Relation between o-equivalence and EA-equivalence for Niho bent functions*

Diana Davidova[†], Lilya Budaghyan,[†] Claude Carlet[‡,†]
Tor Helleseth,[†] Ferdinand Ihringer[§], Tim Penttila[¶]

Abstract

Boolean functions, and bent functions in particular, are considered up to so-called EA-equivalence, which is the most general known equivalence relation preserving bentness of functions. However, for a special type of bent functions, so-called Niho bent functions there is a more general equivalence relation called o-equivalence which is induced from the equivalence of o-polynomials. In the present work we study, for a given o-polynomial, a general construction which provides all possible o-equivalent Niho bent functions, and we considerably simplify it to a form which excludes EA-equivalent cases. That is, we identify all cases which can potentially lead to pairwise EA-inequivalent Niho bent functions derived from o-equivalence of any given Niho bent function. Furthermore, we determine all pairwise EA-inequivalent Niho bent functions arising from all known o-polynomials via o-equivalence.

Keywords: Bent function, Boolean function, EA-equivalence, maximum nonlinearity, Magic action, modified Magic action, Niho bent function, o-equivalence, o-polynomials, ovals, hyperovals, Walsh transform.

1 Introduction

Boolean functions of n variables are binary functions over the vector space $\mathbb{F}_2^n$ of all binary vectors of length n, and can be viewed as functions over the Galois field $\mathbb{F}_{2^n}$, thanks to the choice of a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. In this paper, we shall always have this last viewpoint. Boolean functions are used in the pseudo-random generators of stream ciphers and play a central role in their security.

Bent functions, introduced by Rothaus [35] in 1976, are Boolean functions having an even number of variables n, that are maximally nonlinear in the sense that their nonlinearity, the minimum Hamming distance to all affine functions,

*Some results of this paper were presented at Irsee 2014 conference, BFA 2018 and BFA 2019 workshops.

[†]Department of Informatics, University of Bergen, PB 7803, N-5020 Bergen, Norway, e-mail: {Diana.Davidova, Lilya.Budaghyan, Tor.Helleseth}@uib.no

[‡]Department of Mathematics, Universities of Paris 8 and Paris 13, 2 rue de la liberté, 93526 Saint-Denis Cedex, France, e-mail: claude.carlet@univ-paris8.fr

[§]Department of Mathematics: Analysis, Logic and Discrete Mathematics, Ghent University, Belgium, e-mail: ferdinand.ihringer@ugent.be

[¶]Department of Mathematics, Colorado State University, Fort Collins, CO 80523-1874 , e-mail: penttila@math.colostate.edu

is optimal (for more information on bent functions see, for instance, [11]). This corresponds to the fact that their Walsh transform takes the values $\pm 2^{n/2}$, only. Bent functions have attracted a lot of research interest in mathematics because of their relation to difference sets and to designs, and in the applications of mathematics to computer science because of their relations to coding theory and cryptography. Despite their simple and natural definition, bent functions admit a very complicated structure in general. An important focus of research is to find constructions of bent functions. Many methods are known and some of them allow explicit constructions. We distinguish between primary constructions giving bent functions from scratch and secondary constructions building new bent functions from one or several given bent functions (in the same number of variables or in different ones).

Boolean functions, and bent functions in particular, are considered up to so-called EA-equivalence, which is the most general known equivalence relation preserving bentness of functions [3, 4].

Bent functions are often better viewed in their bivariate representation, in the form $f(x, y)$, where x and y belong to $\mathbb{F}_2^m$ or to $\mathbb{F}_{2^m}$, where $m = n/2$. This representation has led to the two general families of explicit bent functions which are the original Maiorana-McFarland [29] and the Partial Spreads ($\mathcal{PS}_{ap}$) classes (this latter class is included in the more general but less explicit $\mathcal{PS}$ class). Bent functions can also be viewed in their univariate form, expressed by means of the trace function over $\mathbb{F}_{2^n}$. Finding explicit bent functions in this trace representation is usually more difficult than in the bivariate representation. References containing information on explicit primary constructions of bent functions in their bivariate and univariate forms are [9, 25]. It is well known that some of these explicit constructions belong to the Maiorana-McFarland class and to the $\mathcal{PS}_{ap}$ class. When, in the early 1970s, Dillon introduced in his thesis [17] the two above mentioned classes, he also introduced another one denoted by H, where bentness was proven under some conditions which were not obvious to achieve. This made class H an example of a non-explicit construction: at that time, Dillon was able to exhibit only functions belonging, up to the affine equivalence (which is a particular case of EA-equivalence), to the Maiorana-McFarland class.

It was observed in [10] that the class of the, so called, Niho bent functions (introduced in [18] by Dobbertin *et al*) is, up to EA-equivalence, equal to the Dillon's class H. Note that functions in class H are defined in their bivariate representation and Niho bent functions had originally a univariate form only. Three infinite families of Niho binomial bent functions were constructed in [18] and one of these constructions was later generalized by Leander and Kholosha [26] into a function with 2^r Niho exponents. Another class was also extended in [20]. In [6] it was proven that some of these infinite families of Niho bent functions are EA-inequivalent to any Maiorana-McFarland function which implied that classes H and Maiorana-McFarland are different up to EA-equivalence.

In the same paper [10], it was shown that Niho bent functions define o-polynomials and, conversely, every o-polynomial defines a Niho bent function. They also discovered that a given o-polynomial F can produce two different (up to EA-equivalence) Niho bent functions, namely, the ones derived from F and its inverse F^{-1}. Since taking the inverse of an o-polynomial is a particular case of the equivalence of o-polynomials, a natural question was to explore this equivalence for construction of further EA-inequivalent cases of Niho bent functions. The first work in this direction was done in [7] where the group

of transformations (introduced in [14]) of order 24 preserving the equivalence of o-polynomials was studied for relation to EA-equivalence. It was shown that these transformations can lead to up to four EA-inequivalent functions including those derived from an o-polynomial and its inverse. That is, two new transformations which can potentially provide EA-inequivalent functions from a given o-polynomial were discovered. Hence, application of the equivalence of o-polynomials can be considered as a construction method for new (up to EA-equivalence) Niho bent functions from the known ones.

Note that the group of transformations from [14] does not cover all possible transformations within equivalence of o-polynomials. A more general group of transformations, so-called the Magic action, was presented in [21], which is an action of a group of transformations acting on projective line on the set of o-permutations. In this paper we study the modified Magic action, a transformation of o-polynomials preserving projective equivalence. We show that o-polynomials are projectively equivalent if and only if they lie on the same orbit under the modified Magic action and the inverse map. Further we prove that, for a given o-polynomial, EA-inequivalent Niho bent functions can arise only from a specific formula involving particular compositions of transformations of the modified magic action and the inverse map. We show that each o-monomial can define up to four EA-inequivalent bent functions. We prove, for instance, that the Pyne hyperoval can give rise to EA-inequivalent Niho bent functions defined by o-polynomials which lie on 3 different orbits of the modified Magic action. For every known o-polynomial we provide an explicit number of pairwise EA-inequivalent Niho bent functions which can be derived via o-equivalence. Moreover, we give an explicit description (involving transformations of the modified magic action and the inverse map) of all o-polynomials providing pairwise EA-inequivalent Niho bent functions.

The paper is organized as follows. In Section 2 we recall necessary background, in Section 3 we define Niho bent functions via o-polynomials and vice versa. In Section 4 we prove that affine equivalence of o-polynomials in some cases yields EA-equivalence of the corresponding Niho bent functions. The known fact that every o-polynomial on $\mathbb{F}_{2^m}$ necessarily defines a vectorial Niho bent function from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_{2^m}$ can be seen as a corollary. In Section 5 the modified magic action is introduced and it is proven that potentially EA-inequivalent Niho bent functions can arise from o-polynomials which lie on the same orbit under the modified Magic action and the inverse map. The main results of the paper are contained in Sections 6 and 7, where we obtain an exact form of the orbit on which o-polynomials should lie to produce potentially EA-inequivalent Niho bent functions. For each of the known o-polynomials we provide the explicit number and representations for all equivalent o-polynomials which provide pairwise EA-inequivalent Niho bent functions.

2 Notation and Preliminaries

2.1 Trace Representation, Boolean Functions in Univariate and Bivariate Forms

For any positive integer k and any r dividing k, the trace function Tr_r^k is the mapping from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$ defined by

$$\mathrm{Tr}_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}} \ .$$

In particular, the *absolute trace* over $\mathbb{F}_{2^k}$ is the function $\mathrm{Tr}_1^k(x) = \sum_{i=0}^{k-1} x^{2^i}$ (in what follows, we just use Tr_k to denote the absolute trace). Recall that the trace function satisfies the transitivity property $\mathrm{Tr}_k = \mathrm{Tr}_r \circ \mathrm{Tr}_r^k$.

The univariate representation of a Boolean function is defined as follows: we identify $\mathbb{F}_2^n$ (the n-dimensional vector space over $\mathbb{F}_2$) with $\mathbb{F}_{2^n}$ and consider the arguments of f as elements in $\mathbb{F}_{2^n}$. An inner product in $\mathbb{F}_{2^n}$ is $x \cdot y = \mathrm{Tr}_n(xy)$. There exists a unique univariate polynomial $\sum_{i=0}^{2^n-1} a_i x^i$ over $\mathbb{F}_{2^n}$ that represents f (this is true for any vectorial function from $\mathbb{F}_{2^n}$ to itself and therefore for any Boolean function since $\mathbb{F}_2$ is a subfield of $\mathbb{F}_{2^n}$). The algebraic degree of f is equal to the maximum 2-weight of the exponents of those monomials with nonzero coefficients in the univariate representation, where the 2-weight $w_2(i)$ of an integer i is the number of ones in its binary expansion. Moreover, f being Boolean, its univariate representation can be written uniquely in the form of

$$f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_{o(j)}(a_j x^j) + a_{2^n-1} x^{2^n-1} \ ,$$

where Γ_n is the set of integers obtained by choosing the smallest element in each cyclotomic coset modulo $2^n - 1$ (with respect to 2), $o(j)$ is the size of the cyclotomic coset containing j, $a_j \in \mathbb{F}_{2^{o(j)}}$ and $a_{2^n-1} \in \mathbb{F}_2$. The function f can also be written in a non-unique way as $\mathrm{Tr}_n(P(x))$ where $P(x)$ is a polynomial over $\mathbb{F}_{2^n}$.

The bivariate representation of a Boolean function is defined in this paper as follows: we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ (where $n = 2m$) and consider the argument of f as an ordered pair (x, y) of elements in $\mathbb{F}_{2^m}$. There exists a unique bivariate polynomial $\sum_{0 \le i,j \le 2^m-1} a_{i,j} x^i y^j$ over $\mathbb{F}_{2^m}$ that represents f. The algebraic degree of f is equal to $\max_{(i,j) \mid a_{i,j} \neq 0}(w_2(i) + w_2(j))$. And f being Boolean, its bivariate representation can be written in the form $f(x, y) = \mathrm{Tr}_m(P(x, y))$, where $P(x, y)$ is some polynomial of two variables over $\mathbb{F}_{2^m}$.

Remark 1. *Let $g(x, y)$ be a Boolean function over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Then one can get a univariate representation of g making the following substitutions:*

$$x = t + t^{2^m} \text{ and } y = \alpha t + (\alpha t)^{2^m},$$

where α is a primitive element of $\mathbb{F}_{2^{2m}}$.

2.2 Walsh Transform and Bent Functions

Let f be an n-variable Boolean function. Its *"sign" function* is the integer-valued function $\chi_f := (-1)^f$. The *Walsh transform* of f is the discrete Fourier

transform of χ_f whose value at point $w \in \mathbb{F}_{2^n}$ is defined by

$$\widehat{\chi}_f(w) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_n(wx)} \ .$$

For even n, a Boolean function f in n variables is said to be *bent* if for any $w \in \mathbb{F}_{2^n}$ we have $\widehat{\chi}_f(w) = \pm 2^{\frac{n}{2}}$.

It is well known (see, for instance, [9]) that the algebraic degree of a bent Boolean function in $n > 2$ variables is at most $\frac{n}{2}$.

Bentness and algebraic degree (when larger than 1) are preserved by extended-affine (EA-) equivalence. Two Boolean functions f and g in n variables are called *EA-equivalent* if there exists an affine permutation A of $\mathbb{F}_{2^n}$ and an affine Boolean function ℓ such that $f = g \circ A + \ell$. If $l = 0$ then f and g are called *affine equivalent*. In the case of vectorial functions there exists a more general notion of equivalence, called *CCZ-equivalence*, but for Boolean functions, it reduces to EA-equivalence, see [3] (as well as for bent vectorial functions [4]).

Two functions F and F' from $\mathbb{F}_{2^n}$ to itself are called EA-equivalent if $A_1 \circ F \circ A_2 + A$ for some affine permutations A_1 and A_2 and for some affine function A. If $A = 0$ then F and F' are called affine equivalent.

For positive integers n and t, a vectorial Boolean function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^t$ is called bent if for any $a \in \mathbb{F}_2^n \setminus \{0\}$ the Boolean function $a \cdot F(x)$ is bent. Bent functions exist if and only if n is even and $t \leq n/2$ (see [30]).

2.3 Projective plane, Ovals, Hyperovals

In the following we give a short introduction to the projective plane. We refer to [16] for a detailed introduction to projective geometry. A projective plane consists of a set of *points* P, a set of *lines* L, and an incidence relation I between P and L. The classical *projective plane* $PG(2,q)$ over $\mathbb{F}_q^3$ has the 1-spaces of $\mathbb{F}_q^3$ as points and the 2-spaces of $\mathbb{F}_q^3$ as lines. A point p is contained in a line ℓ if $p \subseteq \ell$ in $\mathbb{F}_q^3$. A set of points is called *collinear* if they all lie on the same line. Note that $PG(2,q)$ has q^2+q+1 points, q^2+q+1 lines, each line contains $q+1$ points, and each point lies in $q+1$ lines. The group $P\Gamma L(3,q)$ acts naturally on $PG(2,q)$. In particular, it preserves incidence.

Let $\mathcal{O}$ be a set of points in $PG(2,q)$ such that no three points are collinear. It is well-known that $|\mathcal{O}| \leq q+1$ if q is odd and $|\mathcal{O}| \leq q+2$ is q is even. One can see this as follows: Consider a point $P \in \mathcal{O}$. Each of the $q+1$ lines on P contains at most one more points, so $|\mathcal{O}| \leq q+2$. Suppose that equality holds. Then each line contains either 0 or 2 points. Consider a point $R \in \mathcal{O}$. Then there are s lines through R with 2 points and $q+1-s$ lines through R with 0 points. Hence, $q+2 = 2s$, so q is even.

Call a line ℓ *passant*, *tangent*, respectively, *secant* if $|\ell \cap \mathcal{O}| = 0$, $|\ell \cap \mathcal{O}| = 1$, respectively, $|\ell \cap \mathcal{O}| = 2$. If $|\mathcal{O}| = q+1$, then $\mathcal{O}$ is called an *oval*. From the argument above it follows that in this case each point of $\mathcal{O}$ lies on exactly one tangent and q secants. For q even these secants all meet in one point N, the *nucleus* of $\mathcal{O}$. If $|\mathcal{O}| = q+2$, then $\mathcal{O}$ is called a *hyperoval* and we usually write $\mathcal{H}$ instead of $\mathcal{O}$. If $|\mathcal{O}| = q+1$ and q even, then $\mathcal{O} \cup \{N\}$ is a hyperoval.

In the following we limit ourselves to $q = 2^m$ even.

A *frame* of $PG(2,q)$ is a set of four points $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ such that any 3-subset of $\mathcal{P}$ spans $\mathbb{F}_q^3$. The fundamental theorem of projective geometry (for

projective planes) states that $P\Gamma L(3,q)$ acts transitive on frames. As any four points of a hyperoval $\mathcal{H}$ are a frame, we can assume that an oval $\mathcal{O}$ contains $\langle(1,0,0)\rangle, \langle(0,0,1)\rangle, \langle(1,1,1)\rangle \in \mathcal{O}$ and has $\langle(0,1,0)\rangle$ as its nucleus. In the following we usually leave out the brackets $\langle\cdot\rangle$ for the sake of readibility. Hence, we can write $\mathcal{O}$ as

$$\mathcal{O} = \{(x, F(x), 1) : x \in \mathbb{F}_{2^m}\} \cup \{(1,0,0)\},$$

where the polynomial F satisfies the following:

(a) F is a permutation polynomial over $\mathbb{F}_{2^m}$ of degree at most $q-2$ satisfying $F(0) = 0$ and $F(1) = 1$.

(b) For any $s \in \mathbb{F}_{2^m}^*$ the function

$$F_s(x) := \begin{cases} \frac{F(x+s)+F(x)}{x} & \text{if } x \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

is a permutation polynomial. Here and further int he paper we denote $\mathbb{F}_{2^m}^* = \mathbb{F}_{2^m} \setminus \{0\}$.

Such a polynomial F is called an *o-polynomial* and, conversely, each o-polynomial defines an oval. If we do not require $F(1) = 1$, then F is called an *o-permutation*. We write $\mathcal{O}(F)$ for the oval defined by the o-polynomial F, and we write $\mathcal{H}(F)$ for the hyperoval defined by F.

Note that throughout this paper $\mathcal{O}$ consists of points of the form $(x, F(x), 1)$, while in the hyperplane literature, usually the form $(1, x, f(x))$ is used.

For a hyperoval $\mathcal{H}$ we have $2^m + 2$ choices for the nucleus $N \in \mathcal{H}$ to obtain an oval $\mathcal{H} \setminus \{N\}$. Hence, each hyperoval $\mathcal{H}$ defines $2^m + 2$ o-polynomials. Two o-polynomials are called *(projectively) equivalent*, if they define equivalent hyperovals (under the natural action of $P\Gamma L(3,q)$).

2.4 Niho Bent Functions

A positive integer d (always understood modulo $2^n - 1$ with $n = 2m$) is a *Niho exponent* and $t \to t^d$ is a *Niho power function* if the restriction of t^d to $\mathbb{F}_{2^m}$ is linear or, equivalently, if $d \equiv 2^j \pmod{2^m - 1}$ for some $j < n$. As we consider $\mathrm{Tr}_n(at^d)$ with $a \in \mathbb{F}_{2^n}$, without loss of generality, we can assume that d is in the normalized form, i.e., with $j = 0$. Then we have a unique representation $d = (2^m - 1)s + 1$ with $2 \leq s \leq 2^m$. If some s is written as a fraction, this has to be interpreted modulo $2^m + 1$ (e.g., $1/2 = 2^{m-1} + 1$). Following are examples of bent functions consisting of one or more Niho exponents:

1. Quadratic function $\mathrm{Tr}_m(at^{2^m+1})$ with $a \in \mathbb{F}_{2^m}^*$ (here $s = 2^{m-1} + 1$).

2. Binomials of the form $f(t) = \mathrm{Tr}_n(\alpha_1 t^{d_1} + \alpha_2 t^{d_2})$, where $2d_1 \equiv 2^m + 1 \pmod{2^n - 1}$ and $\alpha_1, \alpha_2 \in \mathbb{F}_{2^n}^*$ are such that $(\alpha_1 + \alpha_1^{2^m})^2 = \alpha_2^{2^m+1}$. Equivalently, denoting $a = (\alpha_1 + \alpha_1^{2^m})^2$ and $b = \alpha_2$ we have $a = b^{2^m+1} \in \mathbb{F}_{2^m}^*$ and
$$f(t) = \mathrm{Tr}_m(at^{2^m+1}) + \mathrm{Tr}_n(bt^{d_2}).$$

We note that if $b = 0$ and $a \neq 0$ then f is a bent function listed under number 1. The possible values of d_2 are [18, 20]:

$$d_2 = (2^m - 1)3 + 1,$$
$$6d_2 = (2^m - 1) + 6 \text{ (taking } m \text{ even)}.$$

These functions have algebraic degree m and do not belong to the completed Maiorana-McFarland class [6].

3. Take $1 < r < m$ with $\gcd(r, m) = 1$ and define

$$f(t) = \mathrm{Tr}_n\left(a^2 t^{2^m+1} + (a + a^{2^m}) \sum_{i=1}^{2^{r-1}-1} t^{d_i}\right), \tag{1}$$

where $2^r d_i = (2^m - 1)i + 2^r$ and $a \in \mathbb{F}_{2^n}$ is such that $a + a^{2^m} \neq 0$ [26, 27]. This function has algebraic degree $r + 1$ (see [5]) and belongs to the completed Maiorana-McFarland class [12].

4. Bent functions in a bivariate representation obtained from the known o-polynomials.

Consider the listed above two binomial bent functions. If $\gcd(d_2, 2^n - 1) = d$ and $b = \beta^d$ for some $\beta \in \mathbb{F}_{2^n}$ then b can be "absorbed" in the power term t^{d_2} by a linear substitution of variable t. In this case, up to EA-equivalence, $b = a = 1$. In particular, this applies to any b when $\gcd(d_2, 2^n - 1) = 1$ that holds in both cases except when $d_2 = (2^m - 1)3 + 1$ with $m \equiv 2 \pmod 4$ where $d = 5$. In this exceptional case, we can get up to 5 different classes but the exact situation has to be further investigated.

3 Class $\mathcal{H}$ of Bent Functions and o-polynomials

Here we restrict ourself with fields $\mathbb{F}_{2^n}$ with n even, $n = 2m$.

In his thesis [17], Dillon introduced the class of bent functions denoted by H. The functions in this class are defined in their bivariate form as

$$f(x, y) = Tr_m(y + xF(yx^{2^m-2})),$$

where $x, y \in \mathbb{F}_{2^m}$, and

- F is a permutation of $\mathbb{F}_{2^m}$ s.t. $F(x) + x$ doesn't vanish,
- for any $\beta \in \mathbb{F}_{2^m}^*$ the function $F(x) + \beta x$ is 2-to-1.

Dillon was able to exhibit bent functions in H that also belong to the completed Maiorana-McFarland class. Dillon's class H was modified in [10] into a class $\mathcal{H}$ of the functions:

$$g(x, y) = \begin{cases} Tr_m\Big(xG\Big(\dfrac{y}{x}\Big)\Big), \text{ if } x \neq 0 \\ \qquad Tr_m(\mu y), \text{ otherwise} \end{cases} \tag{2}$$

where $\mu \in \mathbb{F}_{2^m}, G : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ satisfying the following conditions:

$$F : z \mapsto G(z) + \mu z \text{ is a permutation over } \mathbb{F}_{2^m}, \tag{3}$$

$$z \mapsto F(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m} \text{ for any } \beta \in \mathbb{F}_{2^m}^*. \tag{4}$$

Here condition (4) implies condition (3) and it is necessary and sufficient for g being bent. Functions in $\mathcal{H}$ and the Dillon class are the same up to addition of a linear term $Tr_m((\mu + 1)y)$ to (2). Niho bent functions are functions in $\mathcal{H}$ in their univariant representation.

Theorem 1 ([10]). *A polynomial F on $\mathbb{F}_{2^m}$ satisfying $F(0) = 0$ and $F(1) = 1$ is an o-polynomial if and only if*

$$z \mapsto F(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m} \text{ for any } \beta \in \mathbb{F}_{2^m}^*. \tag{5}$$

Hence, obviously every o-polynomial defines a Niho bent function. And vice versa, every Niho bent function defines an o-polynomial since it defines a polynomial F satisfying condition (5) of Theorem 1, and we can derive an o-polynomial $F'(x) = \frac{F(x)+F(0)}{F(1)+F(0)}$ which fixes the requirements $F'(0) = 0$ and $F'(1) = 1$. Note that to get a Niho bent function from a polynomial F it is sufficient that F satisfies only condition (5) while the conditions $F(0) = 0$ and $F(1) = 1$ are not necessary.

In Section 2.3 we saw that each o-polynomial corresponds to a hyperoval and vice versa, each hyperoval corresponds to an o-polynomial. We say that Niho bent functions are *o-equivalent* if they define projectively equivalent hyperovals. As shown in [7, 10], o-equivalent Niho bent functions may be EA-inequivalent. For example, Niho bent functions defined by o-polynomials F and F^{-1} are o-equivalent but they are, in general, EA-inequivalent.

Here is the list of all known o-polynomials (we also give names of the corresponding hyperovals):

1. $F(x) = x^2$, *regular hyperoval*;
2. $F(x) = x^{2^i}$, i and m are coprime, $i > 1$, *irregular translation hyperoval*;
3. $F(x) = x^6$, m is odd, *Segre hyperoval*;
4. $F(x) = x^{3\cdot 2^k+4}$, $m = 2k - 1$, *Glynn I*;
5. $F(x) = x^{2^k+2^{2k}}$, $m = 4k - 1$, *Glynn II*;
6. $F(x) = x^{2^{2k+1}+2^{3k+1}}$, $m = 4k + 1$, *Glynn II*;
7. $F(x) = x^{2^k} + x^{2^k+2} + x^{3\cdot 2^k+4}$, $m = 2k - 1$, *Cherowitzo hyperoval*;
8. $F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$, m is odd, *Payne hyperoval*;
9. $F(x) = \dfrac{\delta^2(x^4 + x) + \delta^2(1 + \delta + \delta^2)(x^3 + x^2)}{x^4 + \delta^2 x^2 + 1} + x^{\frac{1}{2}}$,

   where $Tr_m(\frac{1}{\delta}) = 1$ (if $m \equiv 2 \pmod 4$, then $\delta \notin \mathbb{F}_4$), *Subiaco hyperoval* (for $m = 4$ also known as *Lunelli-Sce hyperoval*);

10. $F(x) = \frac{1}{Tr_m^n}(v)\Big(Tr_m^n(v^r)(x+1)+(x+Tr_m^n(v)x^{\frac{1}{2}}+1)^{1-r}Tr_m^n(vx+v^{2^m})^r\Big)+x^{\frac{1}{2}}$, where m is even, $r = \pm\frac{2^m-1}{3}$, $v \in \mathbb{F}_{2^{2m}}, v^{2^m+1} \neq 1, v \neq 1$, *Adelaide hyperoval.*

11. $F(x) = x^4+x^{16}+x^{28}+\omega^{11}(x^6+x^{10}+x^{14}+x^{18}+x^{22}+x^{26})+\omega^{20}(x^8+x^{20})+\omega^6(x^{12}+x^{24})$ with $\omega^5 = \omega^2+1$ and $m = 5$, *O'Keefe-Penttila hyperoval.*

Note that an o-polynomial F defined on $\mathbb{F}_{2^m}$ has the following form [16]:

$$F(x) = \sum_{k=1}^{\frac{2^m-2}{2}} b_{2k}x^{2k}.$$

4 Vectorial Niho bent functions from o-polynomials

It is known since 2011 that every o-polynomial defines a Boolean Niho bent function [10]. In this section, we revisit the fact that, actually, every o-polynomial on $\mathbb{F}_{2^m}$ defines a vectorial Niho bent function from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$. This connection has been originally observed in [28]. In the present paper, we derive this result by studying some simple transformations of o-polynomials.

Below we show that in some cases, affine equivalence of o-polynomials yields EA-equivalence of the corresponding Niho bent functions. Note that in general if a function F' is affine equivalent to an o-polynomial F then F' is not necessarily an o-polynomial.

Lemma 1. *Let F be an o-polynomial defined on $\mathbb{F}_{2^m}$ and $a, b \in \mathbb{F}_{2^m}^*$. Then $G(x) = aF(bx)$ is an o-polynomial on $\mathbb{F}_{2^m}$ if and only if $a = \frac{1}{F(b)}$ (or, what is the same, $b = F^{-1}(a^{-1})$). The Niho bent functions defined by the o-polynomials F and $G = \frac{1}{F(b)}F(bx)$ are affine equivalent.*

Proof. Suppose $G(x) = aF(bx)$ is an o-polynomial, then $G(0) = aF(0) = 0$ for any $a, b \in \mathbb{F}_{2^m}$ and $1 = G(1) = aF(b)$, hence G is an o-polynomial if and only if $a = \frac{1}{F(b)}$.
The Niho bent function corresponding to the o-polynomial F is $f(x,y) = Tr_m(xF(\frac{y}{x}))$, and the one corresponding to G is
$g(x,y) = Tr_m(xG(\frac{y}{x})) = Tr_m(xaF(b\frac{y}{x})) = Tr_m(xaF(\frac{aby}{ax})) = Tr_m(vF(\frac{u}{v}))$,
where $v = ax$, $u = aby$. Hence, $g = f \circ A$ with $A(x,y) = (ax, aby)$, and, therefore, f and g are affine equivalent. □

Corollary 1. *For every o-polynomial F defined on $\mathbb{F}_{2^m}$ the function $xF(\frac{y}{x})$ from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ is bent. That is, every o-polynomial on $\mathbb{F}_{2^m}$ defines a vectorial Niho bent function $xF(\frac{y}{x})$ from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$.*

Proof. From Lemma 1 we have that for a given o-polynomial F and any $a \in \mathbb{F}_{2^m}^*$ the function $g(x,y) = Tr_m(axF(\frac{by}{x}))$ is Niho bent where $b = F^{-1}(a^{-1})$. Then the function $\bar{g}(x,y) = Tr_m(axF(\frac{y}{x}))$ is also bent since g and $\bar{g}$ are affine equivalent, that is, $g = \bar{g} \circ A$ with $A(x,y) = (x, by)$, and clearly, such a transformation A keeps $\bar{g}$ as a Niho function. □

Lemma 2. *Let F be an o-polynomial on $\mathbb{F}_{2^m}$ and $A(x) = x^{2^j}$ be an automorphism over $\mathbb{F}_{2^m}$. Then the Niho bent functions defined by o-polynomials F and $G = A \circ F \circ A^{-1}$ are affine equivalent.*

Proof. Obviously if F is an o-polynomial, then $G(x) = (F(x^{2^{-j}}))^{2^j}$ is also an o-polynomial.
Consider the Niho bent function defined by G:

$$g(x,y) = Tr_m\Big(xG\Big(\frac{y}{x}\Big)\Big) = Tr_m\Big(xA \circ F \circ A^{-1}\Big(\frac{y}{x}\Big)\Big) =$$
$$Tr_m\Big(x\Big(F\Big(\Big(\frac{y}{x}\Big)^{2^{-j}}\Big)\Big)^{2^j}\Big) = Tr_m\Big(x^{2^{-j}}F\Big(\Big(\frac{y}{x}\Big)^{2^{-j}}\Big)\Big) = Tr_m\Big(uF\Big(\frac{v}{u}\Big)\Big),$$

where $u = x^{2^{-j}}$ and $v = y^{2^{-j}}$. Thus, f and g are affine equivalent ($g = f \circ A$ with $A(x,y) = (x,y)^{2^{-j}}$). □

Lemma 3. *Let F be an o-polynomial on $\mathbb{F}_{2^m}$ and $A_1(x) = x + a$ and $A_2(x) = x + b$ for $a, b \in \mathbb{F}_{2^m}$. Then $G = A_1 \circ F \circ A_2$ is an o-polynomial on $\mathbb{F}_{2^m}$ if and only if $b = F(a)$ and $F(a+1)+F(a) = 1$. Furthermore, the Niho bent functions defined by o-polynomials F and G are EA-equivalent.*

Proof. Suppose $G(x) = A_1 \circ F \circ A_2(x) = F(x+a)+b$ is an o-polynomial. Then $0 = G(0) = F(a) + b$ and, therefore, $F(a) = b$ and $1 = G(1) = F(1+a) + b = F(1+a) + F(a)$.
Further we have
$g(x,y) = Tr_m\Big(xA_1 \circ F \circ A_2\Big(\frac{y}{x}\Big)\Big) = Tr_m\Big(x\Big(F\Big(\frac{y}{x}+a\Big)+b\Big)\Big) =$
$Tr_m\Big(xF\Big(\frac{y+ax}{x}\Big)\Big) + Tr_m(bx) = Tr_m\Big(xF\Big(\frac{u}{x}\Big)\Big) + Tr_m(bx),$

where $u = y + ax$. Thus, g and f are EA-equivalent ($g = f \circ A + l$ with $A(x,y) = (x, y+ax)$ and $l(x,y) = Tr_m(bx)$). □

5 The modified Magic action

Let $\mathcal{F}$ be the collection of all functions $F : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ such that $F(0) = 0$.

The following set

$$P\Gamma L(2,2^m) = \{x \mapsto Ax^{2^j} | A \in GL(2,\mathbb{F}_{2^m}), 0 \le j \le m-1\}$$

is a group of transformations acting on the projective lines, i.e. on the set with the elements of the form: $\{(a \cdot x, a \cdot y) | (x,y) \neq (0,0), x, y \in \mathbb{F}_{2^m}, a \neq 0\}$.

An action of the group $P\Gamma L(2,2^m)$ on $\mathcal{F}$ was introduced and described in [21]. Define the image of $F \in \mathcal{F}$ under the transformation $\psi \in P\Gamma L(2,2^m)$, $\psi : x \mapsto Ax^{2^j}$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,2^m)$, $0 \le j \le m-1$, as a function $\psi F : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ such that

$$\psi F(x) = |A|^{-\frac{1}{2}}\Big[(bx+d)F^{2^j}\Big(\frac{ax+c}{bx+d}\Big) + bxF^{2^j}\Big(\frac{a}{b}\Big) + dF^{2^j}\Big(\frac{c}{d}\Big)\Big].$$

This yields an action of $P\Gamma L(2,2^m)$ on $\mathcal{F}$, which is called *the magic action*. The magic action takes o-permutations to o-permutations and it is a semi-linear

transformation, i.e.
$\psi(F+G) = \psi F + \psi G$, for any $F, G \in \mathcal{F}$,
$\psi a F = a^{2^j} \psi F$, for any $a \in \mathbb{F}_{2^m}$, $F \in \mathcal{F}$, $0 \le j \le m-1$.

Let us recall two theorems (Theorem 4 and Theorem 6) from [21]. For a given o-polynomial F denote $\mathcal{O}(F)$ the oval defined by F.

Theorem 2. *[21] Let F be an o-permutation on $\mathbb{F}_{2^m}$ and let $\psi \in P\Gamma L(2, 2^m)$ be $\psi : x \mapsto Ax^{2^j}$ for $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{F}_{2^m})$ and $0 \le j \le m-1$. Then $G = \psi F$ is also an o-permutation on $\mathbb{F}_{2^m}$. In fact, $\mathcal{O}(G) = \bar{\psi}(\mathcal{O}(F))$, where $\bar{\psi} \in P\Gamma L(3, 2^m)$ is defined by $\bar{\psi} : x \mapsto \bar{A}x^{2^j}$, where $\bar{A} = \begin{pmatrix} d & 0 & c \\ b\psi F(\frac{d}{b}) & |A|^{\frac{1}{2}} & a\psi F(\frac{c}{a}) \\ b & 0 & a \end{pmatrix}$.*

Note that the formulation of the theorem above differs from the one in [21] because in the current paper (following notations of [7]) the points of the oval (or the hyperoval) defined by an o-polynomial F are considered as $(x, F(x), 1)$, meanwhile in [21] the form $(1, x, F(x))$ is used.

Theorem 3. *[21] Let F and G be o-permutations on $\mathbb{F}_{2^m}$, and suppose further that the ovals defined by F and G, i.e. $\mathcal{O}(F)$ and $\mathcal{O}(G)$ are equivalent under $P\Gamma L(3, 2^m)$. Then there exists $\psi \in P\Gamma L(2, 2^m)$ such that $G = \psi F$.*

The magic action can be also described by a collection of generators of $P\Gamma L(2, 2^m)$ [21]:

$$\begin{aligned}
&\sigma_a : x \mapsto \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} x,\ \sigma_a F(x) = a^{-\frac{1}{2}} F(ax),\ a \in \mathbb{F}_{2^m}^*;\\
&\tau_c : x \mapsto \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} x,\ \tau_c F(x) = F(x+c) + F(c),\ c \in \mathbb{F}_{2^m};\\
&\varphi : x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} x,\ \varphi F(x) = xF(x^{-1});\\
&\rho_{2^j} : x \mapsto x^{2^j},\ \rho_{2^j} F(x) = (F(x^{2^{-j}}))^{2^j},\ 0 \le j \le m-1.
\end{aligned} \tag{6}$$

We slightly modify the magic action generators σ_a and τ_c multiplying them by appropriate constants to preserve the image of 1 at 1:

$$\begin{aligned}
&\tilde{\sigma}_a F(x) = \frac{a^{\frac{1}{2}}}{F(a)} \sigma_a F(x) = \frac{1}{F(a)} F(ax),\ a \in \mathbb{F}_{2^m}^*;\\
&\tilde{\tau}_c F(x) = \frac{1}{F(1+c)+F(c)} \tau_c F(x) = \frac{1}{F(1+c)+F(c)} (F(x+c)+F(c)),\ c \in \mathbb{F}_{2^m}.
\end{aligned} \tag{7}$$

The new set of generators

$$H = \{\tilde{\sigma_a}, \tilde{\tau_c}, \varphi, \rho_{2^j} | 0 \le j \le m-1, c \in \mathbb{F}_{2^m}, a \in \mathbb{F}_{2^m}^*$$

preserves the property $F(1) = 1$ of the function F.

The action of the group with the new set of generators H on the set of all functions F defined on $\mathbb{F}_{2^m}$ with the properties $F(0) = 0$ and $F(1) = 1$ will be called *the modified magic action.*

Proposition 1. *Two o-polynomials arise from equivalent hyperovals if and only if they lie on the same orbit of the group generated by H and the inverse map.*

Proof. According to the first part of Theorem 2, the magic action takes o-permutations to o-permutations. Since the generators of the modified magic action differ from the original magic action generators only by constant coefficient (what allows as to preserve the property of $F(1) = 1$ for any o-polynomial F), then the modified magic action takes o-polynomials to o-polynomials.

According to the second part of Theorem 2, if two o-permutations lie on the same orbit under the magic action, then the corresponding ovals are equivalent and have fixed nucleus $(0, 1, 0)$.
Now suppose that two o-polynomials lie on the same orbit under the modified magic action and the inverse map. Since each o-polynomial is an o-permutation, then the corresponding ovals defined by o-polynomials are equivalent and have nucleus $(0, 1, 0)$. As we know, each oval is contained in a unique hyperoval, which is obtained by adding nucleus to the points of oval. So, hyperovals defined by the o-polynomials on the same orbit under the modified magic action are equivalent. Also it is well known that o-polynomials F and F^{-1} define equivalent hyperovals. Thus, we conclude that hyperovals defined by the o-polynomials on the same orbit under the modified magic action and the inverse map are equivalent.

Let's show the converse statement. Suppose that hyperovals $\mathcal{H}(F)$ and $\mathcal{H}(G)$ defined by o-polynomials F and G are equivalent. It means that there is a collineation which maps $\mathcal{H}(F)$ to $\mathcal{H}(G)$. Consider the preimage of $(0, 1, 0)$ under this collineation, there are 3 possible cases:

1. The preimage of $(0, 1, 0)$ is $(0, 1, 0)$. It means that this collineation fixes point $(0, 1, 0)$. So deleting this point from hyperovals $\mathcal{H}(F)$ and $\mathcal{H}(G)$, we will get equivalent ovals with fixed nucleus, hence by Theorem 3, their generator o-polynomials are on the same orbit under the magic action, hence under the modified magic action.

2. The preimage of $(0, 1, 0)$ is $(1, 0, 0)$. Since hyperovals defined by o-polynomial and its inverse o-polynomial are equivalent, then hyperoval $\mathcal{H}(F)$ is equivalent to a hyperoval $\mathcal{H}(F^{-1})$ and by the corresponding collineation the point $(1, 0, 0)$ has preimage $(0, 1, 0)$. So, at the end we have that hyperovals $\mathcal{H}(F^{-1})$ and $\mathcal{H}(G)$ are equivalent and the preimage of $(0, 1, 0)$ is $(0, 1, 0)$. Hence by the previous case 1 (and the fact that an o-polynomial and its inverse belong to the same orbit under modified action and the inverse) o-polynomials F and G are on the same orbit under modified magic action and the inverse map.

The following diagram illustrates the previous decisions.

$$\begin{array}{ccccc} \mathcal{H}(F^{-1}) & \cong & \mathcal{H}(F) & \cong & \mathcal{H}(G) \\ \cup & & \cup & & \cup \\ (0,1,0) & \mapsto & (1,0,0) & \mapsto & (0,1,0) \end{array}$$

3. The preimage of $(0, 1, 0)$ is $(t, f(t), 1)$. Choose an element φ of $P\Gamma L(2, 2^m)$ taking $(1, t)$ to $(0, 1)$ (such authomorphism always exist, for example it can be defined by matrix $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$). Applying φ to F we will get a hyperoval $\mathcal{H}(\varphi F)$ equivalent to $\mathcal{H}(G)$ where the preimage of $(0, 1, 0)$ is $(1, 0, 0)$. Because of the case 2, we get that φF and G belong to the same orbit under the modified magic action and the inverse map and so do F and G. □

We formulate the next theorem without proof. First this result was announced in September 2014 at the Forth Isree Conference "Finite Geometries" [8] by the authors of this paper, the complete proof can be found in [1].

Theorem 4. *Two Niho bent functions are EA-equivalent if and only if the corresponding ovals are equivalent. Hence, the number of EA-equivalence classes of Niho bent functions arising from a hyperoval of $PG(2, 2^m)$ is the number of orbits of the collineation stabiliser of the hyperoval on the points of the hyperoval.*

6 Niho bent functions and the modified magic action

A group of transformations of order 24 with 3 generators preserving o-polynomials was considered in [7]. This group of transformations is a subgroup of the group with the (modified) magic action generators and the inverse map. Precisely, they are the transformations generated by φ, $\tilde{\tau}_1 = \tau_1$ and the inverse map. Only 4 of these transformations can lead to EA-inequivalent Niho bent functions [7].

As a continuation of the work of [7], let's consider the modified magic action generators, and the inverse map and see which of them give rise to EA-inequivalent Niho bent functions. From Proposition 1 it is clear that o-polynomials on the same orbit under the modified magic action and the inverse map and only they are projectively equivalent. Since we are interested in EA-inequivalent Niho bent functions arising from projectively equivalent o-polynomials, we focus on orbits of the modified magic action together with the inverse map. We prove below that to get EA-inequivalent Niho bent functions from a given o-polynomial it is sufficient to use only $\tilde{\tau}$ and φ generators together with inverse map while ρ and $\tilde{\sigma}$ do not play any role in it. Moreover, we show that all EA-inequivalent Niho bent functions can be obtained from a special formula.

6.1 Preliminary results

Following notations of [7] the generator φ will be denoted by $\prime$ when needed. Let's recall the set of generators

$$H = \{\tilde{\tau}_c, \tilde{\sigma}_a, \prime, \rho_{2^j} | c \in \mathbb{F}_{2^m}, a \in \mathbb{F}_{2^m}^*, 0 \le j \le m-1\},$$

where

$$\tilde{\sigma}_a F(x) = \frac{1}{F(a)} F(ax),\ a \in \mathbb{F}_{2^m}^*;$$

$$\tilde{\tau}_c F(x) = \alpha_F^c \tau_c F(x) = \alpha_F^c (F(x+c) + F(c)),\ c \in \mathbb{F}_{2^m}, \text{where } \alpha_F^c = \frac{1}{\tau_c F(1)};$$

$$F'(x) = \varphi F(x) = xF(x^{-1});$$

$$\rho_{2^j} F(x) = (F(x^{2^{-j}}))^{2^j},\ 0 \le j \le m-1;$$

and prove a few statements about the generators of magic action and the inverse map.

Lemma 4. *Let F be an o-polynomial on $\mathbb{F}_{2^m}$. Then the following identities hold:*

$$\tilde{\tau}_c \circ \tilde{\tau}_d F = \tilde{\tau}_{c+d} F, \tag{8}$$
$$\tilde{\sigma}_a \circ \tilde{\sigma}_b F = \tilde{\sigma}_{ab} F, \tag{9}$$
$$\rho_{2^j} \circ \rho_{2^i} F = \rho_{2^{j+i}} F, \tag{10}$$

where $a, b \in \mathbb{F}_{2^m}^*$, $c, d \in \mathbb{F}_{2^m}$, $0 \leq i, j \leq m-1$.

Proof. To prove the first equality note that

$\tau_c \circ \tau_d F(x) = \tau_d F(x+c) + \tau_d F(c) = F(x+c+d) + F(d) + F(c+d) + F(d) = F(x+c+d) + F(c+d) = \tau_{c+d} F.$

Since magic action is a semilinear transformation we get:

$$\tilde{\tau}_c \circ \tilde{\tau}_d F(x) = \frac{1}{F(1+d)+F(d)} \frac{1}{\tilde{\tau}_d F(1+c) + \tilde{\tau}_d(c)} \tau_c(\tau_d(F(x)) =$$
$$\frac{1}{F(1+d)+F(d)} \frac{F(1+d)+F(d)}{F(1+d+c)+F(d+c)} \tau_{c+d} F(x) =$$
$$\frac{1}{F(1+d+c)+F(d+c)} \tau_{c+d} F(x) = \tilde{\tau}_{c+d} F(x).$$

The other two equalities are straightforward to prove:

$$\tilde{\sigma}_a \circ \tilde{\sigma}_b F = \frac{1}{\tilde{\sigma}_b F(a)} \tilde{\sigma}_b F(ax) = \frac{1}{\frac{1}{F(b)} F(ab)} \frac{1}{F(b)} F(abx) = \frac{1}{F(ab)} F(abx) = \tilde{\sigma}_{ab} F(x),$$
$$\rho_{2^i} \circ \rho_{2^j} F(x) = \rho_{2^i}(F(x^{\frac{1}{2^j}}))^{2^j} = F(x^{\frac{1}{2^{j+i}}})^{2^{j+i}} = \rho_{2^{i+j}} F(x).$$

□

Corollary 2. *Let F be an o-polynomial on $\mathbb{F}_{2^m}$ and k a positive integer. Then*

$$(\tilde{\sigma}_{a_1} \circ \tilde{\sigma}_{a_2} \circ \ldots \circ \tilde{\sigma}_{a_k}) F = \tilde{\sigma}_{a_1 \cdot a_2 \cdot \ldots \cdot a_k} F,$$
$$(\tilde{\tau}_{c_1} \circ \tilde{\tau}_{c_2} \circ \ldots \circ \tilde{\tau}_{c_k}) F = \tilde{\tau}_{c_1 + c_2 + \ldots c_k} F,$$
$$(\rho_{2^{i_1}} \circ \rho_{2^{i_2}} \circ \ldots \circ \rho_{2^{i_k}}) F = \rho_{2^{i_1 + i_2 + \cdots + i_k}} F,$$

where $a_1, \ldots, a_k \in \mathbb{F}_{2^m}^*, c_1, \ldots, c_k \in \mathbb{F}_{2^m}$, $0 \leq i_j \leq m-1$ for all $j \in \{1, \ldots, k\}$.

Proof. The proof follows by induction using Lemma 4. □

Lemma 5. *Let F be an o-polynomial on $\mathbb{F}_2^m$. Then the following identities hold:*

$$(\tilde{\tau}_c F)^{-1}(x) = \tilde{\tau}_{F(c)} F^{-1}\Big(\frac{1}{\alpha_F^c} x\Big), \tag{11}$$
$$(\tilde{\sigma}_a F)^{-1}(x) = \tilde{\sigma}_{F(a)} F^{-1}(x), \tag{12}$$
$$(\rho_{2^j} F)^{-1}(x) = \rho_{2^j} F^{-1}(x), \tag{13}$$

where $a \in \mathbb{F}_{2^m}^*$, $c \in \mathbb{F}_{2^m}$ and $0 \leq j \leq m-1$.

Proof. It is easy to see that $\tilde{\tau}_{F(c)}F^{-1}\Big(\frac{1}{\alpha_F^c}\Big) = 1$, therefore

$$(\tilde{\tau}_c F)^{-1}(x) = (\alpha_F^c(F(x+c)+F(c)))^{-1} = F^{-1}\Big(\frac{1}{\alpha_F^c}x + F(c)\Big) + c =$$
$$F^{-1}\Big(\frac{1}{\alpha_F^c}x + F(c)\Big) + F^{-1}(F(c)) = \tilde{\tau}_{F(c)}F^{-1}\Big(\frac{1}{\alpha_F^c}x\Big).$$

Equalities (12) and (13) are straightforwared to prove:

$$(\tilde{\sigma}_a F)^{-1}(x) = \Big(\frac{1}{F(a)}F(ax)\Big)^{-1} = \frac{1}{a}F^{-1}(F(a)x) = \tilde{\sigma}_{F(a)}F^{-1}(x),$$
$$(\rho_{2^j}F)^{-1}(x) = ((F(x^{2^{-j}}))^{2^j})^{-1} = (F(x^{2^{-j}})^{-1})^{2^j} = \rho_{2^j}F^{-1}(x).$$

□

Lemma 6. *Let F be an o-polynomial on $\mathbb{F}_{2^m}$. Then the following identities hold:*

$$\tilde{\tau}_c \circ \rho_{2^j}F = \rho_{2^j} \circ \tilde{\tau}_{c^{2^{-j}}}F, \tag{14}$$
$$\tilde{\tau}_c \circ \tilde{\sigma}_a F = \tilde{\sigma}_a \circ \tilde{\tau}_{ac}F, \tag{15}$$
$$(\rho_{2^j}F)' = \rho_{2^j}F' \tag{16}$$
$$(\tilde{\sigma}_a F)' = \tilde{\sigma}_{\frac{1}{a}}F', \tag{17}$$

where $a \in \mathbb{F}_{2^m}^*$, $c \in \mathbb{F}_{2^m}$, $0 \le j \le m-1$.

Proof. To prove the first equality, transform its left and right sides.

$\tilde{\tau}_c \circ \rho_{2^j}F(x) = \alpha^c_{\rho_{2^j}F}(\rho_{2^j}F(x+c) + \rho_{2^j}F(c)) =$
$\alpha^c_{\rho_{2^j}F}((F((x+c)^{2^{-j}}))^{2^j} + (F(c^{2^{-j}}))^{2^j}) = \alpha^c_{\rho_{2^j}F}((F(x^{2^{-j}}+c^{2^{-j}}))^{2^j} + (F(c^{2^{-j}}))^{2^j}) =$
$\alpha^c_{\rho_{2^j}F}(F(x^{2^{-j}}+c^{2^{-j}}) + F(c^{2^{-j}}))^{2^j}$

On the other hand,

$$\rho_{2^j} \circ \tilde{\tau}_{c^{2^{-j}}}F(x) = (\tilde{\tau}_{c^{2^{-j}}}F(x^{2^{-j}}))^{2^j} = (\alpha_F^{c^{2^{-j}}}(F(x^{2^{-j}}+c^{2^{-j}}) + F(c^{2^{-j}}))^{2^j}.$$

So, it is left to check that $(\alpha_F^{c^{2^{-j}}})^{2^j} = \alpha^c_{\rho_{2^j}F}$. Indeed,

$$\alpha^c_{\rho_{2^j}F} = \frac{1}{\rho_{2^j}F(1+c)+\rho_{2^j}F(c)} = \frac{1}{(F((1+c)^{2^{-j}}))^{2^j} + (F(c^{2^{-j}}))^{2^j}} =$$
$$\Big(\frac{1}{F(1+c^{2^{-j}}) + F(c^{2^{-j}})}\Big)^{2^j} = (\alpha_F^{c^{2^{-j}}})^{2^j}.$$

Thus we proved that $\tilde{\tau}_c \circ \rho_{2^j}F = \rho_{2^j} \circ \tilde{\tau}_{c^{2^{-j}}}F$.

Computing the left and the right sides of equality (15) we get

$$\tilde{\tau}_c \circ \tilde{\sigma}_a F(x) = \alpha^c_{\tilde{\sigma}_a F}(\tilde{\sigma}_a F(x+c) + \tilde{\sigma}_a F(c)) = \alpha^c_{\tilde{\sigma}_a F}(\frac{1}{F(a)}F(a(x+c)) + \frac{1}{F(a)}F(ac)),$$
$$\tilde{\sigma}_a \circ \tilde{\tau}_{ac}F(x) = \frac{1}{\tilde{\tau}_{ac}F(a)}\alpha_F^{ac}(F(ax+ac)+F(ac)).$$

Note that the coefficients $\frac{1}{F(a)}\alpha^c_{\tilde{\sigma}_a F}$ and $\frac{1}{\tilde{\tau}_{ac}F(a)}\alpha^{ac}_F$ are equal which means that $\tilde{\tau}_c \circ \tilde{\sigma}_a F = \tilde{\sigma}_a \circ \tilde{\tau}_{ac} F$. Indeed,

$$\frac{1}{F(a)}\alpha^c_{\tilde{\sigma}_a F} = \frac{1}{F(a)}\frac{1}{\tilde{\sigma}_a F(1+c)+\tilde{\sigma}_a F(c)} = \frac{1}{F(a)}\frac{F(a)}{F(a(1+c))+F(ac)} = \frac{1}{F(a+ac)+F(ac)},$$
$$\frac{1}{\tilde{\tau}_{ac}F(a)}\alpha^{ac}_F = \frac{F(1+ac)+F(ac)}{F(a+ac)+F(ac)}\frac{1}{F(1+ac)+F(ac)} = \frac{1}{F(a+ac)+F(ac)}.$$

The remaining two equalities are proved similarly. For (16) we get

$$\rho_{2^j}F'(x) = (F'(x^{2^{-j}}))^{2^j} = (x^{2^{-j}}F(\frac{1}{x^{2^{-j}}}))^{2^j} = x(F(\frac{1}{x^{2^{-j}}}))^{2^j} = x\rho_{2^j}F(\frac{1}{x}) = (\rho_{2^j}F)'(x).$$

Transforming both sides of Equality (17) we get

$$(\tilde{\sigma}_a F)'(x) = x\tilde{\sigma}_a F\Big(\frac{1}{x}\Big) = \frac{x}{F(a)}F\Big(\frac{a}{x}\Big).$$
$$\tilde{\sigma}_{\frac{1}{a}}F'(x) = \frac{1}{F'(\frac{1}{a})}F'\Big(\frac{x}{a}\Big) = \frac{a}{F(a)}\frac{x}{a}F\Big(\frac{a}{x}\Big) = \frac{x}{F(a)}F\Big(\frac{a}{x}\Big).$$

□

6.2 EA-inequivalent Niho bent functions and orbits

Further we need the following equality from [7]

$$((F')^{-1})' = ((F^{-1})')^{-1} \tag{18}$$

Let's introduce a few notations. Denote by g_F the Niho bent function defined by an o-polynomial F. When Niho bent functions g_F and $g_{\bar{F}}$ are EA-equivalent (EA-inequivalent), we will write $g_F \sim_{EA} g_{\bar{F}}$ (respectively, $g_F \nsim_{EA} g_{\bar{F}}$). We will use notation "$A \overset{(\mathrm{p})}{=} B$", when the expression B is obtained from the expression A using equality number p.

Theorem 5. *Let F be an o-polynomial. Then an o-polynomial $\bar{F}$ obtained from F using one generator of the modified magic action and the inverse map can produce a Niho bent function EA-inequivalent to those defined by F and F^{-1} only if $\bar{F} = (F')^{-1}$.*

Proof. Assume $\bar{F}$ is an o-polynomial which is obtained from o-polynomial F using one generator of the modified magic action and the inverse map, i.e. $\bar{F}$ has one of the following forms: $hF, hF^{-1}, (hF)^{-1}, (hF^{-1})^{-1}$, where $h \in H$.

As we show below, when h is $\tilde{\sigma}_a$, $\tilde{\tau}_c$ or ρ_{2^j}, $\bar{F}$ defines a Niho bent function EA-equivalent to those defined by F or F^{-1}.

a) Let h be $\tilde{\sigma}_a, a \in \mathbb{F}^*_{2^m}$. Then $hF(x) = \tilde{\sigma}_a F(x) = \frac{1}{F(a)}F(ax)$ and by Lemma 1, the corresponding Niho bent function is EA-equivalent to those defined by F. By the same reason $hF^{-1} = \tilde{\sigma}_a F^{-1}$ and F^{-1} define EA-equivalent Niho bent functions. Further note that

$$(hF)^{-1}(x) = (\tilde{\sigma}_a F)^{-1}(x) \overset{(12)}{=} \tilde{\sigma}_{F(a)}F^{-1}(x).$$

Hence, $g_{(\tilde{\sigma}_a F)^{-1}} \sim_{EA} g_{F^{-1}}$ and

$$(hF^{-1})^{-1}(x) = (\tilde{\sigma}_a F^{-1})^{-1}(x) \overset{(12)}{=} \tilde{\sigma}_{F^{-1}(a)}(F^{-1})^{-1}(x) = \tilde{\sigma}_{F^{-1}(a)}F(x),$$

and therefore $g_{(\tilde{\sigma}_a F^{-1})^{-1}} \sim_{EA} g_F$.

b) Suppose h is $\tilde{\tau}_c$ with $c \in \mathbb{F}_{2^m}$. Then $hF(x) = \tilde{\tau}_c F(x) = \alpha_F^c(F(x+c) + F(c))$ and $hF^{-1}(x) = \tilde{\tau}_c F^{-1}$ define Niho bent functions EA-equivalent to those defined by F and F^{-1} respectively (by Lemma 3). Hence,

$$(hF)^{-1}(x) = (\tilde{\tau}_c F(x))^{-1}(x) \overset{(11)}{=} \tau_{F(c)}F^{-1}((\alpha_F^c)^{-1}x)$$

yields that $g_{(hF)^{-1}} \sim_{EA} g_F$ and from

$$(hF^{-1})^{-1}(x) = (\tilde{\tau}_c F^{-1})^{-1}(x) \overset{(11)}{=} \tau_{F^{-1}(c)}(F^{-1})^{-1}\Big(\frac{1}{\alpha_{F^{-1}}^c}x\Big) = \tau_{F^{-1}(c)}F\Big(\frac{1}{\alpha_{F^{-1}}^c}x\Big)$$

follows $g_{(hF^{-1})^{-1}} \sim_{EA} g_F$.

c) Take now $h = \rho_{2^j}$ with $0 \le j \le m-1$. Then $hF(x) = \rho_{2^j}F(x) = (F(x^{2^{-i}}))^{2^i}$ and $hF^{-1}(x) = \rho_{2^j}F^{-1} = (F^{-1}(x^{2^{-i}}))^{2^i}$, and by Lemma 2 we get that $g_{\rho_{2^j}F}$ and $g_{\rho_{2^j}F^{-1}}$ are EA-equivalent to g_F and $g_{F^{-1}}$, respectively. Therefore, from $(hF)^{-1}(x) = (\rho_{2^j}F)^{-1}(x) \overset{(13)}{=} \rho_{2^j}F^{-1}$ and $(hF^{-1})^{-1}(x) = (\rho_{2^j}F^{-1})^{-1} \overset{(13)}{=} \rho_{2^j}F$ it follows that $g_{(\rho_{2^j}F)^{-1}} \sim_{EA} g_{F^{-1}}$ and $g_{(\rho_{2^j}F^{-1})^{-1}} \sim_{EA} g_F$.

d) Consider $h = \prime$. The Niho bent function defined by an o-polynomial $hF(x) = F'(x) = xF(x^{-1})$ is

$$g_{F'}(x,y) = Tr_m(x(F'(\frac{y}{x}))) = Tr_m(x\frac{y}{x}F((\frac{y}{x})^{-1})) = Tr_m(yF(\frac{x}{y})) = g_F(y,x),$$

i.e. $g_{F'} \sim_{EA} g_F$. Similarly, $g_{(F^{-1})'} \sim_{EA} g_{F^{-1}}$.

The function $(hF)^{-1}(x) = (F')^{-1}(x) = (xF(x^{-1}))^{-1}$ can define a Niho bent function EA-inequivalent to those defined by F and F^{-1}. For example, an o-monomial x^{2^i} defines three surely EA-inequivalent Niho bent functions corresponding to o-polynomials F, F^{-1} and $(F')^{-1}$ [7].
Using equality (18), we immediately get that a Niho bent function defined by the o-polynomial $(hF^{-1})^{-1}(x) = ((F^{-1})')^{-1}(x)$ is EA-equivalent to one defined by $(F')^{-1}$. □

We rewrite the equalities of Lemmas 4, 5 and 6 in a more compact way. Equalities (8) - (10) as

$$h_{b_1} \circ h_{b_2}F = h_{b_3}F, \tag{19}$$

where $h_{b_1}, h_{b_2}, h_{b_3}$ are the same generators from the set $H \setminus \{\prime\}$ with different parameters $b_1, b_2, b_3 \in \mathbb{F}_{2^m}$.
Equalities (11) - (13) as

$$(h_{b_1}F)^{-1} = h_{b_2}F^{-1}, \tag{20}$$

where h_{b_1}, h_{b_2} are the same generators from the set $H \setminus \{\prime\}$ with different parameters $b_1, b_2 \in \mathbb{F}_{2^m}$. Note that right and left parts of the equality (11) have

different arguments, but it does not play any role in our study of EA-equivalence of resulting Niho bent functions.
Equalities (14) - (15) as

$$\tilde{\tau}_{c_1} \circ h_b F = h_b \circ \tilde{\tau}_{c_2} F, \tag{21}$$

where $h_b \in \{\tilde{\sigma}_a, \rho_{2^j}\}$. And equalities (16) - (17) as

$$(h_{b_1} F)' = h_{b_2} F', \tag{22}$$

where h_{b_1}, h_{b_2} are the same generators from the set $\{\tilde{\sigma}_a, \rho_{2^j}\}$ with different parameters $b_1, b_2 \in \mathbb{F}_{2^m}$.

To make the formulation of the next theorem more visual instead of using the notation $'$ we will use the initial one, i.e. φ. We will also refer to the original notation φ in some parts of the proof when convenient. Further, by *"reduce o-polynomial"* we mean that the original o-polynomial and the new one (reduced) define EA-equivalent Niho bent functions. When we are saying *"delete generator"* we mean that if we skip this generator the new o-polynomial will define a Niho bent function EA-equivalent to one generated by the original o-polynomial.

Let i be a positive integer and $k_i \geq 0$. By H_i we denote a composition of length k_i of generators φ and $\tilde{\tau}_c$ following each other as follows:

$$H_i = \underbrace{\varphi \circ \tilde{\tau}_{c_{i_1}} \circ \varphi \circ \tilde{\tau}_{c_{i_2}} \circ \dots}_{k_i} \tag{23}$$

That is, if F is an o-polynomial and we denote $T_j = \varphi \circ \tilde{\tau}_{c_{i_j}}$, $0 \leq j < (k_i + 1)/2$ then

$$H_i F = \begin{cases} F & \text{if } k_i = 0, \\ \varphi F & \text{if } k_i = 1, \\ T_1 \circ \ldots \circ T_{s_i} F & \text{if } k_i = 2s_i, \\ T_1 \circ \ldots \circ T_{s_i} \circ \varphi F & \text{if } k_i = 2s_i + 1. \end{cases}$$

In the theorem below we prove that for a given o-polynomial we can derive all EA-inequivalent Niho bent functions only using transformations φ, $\tilde{\tau}_c$ and the inverse map in a special sequence.

Theorem 6. *Let F be an o-polynomial, g_F the corresponding Niho bent function and G_F the class of all functions o-equivalent to g_F. Then o-polynomials of the form*

$$(H_1(H_2(H_3(\dots(H_q F)^{-1}\dots)^{-1})^{-1})^{-1}, \tag{24}$$

where H_i is defined by (23), for all $i \in \{1 \dots q\}$, $q \geq 1$, and $k_i \geq 1$ for $i \geq 3$, $k_i \geq 0$ for $i \leq 2$, provide representatives for all EA-equivalence classes within G_F. That is, up to EA-equivalence, all Niho bent functions o-equivalent to g_F arise from (24).

Proof. Note first that we can get F itself in the form (24) if we take $q = 2$, $k_1 = k_2 = 0$. if $q = 1$ and $k_1 = 0$ then we get F^{-1}. Further we have a restriction $k_i \geq 1$ for $i \geq 3$ to avoid repetitions.

According to Proposition 1 any function o-equivalent to g_F corresponds to an o-polynomial of the form

$$h_1 \circ h_2 \circ \ldots \circ h_k F, \tag{25}$$

where $h_1, h_2, \ldots, h_k$ (for some $k \geq 0$) are generators of the modified magic action and the inverse map. Our aim is to simplify this expression to exclude as many cases leading to EA-equivalent functions as possible. That is, we exclude certain sequences of generators which surely lead to EA-equivalent Niho bent functions. By h_{i_j} we denote a generator of the same type as h_i but with a different parameter.

From Theorem 5 it follows

a) If $h_1 \in H$, then $g_{h_1 \circ h_2 \circ \ldots \circ h_k F} \sim_{EA} g_{h_2 \circ \ldots \circ h_k F}$ and we can consider reduced o-polynomial $h_2 \circ \ldots \circ h_k F$;

b) If h_1 is the inverse map and $h_2 \in H \backslash \{\prime\}$ then $g_{h_1 \circ h_2 \circ \ldots \circ h_k F} \sim_{EA} g_{h_1 \circ h_3 \circ \ldots \circ h_k F}$, so we can consider the reduced o-polynomial $h_1 \circ h_3 \circ \ldots \circ h_k F$.

Hence, if $k = 1$ in (25) then we can get an EA-inequivalent case only if h_1 is the inverse map, and it corresponds to (24) with $q = 1$ and $k_1 = 0$. If $k = 2$ in (25) (and it cannot be reduced to the case $k = 1$) then we can get EA-inequivalent cases only if h_1 is the inverse map and $h_2 = \prime$, and it corresponds to (24) with $q = 1$ and $k_1 = 1$. If $k \geq 3$ we can reduce (25) until at some moment we will get an o-polynomial $h_i \circ h_{i+1} \circ \ldots \circ h_k F$, where h_i is the inverse map and $h_{i+1} = \prime$, that is, we have

$$((h_{i+2} \circ \ldots \circ h_k F)')^{-1}. \tag{26}$$

Note that here and further we assume that k is large enough to allow such a redaction while otherwise, it is easy to see that the process would stop and provide a formula (24) for some parameters.

If $h_{i+2} \in \{\tilde{\sigma}_a, \rho_{2^j}\}$ or h_{i+2} is the inverse map then we can delete the generator h_{i+2} and consider the reduced o-polynomial $h_i \circ h_{i+1} \circ h_{i+3} \circ \ldots \circ h_k F$. Indeed, suppose $h_{i+2} \in \{\tilde{\sigma}_a, \rho_{2^j}\}$ then

$h_i \circ h_{i+1} \circ h_{i+2} \circ \ldots \circ h_k F = ((h_{i+2} \circ \ldots \circ h_k F)')^{-1} \overset{(22)}{=}$

$(h_{(i+2)_1} \circ (h_{i+3} \circ \ldots \circ h_k F)')^{-1} \overset{(20)}{=} h_{(i+2)_2} \circ ((h_{i+3} \circ \ldots \circ h_k F)')^{-1}$

and, according to (a), $g_{h_i \circ h_{i+1} \circ h_{i+2} \circ \ldots \circ h_k F} \sim_{EA} g_{h_i \circ h_{i+1} \circ h_{i+3} \circ \ldots \circ h_k F}$. In the case when h_{i+2} is the inverse map, using (18) we get the same result that the o-polynomials $(((h_{i+3} \circ \ldots \circ h_k F)^{-1})')^{-1} = ((h_{i+3} \circ \ldots \circ h_k F)')^{-1})'$ and $((h_{i+3} \circ \ldots \circ h_k F)')^{-1} = h_i \circ h_{i+1} \circ h_{i+3} \circ \ldots \circ h_k F$ define EA-equivalent Niho bent functions.

If h_{i+2} is $\prime$, then h_{i+1} and h_{i+2} eliminate each other: $h_i \circ h_{i+1} \circ h_{i+2} \circ \ldots \circ h_k F = h_i \circ h_{i+3} \circ \ldots \circ h_k F$. If $h_{i+2} = \tilde{\tau}_c$, then we cannot eliminate it from the o-polynomial $h_i \circ h_{i+1} \circ h_{i+2} \ldots \circ h_k F$.

Further consider an o-polynomial $h_i \circ h_{i+1} \circ h_{i+2} \circ \ldots \circ h_k F$ where h_i is the inverse map, $h_{i+1} = \prime$, $h_{i+2} = \tilde{\tau}_c$, i.e. an o-polynomial

$$((\tilde{\tau}_c \circ h_{i+3} \circ \ldots \circ h_k F)')^{-1}. \tag{27}$$

When $k = i + 2$ then we get $((\tilde{\tau}_c F)')^{-1}$ which has the form (24) with $q = 1$ and $k_1 = 2$. Hence, in (27) we can assume that $k \geq i + 3$. Further we can reduce h_{i+3} from (27) unless h_{i+3} is $\prime$. Indeed, consider first $h_{i+3} \in \{\tilde{\sigma}_a, \rho_{2^j}\}$ then

$((\tilde{\tau}_c \circ h_{i+3} \circ \ldots \circ h_k F)')^{-1} \overset{(21)}{=} ((h_{i+3} \circ \tilde{\tau}_{c_1} \circ h_{i+4} \circ \ldots \circ h_k F)')^{-1} \overset{(22)}{=}$
$(h_{(i+3)_1} \circ (\tilde{\tau}_{c_1} \circ \ldots \circ h_k F)')^{-1} \overset{(20)}{=} h_{(i+3)_2} \circ ((\tilde{\tau}_{c_1} \circ h_{i+4} \circ \ldots \circ h_k F)')^{-1}$.
The last o-polynomial defines a Niho bent function EA-equivalent to one defined by the o-polynomial $((\tilde{\tau}_{c_1} \circ h_{i+4} \circ \ldots \circ h_k F)')^{-1} = h_i \circ h_{i+1} \circ h_{(i+2)_1} \circ h_{i+4} \circ \ldots \circ h_k F$.
If $h_{i+3} = \tilde{\tau}_{c_1}$, then using (8) we immediately get $h_i \circ h_{i+1} \circ h_{i+2} \circ h_{i+3} \circ \ldots \circ h_k F = h_i \circ h_{i+1} \circ h_{(i+2)_1} \circ h_{i+4} \circ \ldots \circ h_k F$, where $h_{(i+2)_1} = \tilde{\tau}_{c+c_1}$.
If h_{i+3} is the inverse map then
$h_i \circ h_{i+1} \circ h_{i+2} \circ h_{i+3} \circ \ldots \circ h_k F = ((\tilde{\tau}_c((h_{i+4} \circ \ldots \circ h_k F)^{-1}))')^{-1} \overset{(20)}{=}$
$(((\tilde{\tau}_{c_1} \circ h_{i+4} \circ \ldots \circ h_k F)^{-1})')^{-1} = (((\tilde{\tau}_{c_1} \circ h_{i+4} \circ \ldots \circ h_k F)')^{-1})'$, defines a Niho bent function EA-equivalent to the one defined by $((\tilde{\tau}_{c_1} \circ h_{i+4} \circ \ldots \circ h_k F)')^{-1} = h_i \circ h_{i+1} \circ h_{(i+2)_1} \circ h_{i+4} \circ \ldots \circ h_k F$.
Note that we could eliminate h_{i+3} as the inverse here because it is followed by $h_{i+2} = \tilde{\tau}_c$, $h_{i+1} = \prime$ and h_i as the inverse map.

Hence, if (25) produces a Niho bent function g EA-inequivalent to those corresponding to F, F^{-1}, $(F')^{-1}$ and $((\tilde{\tau}_c F)')^{-1}$ then g is EA-equivalent to the function corresponding to an o-polynomial

$$(\varphi \circ \tilde{\tau}_{c'} \circ \varphi \circ h_{l'} \circ \ldots \circ h_k F)^{-1}. \tag{28}$$

Now consider an o-polynomial of the form:

$$(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \circ h_l \circ \ldots \circ h_k F)^{-1}. \tag{29}$$

Case 1. First we restrict to the case $h_l, \ldots, h_k \in H$ when considering (29). Note that if l is an even number in (29), then the generator φ acts on h_l; if l is odd, then the generator $\tilde{\tau}_c$ acts on h_l (for some $c \in \mathbb{F}_{2^m}$). We consider l odd case, i.e. $l = 2t+1$ while for l even case the proof is similar and we skip it.
If $h_{2t+1} \in \{\tilde{\sigma}_a, \rho_{2^j}\}$ then
$(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \circ \tilde{\tau}_{c_t} \circ h_{2t+1} \circ \ldots \circ h_k F)^{-1} \overset{(21)}{=}$
$(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \ldots \circ \varphi \circ h_{2t+1} \circ \tilde{\tau}_{c_{t_1}}(h_{2t+2} \circ \ldots \circ h_k F))^{-1} \overset{(22)}{=}$
$(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \ldots \circ h_{(2t+1)_1} \circ \varphi(\tilde{\tau}_{c_{t_1}}(h_{2t+2} \circ \ldots \circ h_k F)))^{-1} \overset{(21)}{=}$
$\ldots$
$(h_{(2t+1)_t}(\varphi(\tilde{\tau}_{c_{1_1}}(\varphi(\ldots(\tilde{\tau}_{c_{t_1}}(h_{2t+2} \circ \ldots \circ h_k F))\ldots)))))^{-1} \overset{(20)}{=}$
$h_{(2t+1)_{t+1}}(\varphi(\tilde{\tau}_{c_{1_1}}(\varphi(\ldots(\tilde{\tau}_{c_{t_1}}(h_{2t+2} \circ \ldots \circ h_k F))\ldots))))^{-1}$,
hence we can reduce the o-polynomial $(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \circ \tilde{\tau}_{c_t} \circ h_{2t+1} \circ \ldots \circ h_k F)^{-1}$, and consider $(\varphi \circ \tilde{\tau}_{c_{1_1}} \circ \varphi \circ \tilde{\tau}_{c_{2_1}} \circ \varphi \circ \ldots \circ \tilde{\tau}_{c_{t_1}} \circ h_{2t+2} \circ \ldots \circ h_k F)^{-1}$.
If $h_{2t+1} = \tilde{\tau}_{c_{t+1}}$ then obviously we can consider o-polynomial
$((\tilde{\tau}_{c_1}(\tilde{\tau}_{c_2}(\ldots(\tilde{\tau}_{c_t+c_{t+1}}(h_{2t+2} \circ \ldots \circ h_k F))' \ldots)')')')^{-1}$.
If $h_{2t+1} = \prime$ then we cannot eliminate it.
Continuing this process we get for this case that the o-polynomial (25) can be reduced to $(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \circ F)^{-1}$ as in (23). This corresponds to the case $q = 1$ in (24).

Case 2. Now we consider (29) and allow $h_l, \ldots, h_k$ to be inverses too. We still assume l be odd and (as we saw earlier in the proof) w.l.o.g. $h_l, \ldots, h_k \in \{\prime, \tilde{\tau}_c, \text{the inverse} | c \in \mathbb{F}_{2^m}\}$. Take h_l the inverse (the other possibilities for h_l were discussed earlier in the proof), i.e. consider the following o-polynomial:

$$(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots (h_{l+1} \circ \ldots \circ h_k F)^{-1})^{-1}. \tag{30}$$

If h_{l+1} is the inverse, then it cancels with h_l. If h_{l+1} is $\tilde{\tau}_{c_{t+1}}$, then
$(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \circ (\tilde{\tau}_{c_{t+1}} \circ h_{l+2} \circ \ldots \circ h_k F)^{-1})^{-1} \overset{(20)}{=}$
$(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \circ \tilde{\tau}_{c_{(t+1)_1}}(h_{l+2} \circ \ldots \circ h_k F)^{-1})^{-1}$,
which is of the form (30) with fewer transformations in the inner brackets.

If h_{l+1} is φ then we get $(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \circ (\varphi \circ h_{l+2} \circ \ldots \circ h_k F)^{-1})^{-1}$.

If further h_{l+2} is $\tilde{\tau}_{c_{t+1}}$, then $(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \circ (\varphi \circ \tilde{\tau}_{c_{t+1}} \circ h_{l+3} \circ \ldots \circ h_k F)^{-1})^{-1}$. If h_{l+2} is the inverse or $h_{l+2} = \varphi$ then we get (30). Indeed, if $h_{l+2} = \varphi$ then it cancels with h_{l+1}, and if h_{l+2} is the inverse then we get:
$(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \circ (\varphi(h_{l+3} \circ \ldots \circ h_k F)^{-1})^{-1})^{-1} \overset{(18)}{=}$
$(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \circ \varphi(\varphi \circ h_{l+3} \circ \ldots \circ h_k F)^{-1})^{-1}$.

Continuing these process we will clearly transform (30) to (24) in a way that these o-polynomials produce EA-equivalent Niho bent functions. □

In this paper, when we say that two o-polynomials F and F' define potentially EA-inequivalent Niho bent functions g_F and $g_{F'}$, it means that either in some cases g_F and $g_{F'}$ are EA-inequivalent, or it is not possible to deduce EA-equivalence with the developed technics which leaves a possibility that g_F and $g_{F'}$ may be EA-inequivalent.

Below we consider some particular cases of formula (24).

Corollary 3. *Let F be an o-polynomial defined on $\mathbb{F}_{2^m}$. Then o-polynomials*

$$F_c^\circ(x) = \Big(\alpha_F^c x\Big(F\Big(\frac{1}{x} + c\Big) + F(c)\Big)\Big)^{-1}, \qquad c \in \mathbb{F}_{2^m} \tag{31}$$

define a sequence of Niho bent functions $g_{F_c^\circ}$ potentially EA-inequivalent to each other for different c, and EA-inequivalent to Niho bent functions defined by F, F^{-1}.

Proof. o-polynomial (31) is the explicit form of o-polynomial (24) for $q = 1, k_1 = 2$. Indeed,
$((\tilde{\tau}_c F)')^{-1}(x) = \Big(x\tilde{\tau}_c F\Big(\frac{1}{x}\Big)\Big)^{-1} = \Big(\alpha_F^c x\Big(F\Big(\frac{1}{x} + c\Big) + F(c)\Big)\Big)^{-1}$.

Note that $F_c^\circ = (F')^{-1}$ for $c = 0$. Hence, the o-polynomial $(F')^{-1}$ is included in the class of o-polynomials F_c°.

For $c = 1$ we get the function $F^\circ = \Big(x\Big(F\Big(\frac{1}{x} + 1\Big) + 1\Big)\Big)^{-1}$ studied in [7] and which can define a Niho bent function EA-inequivalent to those defined by F, F^{-1} and $(F')^{-1}$. For instance, when $F(x) = x^{2^i}$, g_{F° is EA-inequivalent to g_F, $g_{F^{-1}}$ and $g_{(F')^{-1}}$[7].

Using the equality (8) for every $c \in \mathbb{F}_{2^m}$ we can write:

$$F_c^\circ = ((\tilde{\tau}_c F)')^{-1} = ((\tilde{\tau}_1 \circ \tilde{\tau}_{c+1} F)')^{-1} = (\tilde{\tau}_{c+1} F)^\circ.$$

Since F°, F, F^{-1} and $(F')^{-1}$ can define four potentially EA-inequivalent Niho bent functions, we obtain that F_c° can define Niho bent functions potentially EA-inequivalent to those defined by $\tilde{\tau}_{c+1}F$, $(\tilde{\tau}_{c+1}F)^{-1}$, $((\tilde{\tau}_{c+1}F)')^{-1}$. It means that, for any $c \in \mathbb{F}_{2^m}$ a Niho bent function $g_{F_c^\circ}$ can be potentially EA-inequivalent to g_F, $g_{F^{-1}}$ and $g_{F_{c+1}^\circ}$. □

Corollary 4. *Let F be an o-polynomial defined on $\mathbb{F}_{2^m}$. Then o-polynomials*

$$(F_c^*)^{-1} = \Big(\alpha_{F'}^c\Big((1+cx)F\Big(\frac{x}{1+cx}\Big) + cxF\Big(\frac{1}{c}\Big)\Big)\Big)^{-1}, \quad c \in \mathbb{F}_{2^m} \tag{32}$$

define Niho bent functions $g_{(F_c^*)^{-1}}$ which can potentially be EA-inequivalent to each other for different c and EA-inequivalent to Niho bent functions defined by F, $(F')^{-1}$.

Proof. o-polynomial (32) is the explicit form of o-polynomial (24) for $q = 1$ and $k_1 = 3$. Indeed,

$$((\tilde{\tau}_c F')')^{-1}(x) = \Big(\alpha_{F'}^c x\Big(\Big(F'\Big(\frac{1}{x}+c\Big) + F'(c)\Big)\Big)^{-1} =$$
$$\Big(\alpha_{F'}^c x\Big(\frac{1+cx}{x}F\Big(\frac{x}{1+cx}\Big) + cF\Big(\frac{1}{c}\Big)\Big)\Big)^{-1} =$$
$$\Big(\alpha_{F'}^c\Big((1+cx)F\Big(\frac{x}{1+cx}\Big) + cxF\Big(\frac{1}{c}\Big)\Big)\Big)^{-1}.$$

Note that $(F_0^*)^{-1} = F^{-1}$. So the o-polynomial F^{-1} is included in the class of o-polynomials $(F_c^*)^{-1}$ with $c = 0$.
For $c = 1$ we get the function $(F_1^*)^{-1} = ((x+1)F(\frac{x}{x+1}) + x)^{-1}$ also studied in[7], and the Niho bent function associated with it is EA-equivalent to the one defined by F° [7]. But in the general case, for arbitrary $c \in \mathbb{F}_{2^m}$ we can't say that $(F_c^*)^{-1}$ defines an o-polynomial EA-equivalent to those defined by F and F_c°.

Using equalities (8) and (31) note that $(F_c^*)^{-1} = (F')_c^\circ = (\tilde{\tau}_{c+1}F')^\circ$.
Hence, we can say that $(F_c^*)^{-1} = (F')_c^\circ$ defines a Niho bent function potentially EA-inequivalent to Niho bent functions defined by F', $(F')^{-1}$ and $(F')_{c+1}^\circ = (F_{c+1}^*)^{-1}$. □

6.3 The case of o-monomials and the known o-polynomials

Further we study the consequences of the obtained results for the particular cases of o-monomials and the known o-polynomials.

Lemma 7. *For an o-monomial $F(x) = x^d$, the Niho bent functions defined by F_c° and F° are EA-equivalent, for any $c \in \mathbb{F}_{2^m}^*$.*

Proof. We have for $c \neq 0$

$$F_c^\circ(x) = (\varphi \circ \tilde{\tau}_c F)^{-1} = \Big(\alpha_F^c x\Big(\Big(F\Big(\frac{1}{x}+c\Big) + F(c)\Big)\Big)^{-1} =$$
$$\Big(\alpha_F^c x\Big(\Big(\frac{1}{x}+c\Big)^d + c^d\Big)\Big)^{-1} = \Big(\alpha_F^c x\Big(\Big(\frac{1+cx}{x}\Big)^d + c^d\Big)\Big)^{-1} =$$
$$\Big(\alpha_F^c c^d x\Big(\Big(\frac{1+cx}{cx}\Big)^d + 1\Big)\Big)^{-1} = \Big(\alpha_F^c c^{d-1} cx\Big(\Big(\frac{1+cx}{cx}\Big)^d + 1\Big)\Big)^{-1} = \frac{1}{c}F^\circ\Big(\frac{1}{\alpha_F^c c^{d-1}}x\Big).$$

From Lemma 1 it follows that Niho bent functions defined by F_c° and F° are EA-equivalent for any $c \neq 0$. □

From the proof of the previous lemma it is easy to see that for any o-monomial F

$$\varphi \circ \tilde{\tau}_c F(x) = \beta_c\, \varphi \circ \tau_1 F(cx), \tag{33}$$

where $\beta_c = \alpha_F^c c^{d-1}, c \in F_{2^m}^*$.

Lemma 8. *For an o-monomial $F(x) = x^d$, the Niho bent functions defined by $(F_c^*)^{-1}$, $(F^*)^{-1}$ and F° are EA-equivalent, for $c \in \mathbb{F}_{2^m}^*$.*

Proof. $F^*(x) = (x+1)F(\frac{x}{x+1}) + x = (x+1)(\frac{x}{x+1})^d + x$.
For $c \neq 0$ we have

$$(F_c^*)^{-1}(x) = (\varphi \circ \tau_c \circ \varphi F)^{-1} = \Big(\alpha_{F'}^c\Big((1+cx)F\Big(\frac{x}{1+cx}\Big) + cxF\Big(\frac{1}{c}\Big)\Big)\Big)^{-1} =$$
$$\Big(\alpha_{F'}^c\Big((1+cx)\Big(\frac{x}{1+cx}\Big)^d + cx\Big(\frac{1}{c}\Big)^d\Big)\Big)^{-1} =$$
$$\Big(\alpha_{F'}^c\Big(\frac{1}{c}\Big)^d\Big((1+cx)\Big(\frac{cx}{1+cx}\Big)^d + cx\Big)\Big)^{-1} = \frac{1}{c}(F^*)^{-1}\Big(\frac{c^d}{\alpha_{F'}^c}x\Big).$$

Using Lemma 1, we conclude that the Niho bent functions defined by $(F^*)^{-1}$ and $(F_c^*)^{-1}$ are EA-equivalent for $c \neq 0$. According to [7], the Niho bent function defined by $(F^*)^{-1}$ and F° are EA-equivalent, and taking into account Lemma 7, we get that Niho bent functions defined by $(F_c^*)^{-1}$, $(F^*)^{-1}$ and F° are EA-equivalent to each other for any $c \neq 0$. □

From the proof of above lemma it is easy to see that for any o-monomial F

$$\varphi \circ \tilde{\tau}_c \circ \varphi F(x) = \gamma_c\, \varphi \circ \tau_1 \circ \varphi F(cx). \tag{34}$$

where $\gamma_c = \alpha_{F'}^c c^{d-1}, c \in \mathbb{F}_{2^m}^*, F' = \varphi F$.

Further we will need the following equality, which holds for any o-polynomial F

$$\varphi \circ \tau_1 \circ \varphi F = \tau_1 \circ \varphi \circ \tau_1 F. \tag{35}$$

Indeed,
$\tau_1 \circ \varphi \circ \tau_1 F(x) = (1+x)\Big(F\Big(\frac{1}{1+x}+1\Big)+1\Big) + 1 = (1+x)F\Big(\frac{x}{1+x}\Big) + x =$
$\varphi \circ \tau_1 \circ \varphi F(x)$.

To keep notations as simple as possible, since we are interested in EA-equivalence of Niho bent functions and coefficients of arguments of o-polynomial do not affect on EA-equivalence of Niho bent functions as well as coefficient of o-polynomial, then instead of $aF(bx) = G(x)$ we will write $F \approx G$ for $a, b \in \mathbb{F}_{2^m}^*$.

Lemma 9. *Let F be an o-monomial defined on $\mathbb{F}_{2^m}$. Then*

$$\underbrace{\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \dots}_{k} F \approx \begin{cases} \begin{cases} \tau_1 F, & \text{if } t \equiv 0 \mod 4; \\ \varphi \circ \tau_1 F, & \text{if } t \equiv 1 \mod 4; \\ \tau_1 \circ \varphi F, & \text{if } t \equiv 2 \mod 4; \\ \varphi \circ \tau_1 \circ \varphi F, & \text{if } t \equiv 3 \mod 4; \end{cases} & \text{if } k = 2t \\ \begin{cases} \tau_1 \circ \varphi F, & \text{if } t \equiv 0 \mod 4; \\ \varphi \circ \tau_1 \circ \varphi F, & \text{if } t \equiv 1 \mod 4; \\ \tau_1 F, & \text{if } t \equiv 2 \mod 4; \\ \varphi \circ \tau_1 F, & \text{if } t \equiv 3 \mod 4; \end{cases} & \text{if } k = 2t+1, \end{cases}$$

where $t \geq 1$.

Proof. Assume that $k = 2t$, i.e. the orbit in the statment of this lemma has the form $\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \varphi \circ \tilde{\tau}_{c_t} F$. Then

1) For $t = 1$ we have $\varphi \circ \tilde{\tau}_{c_1} F \overset{(33)}{\approx} \varphi \circ \tilde{\tau}_1 F$.

2) For $t = 2$,

$\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} F \overset{(33)}{\approx} \varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tau_1 F \overset{(??)}{\approx} \varphi \circ \tau_1 \circ \varphi \circ \tilde{\tau}_{c_1} F \overset{(33)}{\approx} \varphi \circ \tau_1 \circ \varphi \circ \tau_1 F \overset{(35)}{\approx}$
$\varphi \circ \varphi \circ \tilde{\tau}_1 \circ \varphi F \approx \tau_1 \circ \varphi F$.

3) For $t = 3$,

$\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \tilde{\tau}_{c_3} F \overset{2)}{\approx} \varphi \circ \tilde{\tau}_{c_1} \circ \tau_1 \circ \varphi F \approx \varphi \circ \tilde{\tau}_{c_1+1} \circ \varphi F \overset{(??)}{\approx} \varphi \circ \tau_1 \circ \varphi F$

4) For $t = 4$

$\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \tilde{\tau}_{c_3} \circ \varphi \circ \tilde{\tau}_{c_4} F \overset{3)}{\approx} \varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tau_1 \circ \varphi F \overset{2)}{\approx} \tau_1 \circ \varphi(\varphi F) \approx \tau_1 F.$

Thus for even k ,

$\varphi \circ \tilde{\tau}_{c_1} \circ \ldots \circ \varphi \circ \tilde{\tau}_{c_{t-3}} \circ \varphi \circ \tilde{\tau}_{c_{t-2}} \circ \varphi \circ \tilde{\tau}_{c_{t-1}} \circ \varphi \circ \tilde{\tau}_{c_t} F \overset{4)}{\approx}$
$\varphi \circ \tilde{\tau}_{c_1} \circ \ldots \circ \varphi \circ \tilde{\tau}_{c_{t-4}} \circ \tau_1 F \approx \varphi \circ \tilde{\tau}_{c_1} \circ \ldots \circ \varphi \circ \tilde{\tau}_{c_{t-4}+1} F \overset{4)}{\approx}$
$\ldots$

$$\begin{cases} \tau_1 F, & \text{if } t \equiv 0 \mod 4; \\ \varphi \circ \tilde{\tau}_{c_1} \circ \tau_1 F \overset{1)}{\approx} \varphi \circ \tau_1 F, & \text{if } t \equiv 1 \mod 4; \\ \varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \tau_1 F \overset{2)}{\approx} \tau_1 \circ \varphi F, & \text{if } t \equiv 2 \mod 4; \\ \varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \tilde{\tau}_{c_3} \circ \tau_1 F \overset{3)}{\approx} \varphi \circ \tau_1 \circ \varphi F, & \text{if } t \equiv 3 \mod 4; \end{cases}$$

Note that φF is an o-monomial, therefore we can apply the previous formula to the case of odd k. Indeed,
$\varphi \circ \tilde{\tau}_{c_1} \circ \ldots \circ \varphi \circ \tilde{\tau}_{c_{t-3}} \circ \varphi \circ \tilde{\tau}_{c_{t-2}} \circ \varphi \circ \tilde{\tau}_{c_{t-1}} \circ \varphi \circ \tilde{\tau}_{c_t}(\varphi F) \approx$

$$\begin{cases} \tau_1 \circ \varphi F, & \text{if } t \equiv 0 \mod 4; \\ \varphi \circ \tau_1(\varphi F), & \text{if } t \equiv 1 \mod 4; \\ \tau_1 \circ \varphi(\varphi F) \approx \tau_1 F, & \text{if } t \equiv 2 \mod 4; \\ \varphi \circ \tau_1 \circ \varphi(\varphi F) \approx \varphi \circ \tau_1\ F, & \text{if } t \equiv 3 \mod 4; \end{cases}$$

□

Lemma 10. *Let F be an o-monomial defined on $\mathbb{F}_{2^m}$. Then*

$$\underbrace{\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots}_{k} (\varphi \circ \tau_1 F)^{-1} \approx$$

$$\begin{cases} \begin{cases} (\varphi \circ \tau_1 F)^{-1}, & \textit{if } t \equiv 0 \mod 3; \\ (\varphi \circ \tau_1(\varphi F)^{-1})^{-1}, & \textit{if } t \equiv 1 \mod 3; \\ (\varphi \circ \tau_1 \circ \varphi F^{-1})^{-1}, & \textit{if } t \equiv 2 \mod 3, \end{cases} & \textit{if } k = 2t \\ \begin{cases} (\varphi \circ \tau_1 F^{-1})^{-1}, & \textit{if } t \equiv 0 \mod 3; \\ (\varphi \circ \tau_1(\varphi F^{-1})^{-1})^{-1}, & \textit{if } t \equiv 1 \mod 3; \\ (\varphi \circ \tau_1 \circ \varphi F)^{-1}, & \textit{if } t \equiv 2 \mod 3, \end{cases} & \textit{if } k = 2t+1, \end{cases} \tag{36}$$

where $t \geq 1$.

Proof. Assume that $k = 2t$, i.e. the orbit in the statement of this lemma has the form $\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \varphi \circ \tilde{\tau}_{c_t} (\varphi \circ \tau_1 F)^{-1}$. Then

1) For $t = 1$ we get:

$\varphi \circ \tilde{\tau}_{c_1} (\varphi \circ \tau_1 F)^{-1} \overset{(20)}{\approx} \varphi (\tilde{\tau}_{c_{1_1}} \circ \varphi \circ \tau_1 F)^{-1} \overset{(18)}{\approx} (\varphi (\varphi \circ \tilde{\tau}_{c_{1_1}} \circ \varphi \circ \tau_1 F)^{-1})^{-1} \overset{(??)}{\approx}$

$(\varphi (\varphi \circ \tau_1 \circ \varphi \circ \tilde{\tau}_{c_{1_1}} F)^{-1})^{-1} \overset{(33)}{\approx} (\varphi (\varphi \circ \tau_1 \circ \varphi \circ \tau_1 F)^{-1})^{-1} \overset{(35)}{\approx} (\varphi (\tau_1 \circ \varphi F)^{-1})^{-1} \overset{(20)}{\approx}$

$(\varphi \circ \tau_1 (\varphi F)^{-1})^{-1}$.

2) For $t = 2$

$\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tau_{c_2} (\varphi \circ \tau_1 F)^{-1} \overset{1)}{\approx} \varphi \circ \tilde{\tau}_{c_1} (\varphi \circ \tau_1 (\varphi F)^{-1})^{-1} \overset{1)}{\approx} (\varphi \circ \tau_1 (\varphi (\varphi F)^{-1})^{-1})^{-1} \overset{(18)}{\approx}$

$(\varphi \circ \tau_1 \circ \varphi F^{-1})^{-1}$.

3) For $t = 3$,

$\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \tau_{c_3} (\varphi \circ \tau_1 F)^{-1} \overset{2)}{\approx} \varphi \circ \tilde{\tau}_{c_1} (\varphi \circ \tau_1 \circ \varphi F^{-1})^{-1} \overset{1)}{\approx} (\varphi \circ \tau_1 F)^{-1}$.

Thus,

$\varphi \circ \tilde{\tau}_{c_1} \circ \ldots \varphi \circ \tilde{\tau}_{c_{t-2}} \circ \varphi \circ \tilde{\tau}_{c_{t-1}} \circ \varphi \circ \tilde{\tau}_{c_t} (\varphi \circ \tau_1 F)^{-1} \overset{3)}{\approx}$

$\varphi \circ \tilde{\tau}_{c_1} \circ \ldots \varphi \circ \tilde{\tau}_{c_{t-3}} (\varphi \circ \tau_1 F)^{-1} \overset{3)}{\approx}$

$\ldots$

$$\begin{cases} (\varphi \circ \tau_1 F)^{-1}, \text{ if } t \equiv 0 \mod 3; \\ \varphi \circ \tilde{\tau}_{c_1} (\varphi \circ \tau_1 F)^{-1} \overset{1)}{\approx} (\varphi \circ \tau_1 (\varphi F)^{-1})^{-1}, \text{ if } t \equiv 1 \mod 3; \\ \varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} (\varphi \circ \tau_1 F)^{-1} \overset{2)}{\approx} (\varphi \circ \tau_1 \circ \varphi F^{-1})^{-1}, \text{ if } t \equiv 2 \mod 3. \end{cases}$$

Note that from (18) follows that $\varphi (\varphi \circ \tau_1 F)^{-1} = (\varphi (\tau_1 F)^{-1})^{-1} = (\varphi \circ \tau_1 F^{-1})^{-1}$. Therefor the case of odd k comes down to the previous case. Indeed,

$\varphi \circ \tilde{\tau}_{c_1} \circ \ldots \varphi \circ \tilde{\tau}_{c_{t-2}} \circ \varphi \circ \tilde{\tau}_{c_{t-1}} \circ \varphi \circ \tilde{\tau}_{c_t} \circ \varphi (\varphi \circ \tau_1 F)^{-1} \overset{3)}{\approx}$

$\varphi \circ \tilde{\tau}_{c_1} \circ \ldots \varphi \circ \tilde{\tau}_{c_{t-2}} \circ \varphi \circ \tilde{\tau}_{c_{t-1}} \circ \varphi \circ \tilde{\tau}_{c_t} (\varphi \circ \tau_1 F^{-1})^{-1} \approx$

$$\begin{cases} (\varphi \circ \tau_1 F^{-1})^{-1}, \text{ if } t \equiv 0 \mod 3; \\ (\varphi \circ \tau_1 (\varphi F^{-1})^{-1})^{-1}, \text{ if } t \equiv 1 \mod 3; \\ (\varphi \circ \tau_1 \circ \varphi F)^{-1}, \text{ if } \equiv 2 \mod 3. \end{cases}$$

□

Lemma 11. *Let F be an o-monomial. Then for $q \geq 3$*

$$(H_1 (H_2 (\ldots (H_q F)^{-1} \ldots)^{-1})^{-1})^{-1} \approx \begin{cases} \tau_1 G^{-1}; \\ (\varphi \circ \tau_1 G)^{-1}; \\ \varphi \circ \tau_1 G, \end{cases}$$

where $G \in \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$ and H_i are defined by (23) for all $1 \leq i \leq q$.

Proof. First consider the following cases:

1. $q = 1$. It is easy to see that from Lemma 9 follows

$$(H_1 F)^{-1} \approx \begin{cases} (\tau_1 F)^{-1} \approx \tau_1 F^{-1}; \\ (\varphi \circ \tau_1 F)^{-1}; \\ (\tau_1 \circ \varphi F)^{-1} \approx \tau_1 (\varphi F)^{-1}; \\ (\varphi \circ \tau_1 \circ \varphi F)^{-1}; \end{cases} = \begin{cases} \tau_1 G^{-1}; \\ (\varphi \circ \tau_1 G)^{-1}, \end{cases} \tag{37}$$

where $G \in \{F, \varphi F\}$

2. $q = 2$. Obviously from Lemma 10 we have

$$(H_1(\varphi \circ \tau_1 F)^{-1})^{-1} = \varphi \circ \tau_1 \overline{G}, \tag{38}$$

where $\overline{G} \in \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$.

Using (37) and (38) we get

$$(H_1(H_2F)^{-1})^{-1} \overset{37}{\approx} \begin{cases} (H_1 \circ \tau_1 G_1^{-1})^{-1} \overset{37}{\approx} \begin{cases} \tau_1 G_2^{-1}; \\ (\varphi \circ \tau_1 G_2)^{-1}; \end{cases} \\ (H_1(\varphi \circ \tau_1 G_1)^{-1})^{-1} \overset{38}{\approx} \varphi \circ \tau_1 \overline{G}_2, \end{cases} \tag{39}$$

where
$G_1 \in \{F, \varphi F\}$,
$G_2 \in \{G_1^{-1}, \varphi G_1^{-1}\} = A_1$,
$\overline{G}_2 \in \{G_1, (\varphi G_1)^{-1}, \varphi G_1^{-1}, G_1^{-1}, (\varphi G_1^{-1})^{-1}, \varphi G_1\} = A_2$.
It is easy to see that

$$A_1 = \{F^{-1}, (\varphi F)^{-1}, \varphi F^{-1}, (\varphi F^{-1})^{-1}\},$$

$$A_2 = \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}.$$

Indeed,
if we take $G_1 = F$ in A_2, then we get $\{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$,
if we take $G_1 = \varphi F$, then we get the same set of o-polynomials, since
$(\varphi(\varphi F)^{-1})^{-1} \overset{(18)}{=} ((\varphi F^{-1})^{-1})^{-1} = \varphi F^{-1}$.

Note that all functions in the sets A_1 and A_2 are o-monomials.

3. $q = 3$,

$$(H_1(H_2(H_3F)^{-1})^{-1})^{-1} \overset{(39)}{\approx} \begin{cases} (H_1 \circ \tau_1 G_2^{-1})^{-1} \overset{(37)}{\approx} \begin{cases} \tau_1 G_3^{-1}; \\ (\varphi \circ \tau_1 G_3)^{-1}, \end{cases} \\ (H_1(\varphi \circ \tau_1 G_2)^{-1})^{-1} \overset{(38)}{\approx} \varphi \circ \tau_1 \overline{G}_3 \\ (H_1 \circ \varphi \circ \tau_1 \overline{G}_2)^{-1} \overset{(37)}{\approx} \begin{cases} \tau_1 \tilde{G}_3^{-1}; \\ (\varphi \circ \tau_1 \tilde{G}_3)^{-1}, \end{cases} \end{cases}$$

where $G_3 \in \{G_2^{-1}, \varphi G_2^{-1}\}$, $\overline{G}_3 \in \{G_2, \varphi G_2^{-1}, (\varphi G_2)^{-1}, G_2^{-1}, (\varphi G_2^{-1})^{-1}, \varphi G_2\}$,
$\tilde{G}_3 \in \{\overline{G}_2, \varphi \overline{G}_2\}$, $G_2 \in A_1$, $\overline{G}_2 \in A_2$.
Substituting in the corresponding sets o-monomials from A_1 and A_2, using (18), we get that $G_3, \overline{G}_3, \tilde{G}_3$ belong to A_2, therefore

$$(H_1(H_2(H_3F)^{-1})^{-1})^{-1} \approx \begin{cases} \tau_1 G_3^{-1}; \\ \varphi \circ \tau_1 G_3; \\ (\varphi \circ \tau_1 G_3)^{-1}, \end{cases}$$

where $G_3 \in A_2 = \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$.

We are going to prove this lemma by induction on the length of orbit q. For $q = 3$ the statement of the lemma is true as we saw above. Suppose that it is

true for any $l \leq q-1$ and $l \geq 3$. By our assumption:

$$(H_1(H_2(\dots(H_qF)^{-1}\dots)^{-1})^{-1} \approx \begin{cases} (H_1 \circ \tau_1 G^{-1})^{-1} \overset{(37)}{\approx} \begin{cases} \tau_1 G_1^{-1}; \\ (\varphi \circ \tau_1 G_1)^{-1}, \end{cases} \\ (H_1(\varphi \circ \tau_1 G)^{-1})^{-1} \overset{(38)}{\approx} \varphi \circ \tau_1 \overline{G}_1, \\ (H_1 \circ \varphi \circ \tau_1 G)^{-1} \overset{(37)}{\approx} \begin{cases} \tau_1 \tilde{G}_1^{-1}; \\ (\varphi \circ \tau_1 \tilde{G}_1)^{-1}, \end{cases} \end{cases}$$

where $G \in A_2$, $G_1 \in \{G^{-1}, \varphi G^{-1}\}$, $\overline{G}_1 \in \{G, (\varphi G)^{-1}, \varphi G^{-1}, G^{-1}, (\varphi G^{-1})^{-1}, \varphi G\}$, $\tilde{G}_1 \in \{G, \varphi G\}$. By straightforward computations it is easy to see that all of the sets are equal to A_2, thus

$$(H_1(H_2(\dots(H_qF)^{-1}\dots)^{-1})^{-1} \approx \begin{cases} \tau_1 G^{-1}; \\ (\varphi \circ \tau_1 G)^{-1}; \\ \varphi \circ \tau_1 G, \end{cases}$$

where $G \in \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$, which proves our statement. □

Proposition 2. *The modified magic action and the inverse map applied to o-monomials give at most 4 EA-inequivalent functions. For an o-monomial F the 4 potentially EA-inequivalent bent functions are defined by $F, F^{-1}, (F')^{-1}$ and F°.*

Proof. We use Lemma 11 and discuss the cases $q = 1, 2$ and $q \geq 3$ separately.

1. $q = 1$. According to (37) $(H_1F)^{-1}$ has the following two forms $\tau_1 G^{-1}$ and $(\varphi \circ \tau_1 G)^{-1}$, where $G \in \{F, \varphi F\}$. The first function obviously defines Niho bent functions EA-equivalent to one defined by G^{-1} and therefore to those defined by F^{-1} and $(\varphi F)^{-1}$. The second function defines Niho bent functions EA-equivalent to one defined by F° (by Lemma 8).

2. $q = 2$. From (39) we have:

$$(H_1(H_2F)^{-1})^{-1} \approx \begin{cases} \tau_1 G_2^{-1}; \\ (\varphi \circ \tau_1 G_2)^{-1}; \\ \varphi \circ \tau_1 \overline{G}_2, \end{cases}$$

where
$G_2 \in \{F^{-1}, (\varphi F)^{-1}, \varphi F^{-1}, (\varphi F^{-1})^{-1}\}$,
$\overline{G}_2 \in \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$.

Obviously, $\tau_1 G_2^{-1}$ and $\varphi \circ \tau_1 \overline{G}_2$ define Niho bent function EA-equivalent to those defined by G_2^{-1} and $\overline{G}_2$ respectively, which in their turn define Niho bent functions EA-equivalent to F, F^{-1} and $(F')^{-1}$. $(\varphi \circ \tau_1 G_2)^{-1}$ defines functions EA-equivalent to one defined by F°. Indeed, $(\varphi \circ \tau_1 G_2)^{-1}$ has one of the following forms:

• $(\varphi \circ \tau_1 F^{-1})^{-1} \overset{(20)}{=} (\varphi(\tau_1 F)^{-1})^{-1} \overset{(18)}{=} \varphi(\varphi \circ \tau_1 F)^{-1}$ defines Niho bent function EA-equivalent to $(\varphi \circ \tau_1 F)^{-1} = F^\circ$

• $(\varphi \circ \tau_1 \circ \varphi F^{-1})^{-1}$, by Lemma 8 defines Niho bent functions EA-equivalent to $(\varphi \circ \tau_1 F^{-1})^{-1} = (\varphi(\tau_1 F)^{-1})^{-1} \overset{(18)}{=} \varphi(\varphi \circ \tau_1 F)^{-1}$, which defines functions EA-equivalent to one defined by $(\varphi \circ \tau_1 F)^{-1} = F^\circ$;

• $(\varphi \circ \tau_1 (\varphi F)^{-1})^{-1} \overset{(20)}{=} (\varphi(\tau_1 \circ \varphi F)^{-1})^{-1} \overset{(18)}{=} \varphi(\varphi \circ \tau_1 \circ \varphi F)^{-1}$ defines Niho bent function EA-equivalent to F°(by Lemma 8);

• $(\varphi\circ\tau_1(\varphi F^{-1})^{-1})^{-1} = (\varphi\circ\tau_1\circ\varphi(\varphi F)^{-1})^{-1} \overset{(35)}{=} (\tau_1\circ\varphi\circ\tau_1(\varphi F)^{-1})^{-1} \overset{(20)}{=} \tau_1(\varphi\circ\tau_1(\varphi F)^{-1})^{-1}$ defines Niho bent function EA-equivalent to $(\varphi\circ\tau_1(\varphi F)^{-1})^{-1}$, which by the previous case defines Niho bent function EA-equivalent to F°.

3. For $q \geq 3$ by Lemma 11,

$$(H_1(H_2(\ldots(H_qF)^{-1}\ldots)^{-1})^{-1} \approx \begin{cases}\tau_1G^{-1};\\ (\varphi\circ\tau_1G)^{-1};\\ \varphi\circ\tau_1G,\end{cases}$$

where $G \in \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$.

τ_1G^{-1} and $\varphi\circ\tau_1G$ define Niho bent function EA-equivalent to G^{-1} and G correspondingly, which in their turn define Niho bent functions EA-equivalent to F, F^{-1} and $(\varphi F)^{-1}$.
$(\varphi\circ\tau_1G)^{-1}$ defines Niho bent functions EA-equivalent to F°. Indeed, for G equals to $F^{-1}, (\varphi F)^{-1}, \varphi F^{-1}, (\varphi F^{-1})^{-1}$, we already prove it in the case $q = 2$. If $G = \varphi F$, then $(\varphi\circ\tau_1G)^{-1} = (\varphi\circ\tau_1\circ\varphi F)^{-1}$ which defines Niho bent function EA-equivalent to one defined by F° (by Lemma 8). If $G = F$, then $(\varphi\circ\tau_1F)^{-1} = F^\circ$. □

Proposition 3. *The modified magic action and the inverse map applied to the Frobenius map, give exactly 3 EA-inequivalent functions corresponding to F, F^{-1}, $(F')^{-1}$.*

Proof. For the Frobenius map $F(x) = x^{2^i}$ we have: $F^\circ = (F')^{-1} = x^{\frac{1}{1-2^i}}$. Hence by Proposition 2, F can potentially define 3 EA-inequivalent Niho bent functions corresponding to F, F' and $(F')^{-1}$. This 3 o-polynomials define 3 surly EA-inequivalent Niho bent functions [7]. □

The Payne o-polynomial can be represented via Dickson polynomials. Let us recall **Dickson Polynomials.** For every non-negative integer d Dickson polynomials $D_d(x)$ over $\mathbb{F}_{2^m}$ can be defined by a recursion relation in the following way:
$D_0(x) = 0, D_1(x) = x$, $D_{d+2}(x) = xD_{d+1} + D_d(x)$, for all integers $d \geq 0$.
It satisfies the following roperties:
1. $D_d \circ D_{d'} = D_{dd'}$.
2. If d is co-prime with $2^m - 1$, then D_d is a permutational polynomial.

Using Dickson polynomials we can prove the following results for the Payne o-polynomials.

Lemma 12. *Let $F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$. Then $F_c^\circ = (F_c^*)^{-1}$ for any $c \in \mathbb{F}_{2^m}$.*

Proof. Note first, that $F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}} = D_5(x^{\frac{1}{6}})$. Also it is easy to see that $F' = F$. Indeed,

$$F'(x) = xF(x^{-1}) = xD_5(x^{-\frac{1}{6}}) = x(x^{-\frac{1}{6}} + x^{-\frac{1}{2}} + x^{-\frac{5}{6}}) =$$
$$x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}} = D_5(x^{\frac{1}{6}}) = F(x).$$

Therefore $(F')^{-1} = F^{-1}$, and hence,

$$(F_c^*)^{-1} = ((\tau_cF')')^{-1} = ((\tau_cF)')^{-1} = F_c^\circ, \text{for any } c \in \mathbb{F}_{2^m}.$$

□

Proposition 4. *The modified magic action and the inverse map applied to o-polynomial $F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$ can potentially give EA-inequivalent Niho bent functions corresponding to o-polynomials F and F_c°, $c \in \mathbb{F}_{2^m}^*$.*

Proof. Immediately follows from Lemma 12. □

Example For $m = 5$ we checked computationally that the o-polynomial $F(x) = D_5(x^{\frac{1}{6}})$ over $\mathbb{F}_{2^m}$ defines 6 EA-inequivalent Niho bent functions corresponding to o-polynomials F, F^{-1} and $F_w^\circ, F_{w^3}^\circ, F_{w^5}^\circ$, where w is a primitive element of $\mathbb{F}_{2^m}$.

Remark The modified magic action and the inverse map applied to Subiaco, Adelaide and $x^{2^k} + x^{2^k+2} + x^{3\cdot 2^k+4}$ o-polinomials F can give a sequence of EA-inequivalent functions defined by o-polynomials on the orbits F, F^{-1}, F_c°, $(\tilde{\tau}_c F)_c^\circ$, $(\tilde{\tau}_c(F'))_c^\circ$ and so on.

7 The Known Hyperovals[1]

Over two decades, finite geometers determined the stabilizers of all known hyperovals. In this section we provide an explicit list of all o-polynomials which provide EA-inequivalent Niho bent functions for every of the known hyperoval. We start by giving an overview over the number of EA-inequivalent Niho bent functions for each known hyperoval.

Name	Hyperoval	Condition	Number	Ref.
Regular	x^2	$m = 1$	1	[23, Th. 4.1]
		$m = 2$	1	[23, Th. 4.1]
		$m \geq 3$	2	[23, Th. 4.2]
Irregular Translation	x^{2^i}	$m \geq 3$	3	[23, Th. 4.3]
Segre	x^6	$m = 5$	2	[23, Th. 4.4]
		$m > 5$ odd	4	[23, Th. 4.4]
Glynn I	$x^{3\sigma+4}$	$m \geq 7$ odd $\sigma = 2^{(m+1)/2}$	4	Th. 7
Glynn II	$x^{\sigma+\lambda}$	$m = 7$ $\sigma = 4 = \lambda$	2	Th. 7
		$m > 7$ odd $\sigma = 2^{(m+1)/2}$ $\lambda = 2^k$ for $m = 4k - 1$; $\lambda = 2^{3k+1}$ for $m = 4k + 1$	4	Th. 7

[1] Some of the results will repeat Section 6.2 results. We decided to keep both of them, since we use a mix of algebraic and geometric approach.

Cherowitzo	$x^\sigma + x^{\sigma+2} + x^{3\sigma+4}$	$m = 5$	10	[23, Th. 4.6]
		$m > 5$ prime	$\frac{4m+2^m-2}{m}$	Th. 9
		$m > 5$ odd	$n_C(m)$	[23]
Payne	$x^{1/6} + x^{3/6} + x^{5/6}$	$m \geq 5$ is prime	$\frac{3m+2^{m-1}-1}{m}$	Th. 8
		$m \geq 5$ is odd	$n_P(m)$	Th. 8
Lunelli-Sce (Subiaco)		$m = 4$ ν prim. root $\nu^4 = \nu + 1$	1	[23, Th. 4.1]
Subiaco		$m = 6$ $\lvert\text{Aut}\rvert = 60$	3	[32, p. 98]
		$m = 6$ $\lvert\text{Aut}\rvert = 15$	6	[32, p. 98]
		m odd $m = 7$	12	[34]
		m odd $m > 7$	$n_S(m)$	Th. 11
		$m \equiv 0 \pmod 4$ $m > 6$	$n_S(m)$	Th. 11
		$m \equiv 2 \pmod 4$ $m > 6$ $\lvert\text{Aut}\rvert = 10e$		Th. 12
		$m \equiv 2 \pmod 4$ $m > 6$ $\lvert\text{Aut}\rvert = 5e/2$ $5 \nmid m$		Th. 12
Adelaide		$m = 6$	8	[34]
		$m > 6$ m even	$n_A(m)$	Th. 10
O'Keefe-Penttila		$m = 5$	12	[22, Case 2][2]

Below, for given o-polynomials F_1 and F_2, we denote $F_1 \cong F_2$ if F_1 and F_2 define EA-equivalent Niho bent functions g_{F_1} and g_{F_2}.

Note that a matrix corresponding to the transformation $\varphi \circ \tau_c$ is

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} = \begin{pmatrix} c & 1 \\ 1 & 0 \end{pmatrix},$$

and that $\varphi \circ \tilde{\tau}_c = \alpha_F^c \cdot (\varphi \circ \tau_c)$. Hence, by Theorem 3 the hyperoval defined by the o-polynomial F_c° is obtained from the hyperoval defined by F using the

[2]Notice that the reference claims $1 + 110$ instead of $1 + 11$ orbits due to a typo.

following transformation matrix (the first matrix in the product corresponds to the inverse transformation):

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 \\ 0 & \alpha_F^c & \alpha_F^c F(c)/c \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \alpha_F^c & \alpha_F^c F(c)/c \\ 0 & 0 & 1 \\ 1 & 0 & c \end{pmatrix}.$$

That is,

$$F_c^\circ(x) = \left(\alpha_F^c x \Big(F\Big(\frac{1}{x} + c\Big) + F(c) \Big) \right)^{-1}$$

corresponds to the map

$$A_F^c := \begin{pmatrix} 0 & \alpha_F^c & \alpha_F^c F(c)/c \\ 0 & 0 & 1 \\ 1 & 0 & c \end{pmatrix}.$$

Also recall that the choice of an o-polynomial for a given hyperoval $\mathcal{H}$ only depends on which point of $\mathcal{H}$ is chosen as nucleus, so the o-polynomial is determined by the preimage of $(0,1,0)$. We have

$$A_F^c(c, F(c), 1)^T = (\alpha_F^c F(c) + \alpha_F^c F(c)/c, 1, c + c)^T = (0,1,0).$$

Hence, $F_c^\circ \cong F_d^\circ$ if and only if $\langle (c, F(c), 1) \rangle$ and $\langle (d, F(d), 1) \rangle$ lie in the same point orbit of the stabilizer of $\mathcal{H}$. To summarize, we have the following:

(a) $F_c^\circ \cong F_d^\circ$ if and only if $\langle (c, F(c), 1) \rangle$ and $\langle (d, F(d), 1) \rangle$ lie in the same point orbit;

(b) $F \cong F_c^\circ$ if and only if $\langle (0,1,0) \rangle$ and $\langle (c, F(c), 1) \rangle$ lie in the same point orbit;

(c) $F^{-1} \cong F_c^\circ$ if and only if $\langle (1,0,0) \rangle$ and $\langle (c, F(c), 1) \rangle$ lie in the same point orbit;

(d) $F \cong F^{-1}$ if and only if $\langle (0,1,0) \rangle$ and $\langle (1,0,0) \rangle$ lie in the same point orbit.

As guidelined in [8] we use the known results on orbits of the known hyperovals to get the explicit numbers and representations for o-polynomials which provide o-equivalent but EA-inequivalent Niho bent functions for each of the known hyperoval.

Lemma 13. *Let $m \geq 3$. The two o-polynomials obtained from the regular hyperoval $\mathcal{H}$, that is $F(x) = x^2$, are (up to EA-equivalence for the corresponding Niho bent functions) F and F^{-1}.*

Proof. By [23, Th. 4.2], one point orbit is the nucleus N and the other point orbit is $\mathcal{H} \setminus \{N\}$. Hence, F^{-1} is a representative of the second orbit. □

Lemma 14. *Let $m \geq 3$. The three o-polynomials obtained from the irregular translation hyperoval $\mathcal{H}$, that is $F(x) = x^{2^i}$ with $i > 1$ co-prime to m, are (up to EA-equivalence for the corresponding Niho bent functions) F, F^{-1} and F_0°.*

Proof. By [23, Th. 4.3], one point orbit is the nucleus $N = (0,1,0)$, another point orbit is $N' := (1,0,0)$, and the last point orbit is $\mathcal{H} \setminus \{N, N'\}$. Hence, F, F^{-1}, and F_0° are representatives of the three orbits. □

Lemma 15. *Let $m \geq 5$ be odd. Consider the Segre hyperoval $\mathcal{H}$, that is $F(x) = x^6$.*

(a) If $m = 5$, then the two o-polynomials obtained from $\mathcal{H}$ are (up to EA-equivalence for the corresponding Niho bent functions) F and F_1°.

(b) If $m > 5$, then the two o-polynomials obtained from $\mathcal{H}$ are (up to EA-equivalence for the corresponding Niho bent functions) F, F^{-1}, F_0°, and F_1°.

Proof. By [23, Th. 4.4], for $m = 5$ the point orbits of $\mathcal{H}$ are $\{(1,0,0),(0,1,0),(0,0,1)\}$ and all the remaining points. Hence, $(0,1,0)$ and $(1,1,1)$ are representatives, so we can choose F and F_1° as representatives. For $m > 5$ the first orbit splits into three orbits, so we have to add F^{-1} and F_0° to the previous list. □

Theorem 7. *The collineation stabiliser of a Glynn hyperoval has 4 orbits unless it is of type II and $m = 7$.*

Proof. First consider the case Glynn I. By [23, Th. 4.4] we have 4 orbits unless $(3\sigma+4)^2 - (3\sigma+4) + 1 \equiv 0 \pmod{2^m-1}$. This simplifies to

$$9 \cdot 2^{m+1} + 21 \cdot 2^{(m+1)/2} + 13 \equiv 31 + 21 \cdot 2^{(m+1)/2} \equiv 0 \pmod{2^m-1}.$$

One can easily check that this is never satisfied.

Now consider the case Glynn II. By [23, Th. 4.4] we have 4 orbits unless $(\sigma+\lambda)^2 - (\sigma+\lambda) + 1 \equiv 0 \pmod{2^m-1}$. For $m = 4k-1$, this is

$$2^{(3m+7)/4} - 2^{(m+1)/4} + 3 \equiv 0 \pmod{2^m-1}.$$

Equivality holds only for $m = 7$ as for $m > 7$ the left hand side is smaller than $2^m - 1$. The caluclation for $m = 4k+1$ is similar. □

Similar to Lemma 15, we obtain the following.

Lemma 16. *Let $m \geq 7$ be odd. Consider a hyperoval $\mathcal{H}$ of type Glynn I or Glynn II.*

(a) If $m = 7$, then the two o-polynomials obtained from $\mathcal{H}$ are (up to EA-equivalence for the corresponding Niho bent functions) F and F_1°.

(b) Otherwise, the four o-polynomials obtained from $\mathcal{H}$ are (up to EA-equivalence for the corresponding Niho bent functions) F, F^{-1}, F_0°, and F_1°.

Theorem 8. *The number of orbits of the collineation stabilizer of the Payne hyperoval $\mathcal{H}$ is given by $3 + \frac{2^{m-1}}{m}$ if m is a prime. More generally, the number of orbits are given by*

$$n_P(m) := 3 + \sum_{\ell \,|\, m,\, \ell>1} \left| \mathbb{F}_{2^\ell}^* \setminus \bigcup_{h \;|\; \ell,\; h<\ell} \mathbb{F}_{2^h}^* \right| / (2\ell).$$

For w a primitive element of $\mathbb{F}_q$ and $c = w^{2n}$, we get $F_c^\circ \cong F_d^\circ$ if and only if $d = w^{2^i n}$ or $d = w^{-2^i n}$ for some $i \in \{1,\ldots,m\}$. The o-polynomials F and F^{-1} define Niho bent functions EA-inequivalent to those defined by all other o-polynomials from $\mathcal{H}$.

Proof. By [23, Th. 4.5], the orbits are $\{(0,1,0)\}$, $\{(1,0,0),(0,0,1)\}$, and sets

$$\mathcal{H}_n := \{(w^{n2^i}, f(w^{n2^i}), 1) : i = 1, \ldots, m\} \cup \{(1, f(w^{n2^i}), w^{n2^i}) : i = 1, \ldots, m\},$$

where w is a primitive element of $\mathbb{F}_q$. Notice that $\mathcal{H}_0$ is $\{(1,1,1)\}$. For m prime it is easy to see that each orbit $\mathcal{H}_n$ has length m for $n > 1$, hence the total number of orbits is $3 + \frac{2^{m-1}-1}{m}$. In general, if $w^n \in \mathbb{F}_\ell$ with $\ell \mid m$, then $\{(w^n)^{2^i}\} \in \mathbb{F}_\ell$. This yields the general formula.

The description of the equivalence of F_c° and F_d° follows directly from the explicit description of the orbits. □

For example for $m = 5$, the previous result gives the following representatives for all 6 o-polynomials which can be obtained from the Payne hyperoval:

$$F,\ F^{-1},\ F_1^\circ,\ F_w^\circ,\ F_{w^3}^\circ,\ F_{w^5}^\circ.$$

Theorem 9. *The number of orbits of the collineation stabilizer of the Cherowitzo hyperoval is given by $4 + 2\frac{2^{m-1}-1}{m}$ if m is a prime. More generally, the number of orbits are given by*

$$n_C(m) := 3 + \sum_{\ell \mid m} \left| F^*(2^\ell) \setminus \bigcup_{h \mid \ell,\ h<\ell} \mathbb{F}_{2^h}^* \right| / \ell.$$

For w a primitive element of $\mathbb{F}_q$ and $c = w^{2n}$, we get $F_c^\circ \cong F_d^\circ$ if and only if $d = w^{2^i n}$ for some $i \in \{1, \ldots, m\}$. The Niho bent functions g_F and $g_{F^{-1}}$ are both EA-inequivalent to Niho bent functions defined by all other o-polynomials from $\mathcal{H}$.

Proof. Corollary 4.5 in [2] describes the stabilizer as

$$\{(x,y,z) \mapsto (x^\alpha, y^\alpha, z^\alpha) : \alpha \in \mathrm{Aut}(\mathbb{F}_q)\}.$$

The rest of the calculation is similar to the Payne hyperoval, just that this time the first and second coordinate cannot be interchanged. □

Theorem 10. *Let $[1] := \delta + \delta^{-1}$. For $c \in \mathbb{F}_q$, let*

$$O_c := \{c^{2^h} + \sum_{i=1}^{h-1} [1]^{2^i} : i = 0, \ldots, 2m-1\}.$$

The number of EA-inequivalent Niho bent functions obtained from the Adelaide hyperoval is $n_A(m) := 2 + |\{O_c : c \in F_q\}|$. In particular, for fixed $c \in F_q$, the Niho bent functions defined by the o-polynomials F, F^{-1}, F_c° are pairwise EA-inequivalent. Furthermore, $g_{F_c^\circ}$ and $g_{F_d^\circ}$ are EA-equivalent if and only if $d \in O_c$.

Proof. In [31, Eq. (9)] (in a slightly different representation) the stabilizer of the Adelaide polynomial was determined as the cyclic group generated by the map

$$\theta : x \mapsto \begin{pmatrix} 1 & 0 & [1] \\ 0 & 1 & [1] \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ F(x) \\ 1 \end{pmatrix}^2.$$

From this it is easily verified that θ fixes $(0,1,0)$ and $(1,0,0)$, so g_F and $g_{F^{-1}}$ are not EA-equivalent to those functions defined by any of the other o-polynomials. Furthermore, it is easily checked that the orbit of $(c, F(c), 1)$ is

$$\{(x, F(x), 1) : x \in O_c\}. \qquad \square$$

Theorem 11. *Let $m \geq 7$ with $m \not\equiv 2 \pmod 4$, let*

$$O_c := \{x^{(-1)^{i+1}2^i} : i = 0, \ldots, 2m-1\}.$$

The number of EA-inequivalent Niho bent functions obtained from the Subiaco hyperoval is $n_S(m) := 2 + |\{O_c : c \in F_q\}|$. In particular, for fixed $c \neq 0, 1$, the o-polynomials F, F^{-1}, F_0°, F_c° provide pairwise EA-inequivalent Niho bent functions. Furthermore, $g_{F_c^\circ}$ and $g_{F_d^\circ}$ are EA-equivalent if and only if $d \in O_c$.

Proof. By [24, Th. 13, Th. 16] (see also [15]), the stabilizer of the Subiaco hyperoval $\mathcal{H}$ is generated by the map

$$\theta : x \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ F(x) \\ 1 \end{pmatrix}^2.$$

From this it is easily verified that θ fixes $(0,1,0)$, $\{(1,0,0),(0,0,1)\}$, $(1,1,1)$, so Niho bent functions defined by F, $F^{-1} \cong F_0^\circ$, and F_1° are not EA-equivalent to those defined by any other o-polynomial obtained from $\mathcal{H}$. Furthermore, it is easily checked that the orbit of $(c, F(c), 1)$ is

$$\{(x, F(x), 1) : x \in O_c\}. \qquad \square$$

For $m \equiv 2 \pmod 4$ there are two types of non-equivalent hyperovals, see [33]. In particular, from Theorem 6.6 and Theorem 6.7 in [33] we obtain the following. We are not aware of any nice description of the orbits of the given groups, but the information is sufficient to calculate all o-polynomials efficiently.

Theorem 12. *Let $m \geq 6$ with $m \equiv 2 \pmod 4$.*

(a) If $F(x) = \frac{\delta^2(x^4+x)}{x^4+\delta^2x^2+1} + x^{1/2}$, then g_F is EA-inequivalent to all $g_{F_c^\circ}$ and we have $F^{-1} \cong F_0^\circ$. Furthermore, $F_c^\circ \cong F_d^\circ$ if and only if $(c, F(c), 1)^h = (d, F(d), 1)$ for an element h of the group (of size $10m$) generated by

- *(i)* $(x, y, z) \mapsto (z, y, x)$,
- *(ii)* $(x, y, z) \mapsto (x + \delta z, y + \delta^2 z, z)$,
- *(iii)* $(x, y, z) \mapsto (z^2 + \delta^2 x^2, z^2 + \delta y^2, z^2)$.

(b) If $F(x) = \frac{x^3+x^2+\delta^2x}{x^4+\delta^2x^2+1} + \delta x^{1/2}$, then g_F, $g_{F^{-1}}$, and $g_{F_0^\circ}$ are pairwise EA-inequivalent. Furthermore, $F_c^\circ \cong F_d^\circ$ if and only if $(c, F(c), 1)^h = (d, F(d), 1)^h$ for an element h of the group (of size $5m/2$) generated by

- *(i)* $(x, y, z) \mapsto (x^\sigma, y^\sigma, z^\sigma)$ *for* $\sigma \in Aut(F)$ *with* $\delta^\sigma = \delta$,
- *(ii)* $(x, y, z) \mapsto (z, y + \delta z, x + \delta z)$.

The O'Keefe-Penttila hyperoval for $m = 5$, which is not known to belong to any infinite family, is stabilized by the group generated by

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Hence, most orbits have the form $\{(c, F(c), 1), (1 + c^{-1}, 1 + c^{-1}F(c), 1), ((1 + c)^{-1}, c^{-1}(1 + F(c), 1)\}$. Then, representatives for the 14 o-polynomials obtained from the hyperoval and defining EA-inequivalent Niho bent functions are

$$F,\ F^{-1},\ F_w^\circ,\ F_{w^2}^\circ,\ F_{w^4}^\circ,\ F_{w^5}^\circ,\ F_{w^7}^\circ,\ F_{w^8}^\circ,\ F_{w^{10}}^\circ,\ F_{w^{14}}^\circ,\ F_{w^{16}}^\circ,\ F_{w^{19}}^\circ.$$

Here w is a primtive element of $\mathbb{F}_{2^5}$.

Acknowledgement

The authors would like to thank Alexander Kholosha for useful discussions. This research was supported by Trond Mohn Stiftelse (TMS) foundation. The work of Ferdinand Ihringer is supported by a postdoctoral fellowship of the Research Foundation – Flanders (FWO).

References

[1] K. Abdukhalikov, "Bent functions and line oval", *Finite Fields Appl.*, 47, pp. 97–124, 2017.

[2] L. Bayens, W. Cherowitzo and T. Penttila. "Groups of hyperovals in Desarguesian planes", *Inn. Inc. Geom.*, pp. 6–7, 2007.

[3] L. Budaghyan and C. Carlet, "CCZ-equivalence of single and multi output Boolean functions", AMS Contemporary Math. 518, *Post-proceedings of the conference Fq9*, pp. 43–54, 2010.

[4] L. Budaghyan and C. Carlet, "On CCZ-equivalence and its use in secondary constructions of bent functions", *Preproceedings of International Workshop on Coding and Cryptography WCC 2009*, pp. 19–36, 2009.

[5] L. Budaghyan, A. Kholosha, C. Carlet, and T. Helleseth, "Niho bent functions from quadratic o-monomials", *Proceedings of the 2014 IEEE International Symposium on Information Theory*, pp. 1827–1831, 2014.

[6] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, "Further results on Niho bent functions", *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 6979–6985, 2012.

[7] L. Budaghyan, C. Carlet, T. Helleseth and A. Kholosha, "On o-equivalence of Niho Bent functions", *WAIFI 2014*, Lecture Notes in Comp. Sci. 9061, pp. 155–168, 2015.

[8] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, T. Penttila. "Projective equivalence of ovals and EA-equivalence of Niho bent functions", Book of Abstracts of "Finite geometries fourth Irsee conference", Sept. 2014; the slides from the presentation can be found at https://people.uib.no/lbu061/irsee.pdf

[9] C. Carlet, "Boolean functions for cryptography and error-correcting codes", *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, ser. Encyclopedia of Mathematics and its Applications, Y. Crama and P. L. Hammer, Eds. Cambridge: Cambridge University Press, 2010, vol. 134, ch. 8, pp. 257–397.

[10] C. Carlet and S. Mesnager, "On Dillon's class H of bent functions, Niho bent functions and o-polynomials", *J. Combin. Theory Ser. A*, vol. 118, no. 8, pp. 2392–2410, Nov. 2011.

[11] C. Carlet and S. Mesnager. Four decades of research on bent functions. *Designs, Codes and Cryptography* 78(1), pp. 5–50, 2016.

[12] C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, "On the dual of bent functions with 2^r Niho exponents", *Proceedings of the 2011 IEEE International Symposium on Information Theory.* IEEE, Jul./Aug. 2011, pp. 657–661.

[13] W. E. Cherowitzo and L. Storme, "α-Flocks with oval herds and monomial hyperovals", *Finite Fields Appl.*, vol. 4, no. 2, pp. 185–199, Apr. 1998.

[14] W. Cherowitzo, "Hyperovals in Desarguesian planes of even order", *Ann. Discrete Math.*, 37, pp. 87–94, 1988.

[15] W. Cherowitzo, T. Penttila, I. Pinneri, and G. Royle. "Flocks and Ovals", *Geom. Dedicata*, 60, pp. 17–37, 1996.

[16] P. Dembowski, Finite Geometries, Springer, 1968.

[17] J. F. Dillon, Elementary Hadamard difference sets, Ph.D. dissertation, Univ. Maryland, College Park. MD, USA, 1974.

[18] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, "Construction of bent functions via Niho power functions", *J. Combin. Theory Ser. A*, vol. 113, no. 5, pp. 779–798, Jul. 2006.

[19] D. Glynn, "Two new sequences of ovals in finite desarguesian planes of even order", *Combinatorial Mathematics*, Lecture Notes in Mathematics, vol. 1036, pp. 217–229, 1983.

[20] T. Helleseth, A. Kholosha, and S. Mesnager, "Niho bent functions and Subiaco hyperovals", *Theory and Applications of Finite Fields*, ser. Contemporary Mathematics, M. Lavrauw, G. L. Mullen, S. Nikova, D. Panario, and L. Storme, Eds., vol. 579. Providence, Rhode Island: American Mathematical Society, pp. 91–101, 2012.

[21] C. M. O'Keefe and T. Penttila, "Automorphism Groups of Generalized Quadrangles via an Unusual Action of $P\Gamma L(2, 2^h)$", *Europ J. Combinatorics*, 33, pp. 213–232, 2002.

[22] C. M. O'Keefe and T. Penttila. "A new hyperoval in $PG(2, 32)$", *J. Geom.*, 44, pp. 117–139, 1992.

[23] C. M. O'Keefe and T. Penttila. "Symmetries of Arcs", *J. Combin. Theory Ser. A*, 66, pp. 53–67, 1994.

[24] C. M. O'Keefe and J. Thas. "Collineations of Subiaco and Cherowitzo hyperovals", *Bull. Belg. Math. Soc.*, 3, pp. 177–192, 1996.

[25] A. Kholosha and A. Pott, "Bent and related functions" in *Handbook of Finite Fields*, ser. Discrete Mathematics and its Applications, G. L. Mullen and D. Panario, Eds. London: CRC Press, 2013, ch. 9.3, pp. 255–265.

[26] G. Leander and A. Kholosha, "Bent functions with 2^r Niho exponents", *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5529–5532, Dec. 2006.

[27] N. Li, T. Helleseth, A. Kholosha, and X. Tang, "On the Walsh transform of a class of functions from Niho exponents", *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4662–4667, Jul. 2013.

[28] S. Mesnager, "Bent vectorial functions and linear codes from o-polynomials", *Journal Designs, Codes and Cryptography.* 77(1), pp. 99–116, 2015.

[29] R. L. McFarland, "A family of difference sets in non-cyclic groups", *J. Combin. Theory Ser. A*, vol. 15, no. 1, pp. 1–10, Jul. 1973.

[30] K. Nyberg, " S-boxes and Round Functions with Controllable Linearity and Differential Uniformity", *Proceedings of Fast Software Encryption*, LNCS 1008, 1994, pp. 111-130, 1995.

[31] S. Payne and J. A. Thas. "The stabilizer of the Adelaide oval", *Discrete Math.*, 294, pp. 161–173, 2005.

[32] T. Penttila and I. Pinneri. "Irregular Hyperovals in $PG(64, 2)$", *J. Geom.*, 51, pp. 89–100, 1994.

[33] S. E. Payne, T. Penttila and I. Pinneri. "Isomorphisms Between Subiaco and q-Clan Geometries", *Bull. Belg. Math. Soc.*, 2, pp. 197–222, 1995.

[34] T. Penttila and G. Royle. "On Hyperovals in Small Projective Planes", *J. Geom.*, 54, pp. 91–104, 1995.

[35] O. S. Rothaus, "On "bent" functions," *J. Combin. Theory Ser. A*, vol. 20, no. 3, pp. 300–305, May 1976.

[36] T. L. Vis, "Monomial hyperovals in Desarguesian planes," Ph.D. dissertation, University of Colorado Denver, 2010.