\chi(c) \neq \chi(-c)$. Therefore, the only possibility is $b = c$.

Case 2. $\chi(b) = 1$ and $\chi(c) = -1$. In this case we have

$$F(b) = F(c) \implies b^2(\chi(b) + u) = c^2(\chi(c) + u) \implies \frac{b^2}{c^2} = \frac{u-1}{u+1}.$$

This is a contradiction as $\chi\left(\frac{u-1}{u+1}\right) = \chi((u-1)(u+1)^{-1}) = \chi((u-1)(u+1)) = \chi(u^2-1) = -1$, whereas $\chi\left(\frac{b^2}{c^2}\right) = 1$.

Case 3. $\chi(b) = -1$ and $\chi(c) = 1$. In this case we have

$$F(b) = F(c) \implies b^2(\chi(b) + u) = c^2(\chi(c) + u) \implies \frac{b^2}{c^2} = \frac{u+1}{u-1}.$$

Again, this is a contradiction as $\chi\left(\frac{u+1}{u-1}\right) = \chi((u+1)(u-1)^{-1}) = \chi(u^2-1) = -1$, whereas $\chi\left(\frac{b^2}{c^2}\right) = 1$. This completes the proof. □

5. Conclusion

In this paper, we investigated arithmetization-oriented APN functions. More precisely, we showed that for the known classes of APN power functions over prime fields CCZ-class is consists of EA-classes of APN power maps and their compositional inverses, if they exist. Moreover, we gave a new class of APN binomials over $\mathbb{F}_q$ obtained by modifying the planar

function x^2 over $\mathbb{F}_q$ and showed that it is CCZ-inequivalent to the known classes of APN functions in odd characteristic. We also gave a class of binomials having differential uniformity at most 5 defined via the quadratic character over finite fields of odd characteristic. Sufficient conditions for which this family of binomials is permutation have also been obtained. Experimental results suggest that these functions are new APN for certain values of u and p. We have conjectured that these binomials contain an infinite subfamily of APN functions. We leave open the problem of explicitly finding conditions on u and p for which the binomial corresponding to D_4 is APN. The APN cases corresponding to D in the last column of Table 3 correspond to new unclassified cases. We hope that this paper would attract researchers in discrete mathematics to construct new arithmetization-oriented APN functions.

Acknowledgements

The research of Lilya Budaghyan and Mohit Pal is supported by the Research Council of Norway under Grant No. 314395. The authors would also like to thank Christian Rechberger and Léo Perrin for some useful discussions.

References

[1] M. R. Albrech, L. Grassi, C. Rechberger, A. Roy, T. Tiessen, *MiMC: efficient encryption and cryptographic hashing with minimal multiplicative complexity*. In ASIACRYPT-2016, LNCS, 10031 (2016) 191–219.

[2] A. Aly, T. Ashur, E. Ben-Sasson, S. Dhooghe, A. Szepieniec, *Design of symmetric-key primitives for advanced cryptographic protocols*, IACR Trans. Symm. Cryptol., 2020(3) (2020) 1–45.

[3] M. Barbara, L. Grassi, D. Khovratovich, R. Lueftenegger, C. Rechberger, M. Schofnegger, R. Walch, *Reinforced concrete: Fast hash function for zero knowledge proofs and verifiable computation*, Cryptology ePrint Archive, Report 2021/1038, 2021. `https://eprint.iacr.org/2021/1038`.

[4] C. Bracken, E. Byrne, N. Markin, G. McGuire, *New families of quadratic almost perfect nonlinear trinomials and multinomials*, Finite Fields Appl. 14 (2008) 703–714.

[5] C. Bouvier, P. Briaud, P. Chaidos, L. Perrin, R. Salen, V. Velichkov, D. Willems, *New design techniques for efficient Arithmetization-oriented hash functions: Anemoi permutations and Jive compression mode*, IACR Cryptol. ePrint Arch. p. 840 (2022). `https://eprint.iacr.org/2022/840`

[6] L. Budaghyan, M. Calderini, I. Villa, *On relations between CCZ- and EA-equivalences*, Cryptogr. Commun. 12 (2020) 85–100.

[7] L. Budaghyan, C. Carlet, *Classes of quadratic APN trinomials and hexanomials and related structures*, IEEE Trans. Inf. Theory 54 (2008) 2354–2357.

[8] L. Budaghyan, C. Carlet, A. Pott *New classes of almost bent and almost perfect nonlinear polynomials*, IEEE Trans. Inf. Theory, 52(3) (2006) 1141–1152.

[9] A. Canteaut, T. Beyne, I. Dinur, M. Eichlseder, G. Leander, G. Leurent, M. Naya-Plasencia, L. Perrin, Y. Sasaki, Y. Todo, *Report on the security of stark-friendly hash functions (version 2.0)*, 2020. URL: `https://inria.hal.science/hal-02883253/`.

[10] C. Carlet, P. Charpin, V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems,* Des. Codes Cryptgr. 15 (1998) 125–156.

[11] P. Dembowski, T. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. 103 (1968) 239–258.

[12] H. Dobbertin, D. Mills, E. N. Muller, A. Pott, W. Willems, *APN functions in odd chatacteristic*, Discr. Math. 267 (2003) 95–112.

[13] S. Goldwasser, S. Micali, C. Rackoff, *The knowledge complexity of interactive proof systems*, SIAM Journal on Computing, 18(1) (1989) 186–208.

[14] L. Grassi, D. Khovratovich, C. Rechberger, A. Roy, M. Schofnegger, *Poseidon: a new hash function for zero-knowledge proof systems*. In USENIX Security 2021, USENIX Association, 2021.

[15] T. Helleseth, C. Rong, D. Sandberg, *New families of almost perfect nonlinear power functions*, IEEE Trans. Inf. Theory 45 (1999) 475–485.

[16] E. Leducq, *New families of APN functions in characteristic* 3 *or* 5, In: Arithmetic, Geometry, Cryptography and Coding Theory, Contemporary Mathematics, vol. 574, pp. 115–123. AMS (2012).

[17] R. Lidl, H. Niederreiter, *FiniteFields* (Ed. 2), Encycl. Math. Appl., vol.20, Cambridge Univ. Press, Cambridge (1997).

[18] A. M. Masuda, M. E. Zieve, *Permutation binomials over finite fields*, Trans. Am. Math. Soc. 361 (2009) 4169–4180.
[19] G. J. Ness, T. Helleseth, *A new family of ternary almost perfect nonlinear mappings*, IEEE Trans. Inf. Theory, 53 (2007) 2581–2586.
[20] K. Nyberg, *Differentially uniform mappings for cryptography*, In: T. Helleseth, (ed.) EUROCRYPT-1993. LNCS, 765 (1993) 55–64.
[21] L. Perrin, A. Udovenko, A. Biryukov, *Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem*, Lect. Notes Comput. Sci. 9815, 93–122 (2016).
[22] The Sage Developers, SageMath, the Sage Mathematics Software System (Version 9.5). `http://www.sagemath.org`
[23] A. Szepieniec, *On the use of the Legendre symbol in symmetric cipher design*, Cryptology ePrint Archive, Report 2021/984, 2021. `https://ia.cr/2021/984`.
[24] A. Szepieniec, T. Ashur, S. Dhooghe, *Rescue-prime: a standard specification (SoK)*, Cryptology ePrint Archive, Report 2020/1143, 2020. `https://eprint.iacr.org/2020/1143`.
[25] G. Xu, X. Cao, S. Xu, *Constructing new APN functions and bent functions over finite fields of odd characteristic via the switching method*, Cryptogr. Commun. 8 (2016) 155–171.
[26] X. Zeng, L. Hu, Y. Yang, W. Jiang, *On the inequivalence of Ness-Helleseth APN functions,* `https://eprint.iacr.org/2007/379`
[27] Z. Zha, L. Hu, S. Sun, Y. Sun, *New constructions of APN polynomial functions in odd characteristic*, Appl. Algebra Eng. Commun. Comput. 25 (2014) 249–263.
[28] Z. Zha, X. Wang, *Power functions with low uniformity on odd characteristic finite fields*, Sci. China Math. 53 (2010) 1931–1940.
[29] Z. Zha, X. Wang, *Almost perfect nonlinear power functions in odd characteristic*, IEEE Trans. Inf. Theory 57 (2011) 4826–4832.

Department of Informatics, University of Bergen, PB 7803, N-5020, Bergen, Norway
Email address: `lilya.budaghyan@uib.no`

Department of Informatics, University of Bergen, PB 7803, N-5020, Bergen, Norway
Email address: `mohit.pal@uib.no`