On the Affine Equivalence and Nonlinearity Preserving Bijective Mappings

İsa Sertkaya[1,2] and Ali Doğanaksoy[1,3]

[1] Institute of Applied Mathematics,
Middle East Technical University, Ankara, Turkey
[2] National Research Institute of Electronics and Cryptology,
TÜBİTAK-UEKAE, Gebze, Kocaeli, Turkey
[3] Department of Mathematics,
Middle East Technical University, Ankara, Turkey
isa@uekae.tubitak.gov.tr, aldoks@metu.edu.tr

Abstract. It is well-known that affine equivalence relations keep nonlineaerity invariant for all Boolean functions. The set of all Boolean functions, $\mathcal{F}_n$, over $\mathbb{F}_2^n$, is naturally isomorphic to the 2^n dimensional vector space, $\mathbb{F}_2^{2^n}$. Thus, while analyzing the transformations acting on $\mathcal{F}_n$, $S_{2^{2^n}}$, the group of all bijective mappings, defined from $\mathbb{F}_2^{2^n}$ onto itself should be considered. As it is shown in [1–3], there exist non-affine bijective transformations that preserve nonlinearity. In this paper, first, we prove that the group of affine equivalence relations is isomorphic to the automorphism group of Sylvester Hadamard matrices. Then, we show that new nonlinearity preserving non-affine bijective mappings also exist. Moreover, we propose that the automorphism group of nonlinearity classes, should be studied as a subgroup of $S_{2^{2^n}}$, it contains transformations which are not affine equivalence relations.

Keywords: Boolean functions, nonlinearity, affine equivalence, automorphism groups, Sylvester Hadamard matrices

1 Introduction

A very basic mathematical way to study and analyze a large algebraic set is to partition it into equivalent classes with an equivalence relation, and then construct a representative for each class and analyze the reduced sized set that is composed of representative elements. Such procedure have been very important problem for Boolean functions due to their importance in different disciplines such as switching theory, coding theory and cryptography.

The study of the actions of basic transformations on Boolean functions date back to Harrison [4, 5], later [6–8] where the main concern is the switching theory. In coding theory, affine transformations analyzed especially for the Reed-Muller codes, [9–11].

In cryptography, one of main design criteria is nonlinearity which is defined as the minimum Hamming distance of a function to the affine functions. Hence, partitioning Boolean functions set into disjoint classes with respect to their nonlinearity values, enumerating highly nonlinear Boolean functions, constructing new function types with desired properties are important, yet open problems. Due to the previous studies and their simple structures, generally affine equivalence relations are used for determining the equivalence classes. Meier and Staffelbach, in [12], showed that nonlinearity is invariant under affine mappings acting on input arguments, later Preneel [13] proved affine equivalence relations also preserve nonlinearity. Moreover, in [14], so called CCZ-equivalence is proposed, but in [15], it is proved that two Boolean functions are CCZ-equivalent if and only if they are affine equivalent. Further reading can be found in [16–18].

Naturally, the set of all Boolean functions is isomorphic to the 2^n dimensional vector space $\mathbb{F}_2^{2^n}$ over $\mathbb{F}_2$. Hence, expanding the transformations set to all bijective transformations that can be defined over $\mathbb{F}_2^{2^n}$, namely to the $S_{2^{2^n}}$, is a reasonable extension. In [1–3], the authors analyzed such mappings, and showed existence of non-affine mappings.

In this paper, first, we give notations and review affine equivalence relations, then prove that the group of affine equivalence relations exactly determines, and thus is isomorphic to, the automorphism group of Sylvester Hadamard matrices. Later, we give examples of new nonlinearity preserving non-affine mappings. Moreover, we discuss the definition of the automorphism group of Boolean functions nonlinearity classes and instead of the restricting to affine equivalence relations, we propose that it should be studied as a subgroup of $S_{2^{2^n}}$.

2 Preliminaries

In this section, we fix the notation and state the necessary definitions relating to Boolean functions and nonlinearity criteria in cryptography.

Let $\mathbb{F}_2^n$ be the set of all n-tuples of elements belonging to $\mathbb{F}_2$ (Galois field of order two). Naturally, $\mathbb{F}_2^n$ possesses n-dimensional vector space structure over $\mathbb{F}_2$ and assumes *lexicographical* ordering. Hence, it is possible to represent the vectors of $\mathbb{F}_2^n$ as; $\alpha_0 = (0, 0, \dots, 0) < \alpha_1 = (0, 0, \dots, 0, 1) < \dots < \alpha_{2^n-1} = (1, 1, \dots, 1)$.

A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a mapping from binary n-tuple input to a single binary output. Most common ways to uniquely represent a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is either by its truth table or algebraic normal form:

- The *truth table* of f,

$$T_f = (f(\alpha_0), f(\alpha_1), \dots, f(\alpha_{2^n-1}))$$

  where $\alpha_i \in \mathbb{F}_2^n$ and α_i's are in lexicographic order.
- The *algebraic normal form* of f,

$$f(x_n, x_{n-1}, \dots, x_1) = c_0 \oplus c_1 x_1 \oplus \cdots \oplus c_n x_n \oplus c_{12} x_1 x_2 \oplus \cdots \oplus c_{12\cdots n} x_1 x_2 \cdots x_n$$

  where $c_0, c_1, \dots, c_{12\cdots n} \in \mathbb{F}_2$, or equivalently,

$$ANF_f = (c_0, c_1, \dots, c_{12\dots n}) \ .$$

The set of all Boolean functions defined on $\mathbb{F}_2^n$ is denoted by $\mathcal{F}_n$ and trivially its cardinality $|\mathcal{F}_n|$ is 2^{2^n}. Indeed, by considering truth tables or algebraic normal form coefficients as a vector of length 2^n with elements from $\mathbb{F}_2$, an isomorphism between $\mathcal{F}_n$ and $\mathbb{F}_2^{2^n}$ can be easily constructed.

The degree, $deg(f)$, of the algebraic normal form a function f is called *algebraic degree*, or shortly degree, of f. A Boolean function f is called *affine* if its degree is 1, i.e. it is of the form

$$f(x_n, x_{n-1}, \ldots, x_1) = c_0 \oplus c_1 x_1 \oplus \cdots \oplus c_n x_n$$

or, equivalently,

$$f(x_n, x_{n-1}, \ldots, x_1) = \langle c, x \rangle \oplus c_0 \ .$$

where $c_0 \in \mathbb{F}_2$ and $\langle c, x \rangle = c_1 x_1 \oplus \cdots \oplus c_n x_n$ is the *standard inner product* defined over $\mathbb{F}_2^n$. The set of all affine Boolean functions on $\mathbb{F}_2^n$ is denoted by $\mathcal{A}_n$.

The *Hamming weight* of a vector $\alpha \in \mathbb{F}_2^n$, denoted by $w(\alpha)$, is the number of ones in α. The *support* of a function $f \in \mathcal{F}_n$ is defined to be the set $\{\alpha \in \mathbb{F}_2^n | f(\alpha) = 1\}$ and is denoted by $Supp(f)$. Obviously, Hamming weight of f, $w(T_f)$ or $w(f)$, is equal to the cardinality of the support of f, i.e. $w(f) = |Supp(f)|$.

The *Hamming distance* between two functions $f, g \in \mathcal{F}_n$ is defined as the number of different components in their truth tables and denoted by $d(f,g) = w(f \oplus g)$. The *nonlinearity*, N_f, of a function f is its distance to the nearest affine function:

$$N_f = \min_{g \in \mathcal{A}_n} d(f,g)$$

The *Walsh transform*[4] of a function f is defined as

$$W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, \omega \rangle}$$

where $\omega \in \mathbb{F}_2^n$ and $\langle x, \omega \rangle$ being the standard inner product on $\mathbb{F}_2^n$. The truth table of the Walsh transform,

$$W_f = (W_f(\alpha_0), W_f(\alpha_1), \ldots, W_f(\alpha_{2^n-1}))$$

is called *Walsh Spectrum* of f and it can also be computed by,

$$W_f = \zeta_f H_n$$

where $\zeta_f = ((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$ is the truth table of the *signed function* $(-1)^{f(x)}$ of f and H_n is the $2^n \times 2^n$ *Sylvester Hadamard matrix.*

Nonlinearity of a function f can also be expressed with the Walsh transform of f as

$$N_f = 2^{n-1} - \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)| \ .$$

---

[4] It is also called *Walsh Hadamard transform*, and is the *discrete Fourier transform* of the function $(-1)^{f(x)}$.

A function f is called *bent function* [19, 20], if $W_f(w) = \pm 2^{n/2}$ for any $w \in \mathbb{F}_2^n$. Bent functions attains maximal nonlinearity, but they only exist when n is even. The set of bent functions is, when exists, denoted by $\mathcal{B}_n$.

The $n \times n$ Hadamard matrices whose entries are only ± 1, were first investigated by Sylvester [21], later Hadamard [22] studied such matrices as solutions to the problem of maximum determinant of matrices, for further reading please refer to [23–25].

Definition 1. *[23] Two $n \times n$ Hadamard matrices are equivalent if one can be obtained from the other by performing a finite sequence of permuting the rows or the columns and multiply a row or column by -1.*

Let S_n be the group of all permutation matrices of order n and D_n be the group of all diagonal matrices of order n with diagonal entries are equal to only ± 1. Then, the group of monomial matrices, denoted by $S_n^{\pm}$, is the semi direct product $S_n \ltimes D_n$ of S_n with D_n. Hadamard equivalence, in terms of row and column permutations and negations, is in fact, equivalent to the action of monomial matrices on Hadamard matrices. Under this action, naturally the automorphism group of the given matrix will be the stabilizer.

Definition 2. *[23] The automorphism group of a Hadamard matrix H of order n, $Aut(H)$, is the group of all monomial matrix pairs (P, Q) satisfying $PH = HQ$ with the group operation $\circ$,*

$$(P_1, Q_1) \circ (P_2, Q_2) = (P_1P_2, Q_1Q_2) \ .$$

Hence, the automorphism group of Sylvester Hadamard matrix H_n of order 2^n is

$$Aut(H_n) = \{(P, Q) \in S_{2^n}^{\pm} |\ PH_nQ = H_n\} \ .$$

3 Affine equivalence

Definition 3. *[10] Denote by GL_n the group of all nonsingular matrices of order n on $\mathbb{F}_2$, i.e. the general linear group. Denote by AGL_n the group*

$$\{(A, \alpha)|\ A \in GL_n,\ \alpha \in \mathbb{F}_2^n\},$$

which is the semi direct product $GL_n \ltimes \mathbb{F}_2^n$ of GL_n with $\mathbb{F}_2^n$. The group operation $\circ$ is defined by

$$(A, \alpha) \circ (B, \beta) = (AB, \beta A \oplus \alpha)$$
$$(A, \alpha)^{-1} = (A^{-1}, \alpha A^{-1})$$

Similarly, the group $AGL_n \ltimes \mathcal{A}_n$,

$$\{(A, \alpha, \beta, a)|A \in GL_n,\ \alpha, \beta \in \mathbb{F}_2^n,\ a \in \mathbb{F}_2\}$$

or, with $\tau : x \mapsto xA \oplus \alpha$ and $f(x) = \langle x, \beta\rangle \oplus a$, simply,

$$\{(\tau, f)|\ \tau \in AGL_n,\ f \in \mathcal{A}_n\}$$

is the semi direct product of AGL_n with the affine Boolean functions $\mathcal{A}_n$, where the group operation $\circ$ is

$$(\tau, f) \circ (\sigma, g) = (\tau \circ \sigma,\ \tau(g) + f)$$

$$(\tau, f)^{-1} = (\tau^{-1}, \tau^{-1}(f))$$

The action of the group $AGL_n \ltimes \mathcal{A}_n$ is defined by

$$(\tau, l) : \mathcal{F}_n \mapsto \mathcal{F}_n$$

$$f(x) \mapsto f(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a$$

For any functions $f, g \in \mathcal{F}_n$, f and g are called *affine equivalent* if there exists an bijective mapping $(\tau, l) \in AGL_n \ltimes \mathcal{A}_n$ with $\tau : x \mapsto xA \oplus \alpha$ and $l(x) = \langle x, \beta \rangle \oplus a$ such that

$$f(x) = g(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a\ . \tag{1}$$

Preneel, as stated below, proved that the action of an affine equivalence relation results in a signed permutation on the Walsh spectra of the function. Under the actions of $AGL_n \ltimes \mathcal{A}_n$, algebraic degree, the distribution of absolute Walsh spectra, hence nonlinearity and the distribution of absolute autocorrelation spectra remains invariant [17].

Proposition 1. *[13] Let $f, g \in \mathcal{F}_n$ be two affine equivalent functions such that $f(x) = g(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a$, then for the Walsh transform of f and g the following relation holds.*

$$W_f(\omega) = (-1)^{\langle \alpha, (\omega \oplus \beta)(A^{-1})^t \rangle + a} W_g((\omega \oplus \beta)(A^{-1})^t)$$

In [3], the authors prove that there exists a correspondence between AGL_n and $Aut(H_n)$, such that, for any $\tau \in AGL_n$, (resp. $A \in GL_n$), there exists a unique $(P, Q) \in Aut(H_n)$ with $P \in S_{2^n}$ and $Q \in S^{\pm}_{2^n} \setminus S_{2^n}$, (resp. $Q \in S_{2^n}$). As we state in Theorem 1, we prove that this correspondence extends to an isomorphism between $AGL_n \ltimes \mathcal{A}_n$ and $Aut(H_n)$.

Theorem 1. *For any functions $f, g \in \mathcal{F}_n$, f and g are affine equivalent with Equation 1 if and only if there exists a unique monomial matrix pair $(P, Q) \in Aut(H_n)$ such that*

$$W_f Q = W_g$$

or, equivalently,

$$\zeta_f = \zeta_g P$$

Corollary 1. *For any affine equivalent functions $f, g \in \mathcal{F}_n$, with*

$$f(x) = g(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a$$

the monomial matrix pair $(P, Q) \in Aut(H_n)$ satisfies the following properties:

1. *$P \in S_{2^n}$ if and only if $\beta = 0$, $a = 0$, indeed, $Q \in S_{2^n}$ if and only if $\alpha = 0$.*
2. *$P, Q \in D_{2^n}$ if and only if A is the identity matrix of order n and $\alpha = 0$.*

4 Nonlinearity preserving bijective mappings

Since, the truth table of a function is a vector of length 2^n with elements belonging to $\mathbb{F}_2$, one can construct an isomorphism between the set of all Boolean functions on n variables, $\mathcal{F}_n$, and the vector space $\mathbb{F}_2^{2^n}$. Hence, any map acting on the truth table of a Boolean function can be seen as a map defined from $\mathbb{F}_2^{2^n}$ into itself. Moreover, if a map is bijective (invertible) then obviously, it is a permutation of $\mathbb{F}_2^{2^n}$, and hence is an element of $S_{2^{2^n}}$.

Any map $\psi \in S_{2^{2^n}}$ from $\mathbb{F}_2^{2^n}$ to $\mathbb{F}_2^{2^n}$, is in fact a vectorial Boolean function[5]. Any vectorial Boolean function $\psi : \mathbb{F}_2^{2^n} \to \mathbb{F}_2^{2^n}$ can be represented in the form $T_f \mapsto \psi(T_f)$, that is

$$\psi(x_0, x_1, \ldots, x_{2^n-1}) = (f^0(x_0, x_1, \ldots, x_{2^n-1}), \ldots, f^{2^n-1}(x_0, x_1, \ldots, x_{2^n-1}))$$

where each f^i is a Boolean function from $\mathbb{F}_2^{2^n}$ to $\mathbb{F}_2$ and called the *coordinate* or *component function* of ψ and each x_i being the value of the acted Boolean function at $\alpha_i \in \mathbb{F}_2^n$, i.e. $f(\alpha_i)$.

Since, each $f^i \in \mathcal{F}_{2^n}$, they can be represented by their unique algebraic normal form:

$$f^i(x_0, x_2, \cdots, x_{2^n}) = c_0^{(i)} \oplus c_1^{(i)} x_0 \oplus \ldots \oplus c_{12\cdots 2^n}^{(i)} x_1 x_2 \cdots x_{2^n}.$$

Hence, we have,

$$\psi : T_f \longmapsto \begin{pmatrix} c_0^{(0)} \oplus c_1^{(0)} f(\alpha_0) \oplus \ldots \oplus c_{12\cdots 2^n}^{(0)} f(\alpha_0) f(\alpha_1) \cdots f(\alpha_{2^n-1}) \\ c_0^{(1)} \oplus c_1^{(1)} f(\alpha_0) \oplus \ldots \oplus c_{12\cdots 2^n}^{(1)} f(\alpha_0) f(\alpha_1) \cdots f(\alpha_{2^n-1}) \\ \vdots \\ c_0^{(2^n-1)} \oplus c_1^{(2^n-1)} f(\alpha_0) \oplus \ldots \oplus c_{12\cdots 2^n}^{(2^n-1)} f(\alpha_0) f(\alpha_1) \cdots f(\alpha_{2^n-1}) \end{pmatrix}^t.$$

Then we get,

$$\psi : T_f \longmapsto \left(\underbrace{\begin{bmatrix} c_0^{(0)} \\ c_0^{(1)} \\ \vdots \\ c_0^{(2^n-1)} \end{bmatrix}}_{\lambda_0} \oplus \underbrace{\begin{bmatrix} c_1^{(0)} \\ c_1^{(1)} \\ \vdots \\ c_1^{(2^n-1)} \end{bmatrix}}_{\lambda_1} f(\alpha_0) \oplus \cdots \oplus \underbrace{\begin{bmatrix} c_{2^n}^{(0)} \\ c_{2^n}^{(1)} \\ \vdots \\ c_{2^n}^{(2^n-1)} \end{bmatrix}}_{\lambda_{2^n}} f(\alpha_{2^n-1}) \oplus \right.$$

[5] In the literature, different names are also used such $(2^n, 2^n)$-functions, multi-output Boolean functions, Boolean maps, Substitution boxes (S-Boxes).

$$\left. \underbrace{\begin{bmatrix} c_{12}^{(0)} \\ c_{12}^{(1)} \\ \vdots \\ c_{12}^{(2^n-1)} \end{bmatrix}}_{\lambda_{12}} f(\alpha_0)f(\alpha_1) \oplus \cdots \oplus \underbrace{\begin{bmatrix} c_{12\cdots 2^n}^{(0)} \\ c_{12\cdots 2^n}^{(1)} \\ \vdots \\ c_{12\cdots 2^n}^{(2^n-1)} \end{bmatrix}}_{\lambda_{12\cdots 2^n}} f(\alpha_0)\cdots f(\alpha_{2^n-1}) \right)^t ,$$

or equivalently,

$$\psi : T_f \mapsto (\lambda_0 \oplus AT_f^t \oplus \lambda_{12} f(\alpha_0)f(\alpha_1) \oplus \cdots \oplus \lambda_{12\cdots 2^n} f(\alpha_0)f(\alpha_1)\cdots f(\alpha_{2^n-1}))^t, \tag{2}$$

where A is the matrix is constituted by $[\lambda_1 \ \lambda_2 \ \ldots \ \lambda_{2^n}]$.

Naturally, the bijective maps can be classified with respect to their algebraic forms, as follows.

- $\psi \in S_{2^{2^n}}$ is called *linear* if it is of the form $\psi : T_f \mapsto (AT_f^t)^t$, that is,
  - $\lambda_0 = [0 \ 0 \ \ldots \ 0]^t$,
  - $\lambda_i = [0 \ 0 \ \ldots \ 0]^t$, for all $i \notin \{0, 1, 2, \ldots, 2^n\}$,
  - $A \in GL_{2^n}$, i.e. A is an invertible matrix of order 2^n.
- $\psi \in S_{2^{2^n}}$ is called *affine* if it is of the form $\psi : T_f \mapsto (\lambda_0 \oplus AT_f^t)^t$, that is,
  - $\lambda_i = [0 \ 0 \ \ldots \ 0]^t$, for all $i \notin \{0, 1, 2, \ldots, 2^n\}$,
  - $A \in GL_{2^n}$, i.e. A is an invertible matrix of order 2^n.
- $\psi \in S_{2^{2^n}}$ is called *non-affine* if it has at least one non-zero λ_i, for $i \notin \{0, 1, 2, \ldots, 2^n\}$.

Denote by $\mathcal{P}_N(\mathcal{F}_n)$, the group of all nonlinearity preserving bijective maps acting on the functions with n-variables, i.e.

$$\mathcal{P}_N(\mathcal{F}_n) = \{\psi \in S_{2^{2^n}} | N_f = N_{\psi(T_f)}, \text{ for all } f \in \mathcal{F}_n\} \ .$$

Note that, affine equivalence relations, reviewed in the previous section, are in fact a small subgroup of the affine bijective transformations of the form $\psi : T_f \mapsto (\lambda_0 \oplus AT_f^t)^t$.

Proposition 2. *Any affine equivalence relation $(\tau, l) \in AGL_n \ltimes \mathcal{A}_n$ with $\tau : x \mapsto xA \oplus \alpha$ and $l(x) = \langle x, \beta \rangle \oplus a$, i.e. $f(x) \mapsto f(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a$, for all $f \in \mathcal{F}_n$, can be uniquely represented as $\psi \in S_{2^{2^n}}$, such that,*

$$T_f \mapsto (\lambda_0 \oplus PT_f^t)^t$$

where $P \in S_{2^n}$ is a permutation matrix of order 2^n and λ_0 is the truth table of the affine function l.

In [3], by giving necessary and sufficient conditions to preserve nonlinearity (as stated in Theorem 2), the authors proved that not all of the affine bijective transformations of the form $\psi : T_f \mapsto (\lambda_0 \oplus AT_f^t)^t$ are in $\mathcal{P}_N(\mathcal{F}_n)$. Furthermore, as recalled in Proposition 3, they also shown the existence of non-affine nonlinearity preserving bijective transformations.

Theorem 2. *[3] Let $\psi \in S_{2^{2^n}}$ be an affine bijective transformation so that for all $f \in \mathcal{F}_n$,*

$$\psi : T_f \mapsto (T_l \oplus AT_f^t)^t,$$

where $l \in \mathcal{F}_n$ and $A \in GL_{2^n}$ are fixed.

Then, $\psi \in \mathcal{P}_N(\mathcal{F}_n)$ if and only if $l \in \mathcal{A}_n$ and $A = B \oplus P$, where $P \in S_{2^n}$ corresponds to an element of AGL_n, and B is the matrix of order 2^n over $\mathbb{F}_2$ whose columns are the truth table of affine functions, not necessarily distinct.

Proposition 3. *[3] Let $\psi \in S_{2^{2^n}}$ be a mapping that satisfies the following conditions, with respect to Equation 2,*

1. *λ_0 is the truth table of an affine function,*
2. *the matrix A satisfies the conditions mentioned in Theorem 2,*
3. *λ_i's are the truth table of some affine Boolean functions for all $i \in \{12, 13, \ldots, 12 \cdots 2^n\}$ where not all are the zero affine function.*

Then, $\psi \in \mathcal{P}_N(\mathcal{F}_n)$, i.e. ψ is an non-affine bijective mapping that preserves nonlinearity.

Remark 1. Trivially, the transformations defined in Proposition 3, are non-affine. However, instead of all Boolean functions, when their action on a fixed function f is considered, the image of such transformations for f will be equivalent to an affine mapping. That is to say, such mappings $\psi \in S_{2^{2^n}}$ become

$$T_f \mapsto (PT_f^t \oplus T_l)^t$$

where the function l is the summation of some λ_i's which are strictly determined by $Supp(f)$. Such summations will differ for different functions, therefore, when their algebraic normal form is concerned, these transformations will be non-affine transformations.

Table 1. $|S_{2^{2^n}}|$ and $|\mathcal{P}_N(\mathcal{F}_n)|$ values for $n \leq 5$

n	$\lvert S_{2^{2^n}} \rvert$	$\lvert \mathcal{P}_N(\mathcal{F}_n) \rvert$
2	$16! \approx 2^{44}$	$8! \times 8! \approx 2^{30}$
3	$256! \approx 2^{1684}$	$16! \times 128! \times 112! \approx 2^{1365}$
4	$65536! \approx 2^{954036}$	$32! \times \cdots \times 896! \approx 2^{829564}$
5	$2^{32}! \approx 2^{2^{36.9}}$	$64! \times \cdots \times 27387136! \approx 2^{2^{36.1}}$

Exact determination or classification of $\mathcal{P}_N(\mathcal{F}_n)$, the group of the nonlinearity preserving bijective mappings, is still an open problem. However, for small values of n, where nonlinearity distribution can be extracted by exhaustive search, the cardinality of $\mathcal{P}_N(\mathcal{F}_n)$ can also be computed. Based on the nonlinearity distribution given in Table 2 (in Appendix A), the number of nonlinearity preserving bijective mappings for $n \leq 5$ are presented in Table 1.

So far, the mappings defined in Proposition 3 are the most general form of nonlinearity preserving mappings, in [3], by computer search, it is proved that for $n = 2$, $\mathcal{P}_N(\mathcal{F}_2)$ consists of only these mappings.

Fact 1. *For $n = 3$, the number of bijective mappings defined in Proposition 3 is strictly less than $2^{1056} = 2^{64} \times 16^{248}$, since there exist at most 2^{64} choices for the matrix A and 16 choices for each λ_i for $i \in \{0, 12, 13, \ldots, 12 \cdots 2^n\}$. Similarly, for $n = 4$, it is strictly less than $2^{327856} = 2^{256} \times 32^{65520}$. These cardinalities are strictly less than the values of $|\mathcal{P}_N(\mathcal{F}_3)|$ (respectively $|\mathcal{P}_N(\mathcal{F}_4)|$) given in Table 1. Therefore, Proposition 3 type mappings do not cover all of the nonlinearity preserving mappings.*

This simple cardinality approximation can be applied for larger values of n, and, thus, it can be easily proved that the number of bijective mappings defined in Proposition 3 will be strictly less than $|\mathcal{P}_N(\mathcal{F}_n)|$, since as n increase, the ratio of $|\mathcal{A}_n|$, the number affine functions to $|\mathcal{F}_n|$, the number of all Boolean functions, will decrease.

Even if we have not classified new type of mappings algebraically yet, in order to illustrate such mappings, we present a simple one for $n = 3$ in Example 1 and some examples for $n = 4$ in Appendix B.

Example 1. Let $\psi \in S_{2^{2^3}}$ be,

$$\begin{aligned}\psi : T_f \mapsto \big(&\lambda_0 \oplus AT_f^t \oplus \lambda_{123457} f(\alpha_0)f(\alpha_1)f(\alpha_2)f(\alpha_3)f(\alpha_4)f(\alpha_6) \oplus \\ &\lambda_{1234578} f(\alpha_0)f(\alpha_1)f(\alpha_2)f(\alpha_3)f(\alpha_4)f(\alpha_6)f(\alpha_7) \oplus \\ &\lambda_{123456} f(\alpha_0)f(\alpha_1)f(\alpha_2)f(\alpha_3)f(\alpha_4)f(\alpha_5) \oplus \\ &\lambda_{1234568} f(\alpha_0)f(\alpha_1)f(\alpha_2)f(\alpha_3)f(\alpha_4)f(\alpha_5)f(\alpha_7)\big)^t\end{aligned}$$

where $\lambda_0 = [00001111]^t$, $\lambda_{123457} = \lambda_{1234578} = \lambda_{123456} = \lambda_{1234568} = [00010100]^t$ and A is the matrix;

$$\begin{bmatrix} 1\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,0 \\ 1\,0\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,0\,1\,1 \\ 1\,1\,1\,0\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1\,0 \end{bmatrix}.$$

Trivially, ψ is not an affine mapping, indeed it does not satisfies the conditions given in Proposition 3, since $(0, 0, 0, 1, 0, 1, 0, 0)$ is not truth table of an affine function. Moreover, it can be easily checked that this map is invertible and preserves nonlinearity for all functions.

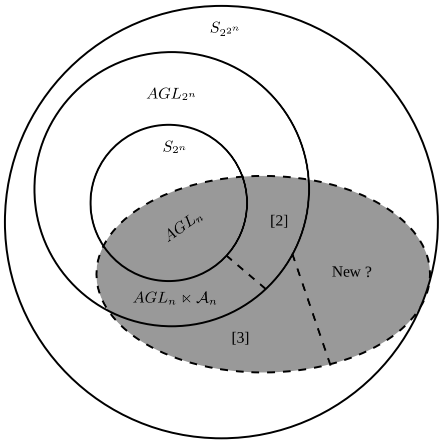

Fig. 1. Classification of nonlinearity preserving bijective transformations

Constructing and classification of such mappings algebraically is still an unanswered problem. Up to the authors knowledge, the current state of classification of nonlinearity preserving mappings can be represented in Figure 1 with the shaded area. Note that in the figure, the subgroups of $S_{2^{2^n}}$ are given exclusively, that is $AGL_n \ltimes \mathcal{A}_n$ represents $AGL_n \ltimes \mathcal{A}_n \setminus AGL_n$, [2] for $\psi : T_f \mapsto (\lambda_0 \oplus AT_f^t)^t$ type mappings, [3] for Proposition 3 type mappings, "New ?" stands for mappings like given in the examples.

5 Automorphism Group of Nonlinearity Classes

Definition 4. *An automorphism of an mathematical object $\mathcal{M}$ is an isomorphism $\varphi : \mathcal{M} \mapsto \mathcal{M}$, i.e. maps $\mathcal{M}$ to itself. The set of all automorphisms of $\mathcal{M}$ forms a group, denoted by $Aut(\mathcal{M})$ and called the automorphism group of $\mathcal{M}$.*

Considering the nonlinearity criteria, partition $\mathcal{F}_n$, the set of all Boolean functions, into nonlinearity classes by gathering all the functions having same nonlinearity value in the same partition. In this way, each partition or class will be composed of only the functions with same nonlinearity values, such as $\mathcal{A}_n$, the set of all affine functions, $\mathcal{B}_n$, the set of all bent functions, etc. .

An interesting question would be what is the automorphism group of these classes. Before investigating this question, definition of automorphism group should be criticized in a cryptological perspective. That is to say, since nonlinearity is so crucial for cryptographers, one only need a bijective transformation that maps a nonlinearity class to itself. Hence, even if the truth table of a function is an element of 2^n dimensional vector space $\mathbb{F}_2^{2^n}$, preserving vector space structure is not the main concern. In fact, when a transformation maps a function to another one in the same class, that transformation does not need to map their closest affine functions to each other.

As it is proved in [26], affine equivalence relations are isometric, i.e. they preserve the Hamming distance, i.e. $d(f,g) = d(\psi(f), \psi(g))$ for all $f, g \in \mathcal{F}_n$. This is a very strong constraint for nonlinearity, since under an action of a map, when nonlinearity is concerned, instead of a specific affine function, minimum distance to affine functions family will be the main concern.

There are some proposals, like [26, 27], that state the automorphism group of $\mathcal{B}_n$ is the group $AGL_n \ltimes \mathcal{A}_n$. Definitely, $AGL_n \ltimes \mathcal{A}_n \subset Aut(\mathcal{B}_n)$, but as it is demonstrated in the previous chapters, there are also other transformations that map $\mathcal{B}_n$ to itself. Hence, those mappings should also be included in $Aut(\mathcal{B}_n)$.

Example 2. For $n = 4$, there are $|\mathcal{P}_N(\mathcal{F}_4)| \approx 2^{829564}$ bijective mappings that preserve nonlinearity. Hence, all of them map $\mathcal{B}_4$ onto itself. However, only $896! \approx 2^{7500}$ of them constitute different permutations on $\mathcal{B}_4$. The number of different transformations belonging to $AGL_4 \ltimes \mathcal{A}_4$ is $(2^4-1)\cdot(2^4-2)\cdot(2^4-4)\cdot(2^4-8)\cdot 16\cdot 32 \approx 2^{23}$. Thus, $AGL_4 \ltimes \mathcal{A}_4$ is only a proper subgroup of $Aut(\mathcal{B}_4)$.

Considering the nonlinearity criteria only, $AGL_n \ltimes \mathcal{A}_n$ is a small subgroup of the automorphism group of the nonlinearity classes of $\mathcal{F}_n$. Theorem 2, Proposition 3 and examples given certainly contribute mappings for the automorphism group of nonlinearity classes. Therefore, determination of the automorphism group should be studied as a subgroup of $S_{2^{2^n}}$, and should not be restricted to $AGL_n \ltimes \mathcal{A}_n$.

6 Conclusion

Besides, the transformations belonging to $AGL_n \ltimes \mathcal{A}_n$, there are algebraically more complex transformations that keep nonlinearity invariant for all Boolean functions. Studying the elements $S_{2^{2^n}}$ and trying to classify them whether they preserve nonlinearity or not is still an open problem. Despite the fact that such a research may seem to be expensive due to their huge cardinality, it may lead to a deeper insight to the highly nonlinear functions. Moreover, nice construction algorithm of highly nonlinear functions with extra desirable criteria can be implemented.

The exact determination of automorphism group of nonlinearity classes of $\mathcal{F}_n$ is another interesting problem. Formerly, it is proposed that automorphism group bents functions is $AGL_n \ltimes \mathcal{A}_n$. On the other hand, as it is investigated in the previous chapters, there are other transformations that keep nonlinearity invariant. Therefore, such propositions should be re-examined and instead of restriction $AGL_n \ltimes \mathcal{A}_n$, these nonlinearity preserving transformations should be also included.

References

1. Sertkaya İ.: Nonlinearity preserving post-transformations. MSc. Thesis, Institute of Applied Mathematics, Middle East Technical University, Ankara (2004)

2. Sertkaya İ., Doğanaksoy A.: On nonlinearity preserving bijective transformations. 2nd National Symposium on Cryptology, Ankara (2006)
3. Sertkaya İ., Doğanaksoy A.: Some results on nonlinearity preserving bijective transformations. Boolean Functions: Cryptography and Applications (BFCA'07), Paris (2007)
4. Harrison, M.A.: The number of transitivity sets of Boolean functions. Journal of the Society for industrial and applied mathematics, **11** (1963) 806–828
5. Harrison, M.A.: On the classification of Boolean functions by the general linear and affine group. Journal of the Society for industrial and applied mathematics, **12** (1964) 284–299
6. Stone, H. and Jackson, C.L.: Structures of affine families of switching functions. IEEE Transactions on Computers, **C-18** (1969) 251–257
7. Denev, J.D. and Tonchev, V.D.: On the number of equivalence classes of Boolean functions under a transformation group. IEEE Transactions on Information Theory, **IT-26** (1980) 625–626
8. Strazdins, I.: Universal affine classification of Boolean functions. Acta Applicandae Mathematicae, **46** (1997) 147–167
9. MacWilliams, F.J., Sloane, N.J.A.: The theory of error-correcting codes. North-Holland, New York (1977)
10. Maiorana, J.A.: A Classification of the cosets of the Reed-Muller code $\mathcal{R}(1,6)$. Mathematics of Computation, 57, **195** (1991) 403–414
11. Hou, X.D.: $AGL(m,2)$ acting on $\mathcal{R}(r,m)/\mathcal{R}(s,m)$. Journal of Algebra, **17** (1995) 921–938
12. Meier, W. and Staffelbach, O.: Nonlinearity criteria for cryptographic functions. Advances in Cryptology, EUROCRYPT'89, Lecture Notes in Computer Science, Springer-Verlag, New York, **434** (1989) 549–562
13. Preneel, B.: Analysis and design of cryptographic hash functions. PhD thesis, Katholieke Universiteit Leuven (1993)
14. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes and Cryptography, **15** (1998) 125–156
15. Budaghyan, L. and Carlet, C.: CCZ-equivalence and Boolean functions. Cryptology ePrint Archive, http://eprint.iacr.org/2009/063, (2009)
16. Fuller J.E.: Analysis of affine equivalent Boolean functions for cryptography. PhD thesis, Queensland University of Technology (2003)
17. Braeken, A.: Cryptographic properties of Boolean functions and S-Boxes. PhD thesis, Katholieke Universiteit Leuven (2006)
18. Carlet, C.: Boolean functions for cryptography and error correcting codes. http://www-rocq.inria.fr/codes/Claude.Carlet/chap-fcts-Bool-corr.pdf
19. Rothaus, O.S.: On "bent" functions. Journal of Combinatorial Theory, Ser. A, **20** (1976) 300–305
20. Dillon, J.F.: Elementary Hadamard difference sets. PhD thesis, University of Maryland (1974)
21. Sylvester, J.J.: Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colors, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. Philosophical Magazine, **34** (1867) 461–475
22. Hadamard, J.: Résolution d'une question relative aux déterminants. Bull. Sciences Math., 2, **17** (1893) 240–246
23. Hall, M. Jr.: Note on the Mathieu group $\mathcal{M}_{12}$. Arch. Math., **13** (1962) 334–340

24. Hall, M. Jr.: Combinatorial Theory. Blaisdell, Walthem, Mass (1967)
25. Horadam, K.J.: Hadamard matrices and their applications. New Jersey (2007)
26. Tokareva, N.: Automorphism group of the set of all bent functions. Cryptology ePrint Archive, http://eprint.iacr.org/2010/255, (2010)
27. Carlet, C. and Mesnager, S.: On Dillon's class H of bent functions, Niho bent functions and o-polynomials. Cryptology ePrint Archive, http://eprint.iacr.org/2010/567, (2010)

Appendix A: Nonlinearity Classes for $n \leq 5$

Table 2. Nonlinearity class cardinalities for $n \leq 5$

N_f	$n = 2$	$n = 3$	$n = 4$	$n = 5$
0	8	16	32	64
1	8	128	512	2048
2	-	112	3840	31744
3	-	-	17920	317440
4	-	-	28000	2301440
5	-	-	14336	12888064
6	-	-	896	57996288
7	-	-	-	215414784
8	-	-	-	647666880
9	-	-	-	1362452480
10	-	-	-	1412100096
11	-	-	-	556408832
12	-	-	-	27387136

Appendix B: Examples of new transformations for $n = 4$

Due to the space constraints, the algebraic normal form of the nonlinearity preserving transformations can not be given explicitly. However, since any transformation is an element of $S_{2^{2^n}}$, it is possible to represent its image by product of disjoint cycles. To do so, the truth table T_f of a function $f \in \mathcal{F}_4$ is represented by an integer in $\mathbb{Z}_{2^{2^4}}$ belonging to the interval $[0, 65535]$, which is evaluated by $\sum_{i=0}^{2^n-1} f(\alpha_i)2^{2^n-1-i}$. For example, the truth table $(0, 0, \ldots, 0, 1, 0)$ is represented with 2.

Based on the function representation given above, the permutations are represented with cycle notation, for example (18, 22, 1905)(2010, 2011), which means the transformation maps the functions $18 \mapsto 22$, $22 \mapsto 1905$, $1905 \mapsto 18$, $2010 \mapsto 2011$, $2011 \mapsto 2010$ and the rest to themselves.

Example 3. Let $\psi \in S_{2^{2^4}}$ be a mapping whose cycle notation is

$$(0,\ 27030,\ 65535)(51,\ 58,\ 6270,\ 2755)(312,\ 1525,\ 48779,\ 64560,\ 51485,\ 4471)$$

Here, for instance, ψ maps the function $(0,0,0,0,0,0,0,0,0,0,1,1,1,0,1,0)$ to $(0,0,0,1,1,0,0,0,0,1,1,1,1,1,1,0)$. It is easy to show that both function's non-linearity value is 4, however, algebraic degree of the former is 3 whereas the latter's is 2. Therefore, ψ can not be equivalent to an affine equivalence relation, since affine equivalence relations also preserve algebraic degree of the functions. Furthermore, when algebraic normal form of ψ is constructed, it can be easily seen that there exist some λ_i which are not truth table of a affine Boolean function.

Example 4. Let $\psi \in S_{2^{2^4}}$ be a permutation of $\mathbb{F}_2^{2^4}$ whose cycle representation is

$$(2,\ 16067,\ 65534,\ 13262,\ 32767,\ 12272)$$

$$(27,\ 13226,\ 58509,\ 63105,\ 27255,\ 38903,\ 1290,\ 636,\ 26202,\ 4976,\ 65520)$$

$$(1436,\ 42559,\ 57838,\ 13999,\ 29374,\ 64681).$$

Again, when the algebraic normal form of ψ is written explicitly, there will be some non-affine terms which are not truth table of affine functions. Furthermore, this transformation also maps some functions of degree 2 to the functions of degree 3, and vice versa.

Example 5. Similarly, assume $\psi \in S_{2^{2^4}}$ be a permutation of $\mathbb{F}_2^{2^4}$ with cycle representation,

$$(0, 26265, 61680, 43690, 39321, 38550, 23205, 15555)$$

$$(129, 189, 503)(263, 3135, 61695, 2625, 24524, 48927, 11915, 593, 12495, 5075)$$

$$(1137, 65252, 1173, 9263, 27775)(1628, 36136, 2716, 17528, 7547, 12013, 56948)$$

$$(2481, 10370, 24808, 4740, 58446)(7214, 40481)(23128, 31126, 23131).$$

As in the previous examples, it can be easily proven that this mapping also possesses contradictions with Proposition 3.