Finite Fields and Their Applications 66 (2020) 101704

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On equivalence between known families of quadratic APN functions[☆]

Lilya Budaghyan, Marco Calderini[*], Irene Villa

Department of informatics, University of Bergen, Norway

ARTICLE INFO

Article history:
Received 8 July 2019
Received in revised form 13 May 2020
Accepted 25 May 2020
Available online xxxx
Communicated by Pascale Charpin

MSC:
94A60
06E30
11T71

Keywords:
CCZ-equivalence
EA-equivalence
APN
Boolean functions

ABSTRACT

This paper is dedicated to a question whether the currently known families of quadratic APN polynomials are pairwise different up to CCZ-equivalence. We reduce the list of these families to those CCZ-inequivalent to each other. In particular, we prove that the families of APN trinomials (constructed by Budaghyan and Carlet in 2008) and multinomials (constructed by Bracken et al. 2008) are contained in the APN hexanomial family introduced by Budaghyan and Carlet in 2008. We also prove that a generalization of these trinomial and multinomial families given by Duan et al. (2014) is contained in the family of hexanomials as well.

1. Introduction

Let n and m be two positive integers, an (n, m)-function, or vectorial Boolean function, is a function F from the finite field $\mathbb{F}_{2^n}$ with 2^n elements to the finite field $\mathbb{F}_{2^m}$ with

[☆] Some results of this paper were presented at the International Workshop on Coding and Cryptography WCC 2019.

[*] Corresponding author.

E-mail addresses: Lilya.Budaghyan@uib.no (L. Budaghyan), Marco.Calderini@uib.no (M. Calderini), Irene.Villa@uib.no (I. Villa).

https://doi.org/10.1016/j.ffa.2020.101704

2^m elements. When $m = 1$ such functions are simply called Boolean functions. Boolean functions and vectorial Boolean functions have been intensively studied due to the large number of applications both in mathematics and computer science. In particular, they have a crucial role in the design of secure cryptographic primitives, such as block ciphers. In this context, vectorial Boolean functions are also called S-boxes.

The differential attack, introduced by Biham and Shamir [2], is among the most efficient attacks on block cipher. To measure the resistance of an S-box to this attack, in [31], Nyberg introduced the notion of *differential uniformity.* A vectorial Boolean function F is called differentially δ-uniform if the equation $F(x) + F(x + a) = b$ has at most δ solutions for any non-zero a and for all b. The smallest possible values for δ is 2, and functions achieving such differential uniformity are called *almost perfect nonlinear* (APN).

Boolean functions used in cryptography must have low differential uniformity. For this reason, functions with low differential uniformity, and in particular APN functions, are an important domain of research for symmetric cryptography.

The differential uniformity, and thus the APN property, is preserved by some transformations of functions, which define equivalence relations between vectorial Boolean functions. Two of these equivalence notions are the extended affine equivalence (EA-equivalence) and Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence). EA-equivalence is a particular case of CCZ-equivalence, which is the most general known equivalence relation preserving the differential uniformity.

An important aspect of the study and the analysis of APN functions, and vectorial Boolean functions in general, is their classification with respect to these equivalence relations. Classifications of APN functions is a hard problem and a complete classification is only known for $n \leq 5$ [7]. There are only few infinite classes of APN functions known: six classes of power functions and fifteen classes of quadratic polynomials CCZ-inequivalent to monomials, presented in Tables 1 and 2. When constructed, some of these 15 families have not been checked for equivalence to already known classes.

In this work we reduce the list of known families of polynomial APN functions by excluding all equivalent cases. Indeed, we show that the class of trinomial APN functions introduced in [9] and the class of multinomials studied in [4] are equivalent. Moreover, we prove that also their generalizations given in [24] coincide with the original ones. Finally we show that these classes can be reduced to the hexanomials introduced in [9]. According to the table of CCZ-inequivalent functions which arise from known APN families (in dimensions up to 11) [16], the remained families of APN functions are pairwise inequivalent in general. We present, then, a complete list of the known families of APN polynomials, which are pairwise CCZ-inequivalent, in Table 3.

2. Preliminaries

Let $n \geq 2$, we denote by $\mathbb{F}_{2^n}^*$ the multiplicative group of $\mathbb{F}_{2^n}$ and by $\mathbb{F}_{2^n}[x]$ the univariate polynomial ring defined over $\mathbb{F}_{2^n}$. Any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can be represented as a univariate polynomial of degree at most $2^n - 1$ in $\mathbb{F}_{2^n}[x]$, that is

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, \quad c_i \in \mathbb{F}_{2^n}.$$

The algebraic degree of a function F is equal to the maximum 2-weight of the exponent i such that $c_i \neq 0$, where the *2-weight* of i is the (Hamming) weight of its binary representation. Functions of algebraic degree 1 are called *affine* and of degree 2 *quadratic*. Affine functions without the constant term are *linear* functions and they can be represented as $L(x) = \sum_{i=0}^{n-1} c_i x^{2^i}$. For any $m \geq 1$ such that $m|n$,

$$Tr_n^m(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}$$

denotes the *trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. When $m = 1$ we denote $Tr_n^1(x)$ by $Tr(x)$.

The *derivative* of F in the direction of $a \in \mathbb{F}_{2^n}^*$ is given by the function $D_aF(x) = F(x+a) + F(x)$. The function F is APN if for every $a \neq 0$ and every b in $\mathbb{F}_{2^n}$, the equation $D_aF(x) = b$ admits at most 2 solutions, or equivalently $|\mathrm{Im}(D_aF)| = 2^{n-1}$, where $\mathrm{Im}(F) = \{F(x) \,|\, x \in \mathbb{F}_{2^n}\}$ is the *image* of F.

There are several equivalence relations of functions for which the APN property is preserved. Two functions F and F' from $\mathbb{F}_{2^n}$ to itself are called:

- affine equivalent if $F' = A_1 \circ F \circ A_2$, where $A_1, A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine permutations;
- EA-equivalent if $F' = F'' + A$, where the map $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is affine and F'' is affine equivalent to F;
- CCZ-equivalent if there exists some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that the image of the graph of F is the graph of F', that is, $\mathcal{L}(G_F) = G_{F'}$, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{2^n}\}$.

The affine equivalence is, obviously, included in the EA-equivalence, and EA-equivalence is a particular case of CCZ-equivalence [19]. Moreover, every permutation is CCZ-equivalent to its inverse [19]. As proven in [14], CCZ-equivalence is more general than EA-equivalence together with taking inverses of permutations. The algebraic degree of a function (if it is not affine) is invariant under EA-equivalence but, in general, it is not preserved by CCZ-equivalence. In general, neither EA-equivalence nor CCZ-equivalence preserves the permutation property.

There are six known infinite families of power APN functions presented in Table 1. Some results on CCZ-inequivalence between these functions were proven in [11]. Recently,

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	[26,31]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	$i+1$	[28,29]
Welch	2^t+3	$n=2t+1$	3	[21]
Niho	$2^t+2^{\frac{t}{2}}-1$, t even	$n=2t+1$	$\frac{t+2}{2}$	[22]
	$2^t+2^{\frac{3t+1}{2}}-1$, t odd		$t+1$	
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$	[1,31]
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$	$i+3$	[23]

in both [34] and [20] Yoshiara and Dempwolff show that two power APN functions are CCZ-equivalent if and only if they are *cyclotomic-equivalent*, i.e. they are EA-equivalent or one is EA-equivalent to the inverse of the second one. Since the algebraic degree is preserved by EA-equivalence, and families in Table 1 have, in general, different algebraic degrees, then all these families differ up to CCZ-equivalence (although they can intersect in some particular cases).

There are also fifteen known infinite families of quadratic APN polynomials CCZ-inequivalent to power functions listed in Table 2. In addition there was also a family of APN functions constructed by Göloğlu [27] but it was proven to be CCZ-equivalent to Gold power functions in [16]. In this paper we show that this list can be reduced to thirteen pairwise CCZ-inequivalent families represented in Table 3.

Regarding to the first two classes in Table 2 (C1 and C2) there is an interesting conjecture that these binomials together with the exceptional example $B(x)=x^3+\mu x^{36}$ defined over $\mathbb{F}_{2^{10}}$ ([25]) are the only possible APN binomials (up to CCZ-equivalence) [6]. On the other hand, in the recent paper [15] it is shown that the APN binomial $B(x)$ is a part of family of APN quadrinomials C15.

3. Equivalence between known families

Note that functions in Table 2 are given with different choices for parameters and coefficients, which in some cases can provide a huge number of different functions. In [16], the authors present a table of all possible pairwise CCZ-inequivalent functions which can be derived from the families of APN functions C1-C12, up to dimension $n=11$. According to this table, families C3 and C11 coincide on small dimensions and are contained in C4. In this section we study the equivalence between families C3 and C11. In addition, we consider two generalizations of these families, given in [24]. We show that such generalizations coincide with the original families. Note that CCZ-equivalence between quadratic APN functions reduces to EA-equivalence [33], so all the equivalences that we prove in the following sections are EA-equivalence.

We recall the conditions for families C3 and C11 in the following theorems.

Table 2
Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions.

N°	Functions	Conditions	In
C1-C2	$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk$, $\gcd(k,p) = \gcd(s,pk) = 1$, $p \in \{3,4\}$, $i = sk \bmod p$, $m = p - i$, $n \geq 12$, u primitive in $\mathbb{F}_{2^n}^*$	[10]
C3	$x^{2^{2i}+2^i} + cx^{q+1} + dx^{q(2^{2i}+2^i)}$	$q = 2^m$, $n = 2m$, $\gcd(i,m) = 1$, $\gcd(2^i+1, q+1) \neq 1$, $dc^q + c \neq 0$, $d \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$, $d^{q+1} = 1$	[9]
C4	$x(x^{2^i} + x^q + cx^{2^i q})$ $+x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q}$	$q = 2^m$, $n = 2m$, $\gcd(i,m) = 1$, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^q X + 1$ has no solution x s.t. $x^{q+1} = 1$	[9]
C5	$x^3 + a^{-1}\,Tr(a^3x^9)$	$a \neq 0$	[12]
C6	$x^3 + a^{-1}\,Tr_n^3(a^3x^9 + a^6x^{18})$	$3\|n$, $a \neq 0$	[13]
C7	$x^3 + a^{-1}\,Tr_n^3(a^6x^{18} + a^{12}x^{36})$	$3\|n$, $a \neq 0$	[13]
C8-C10	$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} +$ $vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k$, $\gcd(k,3) = \gcd(s,3k) = 1$, $v, w \in \mathbb{F}_{2^k}$, $vw \neq 1$, $3\|(k+s)$ u primitive in $\mathbb{F}_{2^n}^*$	[4,5]
C11	$dx^{2^i+1} + d^q x^{q(2^i+1)} +$ $cx^{q+1} + \sum_{s=1}^{m-1} \gamma_s x^{2^s(q+1)}$	$q = 2^m$, $n = 2m$, $\gcd(i,m) = 1$, i, m odd, $c \notin \mathbb{F}_{2^m}$, $\gamma_s \in \mathbb{F}_{2^m}$, d not a cube	[4]
C12	$(x + x^q)^{2^i+1} +$ $u'(ux + u^q x^q)^{(2^i+1)2^j} +$ $u(x + x^q)(ux + u^q x^q)$	$q = 2^m$, $n = 2m$, $m \geq 2$ even, $\gcd(i,m) = 1$ and j even u primitive in $\mathbb{F}_{2^n}^*$, $u' \in \mathbb{F}_{2^m}$ not a cube	[35]
C13	$L(x)^{2^i}x + L(x)x^{2^i}$	$n = km$, $m > 1$, $\gcd(n,i) = 1$ $L(x) = \sum_{j=0}^{k-1} a_j x^{2^{jm}}$ satisfies the conditions in Theorem 6.3 of [8]	[8]
C14	$u(u^q x + x^q u)(x^q + x) + (u^q x + x^q u)^{2^{2i}+2^{3i}}$ $+a(u^q x + x^q u)^{2^{2i}}(x^q + x)^{2^i} + b(x^q + x)^{2^i+1}$	$q = 2^m$, $n = 2m$, $\gcd(i,m) = 1$, u primitive in $\mathbb{F}_{2^n}^*$ $a, b \in \mathbb{F}_{2^m}$ and $X^{2^i+1} + aX + b$ has no solution over $\mathbb{F}_{2^m}$	[32]
C15	$x^3 + ax^{2^k(2^i+1)} + bx^{3\cdot 2^m} + cx^{2^{n+k}(2^i+1)}$	$n = 2m = 10, (a,b,c) = (\beta,0,0), i = 3, k = 2, \mathbb{F}_4^* = \langle\beta\rangle$ $n = 2m, m$ odd, $3 \not\| m, (a,b,c) = (\beta,\beta^2,1)$, $\mathbb{F}_4^* = \langle\beta\rangle$, $i \in \{m-2, m, 2m-1, (m-2)^{-1} \bmod n\}$	[15]

Theorem 3.1 *([9]). Let $n = 2m$, with $m > 1$. Let i be such that $\gcd(i, m) = 1$. Let F be the function over $\mathbb{F}_{2^n}$ defined by*

$$cx^{2^m+1} + x^{2^{2i}+2^i} + dx^{2^m(2^{2i}+2^i)} \tag{C3}$$

where $c, d \in \mathbb{F}_{2^n}$ are such that $d^{2^m+1} = 1$, $d \notin \{\lambda^{(2^i+1)(2^m-1)} : \lambda \in \mathbb{F}_{2^n}\}$ and $dc^{2^m}+c \neq 0$. Then, F is APN over $\mathbb{F}_{2^n}$.

Theorem 3.2 *([4]). Let $n = 2m$, with $m > 1$ an odd integer. Let i be an odd integer such that $\gcd(i, m) = 1$. Let F be the function over $\mathbb{F}_{2^n}$ defined by*

$$cx^{2^m+1} + \sum_{s=1}^{m-1} \gamma_s x^{2^s(2^m+1)} + dx^{2^i+1} + d^{2^m} x^{2^m(2^i+1)} \tag{C11}$$

where $c \notin \mathbb{F}_{2^m}$, $d \in \mathbb{F}_{2^n}$ not a cube and $\gamma_s \in \mathbb{F}_{2^m}$ for each s. Then, F is APN over $\mathbb{F}_{2^n}$.

Remark 3.3. Note that, it is possible to restate Theorem 3.2, i.e. to change the conditions for family C11. That is, assuming m odd and i coprime with m, the condition i odd and d not a cube is equivalent to just request $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\}$. Indeed, if i is odd, then $\{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\} = \{x^3 : x \in \mathbb{F}_{2^{2m}}\}$. If i is even, recalling that (cf. Lemma 11.1 in [30])

$$\gcd(2^i + 1, 2^n - 1) = \begin{cases} 1 & \text{if } \gcd(i, n) = \gcd(2i, n) \\ 2^{\gcd(i,n)} + 1 & \text{if } 2\gcd(i, n) = \gcd(2i, n), \end{cases}$$

we get $\{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\} = \mathbb{F}_{2^{2m}}$, implying existence of no choice for d.

The same can be done for family C3. Indeed, coefficients c and d, satisfying the constrains in Theorem 3.1, exist if and only if $\gcd(2^i + 1, 2^m + 1) \neq 1$ (see [9]). This implies that m is odd since i and m are coprime (it can be easily deduced from $\gcd(2^{2i}-1, 2^{2m}-1) = 2^{\gcd(2i,2m)} - 1 = 3$). Moreover, as shown above, if i is even we have no choice for d, so also i must be odd.

In [24], the authors generalize these two families. In the following, we report the statements of the results given in [24]. However, as we will show in the next section, the parameters of these functions need some adjustment. So we warn the reader that, instead of using the statements below that we copied from the original submission [24], one has to use the adjustments in Theorems 3.6 and 3.8. However, in view of the main result of this paper, it is not necessary to refer to these families any more since they are all included in C4.

Family C11*: Let $n = 2m$, with $m > 1$. Let i, j be such that $i > j$ and $\gcd(i - j, m) = 1$. Let F be the function over $\mathbb{F}_{2^n}$ defined by

$$cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + L(dx^{2^i+2^j} + d^{2^m} x^{2^m(2^i+2^j)}), \tag{1}$$

where $c \notin \mathbb{F}_{2^m}$, d is not in $\{x^{2^i+2^j} : x \in \mathbb{F}_{2^n}\}$, $\gamma_\ell \in \mathbb{F}_{2^m}$ for all ℓ and $L(x) = \sum_{k\in K} x^{2^k}$ such that $\{0,1\} \neq K \subseteq \{0, ..., n\}$ and $\sum_{k\in K} x^{2^k-1}$ is irreducible over $\mathbb{F}_{2^n}$. Then, F is APN over $\mathbb{F}_{2^n}$.

Family C3*: Let $n = 2m$, with $m > 1$. Let i, j be such that $i > j$ and $\gcd(i - j, m) = 1$. Let F be the function over $\mathbb{F}_{2^n}$ defined by

$$cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + L(x^{2^i+2^j}) + dL(x^{2^m(2^i+2^j)}), \tag{2}$$

where $c, d, \gamma_\ell \in \mathbb{F}_{2^n}$ are such that $d^{2^m+1} = 1$, $d \notin \{\lambda^{(2^i+2^j)(2^m-1)} : \lambda \in \mathbb{F}_{2^n}\}$, $dc^q + c \neq 0$, $d = \gamma_\ell^{1-2^m}$ for all ℓ and $L(x) = \sum_{k\in K} x^{2^k}$ such that $\{0,1\} \neq K \subseteq \{0, ..., n\}$ and $\sum_{k\in K} x^{2^k-1}$ is irreducible over $\mathbb{F}_{2^n}$. Then, F is APN over $\mathbb{F}_{2^n}$.

Note that, these types of functions are of the form (or can be reduced to)

$$F(x) = wx^{2^m+1} + Q(x), \tag{3}$$

where Q is a quadratic function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$ and $w \notin \mathbb{F}_{2^m}$. This construction for APN and differentially 4-uniform functions has been further studied in [17,18].

Remark 3.4. The general idea, used in this work, for proving the equivalence between these families is based on the fact that for any element w not in $\mathbb{F}_{2^m}$ we have $\mathbb{F}_{2^n} = w\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$. At this point, considering two functions as in (3),

$$F_1(x) = w_1 x^{2^m+1} + Q_1(x), \quad \text{and} \quad F_2(x) = w_2 x^{2^m+1} + Q_2(x),$$

to prove the equivalence we need to identify a linear permutation L for which $L(F_1(x)) = F_2(x)$. Since $\mathbb{F}_{2^n} = w_1\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m} = w_2\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$ the action of L can be given by defining the images of $w_1\mathbb{F}_{2^m}$ and of $\mathbb{F}_{2^m}$ separately. In particular, L should be such that the vector space $w_1\mathbb{F}_{2^m}$ is mapped into $w_2\mathbb{F}_{2^m}$ with the trivial action $w_1 y \mapsto w_2 y$ (for any $y \in \mathbb{F}_{2^m}$) and $L(Q_1(x)) = Q_2(x)$.

Before proving the equivalence of these families, we correct the results of [24]. Indeed, the first family when m is even cannot be APN. While, for the second one, in addition to restriction of m to be odd, in general is not APN if $L(x) \neq x^{2^k}$ (tested by MAGMA in small dimensions).

3.1. Correction of family C11 and family C3**

For family C11* we have the following result.

Proposition 3.5. *Let $n = 2m$. Let F be a function defined over $\mathbb{F}_{2^n}$ as in (1). Then, if m is even F cannot be APN.*

Proof. Consider the function

$$F(x) = cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_l x^{2^\ell(2^m+1)} + L(dx^{2^i+2^j} + d^{2^m} x^{2^m(2^i+2^j)}),$$

satisfying the properties given in (1).

First of all note that, $L(x) = x(\sum_{k\in K} x^{2^k-1})$ where $\{0,1\} \neq K \subseteq \{0,...,n\}$ and $\sum_{k\in K} x^{2^k-1}$ is irreducible over $\mathbb{F}_{2^n}$. Since $\sum_{k\in K} x^{2^k-1} \neq x+1$ we have that 0 is the only root of $L(x) = 0$. This implies that L is a linear permutation and, moreover, $L(x^{2^m}) = L(x)^{2^m}$. To prove that F cannot be APN for m even we need to prove that there exists $a \in \mathbb{F}_{2^n}$ nonzero such that

$$\Delta(x) = F(x) + F(x+a) + F(a) = 0 \tag{4}$$

admits more than two solutions.

Suppose that x is a solution of (4). Then we obtain

$$\Delta(x) + \Delta(x)^{2^m} = (c + c^{2^m})(x^{2^m}a + a^{2^m}x) = 0.$$

Since $c \notin \mathbb{F}_{2^m}$ we have $x^{2^m}a + a^{2^m}x = 0$, which implies $x = at$ for some $t \in \mathbb{F}_{2^m}$. Substituting $x = at$ in (4) we have

$$L((da^{2^i+2^j} + d^{2^m}a^{2^m(2^i+2^j)})(t^{2^i} + t^{2^j})) = 0.$$

Since L is a linear permutation, this implies that $(da^{2^i+2^j} + d^{2^m}a^{2^m(2^i+2^j)})(t^{2^i} + t^{2^j}) = 0$. Now, from the fact that $d \notin \{x^{2^i+2^j} : x \in \mathbb{F}_{2^n}\}$ the authors in [24] claim that $(da^{2^i+2^j} + d^{2^m}a^{2^m(2^i+2^j)}) \neq 0$ for all nonzero a. However, while for m odd the condition $d \notin \{x^{2^i+2^j} : x \in \mathbb{F}_{2^n}\}$ is sufficient to guarantee $da^{2^i+2^j} \notin \mathbb{F}_{2^m}$, such claim is incorrect when m is even.

Indeed, if m is even, $3 \mid (2^m-1)$ and $3 \nmid (2^m+1)$. Now, let $d = \alpha^k$, with α a primitive element of $\mathbb{F}_{2^n}$ and k some integer. Since $\gcd(i-j, m) = 1$ we have that $i-j$ is odd and thus $\gcd(2^{i-j}+1, 2^n-1) = 3$. So, finding a such that $da^{2^i+2^j} \in \mathbb{F}_{2^m}$ is equivalent to finding a' such that $da'^3 \in \mathbb{F}_{2^m}$. Let $a' = \alpha^h$, we want to determine h such that $(2^m+1) \mid (3h+k)$. Suppose $d \notin \mathbb{F}_{2^m}$, otherwise a' can be just 1. We have two cases, $k \equiv 1, 2 \mod 3$. If $k \equiv 1 \mod 3$, then $3h + k = 3(h+k') + 1$ for some k'. Since m is even $2^{m+1}+1$ is equal to $3h'$ for some h'. Thus, considering $h = h' - k'$ we would have

$3h+k = 3(h+k')+1 = 3h'+1 = 2(2^m+1)$. If $k \equiv 2 \mod 3$, then $3h+k = 3(h+k')+2$ for some k'. Since m is even 2^m-1 is equal to $3h'$ for some h'. Considering $h = h'-k'$, we would have $3h+k = 3(h+k')+2 = 3h'+2 = 2^m+1$. This concludes our proof. □

We can note that, in the previous proof, for analyzing the solutions of (4), we used only the fact that $L(x)$ is a linear permutation with coefficients over $\mathbb{F}_{2^m}$. So, we restate the conditions for family C11* as follows.

Theorem 3.6. *Let $n = 2m$ with m odd. Let i, j be such that $i > j$ and $\gcd(i-j, m) = 1$. Let F be the function over $\mathbb{F}_{2^n}$ defined by*

$$cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + L(dx^{2^i+2^j} + d^{2^m} x^{2^m(2^i+2^j)}), \tag{C11*}$$

where $c \notin \mathbb{F}_{2^m}$, d is not in $\{x^{2^i+2^j} : x \in \mathbb{F}_{2^{2m}}\}$, $\gamma_\ell \in \mathbb{F}_{2^m}$ for all ℓ and $L(x)$ a linear permutation with coefficients over $\mathbb{F}_{2^m}$. Then, F is APN over $\mathbb{F}_{2^n}$.

Remark 3.7. For the second family, some steps of the proof in [24, Theorem 2] do not work in general. When $L(x) = x^{2^k}$, family C3* results to be APN, this can be proved following the steps given in [24], which became legit when L has only one monomial.

While, if L is not of type x^{2^k}, from computational tests done using MAGMA in small dimensions, the function in (2), in general, is not APN.

More precisely, let

$$F(x) = cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + L(x^{2^i+2^j}) + dL(x^{2^m(2^i+2^j)}),$$

satisfying the properties given in (2). Then, F is APN if and only if the equation $\Delta(x) = F(x) + F(x+a) + F(a) = 0$ admits at most two solutions for any nonzero $a \in \mathbb{F}_{2^n}$. It is easy to check that

$$\Delta(x) + d\Delta(x)^{2^m} = (c + dc^{2^m})(x^{2^m}a + a^{2^m}x).$$

Thus, if x is a solution of $\Delta(x) = 0$ we have that $x = at$ for some $t \in \mathbb{F}_{2^m}$. Substituting $x = at$, we obtain

$$L(a^{2^i+2^j}(x^{2^i} + x^{2^j})) + dL(a^{2^m(2^i+2^j)}(x^{2^i} + x^{2^j})^{2^m}) = 0.$$

At this point, in [24, Theorem 2] the authors claim that

$$L(a^{2^i+2^j}(t^{2^i} + t^{2^j})) + dL(a^{2^m(2^i+2^j)}(t^{2^i} + t^{2^j})) = L((a^{2^i+2^j} + da^{2^m(2^i+2^j)})(t^{2^i} + t^{2^j})),$$

which is not true in general. For the case of $L(x) = x^{2^k}$ for some integer k, we have that

$$L(a^{2^i+2^j}(t^{2^i}+t^{2^j}))+dL(a^{2^m(2^i+2^j)}(t^{2^i}+t^{2^j}))=L((a^{2^i+2^j}+d^{2^{n-k}}a^{2^m(2^i+2^j)})(t^{2^i}+t^{2^j})).$$

So, in this case we would obtain

$$\Delta(x)=L((a^{2^i+2^j}+d^{2^{n-k}}a^{2^m(2^i+2^j)})(t^{2^i}+t^{2^j}))=0,$$

which is equivalent to $(a^{2^i+2^j}+d^{2^{n-k}}a^{2^m(2^i+2^j)})(t^{2^i}+t^{2^j})=0$. Now, $d^{2^{n-k}}\notin\{\lambda^{(2^i+2^j)(2^m-1)}:\lambda\in\mathbb{F}_{2^n}\}$ implies that $a^{2^i+2^j}+d^{2^{n-k}}a^{2^m(2^i+2^j)}\neq 0$, so we can have at most two solutions.

Thus, we consider C3* only with $L(x)=x^{2^k}$, and in this case the exponent k can be included in i and j. Moreover, as for the family C3, from the constrains on c and d we need m odd. So, in this case we have the following.

Theorem 3.8. *Let $n=2m$ with m odd. Let i,j be such that $i>j$ and $\gcd(i-j,m)=1$. Let F be the function over $\mathbb{F}_{2^n}$ defined by*

$$cx^{2^m+1}+\sum_{\ell=1}^{m-1}\gamma_\ell x^{2^\ell(2^m+1)}+x^{2^i+2^j}+dx^{2^m(2^i+2^j)}, \tag{C3*}$$

where $c,d,\gamma_\ell\in\mathbb{F}_{2^n}$ are such that $d^{2^m+1}=1$, $d\notin\{\lambda^{(2^i+2^j)(2^m-1)}:\lambda\in\mathbb{F}_{2^n}\}$, $dc^q+c\neq 0$, $d=\gamma_\ell^{1-2^m}$ for all ℓ. Then, F is APN over $\mathbb{F}_{2^n}$.

3.2. C11 and C3 are equivalent

Computational results performed in [16] for $m=3,4,5$ show that all APN functions of family C11 are equivalent to functions in C3. This leads us to the idea that family C11 is contained in family C3. In the following we are going to show that it is true, firstly showing that family C11 without the sum $\sum_{\ell=1}^{m-1}\gamma_\ell x^{2^\ell(2^m+1)}$ is equivalent to family C3, secondly that every function in family C11 is equivalent to a function in the same family without the sum.

Lemma 3.9. *Let $n=2m$, with m odd. Let i odd be such that $\gcd(i,m)=1$ and consider the APN function*

$$F(x)=cx^{2^m+1}+dx^{2^i+1}+d^{2^m}x^{2^m(2^i+1)}, \tag{5}$$

where $c\in\mathbb{F}_{2^{2m}}\setminus\mathbb{F}_{2^m}$ and $d\notin\{x^{2^i+1}:x\in\mathbb{F}_{2^{2m}}\}$. That is, F belongs to C11. Then, F is EA-equivalent to a function F' of C3.

Proof. Since $c\in\mathbb{F}_{2^{2m}}\setminus\mathbb{F}_{2^m}$ we have $\mathbb{F}_{2^{2m}}=c\mathbb{F}_{2^m}\oplus\mathbb{F}_{2^m}$. Let L be the linear permutation which is the identity map on $c\mathbb{F}_{2^m}$ and the power linear function x^{2^i} on $\mathbb{F}_{2^m}$, that is $L(cy+z)=cy+z^{2^i}$ for all $y,z\in\mathbb{F}_{2^m}$. Then, we obtain

$$F'(x) = \frac{L(F(x))}{d^{2^i}} = c'x^{2^m+1} + x^{2^{2i}+2^i} + d'x^{2^m(2^{2i}+2^i)},$$

with $c' = \dfrac{c}{d^{2^i}}$ and $d' = d^{2^i(2^m-1)}$. Since m is odd and $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\} = \{x^3 : x \in \mathbb{F}_{2^{2m}}\}$ (recall that i is odd) we have $d' \notin \{x^{(2^i+1)(2^m-1)} : x \in \mathbb{F}_{2^{2m}}\}$. Indeed, if $d' \in \{x^{(2^i+1)(2^m-1)} : x \in \mathbb{F}_{2^{2m}}\}$ we have that d' is a cube, but $3 \nmid (2^m - 1)$ and d is not a cube.

Moreover, since $c \notin \mathbb{F}_{2^m}$

$$c'^{\,2^m} d' + c' = \frac{c^{2^m}}{d^{2^i}} + \frac{c}{d^{2^i}} \neq 0,$$

implying that F in (5) is EA-equivalent to an APN function contained in C3 (F' satisfies the conditions of Theorem 3.1). □

Lemma 3.10. *Let $n = 2m$, with m odd. Let i odd be such that $\gcd(i, m) = 1$ and consider an APN function*

$$F(x) = cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + dx^{2^i+1} + d^{2^m} x^{2^m(2^i+1)}$$

as in Theorem 3.2. Then, F is EA-equivalent to a function as in (5)

$$F'(x) = c'x^{2^m+1} + d'x^{2^i+1} + d'^{\,2^m} x^{2^m(2^i+1)},$$

where c' and d' satisfy the conditions in Theorem 3.2.

Proof. Assume $1 \le t \le m-1$ be such that $\gamma_t \neq 0$. We can assume that $\gamma_t = 1$. Indeed, since $\gamma_t \in \mathbb{F}_{2^m}$, dividing F by γ_t the function F/γ_t would satisfy the hypothesis of Theorem 3.2. Consider the following linear function with $w \in \mathbb{F}_{2^m}^*$ (we will study its permutation property later)

$$L(x) = (w + (c + c^{2^m})^{2^t})x + x^{2^t} + wx^{2^m} + x^{2^{m+t}}. \tag{6}$$

Let $u = dx^{2^i+1} + d^{2^m} x^{2^m(2^i+1)} \in \mathbb{F}_{2^m}$, then we obtain

$$\begin{aligned} L(F(x)) = (w + (c + c^{2^m})^{2^t})[u + cx^{2^m+1} + \sum_{l=1}^{m-1} \gamma_l x^{2^l(2^m+1)}] \\ + u^{2^t} + c^{2^t} x^{2^t(2^m+1)} + \sum_{l=1}^{m-1} \gamma_l^{2^t} x^{2^{l+t}(2^m+1)} \\ + w[u + c^{2^m} x^{2^m+1} + \sum_{l=1}^{m-1} \gamma_l x^{2^l(2^m+1)}] \end{aligned}$$

$$
\begin{aligned}
&+ u^{2^t} + c^{2^{m+t}} x^{2^t(2^m+1)} + \sum_{l=1}^{m-1} \gamma_l^{2^t} x^{2^{l+t}(2^m+1)} \\
&= (w + (c+c^{2^m})^{2^t} + w)u + ((w + (c+c^{2^m})^{2^t})c + wc^{2^m})x^{2^m+1} \\
&\quad + (c+c^{2^m})^{2^t} x^{2^t(2^m+1)} + \sum_{l=1}^{m-1} \gamma_l (w + (c+c^{2^m})^{2^t} + w) x^{2^l(2^m+1)} \\
&= (c+c^{2^m})^{2^t} u + (w(c+c^{2^m}) + c(c+c^{2^m})^{2^t})x^{2^m+1} \\
&\quad + \sum_{l=1, l\neq t}^{m-1} \gamma_l (c+c^{2^m})^{2^t} x^{2^l(2^m+1)}
\end{aligned}
$$

Hence

$$
\frac{L(F(x))}{(c+c^{2^m})^{2^t}} = u + (w(c+c^{2^m})^{1-2^t} + c)x^{2^m+1} + \sum_{l=1, l\neq t}^{m-1} \gamma_l x^{2^l(2^m+1)}.
$$

Let $c' = w(c+c^{2^m})^{1-2^t} + c$. Also the condition $c' \notin \mathbb{F}_{2^m}$ is satisfied since we have

$$
\begin{aligned}
c'^{2^m} + c' &= w^{2^m}(c+c^{2^m})^{1-2^t} + c^{2^m} + w(c+c^{2^m})^{1-2^t} + c \\
&= (w^{2^m} + w)(c+c^{2^m})^{1-2^t} + (c+c^{2^m}) \ = \ (c+c^{2^m}).
\end{aligned}
$$

Therefore we managed, from the original general formula C11, to obtain a similar one in which the monomial $x^{2^t(2^m+1)}$ is not present any more and the rest of the components of the sum is left unchanged. If the same procedure is applied for any j such that $\gamma_j \neq 0$ we are able to obtain a function of the form (5).

Now we only need to show that $L(x)$ of equation (6) is a permutation.

We have that

$$
L(x) = (x + x^{2^m})^{2^t} + w(x + x^{2^m}) + (c + c^{2^m})^{2^t} x.
$$

Assume that $x \in \mathbb{F}_{2^m}$ then $L(x) = (c + c^{2^m})^{2^t} x$ is null if and only if $x = 0$. Otherwise consider $x \notin \mathbb{F}_{2^m}$ and let $y = x + x^{2^m} \in \mathbb{F}_{2^m}^*$, we have $L(x) = y^{2^t} + wy + (c + c^{2^m})^{2^t} x$. If $L(x) = 0$ then

$$
x = \frac{y^{2^t} + wy}{(c + c^{2^m})^{2^t}}.
$$

Since $w \in \mathbb{F}_{2^m}$ then we have that the right hand-side belongs to $\mathbb{F}_{2^m}$ that leads to a contradiction. Therefore L is a linear permutation. □

We have that C3 can be reduced to C11 reversing the computation done for (5) (an explicit computation is given in the next section when we prove that C3* is included in C11*). So we have proved:

Proposition 3.11. *Families C3 and C11 are EA-equivalent.*

3.3. C11 is equivalent to C11*

Using Remark 3.4 the equivalence is almost straightforward, however we want to make clear to the reader how to construct such equivalence. Obviously, C11 is a particular case of C11*. We show that also C11* can be reduced to C11.

Let

$$F(x) = cx^{2^m+1} + \sum_{l=1}^{m-1} \gamma_l x^{2^l(2^m+1)} + L(dx^{2^i+2^j} + d^{2^m} x^{2^m(2^i+2^j)}),$$

as in Theorem 3.6.

Without loss of generality, we can consider $j = 0$, and using the same technique as in Lemma 3.10 we can remove the summation $\sum_{l=1}^{m-1} \gamma_l x^{2^l(2^m+1)}$. Hence we end up with

$$F'(x) = c'x^{2^m+1} + L'(d'x^{2^i+1} + d'^{2^m} x^{2^m(2^i+1)}) = c'x^{2^m+1} + Q'(x), \tag{C11*}$$

for some $c' \notin \mathbb{F}_{2^m}$, $d' \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\}$ and L' is a linear permutation with coefficients over $\mathbb{F}_{2^m}$.

Therefore, as explained in Remark 3.4, with the linear map L'' which acts as the identity map on $c'\mathbb{F}_{2^m}$ and as the linear function L'^{-1} on $\mathbb{F}_{2^m}$, we obtain

$$L'' \circ F'(x) = c'x^{2^m+1} + d'x^{2^i+1} + d'^{2^m} x^{2^m(2^i+1)}.$$

Since the constrains on the coefficients are the same for C11* and C11, we have obtained our claim.

Proposition 3.12. *Families C11* and C11 are EA-equivalent.*

3.4. C3 is equivalent to C11*

Now, we show that family C3* as in Theorem 3.8, which contains C3, is equivalent to C11.

Let $n = 2m$ with m odd and consider the APN function defined over $\mathbb{F}_{2^n}$

$$F(x) = cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + x^{2^i+2^j} + dx^{2^m(2^i+2^j)},$$

where $c, d, \gamma_\ell \in \mathbb{F}_{2^n}$ satisfy the constrains of Theorem 3.8.

Since $d^{2^m+1} = 1$, there exists d' such that ${d'}^{2^m-1} = d$. Moreover, since d is not contained in $\{x^{(2^i+2^j)(2^m-1)} : x \in \mathbb{F}_{2^{2m}}\}$ we have $d' \notin \{x^{(2^i+2^j)} : x \in \mathbb{F}_{2^{2m}}\}$.

Multiplying F by d', we obtain

$$F'(x) = d'F(x) = d'cx^{2^m+1} + \sum_{\ell=1}^{m-1} d'\gamma_\ell x^{2^\ell(2^m+1)} + d'x^{2^i+2^j} + {d'}^{2^m} x^{2^m(2^i+2^j)}.$$

Since $c + c^{2^m}d \neq 0$ we have that $d'c + (d'c)^{2^m} = d'(c + c^{2^m}d) \neq 0$, so $d'c \notin \mathbb{F}_{2^m}$. Moreover, since $d = \gamma_\ell^{1-2^m}$ for all ℓ such that $\gamma_\ell \neq 0$, we have that $(d'\gamma_\ell)^{2^m} = d'(d\gamma_\ell^{2^m}) = d'(\gamma_\ell^{1-2^m}\gamma_\ell^{2^m})$ which implies $d'\gamma_\ell \in \mathbb{F}_{2^m}$ for all γ_ℓ. Thus, $F'(x)$ is an element of C11*, which is EA-equivalent to C11 from Proposition 3.12. Then, from Proposition 3.11 we can conclude the following.

Proposition 3.13. *Families C11 and C3* are EA-equivalent.*

We summarize our results in the following theorem.

Theorem 3.14. *Families C3, C11, C3* and C11* are all EA-equivalent to each other.*

We conclude this section showing that, for any fixed i, all the functions contained in these families are EA-equivalent to each other.

Proposition 3.15. *Let $n = 2m$ with m odd and let i be such that $\gcd(n, i) = 1$. Let*

$$F(x) = cx^{2^m+1} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}, \quad F'(x) = c'x^{2^m+1} + d'x^{2^i+1} + {d'}^{2^m}x^{2^m(2^i+1)}$$

be two APN functions of family C11, that is, $c, c' \notin \mathbb{F}_{2^m}$ and $d, d' \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^n}\}$. Then, F and F' are affine equivalent.

Proof. Let us fix d not a cube, consider $c, c' \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and the functions

$$F(x) = cx^{2^m+1} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)} \text{ and } F'(x) = c'x^{2^m+1} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}.$$

Then, considering the linear permutation L which is the identity on $\mathbb{F}_{2^m}$ and that maps $c\mathbb{F}_{2^m}$ into $c'\mathbb{F}_{2^m}$, we immediately have $L \circ F = F'$.

Now, let us fix the coefficient $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and d not a cube. Consider the two functions

$$F(x) = cx^{2^m+1}+dx^{2^i+1}+d^{2^m}x^{2^m(2^i+1)} \text{ and } F'(x) = cx^{2^m+1}+d^2x^{2^i+1}+(d^2)^{2^m}x^{2^m(2^i+1)}.$$

Then, we have that

$$F(x^{1/2})^2 = c^2x^{2^m+1} + d^2x^{2^i+1} + (d^2)^{2^m}x^{2^m(2^i+1)}$$

is equivalent to F' from the argument above. Thus, F is equivalent to F'.

Now, let $U = \{x^{2^i+1} : x \in \mathbb{F}_{2^n}^*\} = \{x^3 : x \in \mathbb{F}_{2^n}^*\}$ (i is odd), for any $u \in U$,

$$F(x) = cx^{2^m+1} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}$$

and

$$F'(x) = cx^{2^m+1} + dux^{2^i+1} + (du)^{2^m}x^{2^m(2^i+1)}$$

are equivalent. Indeed, we can apply the substitution $x \mapsto \lambda x$ for some $\lambda \in \mathbb{F}_{2^n}^*$ such that $\lambda^{2^i+1} = u$, and we have that $F(\lambda x) = c\lambda^{2^m+1}x^{2^m+1} + dux^{2^i+1} + (du)^{2^m}x^{2^m(2^i+1)}$ is equivalent to $F'(x)$.

Now, since we can partition all non-cube elements as $dU \cup d^2U$ for some d not a cube, from the arguments above we have our claim. □

3.5. Equivalence with hexanomials (family C4 in Table 2)

The following family of APN hexanomials was constructed in [9].

Theorem 3.16 *([9]). Let n and i be any positive integers, $n = 2m$, $\gcd(i, m) = 1$, and $\bar{c}, \bar{d} \in \mathbb{F}_{2^n}$ be such that $\bar{d} \notin \mathbb{F}_{2^m}$. Then, the function*

$$H(x) = \bar{d}x^{2^i(2^m+1)} + x^{(2^m+1)} + x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m}$$

is APN if and only if the equation

$$x^{2^i+1} + \bar{c}x^{2^i} + \bar{c}^{2^m}x + 1 = 0$$

has no solution x such that $x^{2^m+1} = 1$.

The existence of coefficients $\bar{c}$ satisfying the conditions of the theorem above has been studied in [3]. In [27], Göloğlu characterizes and computes the number of such $\bar{c}$'s.

The family of hexanomials given in the previous theorem can be expressed as pentanomials.

Lemma 3.17. *Let n and i be positive integers such that $n = 2m$ and $\gcd(i, m) = 1$. Let*

$$P(x) = \bar{d}x^{(2^m+1)} + x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m},$$

with $\bar{c}, \bar{d} \in \mathbb{F}_{2^n}$ be such that $\bar{d} \notin \mathbb{F}_{2^m}$. Then, P is APN if and only if the equation

$$x^{2^i+1} + \bar{c}x^{2^i} + \bar{c}^{2^m}x + 1 = 0$$

has no solution x such that $x^{2^m+1} = 1$.

Moreover, the family of hexanomials given in Theorem 3.16 and this family of pentanomials are EA-equivalent.

Proof. The APN property of the pentanomial P can be proved following the same steps of [9, Theorem 2]. Thus, we prove only the equivalence between the two families.

Let

$$H(x) = \bar{d}x^{2^i(2^m+1)} + x^{(2^m+1)} + x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m}$$

as in Theorem 3.16. Applying the linear permutation (as in (6)) $L(x) = (w + (\bar{d} + \bar{d}^{2^m})^{2^{n-i}})x + wx^{2^m} + x^{2^{n-i}} + x^{2^{m-i}}$ with $w = (\bar{d} + \bar{d}^{2^m})^{2^{n-i}-1} \in \mathbb{F}_{2^m}^*$, we obtain

$$H'(x) = \frac{L(H(x))}{(\bar{d} + \bar{d}^{2^m})^{2^{n-i}}} = \bar{d}'x^{2^i(2^m+1)} + x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m},$$

where $\bar{d}' = w(\bar{d} + \bar{d}^{2^m})^{1-2^{n-i}} + \bar{d} = 1 + \bar{d} \notin \mathbb{F}_{2^m}$. Since $\mathbb{F}_{2^{2m}} = \bar{d}'\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$ we can apply a linear permutation which is $x^{2^{n-i}}$ on $\bar{d}'\mathbb{F}_{2^m}$ and the identity on $\mathbb{F}_{2^m}$ in order to obtain the EA-equivalent function

$$P(x) = d''x^{2^m+1} + x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m},$$

where $d'' = 1 + \bar{d}^{2^{n-i}}$. Thus, we have that the hexanomial with coefficients $\bar{d}$ and $\bar{c}$ can be reduced to the pentanomial with coefficients $1 + \bar{d}^{2^{n-i}}$ and $\bar{c}$.

On the other hand, let

$$P(x) = \bar{d}x^{2^m+1} + x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m}$$

be APN with $\bar{d} \notin \mathbb{F}_{2^m}$. Then, there exist $\bar{d}' \notin \mathbb{F}_{2^m}$ such that $\bar{d} = 1 + \bar{d}'^{2^{n-i}}$. Thus, since we used linear permutations for reducing an hexanomial to a pentanomial, we can reverse the steps above and we would obtain the APN hexanomial

$$H(x) = \bar{d}'x^{2^i(2^m+1)} + x^{(2^m+1)} + x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m}.$$

Then, the two families coincide. □

We are going to show below that C11 (and thus C3) is contained in C4.

Without loss of generality, from the arguments given in Lemma 3.10, we can consider functions of the form

$$F(x) = cx^{2^m+1} + x^{2^i(2^m+1)} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}, \tag{7}$$

with $c \in \mathbb{F}_{2^{2m}} \setminus \mathbb{F}_{2^m}$ and $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\}$.

Consider a linear permutation of the type $x + \gamma x^{2^m}$ $(\gamma^{2^m+1} \neq 1)$. Evaluating $F(x + \gamma x^{2^m})$ and deleting terms of algebraic degree less than 2, we obtain

$$\widetilde{F}(x) = \begin{array}{l} (c + c\gamma^{2^m+1})x^{2^m+1} + (1 + \gamma^{2^i(2^m+1)})x^{2^i(2^m+1)} \\ \left.\begin{array}{l} +(d + d^{2^m}\gamma^{2^m(2^i+1)})x^{2^i+1} + (d^{2^m} + d\gamma^{2^i+1})x^{2^m(2^i+1)} \\ +(d\gamma^{2^i} + d^{2^m}\gamma^{2^m})x^{2^{m+i}+1} + (d^{2^m}\gamma^{2^{m+i}} + d\gamma)x^{2^i+2^m} \end{array}\right\} = u. \end{array}$$

Now, using a linear permutation as in (6), it is possible to delete the monomial $(1 + \gamma^{2^i(2^m+1)})x^{2^i(2^m+1)}$ since $(1+\gamma^{2^i(2^m+1)})$ and u are in $\mathbb{F}_{2^m}$. Indeed, let $\gamma' = (1+\gamma^{2^i(2^m+1)})$ and $L(x) = (w+(c+c^{2^m})^{2^i}\frac{\gamma'}{\gamma'^{2^i}})x+x^{2^i}+wx^{2^m}+x^{2^{m+i}}$ for some $w \in \mathbb{F}_{2^m}^*$. Then, following the same steps as in Lemma 3.10, we have

$$F'(x) = \frac{L(\widetilde{F}(x)/\gamma')}{\left(\frac{c}{\gamma'} + \frac{c^{2^m}}{\gamma'}\right)^{2^i}} = c'x^{2^m+1} + u,$$

for some $c' \notin \mathbb{F}_{2^m}$ depending on L. Denoting by $a = (d + d^{2^m}\gamma^{2^m(2^i+1)})$ and $b = (d\gamma^{2^i} + d^{2^m}\gamma^{2^m})$ we get

$$F'(x) = c'x^{2^m+1} + (ax^{2^i+1} + a^{2^m}x^{2^m(2^i+1)} + bx^{2^{m+i}+1} + b^{2^m}x^{2^i+2^m}). \tag{8}$$

Now, since i and m are odd and $\gcd(i, m) = 1$, $x^{2^{m+i}+1}$ is a permutation of $\mathbb{F}_{2^n}$, which means that there exists $\lambda \in \mathbb{F}_{2^n}^*$ such that $\lambda^{2^{m+i}+1} = b$. Then, substituting $x \mapsto \lambda^{-1}x$ in (8), we obtain

$$F''(x) = \underbrace{c''x^{2^m+1}}_{c''\mathbb{F}_{2^m}} + \underbrace{\frac{a}{\lambda^{2^i+1}}x^{2^i+1} + \left(\frac{a}{\lambda^{2^i+1}}\right)^{2^m} x^{2^m(2^i+1)} + x^{2^{m+i}+1} + x^{2^i+2^m}}_{\mathbb{F}_{2^m}},$$

where $c'' = c'/\lambda^{2^m+1}$. Since $\mathbb{F}_{2^n} = c''\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$ we can perform a substitution $x \mapsto x^{2^{m-i}}$ and then apply a linear map L which is $x^{2^{m+i}}$ on $c''\mathbb{F}_{2^m}$ and the identity on $\mathbb{F}_{2^m}$. Thus, denoting by $\tilde{c} = (c'')^{2^{m+i}}$, we obtain the EA-equivalent function

$$\bar{F}(x) = L(F''(x^{2^{m-i}})) = \tilde{c}x^{2^m+1} + \frac{a}{\lambda^{2^i+1}}x^{2^m+2^j} + \left(\frac{a}{\lambda^{2^i+1}}\right)^{2^m} x^{(2^{m+j}+1)} + x^{2^j+1} + x^{2^m(2^j+1)}, \tag{9}$$

where $j = m - i$ is even and $\gcd(j, m) = 1$.

Denoting $\bar{a} = \left(\frac{a}{\lambda^{2^i+1}}\right)^{2^m}$, since $\bar{F}(x)$ is APN and $c'' \notin \mathbb{F}_{2^m}$ from Lemma 3.17 we have that

$$x^{2^j+1} + \bar{a}x^{2^j} + \bar{a}^{2^m}x + 1 = 0$$

Table 3
Refined list of known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions.

N°	Functions	Conditions	In
F1-F2	$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk$, $\gcd(k, p) = \gcd(s, pk) = 1$, $p \in \{3, 4\}$, $i = sk \bmod p$, $m = p - i$, $n \geq 12$, u primitive in $\mathbb{F}_{2^n}^*$	[10]
F3	$sx^{q+1} + x^{2^i+1} + x^{q(2^i+1)}$ $+cx^{2^iq+1} + c^q x^{2^i+q}$	$q = 2^m$, $n = 2m$, $\gcd(i, m) = 1$, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^q X + 1$ has no solution x s.t. $x^{q+1} = 1$	[9]
F4	$x^3 + a^{-1}\,Tr(a^3x^9)$	$a \neq 0$	[12]
F5	$x^3 + a^{-1}\,Tr_n^3(a^3x^9 + a^6x^{18})$	$3\|n$, $a \neq 0$	[13]
F6	$x^3 + a^{-1}\,Tr_n^3(a^6x^{18} + a^{12}x^{36})$	$3\|n$, $a \neq 0$	[13]
F7-F9	$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} +$ $vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k$, $\gcd(k, 3) = \gcd(s, 3k) = 1$, $v, w \in \mathbb{F}_{2^k}$, $vw \neq 1$, $3\|(k + s)$ u primitive in $\mathbb{F}_{2^n}^*$	[4,5]
F10	$(x + x^{2^m})^{2^i+1} +$ $u'(ux + u^{2^m}x^{2^m})^{(2^i+1)2^j} +$ $u(x + x^{2^m})(ux + u^{2^m}x^{2^m})$	$n = 2m$, $m \geq 2$ even, $\gcd(i, m) = 1$ and $j \geq 2$ even u primitive in $\mathbb{F}_{2^n}^*$, $u' \in \mathbb{F}_{2^m}$ not a cube	[35]
F11	$L(x)^{2^i}x + L(x)x^{2^i}$	$n = km$, $m > 1$, $\gcd(n, i) = 1$ $L(x) = \sum_{j=0}^{k-1} a_j x^{2^{jm}}$ satisfies the conditions in Theorem 6.3 of [8]	[8]
F12	$u(u^qx + x^qu)(x^q + x) + (u^qx + x^qu)^{2^{2i}+2^{3i}}$ $+a(u^qx + x^qu)^{2^{2i}}(x^q + x)^{2^i} + b(x^q + x)^{2^i+1}$	$q = 2^m$, $n = 2m$, $\gcd(i, m) = 1$, u primitive in $\mathbb{F}_{2^n}^*$ $X^{2^i+1} + aX + b$ has no solution over $\mathbb{F}_{2^m}$	[32]
F12	$x^3 + ax^{2^k(2^i+1)} + bx^{3\cdot 2^m} + cx^{2^{n+k}(2^i+1)}$	$n = 2m = 10, (a, b, c) = (\beta, 0, 0), i = 3, k = 2, \mathbb{F}_4^* = \langle\beta\rangle$ $n = 2m, m$ odd, $3 \nmid m, (a, b, c) = (\beta, \beta^2, 1)$, $\mathbb{F}_4^* = \langle\beta\rangle$, $i \in \{m - 2, m, 2m - 1, (m - 2)^{-1} \mod n\}$	[15]

has no nonzero solution such that $x^{2^m+1}=1$. Hence, the function $\bar{F}(x)$ is equivalent to a pentanomial (and thus to an hexanomial) as in Lemma 3.17.

Therefore, we have proved the following result:

Theorem 3.18. *The families C3, C3*, C11 and C11* coincide and they are included in C4. In particular, the hexanomials admit a representation as pentanomials in the following form*

$$P(x)=\bar{d}x^{2^m+1}+x^{2^i+1}+x^{2^m(2^i+1)}+\bar{c}x^{2^{m+i}+1}+\bar{c}^{2^m}x^{2^i+2^m},$$

satisfying the conditions in Lemma 3.17.

Moreover, when m and i are odd, $P(x)$ is EA-equivalent to a pentanomial of type

$$\bar{P}(x)=dx^{2^m+1}+x^{2^j+1}+x^{2^m(2^j+1)}+cx^{2^{m+j}+1}+c^{2^m}x^{2^j+2^m},$$

where d and c satisfy the same conditions of $\bar{d}$ and $\bar{c}$ above, and $j=m-i$.

Proof. We need to prove only that when m is odd the case i odd is equivalent to a pentanomial relative to the even case $j=m-i$. This can be done with the same steps as used above to compute $\bar{F}(x)$ in (9) from $F''(x)$ of (8), with the only difference that in this case the coefficient a of $F''(x)$ is equal to 1. □

4. Conclusion

In this paper we proved that, after corrections, the generalizations introduced in [24] of the families of APN trinomials and multinomials constructed in [9] and in [4], respectively, coincide with the original families. Moreover, we showed that the APN trinomials and multinomials are EA-equivalent to each other and they are contained in the family of the APN hexanomials, introduced in [9].

Using the obtained results we reduce the list of known families of APN polynomials (which are CCZ-inequivalent to power functions) to those pairwise CCZ-inequivalent to each other. This refined list is presented in Table 3.

Acknowledgments

The research of this paper was supported by Trond Mohn Foundation.

References

[1] T. Beth, C. Ding, On almost perfect nonlinear permutations, in: Advances in Cryptology-EUROCRYPT'93, in: Lecture Notes in Computer Science, vol. 765, Springer-Verlag, New York, 1993, pp. 65–76.

[2] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, J. Cryptol. 4 (1) (1991) 3–72.

[3] A.W. Bluher, On existence of Budaghyan-Carlet APN hexanomials, Finite Fields Appl. 24 (2013) 118–123.

[4] C. Bracken, E. Byrne, N. Markin, G. McGuire, New families of quadratic almost perfect nonlinear trinomials and multinomials, Finite Fields Appl. 14 (3) (2008) 703–714.

[5] C. Bracken, E. Byrne, N. Markin, G. McGuire, A few more quadratic APN functions, Cryptogr. Commun. 3 (1) (2011) 43–53.

[6] J. Bierbrauer, G.M. Kyureghyan, Crooked binomials, Des. Codes Cryptogr. 46 (2008) 269–301.

[7] M. Brinkmann, G. Leander, On the classification of APN functions up to dimension five, Des. Codes Cryptogr. 49 (1–3) (2008) 273–288.

[8] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, I. Villa, Constructing APN functions through isotopic shift, IEEE Trans. Inf. Theory (2020), https://doi.org/10.1109/TIT.2020.2974471.

[9] L. Budaghyan, C. Carlet, Classes of quadratic APN trinomials and hexanomials and related structures, IEEE Trans. Inf. Theory 54 (5) (2008) 2354–2357.

[10] L. Budaghyan, C. Carlet, G. Leander, Two classes of quadratic APN binomials inequivalent to power functions, IEEE Trans. Inf. Theory 54 (9) (2008) 4218–4229.

[11] L. Budaghyan, C. Carlet, G. Leander, On inequivalence between known power APN functions, in: O. Masnyk-Hansen, J.-F. Michon, P. Valarcher, J.-B. Yunes (Eds.), Proceedings of the Conference BFCA'08, Copenhagen.

[12] L. Budaghyan, C. Carlet, G. Leander, Constructing new APN functions from known ones, Finite Fields Appl. 15 (2) (2009) 150–159.

[13] L. Budaghyan, C. Carlet, G. Leander, On a construction of quadratic APN functions, in: Proceedings of IEEE Information Theory Workshop, ITW'09, Oct. 2009, pp. 374–378.

[14] 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.

[15] L. Budaghyan, T. Helleseth, N. Kaleyski, A new family of APN quadrinomials, Cryptology ePrint Archive, Report 2019/994.

[16] L. Budaghyan, T. Helleseth, N. Li, B. Sun, Some results on the known classes of quadratic APN functions, in: S. El Hajji, A. Nitaj, E. Souidi (Eds.), Codes, Cryptology and Information Security, C2SI 2017, in: Lecture Notes in Computer Science, vol. 10194, Springer, Cham, 2017, pp. 3–16.

[17] C. Carlet, Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions, Des. Codes Cryptogr. 59 (1–3) (2009) 89–109.

[18] C. Carlet, More constructions of APN and differentially 4-uniform functions by concatenation, Sci. China Math. 56 (7) (2013) 1373–1384.

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

[20] U. Dempwolff, CCZ equivalence of power functions, Des. Codes Cryptogr. 86 (3) (2018) 665–692.

[21] H. Dobbertin, Almost perfect nonlinear power functions over $GF(2^n)$: the Welch case, IEEE Trans. Inf. Theory 45 (1999) 1271–1275.

[22] H. Dobbertin, Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case, Inf. Comput. 151 (1999) 57–72.

[23] H. Dobbertin, Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5, in: Proceedings of Finite Fields and Applications FQ5, 2000, pp. 113–121.

[24] X.Y. Duan, Y.L. Deng, Two classes of quadratic crooked functions, Appl. Mech. Mater. 513–517 (2014) 2734–2738.

[25] Y. Edel, G.M. Kyureghyan, A. Pott, A new APN function which is not equivalent to a power mapping, IEEE Trans. Inf. Theory 52 (2006) 744–747.

[26] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, IEEE Trans. Inf. Theory 14 (1968) 154–156.

[27] F. Göloğlu, Almost perfect nonlinear trinomials and hexanomials, Finite Fields Appl. 33 (2015) 258–282.

[28] H. Janwa, R. Wilson, Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes, in: Proceedings of AAECC-10, in: LNCS, vol. 673, Springer-Verlag, Berlin, 1993, pp. 180–194.

[29] T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes, Inf. Control 18 (1971) 369–394.

[30] R.J. McEliece, Finite Fields for Computer Scientists and Engineers, Kluwer Academic Publishers, 1987.

[31] K. Nyberg, Differentially uniform mappings for cryptography, in: Advances in Cryptography, EUROCRYPT'93, in: Lecture Notes in Computer Science, vol. 765, 1994, pp. 55–64.
[32] H. Taniguchi, On some quadratic APN functions, Des. Codes Cryptogr. 87 (2019) 1973–1983.
[33] S. Yoshiara, Equivalences of quadratic APN functions, J. Algebraic Comb. 35 (2012) 461–475.
[34] S. Yoshiara, Equivalences of power APN functions with power or quadratic APN functions, J. Algebraic Comb. 44 (3) (2016) 561–585.
[35] Y. Zhou, A. Pott, A new family of semifields with 2 parameters, Adv. Math. 234 (2013) 43–60.