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

L. Budaghyan[a], M. Calderini[a], I. Villa[a]

[a] *Department of informatics, University of Bergen*

**Abstract**

We study 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 CCZ-equivalent to 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 CCZ-equivalent to the family of hexanomials as well.

**Keywords**: CCZ-equivalence, EA-equivalence, APN, Boolean functions
*MSC*: 94A60, 06E30, 11T71

## 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 $2^m$ 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 [1], is among the most efficient attacks on block cipher. To measure the resistance of an S-box to this attack, in [26], Nyberg introduced the notion of *differential uniformity*. A vectorial Boolean function $F$ is called differentially $\delta$-uniform if the equation $F(x) + F(x + a) = b$ has at most $\delta$ solutions for any non-zero $a$ and for all $b$. The smallest possible values for $\delta$ is 2, and functions achieving such differential uniformity are called *almost perfect nonlinear* (APN).

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

*Email addresses:* lilya.budaghyan@uib.no (L. Budaghyan), marco.calderini@uib.no (M. Calderini), irene.villa@uib.no (I. Villa)

Boolean function 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 more 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 $n \leq 5$ [5]. There are only few infinite classes of APN functions known: six classes of power functions and 14 classes of quadratic polynomials CCZ-inequivalent to monomials presented in Tables 1 and 2. When constructed some of these 14 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 [7] and the class of multinomials studied in [2] are equivalent. Moreover, we prove that also their generalizations given in [19] coincide with the original ones. Finally we show that these classes can be reduced to the hexanomials introduced in [7]. According to the table of all CCZ-inequivalent functions which arise from known APN families (in dimensions up to 11) [13], the remained families of APN functions are pairwise inequivalent in general. We present 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 will 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 mappings $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ 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 [14]. Moreover, every permutation is CCZ-equivalent to its inverse [14]. As proven in [12], 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 the functions in Table 1 were proven in [9]. Recently, in both [28] and [15] Yoshiara and Dempwolff show that two APN power 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 the EA-equivalence, and families in Table 1 have different algebraic degrees in general, then all these families differ up to CCZ-equivalence (although they can intersect in some particular cases). There are also fourteen known infinite families of quadratic APN polynomials CCZ-inequivalent to power functions listed in Table 2. W will show that this list can be reduced to 12 pairwise CCZ-inequivalent families represented in Table 3.

## 3. Equivalence between known families

In [13], the authors present a table of all possible pairwise CCZ-inequivalent functions which can be derived from the known families of APN functions, up to dimension $n = 11$.

Table 1: Known APN power functions $x^d$ over $\mathbb{F}_{2^n}$

| Functions | Exponents $d$ | Conditions | Degree | In |
|---|---|---|---|---|
| Golden | $2^i+1$ | $\gcd(i,n)$=1 | 2 | [21, 26] |
| Kasami | $2^{2i}-2^i+1$ | $\gcd(i,n)$=1 | $i$+1 | [23, 24] |
| Welch | $2^t+3$ | $n=2t+1$ | 3 | [16] |
| Niho | $2^t+2^{\frac{t}{2}}-1$, $t$ even<br>$2^t+2^{\frac{3t+1}{2}}-1$, $t$ odd | $n=2t+1$ | $\frac{t+2}{2}$<br>$t$+1 | [17] |
| Inverse | $2^{2t}-1$ | $n=2t+1$ | $n-1$ | [4, 26] |
| Dobbertin | $2^{4i}+2^{3i}+2^{2i}+2^i-1$ | $n=5i$ | $i+3$ | [18] |

According to this table, families C3 and C11 coincide on small dimensions and are contained in C4. In this section we will study the equivalence between families C3 and C11. Moreover, we will consider also two generalizations of these families given in [19]. We will show that such generalizations coincide with the original families.

First of all, note that, considering family C11, for $i$ such that $\gcd(i,m)=1$ the condition given in Table 2, that is, $i$ odd and $d$ not a cube is equivalent to request just $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\}$ (recall that $m$ is odd). 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 [25])

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

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

Moreover, for family C3, we have that coefficients $c$ and $d$ satisfying the constrains in Table 2 exist if and only if $\gcd(2^i+1, 2^m+1) \neq 1$ (see [7]). 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 above, if $i$ is even we have no choice for $d$, so also $i$ must be odd.

The generalizations of these families, given in [19], are the following

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

defined over $\mathbb{F}_{2^{2m}}$ where $m, i$ and $j$ integers such that $\gcd(i-j,m)=1$ $(i>j)$, $\gamma_\ell \in \mathbb{F}_{2^m}$ for all $\ell$, $c \notin \mathbb{F}_{2^m}$, $d$ is not in $\{x^{2^i+2^j} : x \in \mathbb{F}_{2^{2m}}\}$ 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.

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

| $N^\circ$ | 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 $\mathbb{F}_{2^n}^*$ | [8] |
| C3 | $x^{2^{2i}+2^i}+cx^{q+1}+dx^{q(2^{2i}+2^i)}$ | $q=2^m$, $n=2m$, $\gcd(i,m)=1$, $\gcd(2^i+1,q+1)\neq 1$, $dc^q+c\neq 0$, $d\notin\{\lambda^{(2^i+1)(q-1)},\lambda\in\mathbb{F}_{2^n}\}$, $d^{q+1}=1$ | [7] |
| C4 | $x(x^{2^i}+x^q+cx^{2^iq})$ $+x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$ | $q=2^m$, $n=2m$, $\gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}$, $s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q$, $X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution $x$ s.t. $x^{q+1}=1$ | [7] |
| C5 | $x^3+a^{-1}Tr(a^3x^9)$ | $a\neq 0$ | [10] |
| C6 | $x^3+a^{-1}Tr_n^3(a^3x^9+a^6x^{18})$ | $3\|n$, $a\neq 0$ | [11] |
| C7 | $x^3+a^{-1}Tr_n^3(a^6x^{18}+a^{12}x^{36})$ | $3\|n$, $a\neq 0$ | [11] |
| 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 $\mathbb{F}_{2^n}^*$ | [2, 3] |
| C11 | $dx^{2^i+1}+d^qx^{q(2^i+1)}+$ $cx^{q+1}+\sum_{s=1}^{m-1}\gamma_sx^{2^s(q+1)}$ | $q=2^m$, $n=2m$, $\gcd(i,m)=1$, $i,m$ odd, $c\notin\mathbb{F}_{2^m}$, $\gamma_s\in\mathbb{F}_{2^m}$, $d$ not a cube | [2] |
| C12 | $(x+x^q)^{2^i+1}+$ $u'(ux+u^qx^q)^{(2^i+1)2^j}+$ $u(x+x^q)(ux+u^qx^q)$ | $q=2^m$, $n=2m$, $m\geq 2$ even, $\gcd(i,m)=1$ and $j$ even $u$ primitive in $\mathbb{F}_{2^n}^*$, $u'\in\mathbb{F}_{2^m}$ not a cube | [29] |
| C13 | $a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+$ $ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$ | $n=3m$, $m$ odd $L(x)=ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions in Theorem 6.3 of [6] | [6] |
| C14 | $u(u^qx+x^qu)(x^q+x)+(u^qx+x^qu)^{2^{2i}+2^{3i}}$ $+a(u^qx+x^qu)^{2^{2i}}(x^q+x)^{2^i}+b(x^q+x)^{2^i+1}$ | $q=2^m$, $n=2m$, $\gcd(i,m)=1$ $a,b\in\mathbb{F}_{2^m}$ and $X^{2^i+1}+aX+b$ has no solution over $\mathbb{F}_{2^m}$ | [27] |

The second APN family introduced in [19] is given by

$$cx^{2^m+1}+\sum_{\ell=1}^{m-1}\gamma_\ell x^{2^\ell(2^m+1)}+L(x^{2^i+2^j})+dL(x^{2^m(2^i+2^j)}), \qquad \text{(C3*)}$$

such that $m, i$ and $j$ are integers with the same properties as above, $L(x) = \sum_{k\in K} x^{2^k}$ such that $\{0,1\} \neq K \subseteq \{0,...,n\}$ and $\sum_{k\in K} x^{2^k-1}$ is irreducible and the coefficients $c, d$ and $\gamma_\ell$'s such that $c+c^{2^m}d \neq 0$, $d$ not in $\{x^{2^i+2^j} : x \in \mathbb{F}_{2^{2m}}\}$ and $d = \gamma_\ell^{1-2^m}$ for all $\ell$ such that $\gamma_\ell \neq 0$.

Before proving the equivalence with C3 and C11, we will correct the results of [19]. 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 it seems to be not APN if $L(x) \neq x^{2^k}$ (tested by MAGMA in small dimensions).

### *3.1.* Correction of family C11* and family C3*

Consider the function

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

First of all note that from the conditions above we have that $L$ is a linear permutation, indeed we can directly suppose that $L$ is any linear permutation with coefficients in $\mathbb{F}_{2^m}$.

Following the proof given in [19] we have that if the equation

$$\Delta(x) = F(x) + F(x+a) + F(a) = 0$$

has solution $x$, then $x = at$ with $t \in \mathbb{F}_{2^m}$ (obtained from $\Delta(x) + (\Delta(x))^{2^m} = 0$), which reduces the equation above to the condition

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

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 $d \notin \{x^{2^i+2^j} : x \in \mathbb{F}_{2^{2m}}\}$ the authors in [19] 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 $d \notin \{x^{2^i+2^j} : x \in \mathbb{F}_{2^{2m}}\}$ is sufficient to guarantee $da^{2^i+2^j} \notin \mathbb{F}_{2^m}$, such claim is incorrect when $m$ is even.

We will prove that, when $m$ is even, for any $d$ there exists $a \in \mathbb{F}^*_{2^{2m}}$ such that $da^{2^i+2^j} \in \mathbb{F}_{2^m}$. Indeed, if $m$ is even, then $3 \mid (2^m - 1)$ and $3 \nmid (2^m + 1)$. Now, let $d = \alpha^k$, with $\alpha$ a primitive element of $\mathbb{F}_{2^{2m}}$, 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 $h'$, thus considering $h = h' - k'$ we would have $3h + k = 3(h + k') + 2 = 3h' + 2 = 2^m + 1$. This concludes our proof. So

the first family of functions needs the restriction of $m$ odd.

For the second family, the steps of the proof in [19, 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 [19], 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 (C3*) in general is not APN. Thus, we will consider (C3*) only with $L(x) = x^{2^k}$.

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

such that $m, i$ and j integers with the same properties as above and the coefficients $c, d$ and $\gamma_\ell$'s are such that $c + c^{2^m} d \neq 0$, $d$ not in $\{x^{(2^i+2^j)(2^m-1)} : x \in \mathbb{F}_{2^{2m}}\}$ and $d = \gamma_\ell^{1-2^m}$ for all $\ell$ such that $\gamma_\ell \neq 0$. We dropped the exponent $2^k$ of the linear function $L$ because $k$ can be included in $i$ and $j$. Note that, as for C3, from the constrains on $c$ and $d$ we need $m$ odd.

### *3.2.* C11 and C3 are equivalent

Computational results performed in [13] for $m = 3, 4, 5$ show that all APN functions of family C11 are equivalent to functions of 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.

Let us consider a simplified version of C11, without the sum component,

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

Since $c \in \mathbb{F}_{2^{2m}} \setminus \mathbb{F}_{2^m}$ we have $\mathbb{F}_{2^{2m}} = c\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$. Then, considering the linear function $L$ which is the identity map on $c\mathbb{F}_{2^m}$ and the power linear function $x^{2^i}$ on $\mathbb{F}_{2^m}$ we obtain

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

with $c' = \dfrac{c}{d^{2^i}}$ and $d' = d^{2^i(2^m-1)}$. Since, $m$ is odd and $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\}$ 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 (1) is equivalent to an APN function contained in C3.

Consider now the general formula for C11:

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

we will show that it is possible to reduce it to a function of the type (1).
Assume $1 \leq t \leq m-1$ be such that $\gamma_t \neq 0$. We can suppose that $\gamma_t = 1$. Indeed, since $\gamma_t \in \mathbb{F}_{2^m}$, there exists a non-zero element $\lambda_t$ such that $\gamma_t = \lambda_t^{2^t(2^m+1)}$. Applying the substitution $x \to \lambda_t^{-1} x$ we obtain an equivalent function such that $\gamma_t = 1$.
Consider the following linear function with $w \in \mathbb{F}_{2^m}^*$ (we will study its permutation property later)

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

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

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

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 on $c'$ 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 (1).

Now we only need to show that $L(x)$ of equation (2) 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 (1) (an explicit computation is given in the next section when we prove that (C3*) is included in (C11*)). So we have proved:

**Lemma 3.1.** *Families C3 and C11 are equivalent.*

### *3.3.* (C11*) is equivalent to C11

Obviously, C11 is a particular case of (C11*). However, also (C11*) can be reduced to C11.

Let us consider

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

satisfying the constrains of (C11*). First of all, we can suppose that $j$ is equal to 0, otherwise we can just include the power $2^j$ in the linear permutation $L$ and substitute $d$ with $d^{1/2^j}$. So, we have

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

Now we can also suppose that in (C11*) the coefficients $\gamma_\ell$ are all equal to 0. Indeed as in section 3.2, supposing $\gamma_h = 1$ (in case $\gamma_h \neq 1$ we can perform the change of variable $x \mapsto \gamma_h^{-\frac{1}{2^h(2^m+1)}} x$) and applying the linear permutation $L'(x) = (w+(c+c^{2^m})^{2^h})x+x^{2^h}+wx^{2^{m+h}}$ we can delete the coefficient $\gamma_h$ obtaining a function equivalent to (C11*), that is,

$$\frac{L'(F(x))}{(c+c^{2^m})^{2^h}} = c'x^{2^m+1} + \sum_{\substack{\ell=1 \\ \ell\neq h}}^{m-1} \gamma'_\ell x^{2^\ell(2^m+1)} + L(dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}),$$

where $d$ is exactly the same coefficient as in $F$, and $c'$ and $\gamma'_\ell$ satisfying the constrains of (C11*). So, we can suppose that $F(x) = cx^{2^m+1} + L(dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)})$.

Now, $c \in \mathbb{F}_{2^{2m}} \setminus \mathbb{F}_{2^m}$ and, as above, we have $\mathbb{F}_{2^{2m}} = c\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$. Then, considering the linear function $L'$ which is the identity map on $c\mathbb{F}_{2^m}$ and the linear function $L^{-1}$ on $\mathbb{F}_{2^m}$ (recall that $L$ is a permutation with coefficient in $\mathbb{F}_{2^m}$) we obtain

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

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

**Lemma 3.2.** *Families (C11*) and C11 coincide.*

### *3.4.* (C3*) is equivalent to C11

Now we will prove that family (C3*), which contains C3, is equivalent to C11.

First of all, consider $c, d, \gamma_\ell$ satisfying the constrains of (C3*). Since $d^{2^m+1} = 1$, there exists $d'$ such that $d'^{2^m-1} = d$. Moreover, since $d$ is not in $\{x^{(2^i+2^j)(2^m-1)} : x \in \mathbb{F}_{2^{2m}}\}$ we have $d' \notin \{x^{(2^i+2^j)} : x \in \mathbb{F}_{2^{2m}}\}$.
Let $F(x) = cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + x^{2^i+2^j} + dx^{2^m(2^i+2^j)}$. 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 $\ell$ 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 $\gamma_\ell$. Thus $F'(x)$ is an element of (C11*), which is equivalent to C11.

**Lemma 3.3.** *Families C11 and (C3*) are equivalent.*

We summarize our results in the following theorem.

**Theorem 3.4.** *Families C3, C11, (C3*) and (C11*) are all equivalent to each other.*

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

**Proposition 3.5.** *Let $n = 2m$ with $m$ odd and let $i$ be such that $\gcd(n, i) = 1$. Let*

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

*and*

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

*be two APN functions of family C11. 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

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

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 $c'\mathbb{F}_{2^m}$ with the map $cx \mapsto c'x$, 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

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

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 partitioned 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 Table2)**

The following family of APN hexanomials was constructed in [7].

**Theorem 3.6** ([7])**.** *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 $x^{2^m+1} = 1$.*

Coefficient $\bar{c}$ satisfying the conditions of the theorem above are characterized in [22, Theorem 11] as well as the number of such $\bar{c}$'s [22, Theorem 12] .

We are going to show below that C11 (and thus C3) is contained in C4. In the previous sections, we have proved that we can consider functions C11 without the part $\sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)}$, that is, it is sufficient to consider function (1) which we transform as follows

$$F(x) = cx^{2^m+1} + x^{2^i(2^m+1)} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}, \tag{3}$$

with $c \in \mathbb{F}_{2^{2m}} \setminus \mathbb{F}_{2^m}$ and $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\}$. Indeed, using linear permutations as in (2), we can obtain from functions (3) all possible functions (1), and vice versa.

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

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

Now, using a linear permutation as in (2), it is possible 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 above, 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

$$F'(x) = c'x^{2^m+1} + (ax^{2^i+1} + a^{2^m}x^{2^m(2^i+1)} + bx^{2^{m+i}+1} + b^{2^m}x^{2^i+2^m}). \tag{4}$$

Now, since $i$ and $m$ are odd and $\gcd(i, m) = 1$ then $x^{2^{m+i}+1}$ 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 (4) we obtain

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

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 $x^{1/2^{m-i}}$ on $c''\mathbb{F}_{2^m}$ and the identity on $\mathbb{F}_{2^m}$. Thus, denoting by $c = (c'')^{1/2^{m-i}}$, we obtain the equivalent function

$$\bar{F}(x) = L(F''(x^{2^{m-i}})) = cx^{2^m+1} + \frac{a}{\lambda^{2^i+1}}x^{2^m+2^j} + \left(\frac{a}{\lambda^{2^i+1}}\right)^{2^m} x^{(2^{m+j}+1)} + x^{2^j+1} + x^{2^m(2^j+1)}, \tag{5}$$

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

On the other hand, let $i$ be an integer with $\gcd(i, m) = 1$ and consider a hexanomial

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

Applying the linear permutation (as in (2)) $L(x) = (w+(\bar{d}+\bar{d}^{2^m})^{1/2^i})x + wx^{2^m} + x^{1/2^i} + x^{2^{m-i}}$ for some $w \in \mathbb{F}_{2^m}^*$, we obtain

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

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

$$H''(x) = d''x^{2^m+1} + x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m}, \tag{6}$$

where $d'' = \bar{d}'^{(1/2^i)}$. Then, the family of the hexanomials can be expressed as pentanomials and the constrain on the coefficient $\bar{c}$ is the same of the hexanomials. Indeed, following the same steps of the proof of [7, Theorem 2], a function $H''$ as in (6), with $d'' \notin \mathbb{F}_{2^m}$ and $\gcd(i, m) = 1$, is APN if and only if

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

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

Coming back to our function in (5), from the arguments above, since $\bar{F}(x)$ is APN and $c'' \notin \mathbb{F}_{2^m}$, denoting $\bar{a} = \left(\frac{a}{\lambda^{2^i+1}}\right)^{2^m}$, we have that

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

has no nonzero solution such that $x^{2^m+1} = 1$. So, the function $\bar{F}(x)$ is equivalent to a hexanomials.

Hence we have proved the following result:

**Theorem 3.7.** *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*

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

*with $\bar{d} \notin \mathbb{F}_{2^m}$ and $\bar{c}$ such that 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, when $m$ and $i$ are odd, $H'(x)$ is equivalent to a pentanomial of type*

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

*with $j = m - i$.*

*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 (5) from $F''(x)$ of (4), with the only difference that in this case the coefficient $a$ of $F''(x)$ is equal to 1. □

### *3.6.* The particular case of C12 with $j = 0$

In the following we will show that also for class C12 of Table 2 when $j = 0$ it is equivalent to a hexanomial.

Let $n = 2m = 4t$ and consider a function $F$ of type C12 in the case of $j = 0$,

$$F(x) = (x + x^{2^m})^{2^i+1} + u'(ux + u^{2^m}x^{2^m})^{2^i+1} + u(x + x^{2^m})(ux + u^{2^m}x^{2^m}),$$

with $u$ a primitive element of $\mathbb{F}_{2^n}^*$, $u' \in \mathbb{F}_{2^m}$ not a cube and $i$ such that $\gcd(i, m) = 1$.

We can see, by a direct computation, that $F$ is EA-equivalent to

$$F'(x) = dx^{2^m+1} + ax^{2^i+1} + a^{2^m}x^{2^m(2^i+1)} + bx^{2^{m+i}+1} + b^{2^m}x^{2^i+2^m},$$

with $d = u^2 + u^{2^m+1}$, $a = 1 + u' u^{2^i+1}$ and $b = 1 + u' u^{2^{m+i}+1}$.

We need to prove that there exists an element $\lambda$ such that $\lambda^{2^i+1} = 1 + u' u^{2^i+1}$. Since $m$ is even we have that $\gcd(3, 2^m + 1) = 1$ and then we can divide the set $\mathbb{F}_{2^n}^*$ as

$$\mathbb{F}_{2^n}^* = U \cup \rho U \cup \rho^2 U$$

with

$$U := \{x^{2^i+1} : x \in \mathbb{F}_{2^n}^*\} = \{x^3 : x \in \mathbb{F}_{2^n}^*\}.$$

and $\rho = u^{2^m+1} \in \mathbb{F}_{2^m}$.

Now, we can have three cases

- $1 + u' u^{2^i+1} \in U$,
- $1 + u' u^{2^i+1} \in \rho U$,
- $1 + u' u^{2^i+1} \in \rho^2 U$.

If we have the first case the poof is done. Otherwise, suppose that $1 + u' u^{2^i+1} \in \rho U$ (or $1 + u' u^{2^i+1} \in \rho^2 U$) and multiply $F'(x)$ by $\rho^2 \in \mathbb{F}_{2^m}$ (or multiply by $\rho \in \mathbb{F}_{2^m}$) obtaining

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

with $d' \notin \mathbb{F}_{2^m}$ and $a' \in U$. Let us consider an element lambda $\lambda$ such that $\lambda^{2^i+1} = a'$, then substituting $x \mapsto \lambda^{-1} x$ we will obtain an APN function which is equivalent to $H'(x)$ as in Theorem 3.7.

## 4. Some conditions on the coefficients of the hexanomials

From the equivalences of C11 and C12 (restricted to the case $j = 0$) with the family C4, we can obtain some conditions on the coefficients of the hexanomials which permit to determine some elements $c \in \mathbb{F}_{2^n}$ such that the equation

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

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

### *4.1.* Case $n = 2m$ with $m$ odd

We have proved that an element of family C11 can be reduced to an element of C4. In particular, from the proof we have immediately the following.

**Proposition 4.1.** *Let $n = 2m$ with $m$ odd and $i \leq m$ be an even integer such that $\gcd(i, m) = 1$. For all $d \notin \{x^{2^{m-i}+1} : x \in \mathbb{F}_{2^n}^*\}$ and $\gamma \in \mathbb{F}_{2^n}^*$ such that $\gamma^{2^m+1} \neq 1$, define*

$$a = d + d^{2^m}\gamma^{2^m(2^{m-i}+1)} \text{ and } b = d\gamma^{2^{m-i}} + d^{2^m}\gamma^{2^m}.$$

*Then, the element*

$$c = a^{2^m} b^{-\frac{2^{n-i}+2^m}{2^{n-i}+1}}$$

*is such that the equation*

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

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

*4.2.* **Case $n = 2m$ with $m$ even**

In this case we have proved that the family C12 (restricted to the case $j$=0) can be reduced to C4. In particular, from the proof we immediately get the following.

**Proposition 4.2.** *Let $n = 2m$ with $m$ even and $i \leq m$ be an integer co-prime with $n$. For all $u' \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^n}^*\}$ and $u' \in \mathbb{F}_{2^m}$, and for all primitive elements $u$ of $\mathbb{F}_{2^n}$, define the sets*

$$\Lambda_{u,k}^{u'} := \{\lambda : \lambda^{2^i+1} = \rho^k(1 + u'\, u^{2^i+1})\},$$

*where $\rho = u^{2^m+1}$ and $k = 0, 1, 2$.*

*Then, for any $\lambda \in \Lambda_{u,k}^{u'}$ the element*

$$c = \frac{\rho^k(1 + u'\, u^{2^{m+i}+1})}{\lambda^{2^{i+m}+1}}$$

*is such that the equation*

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

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

**Remark 4.3.** *Using the software MAGMA, when $n = 2m$ with $m = 3, 5, 7$ (odd case), for even values of $i$ co-prime with $m$ Proposition 4.1 provides all possible values $c$ such that the equation*

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

*has no solution $x$ such that $x^{2^m+1} = 1$.*
*For $m = 2, 4$, Proposition 4.2 covers all possible values $c$, for all integers $i$ such that $\gcd(i, m) = 1$. However, for $m = 6$ Proposition 4.2 gives 1008 possible values of $c$'s out of 1344, for all integers $i$ such that $\gcd(i, m) = 1$.*

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

| $N^\circ$ | 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 $\mathbb{F}_{2^n}^*$ | [8] |
| F3 | $sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}$ $+cx^{2^iq+1}+c^qx^{2^i+q}$ | $q=2^m$, $n=2m$, $\gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}$, $s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q$, $X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution $x$ s.t. $x^{q+1}=1$ | [7] |
| F4 | $x^3+a^{-1}\,Tr(a^3x^9)$ | $a\neq 0$ | [10] |
| F5 | $x^3+a^{-1}\,Tr_n^3(a^3x^9+a^6x^{18})$ | $3\|n$, $a\neq 0$ | [11] |
| F6 | $x^3+a^{-1}\,Tr_n^3(a^6x^{18}+a^{12}x^{36})$ | $3\|n$, $a\neq 0$ | [11] |
| 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 $\mathbb{F}_{2^n}^*$ | [2, 3] |
| 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 | [29] |
| F11 | $a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+$ $ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$ | $n=3m$, $m$ odd $L(x)=ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions in Theorem 6.3 of [6] | [6] |
| F12 | $u(u^qx+x^qu)(x^q+x)+(u^qx+x^qu)^{2^{2i}+2^{3i}}$ $+a(u^qx+x^qu)^{2^{2i}}(x^q+x)^{2^i}+b(x^q+x)^{2^i+1}$ | $q=2^m$, $n=2m$, $\gcd(i,m)=1$ $X^{2^i+1}+aX+b$ has no solution over $\mathbb{F}_{2^m}$ | [27] |

## 5. Conclusion

In this paper we proved that, after corrections, the generalizations introduced in [19] of the families of APN trinomials and multinomials constructed in [7] and in [2], respectively, coincide with the original families. Moreover, we showed that the APN trinomials and multinomials are equivalent to each other and they are contained in the family of the APN hexanomials, introduced in [7]. Further we proved that a particular case of the APN family introduced by Zhou and Pott in [29] is equivalent to a function in the family of APN hexanomials. In the last part, we derived precise conditions for coefficients of the APN hexanimials from the equivalence proofs.

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.

**Acknowledgements**

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

**References**

[1] E. Biham, A. Shamir: *Differential Cryptanalysis of DES-like Cryptosystems*. J. Cryptology 4(1), 3-72 (1991)

[2] C. Bracken, E. Byrne, N. Markin, G. McGuire: *New Families of Quadratic Almost Perfect Nonlinear Trinomials and Multinomials*. Finite Fields and Their Applications 14(3), 703–714 (2008)

[3] C. Bracken, E. Byrne, N. Markin, and G. McGuire, *A Few More Quadratic APN Functions*, Cryptography and Communications, 3(1), 2011, pp. 43-53.

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

[5] M. Brinkmann, G. Leander, *On the classification of APN functions up to dimension five*. Designs, Codes and Cryptography, 49(1-3), 273-288, 2008.

[6] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, I. Villa, *Constructing APN functions through isotopic shift*. Cryptology ePrint Archive, Report 2018/769.

[7] L. Budaghyan, C. Carlet: *Classes of Quadratic APN Trinomials and Hexanomials and Related Structures*. IEEE Trans. Inform. Theory 54(5), 2354-2357 (2008)

[8] L. Budaghyan, C. Carlet, and G. Leander, *Two classes of quadratic APN binomials inequivalent to power functions*, IEEE Trans. Inform. Theory, 54(9), 2008, pp. 4218-4229.

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

[10] L. Budaghyan, C. Carlet, and G. Leander, *Constructing new APN functions from known ones*, Finite Fields and Their Applications, vol.15, issue 2, Apr. 2009, pp. 150-159.

[11] L. Budaghyan, C. Carlet, and G. Leander, *On a construction of quadratic APN functions*, Proceedings of IEEE Information Theory workshop ITW'09, Oct. 2009, pp. 374-378.

[12] L. Budaghyan, C. Carlet, and A. Pott, *New classes of almost bent and almost perfect nonlinear polynomials.* IEEE Transactions on Information Theory 52.3 (2006): 1141-1152.

[13] L. Budaghyan, T. Helleseth, N. Li, B. Sun, *Some Results on the Known Classes of Quadratic APN Functions.* In: El Hajji S., Nitaj A., Souidi E. (eds) Codes, Cryptology and Information Security. C2SI 2017. Lecture Notes in Computer Science, vol 10194. Springer, Cham (2017)

[14] C. Carlet, P. Charpin, and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems.* Designs, Codes and Cryptography 15.2 (1998): 125-156. Sci., vol. 5203, Springer-Verlag, Berlin, 2008, pp. 368–376.

[15] U. Dempwolff, *CCZ equivalence of power functions*, Designs, Codes and Cryptography 86(3), pp. 665–692, 2018.

[16] H. Dobbertin, *Almost perfect nonlinear power functions over $GF(2^n)$: the Welch case*, IEEE Trans. Inform. Theory, 45, 1999, pp. 1271-1275.

[17] H. Dobbertin, *Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case*, Inform. and Comput., 151, 1999, pp. 57-72.

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

[19] Duan, Xue Ying, and Yu Long Deng. *Two Classes of Quadratic Crooked Functions.* Applied Mechanics and Materials. Vol. 513. Trans Tech Publications, 2014.

[20] Y. Edel, and A. Pott, *A new almost perfect nonlinear function which is not quadratic.* Adv. in Math. of Comm. 3.1 (2009): 59-81.

[21] R. Gold, *Maximal recursive sequences with 3-valued recursive cross-correlation functions*, IEEE Trans. Inform. Theory, 14, 1968, pp. 154-156.

[22] F. Göloğlu: *Almost Perfect Nonlinear Trinomials and Hexanomials.* Finite Fields and Their Applications 33, 258–282 (2015)

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

[24] T. Kasami, *The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes*, Inform. and Control, 18, 1971, pp. 369-394.

[25] McEliece, *Finite Fields for Computer Scientists and Engineers*, 1987.

[26] K. Nyberg, *Differentially uniform mappings for cryptography*, Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science 765, 1994, pp. 55-64.

[27] H. Taniguchi, *On some quadratic APN functions*, Des. Codes Cryptogr., `https://doi.org/10.1007/s10623-018-00598-2`, 2019.

[28] S. Yoshiara, *Equivalences of power APN functions with power or quadratic APN functions*, Journal of Algebraic Combinatorics, vol. 44, N. 3. Nov. 2016, pp. 561-585.

[29] Y. Zhou and A. Pott. *A New Family of Semifields with 2 Parameters*. Advances in Mathematics, 234:43-60, 2013.