Ikonion Journal of Mathematics

https://dergipark.org.tr/tr/pub/ikjm

Research Article

Open Access

https://doi.org/ 10.54286/ikjm.1836416

ISSN: 2687-6531

On the Carlet's Bivariate APN Construction and Representations of Dobbertin Power Functions

İlksen Acunalp Erleblebici[1], **Ahmet Sınak**[2], **Oğuz Yayla**[1]

Keywords

APN functions, Bivariate APN construction, Dobbertin power function

Abstract — In this paper we present necessary and sufficient conditions on some families of bivariate and biprojective almost perfect nonlinear (APN) functions. In the first part, we follow the extended methods given by Calderini et al in 2021, and give necessary and sufficient conditions for Carlet's bivariate APN functions. We also give APN-ness conditions for biprojective functions in some special cases. In the second part, we study the representation of the Dobbertin power function following methods given by Budaghyan et al. in 2022 and give new representations for this kind of functions.

Subject Classification (2020): 94A60, 11T06.

1. Introduction

Vectorial boolean functions, which accept binary sequences of length n as input and produce binary sequences of length m as output (with n and m being positive integers), hold significant significance in the realm of cryptography within the field of computer science. The security and effectiveness of cryptographic systems are closely tied to the ability of these functions to withstand various types of cryptographic attacks. Moreover, they find wide-ranging utility in diverse domains, including sequence design, combinatorics, coding theory, and projective geometry. Indeed, differential uniformity and nonlinearity are two important cryptographic properties of functions. APN functions are the vectorial boolean functions with perfect differential uniformity.

Due to their great resilience to differential attacks and simple hardware implementation, APN power functions of the form $F(x) = x^d$ with low differential uniformity have been the subject of much research in recent years.

Vectorial Boolean functions are implemented in a cryptosystem as substitution boxes (S-boxes) in block ciphers in order to create confusion, and nonlinear combining or filtering functions in the pseudo-random generators of stream ciphers. S-boxes must be resistant to differential cryptanalysis [2]. Differential crypt-

[1]Institute of Applied Mathematics, Middle East Technical University, 06800, Çankaya, Ankara, Türkiye
[2]Department of Mathematics, Faculty of Science, Akdeniz University, 07070, Antalya, Türkiye
Article History: Received: 05.12.2025 - Accepted: 15.06.2026 - Published: 16.07.2026

Table 1. Known APN power functions x^d over $\mathbb{F}_2^n$.

Functions	Exponents d	Conditions	Degree	In
Gold	2^i+1	$\gcd(i,n)=1$	2	[16], [20]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	$i+1$	[17], [18]
Welch	2^t+3	$n=2t+1$	3	[13]
Niho	$2^t+2^{\frac{t}{2}}-1$, t even $2^t+2^{\frac{3t+1}{2}}-1$, t odd	$n=2t+1$	$\frac{t+2}{2}$ $t+1$	[14]
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$	[1], [20]
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$	$i+3$	[15]

analysis involves studying how variations in the input can influence the resulting differences in the output. Let F be any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, F is called differentially δ-uniform if the equation $D_aF(x) = F(x)+F(x+a) = b$ has at most δ solutions for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^m$. If x_1 is a solution of the equation then $x_1 + a$ is also a solution. So the smallest possible value of differential uniformity is 2, then there is a minimum limit of 2, as $\delta \geq 2$. The function's resistance to differential cryptanalysis depends on its differential uniformity being small. APN functions have $\delta = 2$ and they are resistant to differential cryptanalysis.

APN functions play a significant role in symmetric cryptography. These functions can be constructed using various methods, resulting in infinite families of APN functions. Since the 1990s, only a small number of infinite families of APN functions have been discovered. There are six known infinite families of APN monomials (or APN power functions), listed in Table 1, represented by $F(x) = x^d$ over $\mathbb{F}_{2^n}$, where d is a positive integer. The column "Degree" denotes the algebraic degree of the corresponding power function. There are also about fifteen known infinite families of quadratic APN polynomials; see [7]. This highlights the difficulty of constructing new APN functions.

Among the known APN functions, exceptional APN power functions occupy a prominent position due to their remarkable algebraic and cryptographic properties. For this reason, we study different representations of these functions. Such investigations may provide further insight into their algebraic structure and cryptographic behavior.

1.1. Contribution

The main contributions of this paper are twofold. First, we extend the APN conditions derived from Carlet's bivariate construction [8] and its generalizations for several subclasses of bivariate and biprojective functions. Second, we present new cyclotomic representations for the Dobbertin APN power function $F(x) = x^d$.

More precisely, our contributions include:

1. We generalize the necessary no-root conditions for the APN families F_1, F_2, and F_3 arising from the generic Carlet-type construction, as presented in [7]. This is achieved by extending the conditions on the divisibility of the exponents (Lemmas 3.6, 3.8, and 3.10).

2. For specific subclasses of F_1 and F_2, and a subclass of F_3, we provide new **no-root criteria, including necessary and sufficient conditions in some special cases** (Theorems 3.11 and others). These conditions relate the APN property to the non-existence of roots for specific linearized polynomials, which is a key approach in constructing and characterizing APN functions.

3. We apply similar arguments to the families of Biprojective APN functions (f_1, f_2, f_3, f_4) introduced in [7], deriving new necessary conditions for them to be APN for the special cases $i = 0$ and $i = 1$ (Corollaries 3.14 and related corollaries).

4. We demonstrate that the Dobbertin power function x^d over $\mathbb{F}_{2^{5i}}$ is cyclotomically equivalent to six new families of power functions, extending the known optimal representations from [4]. We provide six new representations for the exponent d and six new representations for its multiplicative inverse d^{-1} (Corollaries 4.2 and 4.4).

1.2. Outline

The remainder of this paper is organized as follows. Section 2 provides the necessary preliminaries and background on APN functions, APN power functions, and the equivalence relations used throughout the paper. In Section 3, we study APN functions arising from Carlet's bivariate construction. We first derive new no-root criteria and APN conditions for the families F_1, F_2, and F_3, and then extend the discussion to the families of biprojective APN functions. Section 4 is devoted to the Dobbertin APN power function, where we establish new cyclotomic representations for its exponent and its multiplicative inverse. Finally, Section 5 concludes the paper and discusses the significance of the obtained results and possible directions for future research.

2. Preliminaries

Let n be a positive integer. $\mathbb{F}_{2^n}$ denotes the finite field comprising 2^n elements, while $\mathbb{F}_{2^n}^*$ signifies the set containing its non-zero elements, forming its multiplicative group. A Boolean function, denoted as f, is a function that accepts a sequence of 0s and 1s as input and produces either 0 or 1 as output. Furthermore, a vectorial Boolean function represents an extension of traditional Boolean functions. The functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ are called vectorial Boolean function or (n, m)-functions. Given such a function F, the Boolean functions $f_1, \ldots, f_m$ such that

$$F(x) = F(x_1, \ldots, x_n) = (f_1(x), \ldots, f_m(x))$$

are referred to as F's coordinate functions. The component functions of F are the linear combinations of these coordinate functions with non-zero coefficients. When the values of m and n are left unspecified, functions labeled as (n, m)-functions are commonly known as vectorial Boolean functions or S-boxes. These S-boxes serve as the nonlinear components in block ciphers, as described in reference [12].

2.1. Representations of Vectorial Boolean Functions

The algebraic normal form (ANF) of any (n, m)-function F is represented as:

$$\sum_{I \subseteq \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i\right); a_I \in \mathbb{F}_2^m.$$

It satisfies the relations $a_I = \sum_{x \in \mathbb{F}_2^n | supp(x) \subseteq I} F(x)$ and $F(x) = \sum_{I \subseteq supp(x)} a_I$, where $supp(x) = \{i \in \{1, \ldots, n\} \mid x_i = 1\}$.

Indeed, the algebraic degree of a function, as defined, is a crucial measure of its complexity in terms of the ANF. Specifically, it represents the highest degree of monomials (terms) with nonzero coefficients in the

ANF.

When the dimensions of the input and output spaces of a vectorial Boolean function are equal (i.e., $m = n$), a second representation known as the univariate representation can be employed. In this representation, every vectorial Boolean function F can be distinctly represented as a polynomial in the polynomial ring over the field with 2^n elements, denoted as $\mathbb{F}_{2^n}[X]$ using Lagrange interpolation. The polynomial's degree is at most $2^n - 1$, and it is represented as:

$$F(X) = \sum_{0 \le i < 2^n} A_i X^i,\ A_i \in \mathbb{F}_{2^n}.$$

The polynomial $F(X)$ captures the behavior of the vectorial Boolean function F over the binary vector X. When we assume that $n = 2m$, it implies that the dimension of the input space is twice the dimension of the output space. In this context, it's possible to identify the finite field $\mathbb{F}_{2^n}$ with the direct product of $\mathbb{F}_{2^m}$ and itself, i.e., $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

A linear map $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is an $\mathbb{F}_2$-linear vector space endomorphism of $\mathbb{F}_{2^n}$. The univariate representation of a linear map L takes the form:

$$L(X) = \sum_{0 \le i < n} B_i X^{2^i},\ B_i \in \mathbb{F}_{2^n}.$$

This representation is known as a linearized polynomial, and its algebraic degree is at most one.

An affine map $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined as $A(X) = L(X) + C$ where L is linear map and $C \in \mathbb{F}_{2^n}$ is a constant. Affine maps combine linear transformations with translations.

Quadratic functions are a subset of (n, m)-functions with an algebraic degree at most 2. If L is a linear map, and $C \in \mathbb{F}_{2^n}$ is a constant, then they can be represented as:

$$Q(X) = \sum_{0 \le i \ne j < n} A_{i,j} X^{2^i + 2^j} + L(X) + C, A_{i,j} \in \mathbb{F}_{2^n}.$$

where L is linear map and $C \in \mathbb{F}_{2^n}$ is a constant. Quadratic functions encompass more complex transformations compared to linear or affine functions.

For $m \mid n$, define the trace function $\mathrm{Tr}_n^m = \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ as $\mathrm{Tr}_n^m(x) = \sum_{i=0}^{n/m-1} x^{2^{mi}}$. If $m = 1$, Tr_n^1 is denoted by Tr_n.

2.2. Differential Uniformity and Nonlinearity of Vectorial Boolean Functions

Derivative of a function F, denoted as $D_a F$, is a mathematical tool used to explain how a change in the input of a (n, n)-function F affects the resulting difference in the output. It helps analyze the relationship between differences in inputs and their corresponding differences in outputs. $D_a F(x) = F(x + a) + F(x)$ is the definition of the derivative of a function F.

The "differential uniformity" Δ_F of a (n, n)-function F is defined as the maximum number of solutions $x \in \mathbb{F}_{2^n}$ to the equation $F(x) + F(x + a) = b$, where both a and b are elements of the finite field $\mathbb{F}_{2^n}$, and $a \neq 0$,

$$\Delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^m}} |\{x \in \mathbb{F}_{2^n} : F(a + x) + F(x) = b\}|.$$

If x_1 is a solution of the equation $F(a + x) + F(x) = b$, then $x_1 + a$ is also a solution. Therefore, Δ_F is always

even and hence satisfies $\Delta_F \geq 2$. Indeed, APN functions are a class of (n,n)-functions where $\Delta_F = 2$. The parameter Δ_F represents the maximum differential uniformity of the function, and when it equals 2, it signifies that the function has optimal resistance to differential cryptanalysis.

A quadratic function F is APN if and only if the following equation holds for every $A \in \mathbb{F}_{2^n}^*$ and the equation has exactly two solutions:

$$F(X+A)+F(X)+F(A)+F(0)=0.$$

The Walsh transform is a useful tool for examining any (n,m)-function F. The Walsh transform of $F:\mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$ is defined as

$$W_F(a,b)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_m(bF(x))+\mathrm{Tr}_n(ax)}$$

for $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}$. The nonlinearity of an (n,m)-function F can be expressed using the formula:

$$2^{n-1}-\frac{1}{2}max_{a\in\mathbb{F}_{2^n}^*,b\in\mathbb{F}_{2^m}}|W_F(a,b)|.$$

For (n,n)-functions, the nonlinearity is limited from above by $2^{n-1}-2^{\frac{n-1}{2}}$ [11]. Functions achieving this upper bound are known as *almost bent* (AB) functions.

AB functions are a subset of (n,n)-functions that attain the highest possible nonlinearity for odd values of n. They provide the highest resistance to linear cryptanalysis. AB functions provide formidable resilience against differential and linear cryptanalysis. AB functions have specific constraints, such as challenges in combining them with vectorial functions to achieve high algebraic degrees.

Bent functions are defined for even values of n and have nonlinearity equal to $2^{n-1}-2^{\frac{n}{2}}$. They are conjectured to have the highest possible nonlinearity for even values of n. Bent functions are highly resistant to various cryptanalysis techniques.

2.3. Equivalence Relations on Vectorial Boolean Functions

In the study and classification of APN and AB functions in the literature, various equivalence relations are used to group functions that exhibit similar cryptographic properties. Two commonly used equivalence relations are CCZ-equivalence and EA-equivalence. Both CCZ-equivalence and EA-equivalence are valuable tools in the analysis and classification of cryptographic functions. They help researchers identify functions that can be used interchangeably in cryptographic algorithms while preserving desired security properties, such as resistance to differential attacks and nonlinearity. These equivalence relations simplify the study of function classes and aid in the design and evaluation of secure cryptographic systems. But for several significant families of functions, the two equivalence relations coincide. Most notably, two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent [22]. Due to this fact, EA-equivalence may be simpler to use in some situations. In the context of power functions, particularly in finite fields, it is indeed the case that CCZ-equivalence and cyclotomic equivalence are equivalent [23]. This is a notable property when dealing with power functions, and it simplifies the classification and analysis of such functions.

2.3.1. EA-equivalence

Two functions $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $A_1 \circ F \circ A_2$, where $A_1, A_2 = \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine permutations, are called affine equivalent if they can be transformed into each other through a composition of affine permutations. This means that they exhibit similar properties under affine transformations.

Two functions F and F', where F' is defined as $F' = A_1 \circ F \circ A_2 + A$, and A is an affine function, are called extended affine (EA)-equivalent if they can be transformed into each other through an affine transformation involving an additional affine function A. In other words, they are equivalent under a more general class of transformations that include both affine permutations and an additional affine term.

Notably, if the original function F is not affine, then the functions F and F' (related through EA equivalence) have the same algebraic degree. This means that their algebraic properties remain unchanged even after the additional affine transformation.

2.3.2. CCZ-equivalence

Two functions $F, F' = \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called Carlet-Charpin-Zinoviev equivalent, CCZ-equivalent, if their respective graphs, denoted as G_F and $G_{F'}$, are affine equivalent where $G_F = \{(x, F(x)) \mid x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) \mid x \in \mathbb{F}_{2^n}\}$. In other words, they exhibit similar properties under affine transformations of their input-output pairs.

CCZ-equivalence implies the existence of an affine automorphism $\mathscr{L} = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that for any pair (x, y) in the graph G_F such that $y = F(x)$, the corresponding pair in the graph $G_{F'}$ satisfies $L_2(x, y) = F'(L_1(x, y))$. Because $\mathscr{L}$ is an affine automorphism and thus a permutation, the function $L_1(x, F(x))$ must also be a permutation [5]. This means that it bijectively maps elements of $\mathbb{F}_{2^n}$ to itself.

CCZ-equivalence is more general than EA-equivalence [6]. While EA-equivalence considers transformations that involve affine permutations and an additional affine term, CCZ-equivalence encompasses a broader set of affine transformations that align the graphs of two functions under an affine automorphism. Importantly, any permutation is CCZ-equivalent to its inverse [10], highlighting the generality and flexibility of CCZ-equivalence in capturing the properties of cryptographic functions.

2.3.3. Cyclotomic equivalence

Cyclotomic equivalence is used to classify two power functions $F(x) = x^d$ and $G(x) = x^e$ over $\mathbb{F}_{2^n}$ based on their exponents d and e, where d,e and n are positive integers. Two power functions are considered cyclotomically equivalent if specific conditions related to their exponents are met. Two power functions $F(x) = x^d$ and $G(x) = x^e$ over $\mathbb{F}_{2^n}$ are considered cyclotomically equivalent if one of the following conditions is satisfied:

- $d \equiv 2^k e \mod (2^n - 1)$ for some integer k or
- $d^{-1} \equiv 2^k e \mod (2^n - 1)$ for some positive integer k if $\gcd(d, 2^n - 1) = 1$, where d^{-1} represents the multiplicative inverse of d modulo $2^n - 1$.

Cyclotomic equivalence offers the advantage of being easier to test than both extended affine (EA) and Carlet-Charpin-Zinoviev (CCZ) equivalence, which involve more complex transformations and conditions.

2.4. APN Power Functions

Power functions were the first discovered APN functions since if we take $F(x) = x^d$, power function, then F is APN if and only if the derivative D_1F is a two-to-one mapping i.e. for any $a \neq 0$

$$D_aF(x) = (x+a)^d + x^d = a^d D_1F(x/a)$$

then D_aF is two to one mapping if and only if D_1F is two-to-one. As mentioned before there are six known infinite families of APN monomials presented in Table 1.

The conjecture by Dobbertin [15] that the classification of monomial APN functions is comprehensive up to CCZ-equivalence suggests that any monomial APN function can be transformed, through CCZ-equivalence, into an instance belonging to one of the families of functions listed in Table 1.

The power APN functions play an important role through the known APN functions. The Gold, Kasami, Welch, and Niho APN power functions are well-known in the field of cryptography for their cryptographic properties. These functions exhibit a special property related to their classical Walsh spectrum, depending on whether n is odd or even: These functions are considered as AB, which stands for almost bent functions when n is odd. AB functions are a subset of APN functions and have the highest possible nonlinearity for odd values of n. In this case, the functions are known to have optimal resistance to differential cryptanalysis. For even values of n, the Walsh coefficients of these functions take values from the set $\{0, \pm 2^{n/2}, \pm 2^{n+2/2}\}$ in their classical Walsh spectrum. Even though they are not strictly AB for even n, they still exhibit strong cryptographic properties and provide resistance to certain types of cryptanalysis. The inverse function is differentially 4-uniform for even values of n, whereas it is APN for odd values of n. Since the algebraic degree of any AB function cannot exceed $(n+1)/2$, the inverse APN function, which has algebraic degree $n-1$, is not an AB function [10]. The inverse function's Walsh spectrum was determined in [19] by Lachaud and Wolfmann. The inverse function has the best known nonlinearity for n even since it contains all integers with $t = 0 \mod (4)$ in the range $-2^{n/2+1}, \ldots, 2^{n/2+1}$ if n is even.

Canteaut and Dobbertin independently discovered the final instance of APN power functions in 1999, and Dobbertin proved it in 2000 [15]. The nonlinearity and Walsh spectrum of the Dobbertin family of power functions remained undisclosed until certain observations and computational data were gathered concerning the differential spectrum of power functions denoted as x^d. These power functions have exponents of the form $d = \sum_{i=1}^{k-1} 2^{ni} - 1$ over the field $\mathbb{F}_2^{nk}$. It is worth noting that the exponents of both the inverse and the Dobbertin family fall under this specific form, and this data is presented in [4].

The known infinite families of non-power APN functions are surveyed in [12]. APN polynomials, which are CCZ-inequivalent to monomials, are all quadratic at this time. In dimension 6, there is just one known instance of an APN function that is neither quadratic nor power:

$$x^3 + a^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + \mathrm{Tr}_2(x^{21}) + \mathrm{Tr}_3(a^{18}x^9) + a^{14}\mathrm{Tr}_6(a^{52}x^3 + a^6x^5 + a^{19}x^7 + a^{28}x^{11} + a^2x^{13}).$$

For further information on APN function constructions, take a look at [3, 7, 8].

3. APN Functions Specific to Carlet's Bivariate APN Construction

Let $n = 2m$ and define $F : (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \longrightarrow (B(x, y), G(x, y)) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. In [9], Carlet considered the simplest Maiorana-McFarland function $B(x, y) = xy$ and gave three conditions for F to be APN:

i. The function $x \to G(x, y)$ is APN for any fixed y.

ii. The function $y \to G(x, y)$ is APN for any fixed x.

iii. The function $G(x, bx + c)$ is APN for any b and c.

Since G is quadratic, it can be assumed that $c = 0$. Then the following APN class is revealed.

Theorem 3.1 (Carlet [9])**.** Let $n = 2m$; let i, j be such that $\gcd(i - j, m) = 1$ and let $s, t \neq 0$, u and v in $\mathbb{F}_{2^m}$. Set $G(x, y) = sx^{2^i+2^j} + ux^{2^i}y^{2^j} + vx^{2^j}y^{2^i} + ty^{2^i+2^j}$. Then $F(x, y) = (xy, G(x, y))$ is APN if and only if the polynomial $G(X, 1) = sX^{2^i+2^j} + uX^{2^i} + vX^{2^j} + t$ has no zero in $\mathbb{F}_{2^m}$.

This method was also used later by Zhou–Pott [24] and Taniguchi [21] to construct new APN classes. We record their results below.

Theorem 3.2 (Zhou–Pott [24])**.** Let $n = 2m$, m even, and let i and j be integers such that $\gcd(i, m) = 1$. Set $G(x, y) = x^{2^i+1} + \alpha y^{2^j(2^i+1)}$. Then $F(x, y) = (xy, G(x, y))$ is APN if and only if $\alpha \notin \{u^{2^i+1}(t^{2^i} + t)^{1-2^j} : u, t \in \mathbb{F}_{2^m}\}$. In particular if j is even, then F is APN if and only if α is not a cube.

Theorem 3.3 (Taniguchi [21])**.** Let $n = 2m$ and i be an integer such that $\gcd(i, m) = 1$. Set $G(x, y) = x^{2^{2i}+2^{3i}} + ax^{2^{2i}}y^{2^i} + by^{2^i+1}$ with $a \in 0, 1$. Then $F(x, y) = (xy, G(x, y))$ is APN if and only if $X^{2^i+1} + aX + b$ has no zero in $\mathbb{F}_{2^m}$.

3.1. Three Cases of APN Functions From Carlet's Construction

Based on the following theorem and lemma from [7], we derive new results on bivariate APN functions. We consider the particular case of the general bivariate construction where the linear functions are monomial linear functions, namely

$$G(x, y) = a(x^{2^i+1})^{2^k} + b(x^{2^i}y)^{2^h} + c(xy^{2^i})^{2^r} + d(y^{2^i+1})^{2^s}.$$

With this notation, the following result is given in [7].

Theorem 3.4 ([7])**.** Let

$$F(x, y) = (xy, a(x^{2^i+1})^{2^k} + b(x^{2^i}y)^{2^h} + c(xy^{2^i})^{2^r} + d(y^{2^i+1})^{2^s})$$

be an APN function over $\mathbb{F}_{2^{2m}}$. Then, F is EA-equivalent to one of the following functions
$F_1(x, y) = (xy, x^{2^i+1} + x^{2^{i+h}}y^{2^h} + b'x^{2^k}y^{2^{i+k}} + c'y^{2^{i+r}+2^r})$,
$F_2(x, y) = (xy, x^{2^i+1} + x^{2^k}y^{2^{i+k}} + c'y^{2^{i+r}+2^r})$,
$F_3(x, y) = (xy, x^{2^i+1} + c'y^{2^{i+r}+2^r})$, for some $b', c' \in \mathbb{F}_{2^m}$ and $c' \neq 0$.

The following lemma gives the requirement for the family F_1 given in Theorem 3.4 to be APN, when $h = m/2$, $k, r = 0$.

Lemma 3.5. [7, Lemma 6.1] Let $n = 2m$ with $m > 2$ even. Let i coprime with m. If $F(x,y) = (xy, x^{2^i+1} + x^{2^{i+m/2}}y^{2^{m/2}} + bxy^{2^i} + cy^{2^i+1})$ is APN, then $cX^{2^i+1} + bX^{2^i} + X^{2^{m/2}} + 1$ has no zero in $\mathbb{F}_{2^m}$.

The following results extend the known no-root criteria for special subclasses of Carlet-type APN constructions by reducing the APN property to the non-existence of roots of associated polynomials over finite fields.

We now give a general result for the family F_1 of functions. The divisibility assumptions in the following lemma may be considered up to any ordering of h, k, r ending with m.

Lemma 3.6. Let h, k, r, m be positive integers such that h divides k, k divides r, r divides m. Let $n = 2m$ with $m > 2$ even. Let i coprime with m. If $F_1(x,y) = (xy, x^{2^i+1} + x^{2^{i+h}}y^{2^h} + bx^{2^k}y^{2^{i+k}} + cy^{2^{i+r}+2^r})$ is APN, then $cX^{2^i+1+2^r} + bX^{2^{i+k}} + X^{2^h} + 1$ has no zero in $\mathbb{F}_{2^m}$.

Proof.
Denote $F(x,y) = (xy, G(x,y))$ with $G(x,y) = x^{2^i+1} + x^{2^{i+h}}y^{2^h} + bx^{2^k}y^{2^{i+k}} + cy^{2^{i+r}+2^r}$. Since F_1 is APN, G satisfies the following conditions

i. The function $x \to G(x,y)$ is APN for any fixed y;

ii. The function $y \to G(x,y)$ is APN for any fixed x;

iii. The function $G(x, \beta x + \gamma)$ is APN for any β and γ.

The conditions (i) and (ii) are clearly satisfied. We deal with the third one. We can consider $\gamma = 0$ since G is quadratic. We have $G(x,\beta x) = x^{2^i+1} + \beta^{2^h}x^{2^{i+h}}x^{2^h} + b\beta^{2^{i+k}}x^{2^k}x^{2^{i+k}} + c\beta^{2^{i+r}+2^r}x^{2^{i+r}+2^r}$. If we take $x \in \mathbb{F}_{2^h}$ with h dividing k, k dividing r, r dividing m, then we have the function $F'(x) = (1 + \beta^{2^h} + b\beta^{2^{i+k}} + c\beta^{2^{i+r}+2^r})x^{2^{i+1}}$. If there exist β such that $1 + \beta^{2^h} + b\beta^{2^{i+k}} + c\beta^{2^{i+r}+2^r} = 0$, then for any $a \in \mathbb{F}_{2^h}^*$ and for any $x \in \mathbb{F}_{2^h}$, $F'(x) + F'(x+a) = 0$ imply that $G(x,\beta x)$ is not APN.

A similar no-root condition can be proven for a sub-class of the family F_1, which we give in the following theorem.

Theorem 3.7. Let $n = 2m$ with $m > 2$ even. Let $i < m/2$ coprime with m, let $h = m/4$, $k = 2m/4$, $r = 3m/4$. Let

$$A(X) = X^{2^h}, \quad B(X) = bX^{2^{i+k}}, \quad C(X) = cX^{2^{i+r}+2^r}$$

be monomials for some $b, c \in \mathbb{F}_{2^m}$ and the determinant be a polynomial

$$D(X) = \begin{vmatrix} 1 & A(X) & B(X) & C(X) \\ C(X)^{2^{m/4}} & 1 & A(X)^{2^{m/4}} & B(X)^{2^{m/4}} \\ B(X)^{2^{m/2}} & C(X)^{2^{m/2}} & 1 & A(X)^{2^{m/2}} \\ A(X)^{2^{3m/4}} & B(X)^{2^{3m/4}} & C(X)^{2^{3m/4}} & 1 \end{vmatrix} \in \mathbb{F}_{2^m}[X].$$

Then, $F_1(x,y) = (xy, x^{2^i+1} + x^{2^{i+h}}y^{2^h} + bx^{2^k}y^{2^{i+k}} + cy^{2^{i+r}+2^r})$ is APN if and only if $D(X) \in \mathbb{F}_{2^m}[X]$ has no zero.

Proof.

We set $G(x,y) = x^{2^i+1} + x^{2^{i+h}}y^{2^h} + bx^{2^k}y^{2^{i+k}} + cy^{2^{i+r}+2^r}$, then $G(x,\beta x) = x^{2^i+1} + \beta^{2^h}x^{2^{i+h}}x^{2^h} + b\beta^{2^{i+k}}x^{2^k}x^{2^{i+k}} + c\beta^{2^{i+r}+2^r}x^{2^{i+r}+2^r}$. $G(x,\beta x) = L_\beta(x^{2^i+1})$ for $L_\beta(x) = x + \beta^{2^h}x^{2^h} + b\beta^{2^{i+k}}x^{2^k} + c\beta^{2^{i+r}+2^r}x^{2^r}$. Therefore, F_1 is APN

if and only if L_β is a permutation of $\mathbb{F}_{2^m}$. We have $h = m/4$, $k = 2m/4$, $r = 3m/4$. Then $L_\beta(x) = x + A(\beta)x^{2^{m/4}} + B(\beta)x^{2^{2m/4}} + C(\beta)x^{2^{3m/4}}$ for $A(\beta) = \beta^{2^h}$, $B(\beta) = b\beta^{2^{i+k}}$, $C(\beta) = c\beta^{2^{i+r}+2^r}$. L_β is a permutation if and only if

$$D(\beta) = \begin{vmatrix} 1 & A(\beta) & B(\beta) & C(\beta) \\ C(\beta)^{2^{m/4}} & 1 & A(\beta)^{2^{m/4}} & B(\beta)^{2^{m/4}} \\ B(\beta)^{2^{m/2}} & C(\beta)^{2^{m/2}} & 1 & A(\beta)^{2^{m/2}} \\ A(\beta)^{2^{3m/4}} & B(\beta)^{2^{3m/4}} & C(\beta)^{2^{3m/4}} & 1 \end{vmatrix}$$

is nonzero. L_β is a permutation for any β if and only if the polynomial $D(X) \in \mathbb{F}_{2^m}[X]$ has no zero.

We extend the necessary condition given [7] for a function F_2.

Lemma 3.8. Let h, k, r, m be integers such that they divide each other in any order ending with m. Let $n = 2m$ with $m > 2$ even. Let i be coprime to m, and let $c \in \mathbb{F}_{2^m}$. If $F_2(x, y) = (xy, x^{2^i+1} + x^{2^k} y^{2^{i+k}} + cy^{2^{i+r}+2^r})$ is APN, then $cX^{2^i+1+2^r} + X^{2^{i+k}} + 1$ has no zero in $\mathbb{F}_{2^m}$.

Proof.

We have $F(x, y) = (xy, G(x, y))$ with $G(x, y) = x^{2^i+1} + x^{2^k} y^{2^{i+k}} + cy^{2^{i+r}+2^r}$. As in the extension of previous lemma we dealt with the third condition. $G(x, \beta x) = x^{2^i+1} + \beta^{2^{i+k}} x^{2^k} x^{2^{i+k}} + c\beta^{2^{i+r}+2^r} x^{2^{i+r}+2^r}$. If we take $x \in \mathbb{F}_{2^k}$, since k divides r and r divides m, we have the function $F'(x) = (1 + \beta^{2^{i+k}} + c\beta^{2^{i+r}+2^r})x^{2^{i+1}}$. If there exist β such that $1 + \beta^{2^{i+k}} + c\beta^{2^{i+r}+2^r} = 0$, then for any $a \in \mathbb{F}_{2^k}^*$ and for any $x \in \mathbb{F}_{2^k}$ $F'(x) + F'(x + a) = 0$ imply that $G(x, \beta x)$ is not APN.

A no-root condition for a sub-class of the family F_2 is presented in the following theorem.

Theorem 3.9. Let $n = 2m$ with $m > 2$ even. Let $i < m/2$ coprime with m and $k = m/3$, $r = 2m/3$. Let $A(X) = X^{2^{i+k}}$, $B(X) = cX^{2^{i+r}+2^r}$ be monomials for some $c \in \mathbb{F}_{2^m}$ and the determinant $D(X)$ be a polynomial

$$D(X) = \begin{vmatrix} 1 & A(X) & B(X) \\ B(X)^{2^{m/3}} & 1 & A(X)^{2^{m/3}} \\ A(X)^{2^{2m/3}} & B(X)^{2^{2m/3}} & 1 \end{vmatrix} \in \mathbb{F}_{2^m}[X].$$

Then, $F_2(x, y) = (xy, x^{2^i+1} + x^{2^k} y^{2^{i+k}} + cy^{2^{i+r}+2^r})$ is APN if and only if $D(X)$ has no zero in $\mathbb{F}_{2^m}[X]$.

Proof.

We set $G(x, y) = x^{2^i+1} + x^{2^k} y^{2^{i+k}} + cy^{2^{i+r}+2^r}$ then $G(x, \beta x) = x^{2^i+1} + \beta^{2^{i+k}} x^{2^k} x^{2^{i+k}} + c\beta^{2^{i+r}+2^r} x^{2^{i+r}+2^r}$. $G(x, \beta x) = L_\beta(x^{2^i+1})$ for $L_\beta(x) = x + \beta^{2^{i+k}} x^{2^k} + c\beta^{2^{i+r}+2^r} x^{2^r}$. F_2 is APN if and only if L_β is a permutation of $\mathbb{F}_{2^m}$. We note that L_β is a linearized polynomial. We have $k = m/3$, $r = 2m/3$. Then, $L_\beta(x) = x + Ax^{2^{m/3}} + Bx^{2^{2m/3}}$ for $A = \beta^{2^{i+k}}$, $B = c\beta^{2^{i+r}+2^r}$. L_β is a permutation for any β if and only if

$$\begin{vmatrix} 1 & A & B \\ B^{2^{m/3}} & 1 & A^{2^{m/3}} \\ A^{2^{2m/3}} & B^{2^{2m/3}} & 1 \end{vmatrix}$$

is nonzero. Hence, this property holds if and only if the polynomial $D(X) \in \mathbb{F}_{2^m}[X]$ has no zero.

In the remaining part of this section, we deal with the family F_3, and present sufficient condition in Lemma 3.10 and a necessary-sufficient condition in Theorem 3.11 for some of its subclasses.

Lemma 3.10. Let $n = 2m$ with $m > 2$ even. Let i coprime with m and r divides m. If

$$F_3(x, y) = (xy, x^{2^i+1} + cy^{2^{i+r}+2^r})$$

is APN, then $cX^{2^i+1+2^r} + 1$ has no zero in $\mathbb{F}_{2^m}$.

Proof.
We set $F(x, y) = (xy, G(x, y))$ with $G(x, y) = x^{2^i+1} + cy^{2^{i+r}+2^r}$. As in the extension of previous lemmas we dealt with the third condition. $G(x, \beta x) = x^{2^i+1} + c\beta^{2^{i+r}+2^r} x^{2^{i+r}+2^r}$. If we take $x \in \mathbb{F}_{2^r}$, and if r divides m then we have the function $F'(x) = (1 + c\beta^{2^{i+r}+2^r})x^{2^i+1}$. If there exist β such that $1 + c\beta^{2^{i+r}+2^r} = 0$, then for any $a \in \mathbb{F}_{2^r}^*$ and for any $x \in \mathbb{F}_{2^r}$, $F'(x) + F'(x + a) = 0$ imply that $G(x, \beta x)$ is not APN.

Theorem 3.11. Let $n = 2m$ with $m > 2$ even. Let $i < m/2$ coprime with m and $r = m/2$. Then,

$$F_3(x, y) = (xy, x^{2^i+1} + cy^{2^{i+r}+2^r})$$

is APN if and only if

$$1 + (cX^{2^{i+r}+2^r})^{2^{m/2+1}}$$

has no zero in $\mathbb{F}_{2^m}$.

Proof.
We set $G(x, y) = x^{2^i+1} + cy^{2^{i+r}+2^r}$ then $G(x, \beta x) = x^{2^i+1} + c\beta^{2^{i+r}+2^r} x^{2^{i+r}+2^r}$ and $G(x, \beta x) = L_\beta(x^{2^i+1})$ for $L_\beta(x) = x + c\beta^{2^{i+r}+2^r} x^{2^r}$. F_3 is APN if and only if L_β is a permutation of $\mathbb{F}_{2^m}$. $L_\beta(x) = x + Ax^{2^{m/2}}$, $A = c\beta^{2^{i+r}+2^r}$. L_β is a permutation if and only if

$$\begin{vmatrix} 1 & A \\ A^{2^{m/2}} & 1 \end{vmatrix}$$

is nonzero. So L_β is a permutation for any β if and only if

$$1 + (cX^{2^{i+r}+2^r})^{2^{m/2+1}}$$

has no zero in $\mathbb{F}_{2^m}$.

3.2. Biprojective Almost Perfect Nonlinear Functions

Let $q = 2^k$ and $m \in \mathbb{Z}^+$. A polynomial of type $X^{q+1} + aX^q + bX + c \in \mathbb{F}_{2^m}[X]$ is called projective, and a polynomial of type $ax^{q+1} + bx^q y + cxy^q + dy^{q+1} \in \mathbb{F}_{2^m}[x, y]$ is called bivariate projective (or biprojective) polynomial of degree $q + 1$.

The transition from the generic Carlet-type constructions to biprojective families relies on a natural algebraic generalization. By substituting the monomial components in the Maiorana-McFarland framework with biprojective polynomials, the essential structural symmetries required to satisfy the APN conditions are preserved. Specifically, the core principle of Carlet's method—reducing the differential uniformity problem to the non-existence of roots of associated linearized polynomials—remains effective because biprojective forms maintain compatible linearity properties under differentiation. This algebraic intuition motivates the extension of the construction methods given in Section 3.1 to the following generalized representations.

A general representation of the bivariate construction with two biprojective polynomials over $\mathbb{F}_{2^m}$ is given

by

$$F(x,y)=(Ax^{2^i+1}+Bx^{2^i}y+Cxy^{2^i}+Dy^{2^i+1},ax^{2^j+1}+bx^{2^j}y+cxy^{2^j}+dy^{2^j+1}).$$

Then we consider Theorem 7.1 in [7] as follows;

Theorem 3.12. [7, Theorem 7.1] Let m be a positive even integer, $n=2m$, $i,j\leq m/2$ and

$$F(x,y)=(Ax^{2^i+1}+Bx^{2^i}y+Cxy^{2^i}+Dy^{2^i+1},ax^{2^j+1}+bx^{2^j}y+cxy^{2^j}+dy^{2^j+1})$$

be APN over $\mathbb{F}_{2^n}$. Then F is EA-equivalent to one of the following functions:

1. $f_1(x,y)=(x^{2^i+1}+x^{2^i}y+Axy^{2^i}+By^{2^i+1},x^{2^j+1}+ax^{2^j}y+bxy^{2^j}+cy^{2^j+1})$
2. $f_2(x,y)=(x^{2^i+1}+xy^{2^i}+Ay^{2^i},x^{2^j+1}+ax^{2^j}y+bxy^{2^j}+cy^{2^j+1})$
3. $f_3(x,y)=(x^{2^i+1}+Ay^{2^i+1},x^{2^j+1}+x^{2^j}y+axy^{2^j}+by^{2^j+1})$
4. $f_4(x,y)=(x^{2^i+1}+Ay^{2^i+1},x^{2^j+1}+axy^{2^j}+by^{2^j+1})$, where $a\in\{0,1\}$.

In the following subsections, we look for the conditions of Families f_1, f_2, f_3 and f_4 by using Carlet's method that is used in Section 3.1. A general result covering all these families is not derived here. Instead, we present results for the cases $i=0$ and $i=1$. It would be a good future work to extend them.

3.3. Family f_1

We now consider the function $f_1(x,y)=(x^{2^i+1}+x^{2^i}y+Axy^{2^i}+By^{2^i+1},x^{2^j+1}+ax^{2^j}y+bxy^{2^j}+cy^{2^j+1})$ and prove new requirements in order to say that f_1 is APN by using similar arguments as in Section 3.1. We firstly consider the case $i=0$. If $i=0$ is substituted, we get

$$f_1(x,y)=(x^2+xy+Axy+By^2,x^{2^j+1}+ax^{2^j}y+bxy^{2^j}+cy^{2^j+1}).$$

We define $B_{1,0}(x,y):=x^2+xy+Axy+By^2$ and $G_{1,0}(x,y):=x^{2^j+1}+ax^{2^j}y+bxy^{2^j}+cy^{2^j+1}$. We know that the function f_1 is APN if the system of equations

$$B_{1,0}(x,y)+B_{1,0}(x+a,y+b)=c$$

$$G_{1,0}(x,y)+G_{1,0}(x+a,y+b)=d$$

has 0 or 2 solutions for every $a,b\in\mathbb{F}_{2^m}^*$, and for every $c,d\in\mathbb{F}_{2^m}$. As $B_{1,0}(x,y)=x^2+xy+Axy+By^2$, we get $bx+ay+Abx+Aay=c$ by replacing c with $c+ab+Aab+Bb^2+a^2$ in the equation $B_{1,0}(x,y)+B_{1,0}(x+a,y+b)=c$. Then, we need to check the number of solutions in the equation

$$G_{1,0}(x,\frac{c+b(A+1)x}{a(A+1)})+G_{1,0}(x+a,\frac{c+b(A+1)x}{a(A+1)}+b)=d,$$

for $a(A+1)\neq 0$. Changing c into $a(A+1)c$ and x into ax and defining $G_{a,b,c}(x):=G_{1,0}(ax,bx+c)$, we get that the function f_1 is APN if and only if $G_{a,b,c}$ is an APN function. So, we have the same result with the Carlet's construction [9] of the case $B(x,y)=xy$, that is discussed in the previous section. From this observations above, we have the following corollary.

Corollary 3.13. Let $f_1(x,y) = (x^2 + xy + Axy + By^2, x^{2^j+1} + ax^{2^j}y + bxy^{2^j} + cy^{2^j+1})$ and define $G_{a,b,c}(x) := G_{1,0}(ax, bx+c)$. For $a(A+1) \neq 0$, the function f_1 is APN if and only if $G_{a,b,c}$ is an APN function.

For $i = 1$, we have $f_1(x,y) = (x^3 + x^2y + Axy^2 + By^3, x^{2^j+1} + ax^{2^j}y + bxy^{2^j} + cy^{2^j+1})$, and $B_{1,1}(x,y) := x^3 + x^2y + Axy^2 + By^3$, $G_{1,1}(x,y) := x^{2^j+1} + ax^{2^j}y + bxy^{2^j} + cy^{2^j+1}$. Dealing with the equation $B_{1,1}(x,y) + B_{1,1}(x+a, y+b) = c$, by changing c into $c + a^3 + a^2b + Aab^2 + bB^3$, we have $(a+b)x^2 + (a^2+Ab^2)x + (Aa+Bb)y^2 + (a^2+Bb^2)y = c$. Taking s, $u \neq 0$, v and t instead of $a+b$, a^2+Ab^2, $Aa+Bb$ and a^2+Bb^2 respectively, we get $sx^2 + ux + vy^2 + ty = c$. Then if we take $d = c + vy^2 + ty$, we have $sx^2 + ux + d = 0$. Taking $y = \frac{sx}{u}$ and $k = \frac{sd}{u^2}$, we have the formula $y^2 + y + k = 0$. If m is odd, this formula has a root

$$y_1 = \sum_{j\in J} k^{2^j} = \sum_{i\in I} k^{2^i},$$

where $J = \{0,2,4,\ldots,m-1\}$ and $I = \{1,3,5,\ldots,m-2\}$. For $m = 3$, $I = \{1\}$ and $J = \{0,2\}$ we have $y_1 = k^2$. So the roots of the formula $(a+b)x^2+(a^2+Ab^2)x+(Aa+Bb)y^2+(a^2+Bb^2)y = c$ are $x_1 = \frac{a+b}{a^2+Ab^2}(\frac{c+(Aa+Bb)y^2+(a^2+Bb^2)y}{a^2+Ab^2})^2$ and $x_2 = \frac{a^2+Ab^2}{a+b}[(\frac{(a+b)(c+(Aa+Bb)y^2+(a^2+Bb^2)y}{(a^2+Ab^2)^2})^2 + 1]$ for $a^2 + Ab^2 \neq 0$.

Now, we consider the number of solutions in the equation $G_{1,1}(x,y)+G_{1,1}(x+a,y+b) = d$ by taking $A = B = 1$. Then

$$G_{1,1}((a+b)(c+y^2+y)^2, (a+b)y) + G_{1,1}((a+b)(c+y^2+y)^2 + a_0, (a+b)y + b_0) = d$$

for every nonzero $a_0, b_0 \in \mathbb{F}_2^m$ must have no solution or one solution for the root x_1 and one solution for the root x_2. If $G_{1,1}$ has two solutions for the root x_1, then it has two solutions for the other root x_2. This contradicts to the fact that $G_{1,1}$ is APN. Hence we proved the following.

Corollary 3.14. Let

$$f_1(x,y) = (x^3 + x^2y + xy^2 + y^3, x^{2^j+1} + ax^{2^j}y + bxy^{2^j} + cy^{2^j+1}).$$

For $a^2 + Ab^2 \neq 0$ the function f_1 is APN if and only if

$$G_{1,1}((a+b)(c+y^2+y)^2, (a+b)y) + G_{1,1}((a+b)(c+y^2+y)^2 + a_0, (a+b)y + b_0) = d$$

for every nonzero $a_0, b_0 \in \mathbb{F}_2^m$ must have no solution or one solution for the root x_1 and one solution for the root x_2.

3.4. Family f_2

In this section, we consider $f_2(x,y) = (x^{2^i+1} + xy^{2^i} + Ay^{2^i}, x^{2^j+1} + ax^{2^j}y + bxy^{2^j} + cy^{2^j+1})$, using arguments similar to those in Subsection 3.3 we get the following results for $i = 0$ and $i = 1$, respectively.

Corollary 3.15. Let $f_2(x,y) = (x^2+xy+Ay, x^{2^j+1}+ax^{2^j}y+bxy^{2^j}+cy^{2^j+1})$ and define $G_{a,b,c}(x) := G_{2,0}(ax, bx+c)$. For $b \neq 0$, f_2 is APN if and only if $G_{a,b,c}$ is an APN function.

Corollary 3.16. Let $f_2(x,y) = (x^3 + xy^2 + y^2, x^{2^j+1} + ax^{2^j}y + bxy^{2^j} + cy^{2^j+1})$. For $a^2 + b^2 \neq 0$ and $m = 3$ the function f_2 is APN if and only if the equation

$$G_{2,1}(a(c+by(ay+by+b)^2, (a+b)y) + G_{2,1}(a(c+by(ay+by+b))^2 + (a+b)a, (a+b)y + b) = d$$

must have zero solution or one solution for the root x_1 and one solution for the root x_2.

3.5. Family f_3

Now we consider the function $f_3(x,y) = (x^{2^i+1} + Ay^{2^i+1}, x^{2^j+1} + x^{2^j}y + axy^{2^j} + by^{2^j+1})$.

Corollary 3.17. Let $f_3(x,y) = (x^2 + Ay^2, x^{2^j+1} + x^{2^j}y + axy^{2^j} + by^{2^j+1})$. f_3 is APN if and only if $G_{3,0}(x,y) = x^{2^j+1} + x^{2^j}y + axy^{2^j} + by^{2^j+1}$ is APN.

Corollary 3.18. Let $f_3(x,y) = (x^3 + Ay^3, x^{2^j+1} + x^{2^j}y + axy^{2^j} + by^{2^j+1})$. For $a \neq 0$, f_3 is APN if and only if the equation $G_{3,1}(a(c + Aby^2 + Ab^2y)^2, a^3y) + G_{3,1}(a(c + Aby^2 + Ab^2y)^2 + a, a^3y + b) = d$ must have zero solution or one solution for the root x_1 and one solution for the root x_2

We note that Family f_4 can be handled similarly to Family f_3.

4. Dobbertin Power Function's Representations

In this section, it appears that we are considering a specific power function denoted as x^d, where the exponent d is given by:

$$d = 2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1.$$

and $n = 5m$. The power function x^d is a monomial and is of particular interest in the study of APN functions in cryptography due to its cryptographic properties.

It has been demonstrated in [4] that the Dobbertin power function can be expressed as the composition of a cubic power function and the inverse of a quadratic power function.

We examine x^d to represent as the composition of two functions which are different from those shown in [4] with respect to binary weight. We prove that x^d is equivalent to a power function composed from a cubic power function and the inverse of a quadratic power function with six different representations in the following lemma. We see that the first two congruences are different from the four congruences given in [4].

Lemma 4.1. The following equivalences hold for any positive integer m:

$$\begin{aligned}
\textstyle\sum_{i=1}^{4} 2^{im} - 1 &\equiv 2^{3m+1}\tfrac{2^{4m}+2^m+1}{2^m+1} \\
&\equiv 2^{3m+1}\tfrac{2^{3m}+2^m+1}{2^{2m}+1} \\
&\equiv 2^{m+1}\tfrac{2^{2m}+2^m+1}{2^{4m}+1} \\
&\equiv 2^{m+1}\tfrac{2^{3m}+2^m+1}{2^{3m}+1} \\
&\equiv 2^{m+1}\tfrac{2^{3m}+2^{2m}+1}{2^{2m}+1} \\
&\equiv 2^{2m+1}\tfrac{2^{2m}+2^m+1}{2^m+1} \mod (2^{5m}-1)
\end{aligned}$$

Proof.

Similar to [4], we consider first congruence and prove that $2^m + 1$ is invertible modulo $2^{5m} - 1$. To show that we need that $\gcd(2^m + 1, 2^{5m} - 1)$. Then

$$\gcd(2^i + 1, 2^j - 1) = \begin{cases} 1, & \text{if } j/\gcd(i,j) \text{ is odd;} \\ 2^{\gcd(i,j)} + 1, & \text{if } j/\gcd(i,j) \text{ is even.} \end{cases}$$

We have $\gcd(2^m + 1, 2^{5m} - 1) = 1$ since $\gcd(m, 5m) = m$. If we replace 2^m by x, we have the equivalence $(x+1)(x^4 + x^3 + x^2 + x - 1) \equiv 2x^3(x^4 + x + 1) \mod (x^5 - 1)$. Computing the left-hand side of this equivalence,

we have $(x+1)(x^4+x^3+x^2+x-1) = x^5+2x^4+2x^3+2x^2-1 \equiv 2x^4+2x^3+2x^2 \mod (x^5-1)$. Then considering right-hand side we have $2x^7+2x^4+2x^3$ and we have $x^5=1$, so we have the equivalence. We can prove other five statements of lemma similarly since $2^{2m}+1$, $2^{3m}+1$ and $2^{4m}+1$ are invertible modulo $(2^{5m}-1)$. The corollary that follows is an obvious result of Lemma 4.1.

Corollary 4.2. Let x^d be the power function defined over the field $\mathbb{F}_{2^{5m}}$ with $d = 2^{4m}+2^{3m}+2^{2m}+2^m-1$. Then x^d is cyclotomically equivalent to the power functions with the exponents $\frac{2^{4m}+2^m+1}{2^m+1}$, $\frac{2^{3m}+2^m+1}{2^{2m}+1}$, $\frac{2^{2m}+2^m+1}{2^{4m}+1}$, $\frac{2^{3m}+2^m+1}{2^{3m}+1}$, $\frac{2^{3m}+2^{2m}+1}{2^{2m}+1}$, $\frac{2^{2m}+2^m+1}{2^m+1}$. We know from [4] that these representations are optimal in terms of their weight.

We know that two power functions $F(x) = x^d$ and $G(x) = x^e$ over $\mathbb{F}_{2^n}$, where d, e, n are positive integers, are said to be cyclotomically equivalent if $d \equiv 2^k e \mod 2^n-1$ for some positive integer k, or if $d^{-1} \equiv 2^k e \mod 2^n-1$ for some positive integer k in the case that $\gcd(d, 2^n-1) = 1$, with d^{-1} being the multiplicative inverse of d modulo 2^n-1. Then we consider the multiplicative inverse d^{-1} of the power d and we try to represent d^{-1} as the fraction of two numbers by doing computer search and we have the lemma as follows.

Lemma 4.3. The following equivalences hold for any positive odd integer m:

$$\begin{aligned}
\frac{1}{\sum_{i=1}^{4} 2^{im}-1} &\equiv 2^{3m-1}\frac{2^m+1}{2^{2m}+2^m+1} \\
&\equiv 2^{2m-1}\frac{2^{2m}+1}{2^{3m}+2^m+1} \\
&\equiv 2^{m-1}\frac{2^{3m}+1}{2^{3m}+2^{2m}+1} \\
&\equiv 2^{2m-1}\frac{2^m+1}{2^{4m}+2^m+1} \\
&\equiv 2^{m-1}\frac{2^{2m}+1}{2^{4m}+2^{2m}+1} \\
&\equiv 2^{m-1}\frac{2^m+1}{2^{4m}+2^{3m}+1} \mod (2^{5m}-1)
\end{aligned}$$

Proof.

We first prove that, $2^{2m}+2^m+1$, $2^{3m}+2^m+1$, $2^{3m}+2^{2m}+1$, $2^{4m}+2^m+1$, $2^{4m}+2^{2m}+1$ and $2^{4m}+2^{3m}+1$ are invertible modulo $2^{5m}-1$. We consider the first one and prove that

$$\gcd(2^{2m}+2^m+1, 2^{5m}-1) = 1$$

when m is odd. The others can be proven similarly. By Euclidean algorithm, we get the following equation array:

$$\begin{aligned}
\gcd(2^{2m}+2^m+1, 2^{5m}-1) &= \gcd(2^{2m}+2^m+1, 2^{5m}-1 \mod (2^{2m}+2^m+1)) \\
&= \gcd(2^m+2, 2^{2m}-1) \\
&= \gcd(2^m+2, 3).
\end{aligned}$$

$$\gcd(2^m+2, 3) = \begin{cases} 1, & \text{if } m \text{ is odd;} \\ 3, & \text{if } m \text{ is even.} \end{cases}$$

Then we see that they are relatively prime when m is odd as follows.

If we replace 2^m by x, we show that $(x+1)x^3(x^4+x^3+x^2+x-1) \equiv 2x^2+2x+2 \mod (x^5-1)$. For the left-hand side of this equation we have $2x^7+2x^6+2x^5$ and this is equivalent to $2x^2+2x+2$ modulo (x^5-1). The other congruences are proven in the same way. The following corollary follows from Lemma 4.3.

Corollary 4.4. Let x^d be the power function defined over the field $\mathbb{F}_{2^{5m}}$ with $d = 2^{4m}+2^{3m}+2^{2m}+2^m-1$ and d^{-1} be the multiplicative inverse of d modulo $2^{5m}-1$. Then for any odd integer m, x^d is cyclotomically equivalent to the power functions with the exponents $\frac{2^m+1}{2^{2m}+2^m+1}$, $\frac{2^{2m}+1}{2^{3m}+2^m+1}$, $\frac{2^{3m}+1}{2^{3m}+2^{2m}+1}$, $\frac{2^m+1}{2^{4m}+2^m+1}$, $\frac{2^{2m}+1}{2^{4m}+2^{2m}+1}$

and $\frac{2^m+1}{2^{4m}+2^{3m}+1}$.

The representations obtained in Lemma 4.1 preserve cyclotomic equivalence and therefore correspond to APN power functions with the same cryptographic properties as the original Dobbertin exponent. Their interest lies in providing alternative fractional decompositions of the exponent with different numerator and denominator structures. In particular, the first two representations are not among the four representations reported in [4], showing that the Dobbertin exponent admits a richer family of optimal representations than previously known. Such alternative forms may also be useful in future investigations concerning binary-weight properties, exponent decompositions, and implementation-oriented representations of APN power functions.

5. Conclusion

In this paper, we divided our work into two parts. The first part concerns necessary and sufficient conditions for some families of bivariate APN functions built by Carlet's bivariate APN construction. In the second part, we presented our conclusions about the representation of Dobbertin power function. For the first part, we described Carlet's bivariate APN construction in which APN functions are built by using the simplest Maiorana–McFarland function. Based on Theorem 3.4, we derived necessary and sufficient conditions on functions F_1, F_2 and F_3 to be APN. Then we dealt with four functions defined in Theorem 3.12 and we demonstrated the conditions in Carlet's construction for these functions to be APN in special cases. For the second part, we considered representations of the Dobbertin power function, and reported new cyclotomically equivalent exponents.

The obtained results extend several previously known observations on Carlet's bivariate APN construction and provide additional criteria for identifying APN instances within these families. Furthermore, the new cyclotomic representations of the Dobbertin power function enrich the understanding of the algebraic relationships between APN power functions and may be useful in future investigations of equivalence classes and optimal representations of exceptional APN functions.

Author Contributions

All authors contributed equally to this work. They all read and approved the final version of the manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgement

The authors would like to thank the reviewers for their valuable comments. Oğuz Yayla was supported by TÜBİTAK, Grant number: 123F360.

References

[1] T. Beth, C. Ding, *On almost perfect nonlinear permutations*, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1994, 65–76.

[2] E. Biham, A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Journal of Cryptology, 4(1),

(1991), 3–72.

[3] L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer, Cham, 2015.

[4] L. Budaghyan, M. Calderini, C. Carlet, D. Davidova, N. S. Kaleyski, *On two fundamental problems on APN power functions*, IEEE Transactions on Information Theory, 68(5), (2022), 3389–3403.

[5] L. Budaghyan, C. Carlet, G. Leander, *A class of quadratic APN binomials inequivalent to power functions*, Cryptology ePrint Archive, (2006).

[6] L. Budaghyan, M. Calderini, I. Villa, *On relations between CCZ-and EA-equivalences*, Cryptography and Communications, 12(1), (2020), 85–100.

[7] M. Calderini, L. Budaghyan, C. Carlet, *On known constructions of APN and AB functions and their relation to each other*, Rad Hrvatske akademije znanosti i umjetnosti: Matematičke znanosti(546= 25), (2021), 79–105.

[8] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, 2021.

[9] C. Carlet, *Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions*, Designs, Codes and Cryptography, 59(1), (2011), 89–109.

[10] C. Carlet, P. Charpin, V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Designs, Codes and Cryptography, 15(2), (1998), 125–156.

[11] F. Chabaud, S. Vaudenay, *Links between differential and linear cryptanalysis*, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1995, 356–365.

[12] D. Davidova, *On properties of bent and almost perfect nonlinear functions*, PhD Dissertation, University of Bergen (2021) .

[13] H. Dobbertin, *Almost perfect nonlinear power functions on GF*(2^n)*: The Welch case*, IEEE Transactions on Information Theory, 45(4), (1999), 1271–1275.

[14] H. Dobbertin, *Almost perfect nonlinear power functions on GF*(2^n)*: the Niho case*, Information and Computation, 151(1-2), (1999), 57–72.

[15] H. Dobbertin, *Almost perfect nonlinear power functions on GF*(2^n)*: A new case for n divisible by 5*, In: Jungnickel, D., Niederreiter, H. (eds) Finite Fields and Applications, Springer, 2001, 113–121.

[16] R. Gold, *Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.)*, IEEE transactions on Information Theory, 14(1), (1968), 154–156.

[17] H. Janwal, R. Wilsonat, *Hyperplane sections of Fermat varieties in* P^3 *in char. 2 and some applications to cyclic*, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 10th International Symposium, AAECC-10, San Juan de Puerto Rico, Puerto Rico, May 10-14, 1993. Proceedings, Vol. 673, Springer Science & Business Media, 1993, 180–194.

[18] T. Kasami, *The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes*, Information and Control, 18(4), (1971), 369–394.

[19] G. Lachaud, J. Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes*, IEEE transactions on information theory, 36(3), (1990), 686–692.

[20] K. Nyberg, *Differentially uniform mappings for cryptography*, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1994, 55–64.

[21] H. Taniguchi, *On some quadratic APN functions*, Designs, Codes and Cryptography, 87(9), (2019), 1973–1983.

[22] S. Yoshiara, *Equivalences of quadratic APN functions*, Journal of Algebraic Combinatorics, 35(3), (2012), 461–475.

[23] S. Yoshiara, *Equivalences of power APN functions with power or quadratic APN functions*, Journal of Algebraic Combinatorics, 44, (2016), 561–585.

[24] Y. Zhou, A. Pott, *A new family of semifields with 2 parameters*, Advances in Mathematics, 234, (2013), 43–60.