On the existence and non-existence of some classes of bent-negabent functions

Bimal Mandal[1], Subhamoy Maitra[2], and Pantelimon Stănică[3*]

[1] CARAMBA, INRIA, Nancy – Grand Est., France 54600
[2] Applied Statistics Unit
Indian Statistical Institute, Kolkata, India
[3] Department of Applied Mathematics
Naval Postgraduate School, Monterey 93943, USA
bimalmandal90@gmail.com, subho@isical.ac.in, pstanica@nps.edu

Abstract

In this paper we investigate different questions related to bent-negabent functions. We first take an expository look at the state-of-the-art research in this domain and point out some technical flaws in certain results and fix some of them. Further, we derive a necessary and sufficient condition for which the functions of the form $\mathbf{x}\cdot\pi(\mathbf{y})\oplus h(\mathbf{y})$ (Maiorana–McFarland ($\mathcal{M}$)) is bent-negabent, and more generally, we study the non-existence of bent-negabent functions in the $\mathcal{M}$ class. We also identify some functions that are bent-negabent. Next, we continue the recent work by Mandal et al. [Discr. Appl. Math. 236 (2018), 1–6] on rotation symmetric bent-negabent functions and show their non-existence in larger classes. For example, we prove that there is no rotation symmetric bent-negabent function in $4p^k$ variables, where p is an odd prime. We present the non-existence of such functions in certain classes that are affine transformations of rotation symmetric functions. Keeping in mind the existing literature, we correct here some technical issues and errors found in other papers and provide some novel results.

Keywords: Boolean functions, bent-negabent functions, bent functions, rotation symmetric functions

1 Introduction

Rothaus [17] introduced the class of bent Boolean functions, which have the maximum possible distance from the affine functions, alternatively, they have flat spectrum (in absolute value) under the Walsh-Hadamard transform. Bent functions exist only in even number of variables and the degree of an n-variable bent function is at most $\frac{n}{2}$.

There is a nega-periodic analogue of the bent criteria, where we require the nega-Hadamard spectrum (see Section 2) to be flat: A Boolean function is said to be negabent if its absolute nega-Hadamard spectrum (normalized) values are all equal to 1. For an even number of variables, a function is bent-negabent if it is both bent and negabent. The nega-Hadamard transform of Boolean functions was first proposed by Parker [14] and the bent-negabent functions were

*ORCID: 0000-0002-8622-7120

first introduced by Riera and Parker [18]. The intersection of the bent and negabent sets has been the subject of many prior research works. For more details on this and other properties of Boolean functions we refer to [3, 5, 6, 8, 7, 9, 13, 16, 23] and the references therein.

A Boolean function is said to be rotation symmetric (RotS) if the function is invariant under the cyclic group (see Section 5). From an implementation point of view, RotS functions are more efficient than the general Boolean functions and therefore these are of practical interest in the construction of cryptographic primitives.

First, let us mention some results related to the non-existence of bent functions with an extra property.

- In 2004, Xia et al. [26] proved that there is no homogeneous bent function of degree n in $2n$ variables, $n > 3$.
- In 2008, Stănică and Maitra [23] conjectured that there is no homogeneous rotation symmetric bent function of degree > 2.
- In 2015, Sarkar and Cusick [21] proved that there is no quadratic rotation symmetric bent-negabent function and they further checked that there is no rotation symmetric bent-negabent function for $n \leq 8$.
- Very recently, Mandal et al. [11, Theorem 5] derived a characterization of bent-negabent functions that is related to the autocorrelation spectra, showing that for $n = 2m$, $f \in \mathcal{B}_n$ is bent-negabent if and only if the following conditions are satisfied:

  1. For all nonzero $\mathbf{a} \in \mathbb{F}_2^n$ with even $wt(\mathbf{a})$,
  $$\sum_{\mathbf{x}\in\mathbb{F}_2^n:\ \mathbf{a}\cdot\mathbf{x}=0} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})} = \sum_{\mathbf{x}\in\mathbb{F}_2^n:\ \mathbf{a}\cdot\mathbf{x}=1} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})} = 0.$$
  2. For all nonzero $\mathbf{a} \in \mathbb{F}_2^n$ with odd $wt(\mathbf{a})$,
  $$\sum_{\mathbf{x}\in\mathbb{F}_2^n:\ \bar{\mathbf{a}}\cdot\mathbf{x}=0} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})} = \sum_{\mathbf{x}\in\mathbb{F}_2^n:\ \bar{\mathbf{a}}\cdot\mathbf{x}=1} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})} = 0.$$

  Using this result, the non-existence of rotation symmetric bent-negabent function was inferred for $n = 2p^k$ variables, where p is an odd prime and k is a positive integer.

Exploiting a similar (but more detailed) technique as in [11], in Section 5 we prove further results related to the non-existence of bent-negabent functions. For example, we show that there is no rotation symmetric bent-negabent function in $4p^k$ variables, where p is an odd prime and k is any positive integer. Further, additional conditions are derived for the existence (and non-existence) of n-variable rotation symmetric bent-negabent functions and their affine transformations.

Some existing construction methods and results on bent-negabent functions in $\mathcal{M}$ class are discussed below.

- In 2007, Parker et al. [15] derived some results on Maiorana–McFarland bent-negabent functions. In 2008, Schmidt et al. [19] constructed infinitely many bent-negabent functions in Maiorana–McFarland class and proved that the maximum algebraic degree of an $2m$-variable Maiorana–McFarland bent-negabent function is $m - 1$.

- In 2012, Stănică et al. [22, Theorem 22] constructed a class of bent-negabent functions in $\mathcal{M}$ using complete mapping permutations (π and $\pi \oplus I_m$ both are permutations over $\mathbb{F}_2^m$, where I_m is an identity permutation). Further, they showed [22, Theorem 17] that if a permutation π is weight-sum-invariant, i.e., $wt(\mathbf{x} \oplus \mathbf{y}) = wt(\pi(\mathbf{x}) \oplus \pi(\mathbf{y}))$, for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^m$, then $\mathbf{x} \cdot \pi(\mathbf{y}) \oplus h(\mathbf{y})$ is bent-negabent if and only if h is bent.

- In 2012, Sarkar [20, Theorem 5] proved that the function $\mathrm{Tr}_1^m(x\pi(y) \oplus h(y))$ ($\mathbb{F}_2^m$ is identified with $\mathbb{F}_{2^m}$ and h is any function on $\mathbb{F}_{2^m}$) is bent-negabent if and only if for any nonzero $a, b \in \mathbb{F}_{2^m}$
$$\sum_{y \in \delta_\pi(b,a)} (-1)^{\mathrm{Tr}_1^m(a\pi(y) \oplus h(y) \oplus h(y \oplus b) \oplus by)} = 0.$$
Using this result, in [20, Theorem 6], it was shown that if $\pi(y) = y^{2^i}$, then f is bent-negabent if and only if $\mathrm{Tr}_1^m(h(y))$ is bent.

- In 2013, Su et al. [25, Theorem 5] also constructed bent-negabent functions in the complete $\mathcal{M}$ class using the function $\mathbf{x} \cdot \pi(\mathbf{y}) \oplus h(\mathbf{y})$, where π is a complete mapping polynomial.

- Recently, Stănică et al. [24] proved that all bent functions in the Kerdock code, except for the coset of the symmetric quadratic bent function, are bent-negabent and identified non-orthogonal (nonsingular) linear transformations that preserve bent-negabent property for a special subset.

In Section 3 we revisit some results on bent-negabent functions and point out some incorrect proofs and/or results in several papers on bent-negabent functions and fix some of them. In Section 4 we also derive a necessary and sufficient condition for which a Maiorana–McFarland bent function is negabent using the characterization of bent-negabent functions given in [11, Theorem 5]. As an example, we present a bent-negabent function in six variables, which is not derived from earlier constructions. Further, we present a technical result related to the non-existence of Maiorana–McFarland type bent-negabent functions. In Section 5 we deal with non-existence of rotation symmetric functions. Section 6 concludes the paper.

2 Preliminaries

Let $\mathbb{F}_2$, $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n = \{\mathbf{x} = (x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}_2, 1 \le i \le n\}$ be the prime field of characteristic 2, the extension field of degree n over $\mathbb{F}_2$ and the vector space of dimension n over $\mathbb{F}_2$, respectively. Let '$\oplus$' denote the addition over $\mathbb{F}_2$. For $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$, we define the vector space addition as $\mathbf{x} \oplus \mathbf{y} = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)$, the inner product as $\mathbf{x} \cdot \mathbf{y} = x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n$ and the vector multiplication as $\mathbf{x} * \mathbf{y} = (x_1y_1, x_2y_2, \ldots, x_ny_n)$. The *cardinality* of a set S is denoted by $|S|$. We also identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ (as vector spaces) and take the inner product $x \cdot y = \mathrm{Tr}_1^n(xy)$, where $\mathrm{Tr}_1^n(x) = x \oplus x^2 \oplus x^{2^2} \oplus \cdots \oplus x^{2^{n-1}}$, for all $x \in \mathbb{F}_{2^n}$, is the absolute trace on $\mathbb{F}_{2^n}$. Any function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ (or, equivalently, $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$) is a *Boolean function* in n variables, whose set will be denoted by $\mathcal{B}_n$. Any function $f \in \mathcal{B}_n$ can be uniquely represented as a multivariate polynomial,

$$f(x_1, \ldots, x_n) = \bigoplus_{\mathbf{u}=(u_1,\ldots,u_n) \in \mathbb{F}_2^n} \mu_{\mathbf{u}} (\prod_{i=1}^{n} x_i^{u_i}), \tag{1}$$

where $\mu_{\mathbf{u}} \in \mathbb{F}_2$ and $x_1, \ldots, x_n \in \mathbb{F}_2$. This polynomial form is said to be the *algebraic normal form* (ANF) of $f \in \mathcal{B}_n$. The *Hamming weight* of $\mathbf{x} \in \mathbb{F}_2^n$, $wt(\mathbf{x})$, is defined as $wt(\mathbf{x}) = \sum_{i=1}^{n} x_i$, where the sum is over the ring of integers, $\mathbb{Z}$. The *algebraic degree* of $f \in \mathcal{B}_n$, $\deg(f)$, is defined as $\deg(f) = \max_{\mathbf{u} \in \mathbb{F}_2^n}\{wt(\mathbf{u}) : \mu_{\mathbf{u}} \neq 0\}$. A Boolean function f, defined as in (1), is said to be *homogeneous* of degree $r \geq 1$ if f has degree r and $\mu_{\mathbf{u}} = 0$ for all $\mathbf{u} \in \mathbb{F}_2^n$ such that $wt(\mathbf{u}) \neq r$.

The *Walsh–Hadamard transform* of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{F}_2^n$, denoted by $W_f(\mathbf{u})$, is defined by

$$W_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}}.$$

The multiset $[W_f(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_2^n]$ is the *Walsh–Hadamard spectrum* of f. A function $f \in \mathcal{B}_n$ (for even $n > 0$) is *bent* if and only if $|W_f(\mathbf{u})| = 2^{\frac{n}{2}}$, for all $\mathbf{u} \in \mathbb{F}_2^n$. Equivalently, f is bent if and only if the *autocorrelation*

$$C_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{u})}$$

is zero for all nonzero $\mathbf{u} \in \mathbb{F}_2^n$. The *nega-Hadamard transform* of $f \in \mathbb{F}_2^n$ at $\mathbf{u} \in \mathbb{F}_2^n$, denoted by $\mathcal{N}_f(\mathbf{u})$, is defined by

$$\mathcal{N}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \imath^{wt(\mathbf{x})},$$

where $\imath^2 = -1$. The multiset $[\mathcal{N}_f(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_2^n]$ is the *nega-Hadamard spectrum* of f. An n-variable Boolean function f is *negabent* if the modulus $|\mathcal{N}_f(\mathbf{u})| = 1$, for all $\mathbf{u} \in \mathbb{F}_2^n$. Equivalently, f is negabent [22, Lemma 6] if and only if the *nega-autocorrelation*

$$NC_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{u})} (-1)^{\mathbf{u} \cdot \mathbf{x}}$$

is zero for all nonzero $\mathbf{u} \in \mathbb{F}_2^n$. For an even number of variables, a function $f \in \mathcal{B}_n$ is *bent-negabent* if f is both bent and negabent. The *derivative* $D_{\mathbf{a}}f$ of f at $\mathbf{a} \in \mathbb{F}_2^n$ is defined by

$$D_{\mathbf{a}}f(\mathbf{x}) = f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{a}), \text{ for all } \mathbf{x} \in \mathbb{F}_2^n.$$

The *complement* of an element $\mathbf{a} \in \mathbb{F}_2^n$ is $\bar{\mathbf{a}} = \mathbf{a} \oplus \mathbf{1}$, where $\mathbf{1}$ is the all 1 vector of $\mathbb{F}_2^n$. A Boolean function $f \in \mathcal{B}_n$ is called *symmetric* if $f(y) = f(x)$, for all $y, x \in \mathbb{F}_2^n$ with $wt(y) = wt(x)$ (invariant under any permutation of the input variables). Let $GL(n, \mathbb{F}_2)$ be the set of all binary nonsingular matrices of order n and $SL(n, \mathbb{F}_2)$ be the set of all binary orthogonal matrices of order n.

3 Revisiting some results on bent-negabent functions

In this section we discuss some known results on bent-negabent functions, pointing out some technical flaws in certain proofs and when possible, correcting them. Schmidt et al. [19] claimed that $SL(n, \mathbb{F}_2)$ preserves the bent-negabent property, i.e., if f is bent-negabent, then $f(\mathbf{x}A)$, for all $\mathbf{x} \in \mathbb{F}_2^n$, is also bent-negabent, where $A \in SL(n, \mathbb{F}_2)$. Unfortunately, the proof of [19, Theorem 2] is not exactly correct, as we shall argue next. In that proof, the authors defined $wt(\mathbf{x}) = \mathbf{x} I_n \mathbf{x}^T$ for all $\mathbf{x} \in \mathbb{F}_2^n$, where I_n is the identity matrix of order n and $\mathbf{x}^T$ is the transpose of $\mathbf{x}$ and the matrix operations are over integer $\mathbb{Z}$. Surely, $BI_nB^T = I_n$, where $B \in SL(n, \mathbb{F}_2)$,

and so, they claimed that $wt(\mathbf{x}) = wt(\mathbf{x}B)$, which is not true in general when the operations are over $\mathbb{Z}$. As an example, if $B \in SL(6, \mathbb{F}_2)$ defined by

$$B = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

where $wt(1,0,0,0,0,0) \neq wt(1,1,1,0,0,0) = wt((1,0,0,0,0,0)B)$. If we modify the proof and require perhaps that the weights to be congruent modulo 4 (since they occur in the exponent of the complex i, we have $i^{wt(\mathbf{x})} = i^{wt(\mathbf{x}B) \pmod 4}$), but the claim still that does not hold, in general. We know that $BI_6B^T = I_6$ in binary, but if matrix operations are over $\mathbb{Z}$, then

$$BI_6B^T = \begin{bmatrix} 3 & 2 & 2 & 2 & 0 & 0 \\ 2 & 3 & 2 & 2 & 0 & 0 \\ 2 & 2 & 3 & 2 & 0 & 0 \\ 2 & 2 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Let f be bent-negabent and $AB = I_n$, where $A, B \in SL(n, \mathbb{F}_2)$. Then $f(\mathbf{x}A)$ is bent and, to prove [19, Theorem 2], it is sufficient to show that $f(\mathbf{x}A)$ is negabent. However,

$$\sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}A) \oplus \mathbf{u} \cdot \mathbf{x}} \imath^{wt(\mathbf{x})} = \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{y}) \oplus (\mathbf{u}B^T) \cdot \mathbf{y}} \imath^{wt(\mathbf{y}B)},$$

which is not equal to $\mathcal{N}_f(\mathbf{u}B^T)$, as $\imath^{wt(\mathbf{x})} \neq \imath^{wt(\mathbf{x}B)}$, in general.

Nonetheless, the result given in [19, Theorem 2] is true, and the result can be proved by using the nega-autocorrelation property from [22, Lemma 6], and we shall do that next.

Theorem 1. [19, Theorem 2] *Let $f, g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ be two Boolean functions. Suppose that f and g are related by*

$$g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{a}) \oplus \mathbf{u} \cdot \mathbf{x} \oplus \varepsilon,$$

for all $\mathbf{x} \in \mathbb{F}_2^n$, where $A \in SL(n, \mathbb{F}_2)$, $\mathbf{a}, \mathbf{u} \in \mathbb{F}_2^n$ and $\varepsilon \in \mathbb{F}_2$. If f is bent-negabent, then g is also bent-negabent.

Proof. Let f be bent-negabent and $A \in SL(n, \mathbb{F}_2)$. From [15, Lemma 2], it is sufficient to prove that $g(\mathbf{x}) = f(\mathbf{x}A)$ is negabent. We know [22, Lemma 6] that a function $f \in \mathcal{B}_n$ is negabent if and only if for any nonzero $\mathbf{u} \in \mathbb{F}_2^n$, $NC_f(\mathbf{u}) = 0$. For any nonzero $\mathbf{u} \in \mathbb{F}_2^n$, we have

$$\begin{aligned} NC_g(\mathbf{u}) &= \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{g(\mathbf{x}) \oplus g(\mathbf{x} \oplus \mathbf{u})} (-1)^{\mathbf{u} \cdot \mathbf{x}} = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}A) \oplus f(\mathbf{x}A \oplus \mathbf{u}A)} (-1)^{\mathbf{u} \cdot \mathbf{x}} \\ &= \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{y}) \oplus f(\mathbf{y} \oplus \mathbf{u}A)} (-1)^{\mathbf{u} \cdot (\mathbf{y}A^T)} = \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{y}) \oplus f(\mathbf{y} \oplus \mathbf{u}A)} (-1)^{\mathbf{u}(\mathbf{y}A^T)^T} \\ &= \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{y}) \oplus f(\mathbf{y} \oplus \mathbf{u}A)} (-1)^{\mathbf{u}(A\mathbf{y}^T)} = \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{y}) \oplus f(\mathbf{y} \oplus \mathbf{u}A)} (-1)^{(\mathbf{u}A)\mathbf{y}^T} \\ &= \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{y}) \oplus f(\mathbf{y} \oplus \mathbf{u}A)} (-1)^{(\mathbf{u}A) \cdot \mathbf{y}} = NC_f(\mathbf{u}A), \end{aligned}$$

so g is bent-negabent. □

Fortunately, the result has no further consequences. The error on the weights was picked up in [24, Lem. 17, Prop. 18] (by the current authors), where we identified a set of non-singular binary transformations, which preserve the bent-negabent property by considering all the elements of $SL(n, \mathbb{F}_2)$ are weight invariant. The reason our earlier result [24, Lemma 17] was incorrect is because one can find a matrix $A \in SL(n, \mathbb{F}_2)$ such that $wt(\mathbf{x}) \neq wt(\mathbf{x}A)$, for some $\mathbf{x} \in \mathbb{F}_2^n$. For example, let $B \in SL(n, \mathbb{F}_2)$, where B was previously defined. Note that, $wt(1,0,0,0,0,0) = 1$, but $wt((1,0,0,0,0,0)B) = wt(1,1,1,0,0,0) = 3$. However, the weights do have the same parity as we show below.

Proposition 2. *For any $A \in SL(n, \mathbb{F}_2)$ and $\mathbf{x} \in \mathbb{F}_2^n$, we have $wt(\mathbf{x}) \equiv wt(\mathbf{x}A) \pmod 2$.*

Proof. Let $\mathbf{u}^1, \mathbf{u}^2, \ldots, \mathbf{u}^n$ be the row vectors of $A \in SL(n, \mathbb{F}_2)$. Then $\mathbf{u}^i \cdot \mathbf{u}^j = 1$ if $i = j$ and 0 otherwise, so $wt(\mathbf{u}^i)$ is odd for all $1 \leq i \leq n$. It is easy to check that $wt(\mathbf{0}) = wt(\mathbf{0}A) = 0$. Suppose $\mathbf{x} \in \mathbb{F}_2^n$ with $wt(\mathbf{x}) = r$, $1 \leq r \leq n$, and there exist $1 \leq i_1 < i_2 < \cdots < i_r \leq n$ such that $x_{i_j} = 1$ for $1 \leq j \leq r$, otherwise 0. Then $\mathbf{x}A = \oplus_{j=1}^{r} \mathbf{u}^{i_j}$. Thus, the claim is true for $r = 1$. Let $r = 2$. Then $\mathbf{x}A = \mathbf{u}^{i_1} \oplus \mathbf{u}^{i_2}$, and so, $wt(\mathbf{x}A) = wt(\mathbf{u}^{i_1}) + wt(\mathbf{u}^{i_2}) - 2wt(\mathbf{u}^{i_1} * \mathbf{u}^{i_2})$ is even as $wt(\mathbf{u}^{i_1})$ and $wt(\mathbf{u}^{i_2})$ are odd. Suppose $r = 3$. Then $wt(\mathbf{x}A) = wt(\mathbf{u}^{i_1} \oplus \mathbf{u}^{i_2}) + wt(\mathbf{u}^{i_3}) - 2wt((\mathbf{u}^{i_1} \oplus \mathbf{u}^{i_2}) * \mathbf{u}^{i_3})$ is odd. Using this relation, it is clear that if $wt(\mathbf{x}) = r$ is even (or odd), then $wt(\mathbf{x}A)$ is also even (or odd, respectively). □

Let $\lambda \geq 1$ be an arbitrary positive integer and $\mathcal{NLT}_{inv}(n, \mathbb{F}_2, \lambda)$ [24, Proposition 18] be the set of all nonsingular linear transformation of $GL(n, \mathbb{F}_2)$ defined by

$$\mathcal{NLT}_{inv}(n, \mathbb{F}_2, \lambda) = \{A \in GL(n, \mathbb{F}_2) : wt(\mathbf{x}) \equiv wt(\mathbf{x}A) \pmod{4\lambda}, \text{ for all } \mathbf{x} \in \mathbb{F}_2^n\}.$$

It is clear that $\mathcal{NLT}_{inv}(n, \mathbb{F}_2, \lambda)$ is not empty as $I_n \in \mathcal{NLT}_{inv}(n, \mathbb{F}_2, \lambda)$ and $SL(n, \mathbb{F}_2) \cap \mathcal{NLT}_{inv}(n, \mathbb{F}_2, \lambda) \neq \emptyset$, but $SL(n, \mathbb{F}_2) \not\subseteq \mathcal{NLT}_{inv}(n, \mathbb{F}_2, \lambda)$, for all positive integer λ. It is also true for $n = 4$. Moreover, for any positive integer $\lambda \geq 1$, $\mathcal{NLT}_{inv}(n, \mathbb{F}_2, \lambda) \subseteq \mathcal{NLT}_{inv}(n, \mathbb{F}_2, 1)$. Then Fig. 1 given in [24] can be described in the following way. We denote $\mathcal{NLT}_{inv}(n, \mathbb{F}_2, 1)$ by $\mathcal{NLT}_{inv}(n, \mathbb{F}_2)$.

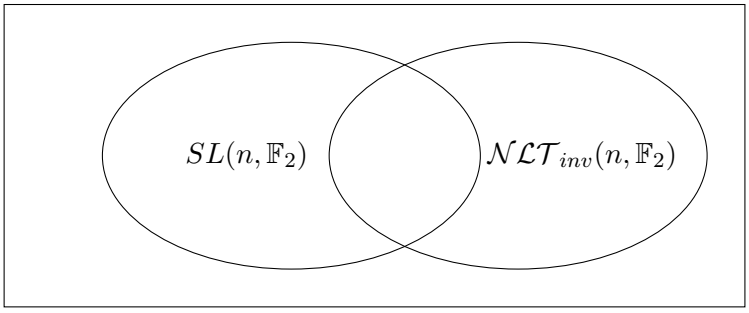

Figure 1: All possible bent-negabent preserving nonsingular linear transformations

4 Bent-negabent functions in the Maiorana–McFarland class

Let $n = 2m$ and the following function $f \in \mathcal{B}_n$ belonging to the Maiorana–McFarland ($\mathcal{M}$) class [10] of bent functions,

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus h(\mathbf{y}),\ \mathbf{x}, \mathbf{y} \in \mathbb{F}_2^m, \tag{2}$$

where π is a permutation over $\mathbb{F}_2^m$ and $h \in \mathcal{B}_m$. The mapping $y \longmapsto y^{2^i}$ over $\mathbb{F}_{2^m}$ is linear, weight-sum-invariant (consider the orthogonal basis), but not a complete mapping polynomial. Thus, [20, Theorem 6] is a special case of [22, Theorem 17]. So, one can easily construct a bent-negabent function in $\mathcal{M}$, where π is not a complete mapping polynomial. For example let $n = 4$, $\pi(y_2, y_1) = (y_2, y_1)$ and $h(y_2, y_1) = y_1 y_2$ for all $y_2, y_1 \in \mathbb{F}_2$. Then $f(\mathbf{x}, \mathbf{y}) = x_1 y_1 \oplus x_2 y_2 \oplus y_1 y_2$, for all $x_i, y_i \in \mathbb{F}_2,\ i = 1, 2$, is a bent-negabent function. Here, π is linear and weight-sum-invariant, but not a complete mapping permutation as $(\pi \oplus I_2)(\mathbf{y}) = \mathbf{0}$.

Now, we focus on identifying a bent-negabent function in $\mathcal{M}$ such that the permutation π is not complete mapping polynomial and not weight-sum-invariant. For that, we derive a necessary and sufficient condition for which the function f in $\mathcal{M}$ is bent-negabent using [11, Theorem 5]. The result [11, Theorem 5] is mainly based on the autocorrelation properties of f and $f \oplus s_2$, where s_2 is symmetric quadratic bent function. Sarkar [20, Theorem 5] also derived a necessary and sufficient condition for which a function in $\mathcal{M}$ is bent-negabent using the nega-autocorrelation property. So, Theorem 4 (shown later) is similar to [20, Theorem 5].The conditions are different when nega-autocorrelation values are calculated at the odd weight inputs. Our result, Theorem 4 (shown later), is more effective in some cases, for example, in showing the non-existence of bent-negabent functions when π satisfies the conditions of Corollary 6.

For any $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m$, define

$$\delta_\pi(\mathbf{a}, \mathbf{b}) = \{\mathbf{x} \in \mathbb{F}_2^m :\ \pi(\mathbf{x}) \oplus \pi(\mathbf{x} \oplus \mathbf{a}) = \mathbf{b}\}. \tag{3}$$

It is clear that $|\delta_\pi(\mathbf{0}, \mathbf{0})| = 2^m$, and if π is permutation and $\mathbf{a} \neq \mathbf{0}$, then $|\delta_\pi(\mathbf{a}, \mathbf{0})| = 0$. If $\delta = \max_{\mathbf{a},\mathbf{b} \in \mathbb{F}_2^m} \{|\delta(\mathbf{a}, \mathbf{b})| :\ \mathbf{a} \neq \mathbf{0}\}$, then π is a *differentially δ-uniform* mapping. Surely, $\delta \equiv 0 \pmod 2$. For all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m$, let us define

$$\begin{aligned}
E_{\mathbf{a}}^0 &= \{\mathbf{x} \in \mathbb{F}_2^m :\ \mathbf{a} \cdot \mathbf{x} = 0\},\ E_{\mathbf{a}}^1 = \{\mathbf{x} \in \mathbb{F}_2^m :\ \mathbf{a} \cdot \mathbf{x} = 1\} = \mathbb{F}_2^m \setminus E_{\mathbf{a}}^0, \\
E_{\mathbf{a},\mathbf{b}}^0 &= \{(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^m \times \mathbb{F}_2^m :\ \mathbf{a} \cdot \mathbf{x} \oplus \mathbf{b} \cdot \mathbf{y} = 0\} = (E_{\mathbf{a}}^0 \times E_{\mathbf{b}}^0) \cup (E_{\mathbf{a}}^1 \times E_{\mathbf{b}}^1), \\
E_{\mathbf{a},\mathbf{b}}^1 &= \{(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^m \times \mathbb{F}_2^m :\ \mathbf{a} \cdot \mathbf{x} \oplus \mathbf{b} \cdot \mathbf{y} = 1\} = (E_{\mathbf{a}}^0 \times E_{\mathbf{b}}^1) \cup (E_{\mathbf{a}}^1 \times E_{\mathbf{b}}^0).
\end{aligned}$$

It is clear that $E_{\mathbf{0}}^0 = \mathbb{F}_2^m$ and $E_{\mathbf{0},\mathbf{b}}^0 = \mathbb{F}_2^m \times E_{\mathbf{b}}^0$. For $\mathbf{0} \neq \mathbf{a} \in \mathbb{F}_2^m$, $E_{\mathbf{a}}^0$ is a linear subspace of dimension $m-1$ (the orthogonal space of $\{\mathbf{0}, \mathbf{a}\}$, denoted by $\{\mathbf{0}, \mathbf{a}\}^\perp$). The dimension of $E_{\mathbf{a}}^{0\perp}$ is then equal to 1 and $E_{\mathbf{a}}^{0\perp} = \{\mathbf{0}, \mathbf{a}\}$.

We know the function $f \in \mathcal{B}_n$ defined as in (2) is bent, so, for any nonzero $(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$, $f(\mathbf{x}, \mathbf{y}) \oplus f(\mathbf{x} \oplus \mathbf{a}, \mathbf{y} \oplus \mathbf{b})$ is balanced, i.e.,

$$\sum_{(\mathbf{x},\mathbf{y}) \in \mathbb{F}_2^m \times \mathbb{F}_2^m} (-1)^{f(\mathbf{x},\mathbf{y}) \oplus f(\mathbf{x} \oplus \mathbf{a}, \mathbf{y} \oplus \mathbf{b})} = 0.$$

First, we assume that $h = 0$. For any $(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$, $f(\mathbf{x}, \mathbf{y}) \oplus f(\mathbf{x} \oplus \mathbf{a}, \mathbf{y} \oplus \mathbf{b}) = \mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b})) \oplus \mathbf{a} \cdot \pi(\mathbf{y} \oplus \mathbf{b})$. Thus, form [11, Theorem 5], we get the following remark immediately.

Remark 3. *A Boolean function $f \in \mathcal{B}_n$ defined as in (2) with $h = 0$ is bent-negabent if and only if the following conditions are satisfied:*

1. *For all nonzero $(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$ with even $wt(\mathbf{a}, \mathbf{b})$,*

$$\sum_{(\mathbf{x},\mathbf{y}) \in E^0_{\mathbf{a},\mathbf{b}}} (-1)^{\mathbf{x}\cdot(\pi(\mathbf{y})\oplus\pi(\mathbf{y}\oplus\mathbf{b}))\oplus\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} = 0.$$

2. *For all nonzero $(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$ with odd $wt(\mathbf{a}, \mathbf{b})$,*

$$\sum_{(\mathbf{x},\mathbf{y}) \in E^0_{\bar{\mathbf{a}},\bar{\mathbf{b}}}} (-1)^{\mathbf{x}\cdot(\pi(\mathbf{y})\oplus\pi(\mathbf{y}\oplus\mathbf{b}))\oplus\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} = 0.$$

By a more detailed analysis of Remark 3, we get the next necessary and sufficient condition for $\mathbf{x} \cdot \pi(\mathbf{y})$ to be bent-negabent.

Theorem 4. *A Boolean function $f \in \mathcal{B}_n$ defined as in (2) with $h = 0$ is bent-negabent if and only if the following conditions are satisfied for any nonzero $(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$:*

1. *If $\mathbf{a} = \mathbf{0}$ and $wt(\mathbf{b})$ is odd, then*

$$|E^0_{\bar{\mathbf{b}}} \cap \delta_\pi(\mathbf{b}, \mathbf{1})| = |E^1_{\bar{\mathbf{b}}} \cap \delta_\pi(\mathbf{b}, \mathbf{1})|.$$

2. *If $wt(\mathbf{a}, \mathbf{b})$ is even, then*

$$\sum_{\mathbf{y} \in E^0_{\mathbf{b}} \cap \delta_\pi(\mathbf{b},\mathbf{a})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} = \sum_{\mathbf{y} \in E^1_{\mathbf{b}} \cap \delta_\pi(\mathbf{b},\mathbf{a})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})}.$$

3. *If $wt(\mathbf{a}, \mathbf{b})$ is odd, then*

$$\sum_{\mathbf{y} \in E^0_{\bar{\mathbf{b}}} \cap \delta_\pi(\mathbf{b},\bar{\mathbf{a}})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} = \sum_{\mathbf{y} \in E^1_{\bar{\mathbf{b}}} \cap \delta_\pi(\mathbf{b},\bar{\mathbf{a}})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})}.$$

Proof. Let $(\mathbf{a}, \mathbf{b})$ be any nonzero element of $\mathbb{F}_2^m \times \mathbb{F}_2^m$ and $f \in \mathcal{B}_n$ defined as in (2) with $h = 0$. *Case* (i): Let $\mathbf{b} = \mathbf{0}$. Then $\mathbf{a} \neq \mathbf{0}$ and $f(\mathbf{x}, \mathbf{y}) \oplus f(\mathbf{x} \oplus \mathbf{a}, \mathbf{y}) = \mathbf{a} \cdot \pi(\mathbf{y})$. If $wt(\mathbf{a})$ is even, then

$$\sum_{(\mathbf{x},\mathbf{y}) \in E^0_{\mathbf{a},\mathbf{0}}} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} = \sum_{\mathbf{x} \in E^0_{\mathbf{a}}} \sum_{\mathbf{y} \in \mathbb{F}_2^m} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} = 0, \quad \text{as } \mathbf{a} \neq \mathbf{0}.$$

Suppose $wt(\mathbf{a})$ is odd. Then,

$$\begin{aligned}
\sum_{(\mathbf{x},\mathbf{y}) \in E^0_{\bar{\mathbf{a}},\mathbf{1}}} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} &= \sum_{\mathbf{x} \in E^0_{\bar{\mathbf{a}}}} \sum_{\mathbf{y} \in E^0_{\mathbf{1}}} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} + \sum_{\mathbf{x} \in E^1_{\bar{\mathbf{a}}}} \sum_{\mathbf{y} \in E^1_{\mathbf{1}}} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} \\
&= 2^{n-1} \left(\sum_{\mathbf{y} \in E^0_{\mathbf{1}}} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} + \sum_{\mathbf{y} \in E^1_{\mathbf{1}}} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} \right) \\
&= 2^{n-1} \sum_{\mathbf{y} \in \mathbb{F}_2^m = E^0_{\mathbf{1}} \cup E^1_{\mathbf{1}}} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} = 0, \quad \text{as } \mathbf{a} \neq \mathbf{0}.
\end{aligned}$$

Case (ii): Let $\mathbf{a} = \mathbf{0}$. Then $\mathbf{b} \neq \mathbf{0}$, and so, $f(\mathbf{x}, \mathbf{y}) \oplus f(\mathbf{x}, \mathbf{y} \oplus \mathbf{b}) = \mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))$ and $\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}) \neq \mathbf{0}$ for all $\mathbf{y} \in \mathbb{F}_2^m$. If $wt(\mathbf{b})$ is even, then

$$\sum_{(\mathbf{x},\mathbf{y}) \in E^0_{\mathbf{0},\mathbf{b}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} = \sum_{\mathbf{y} \in E^0_{\mathbf{b}}} \sum_{\mathbf{x} \in \mathbb{F}_2^m} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} = 0.$$

Suppose $wt(\mathbf{b})$ is odd. Then,

$$\begin{aligned}
&\sum_{(\mathbf{x},\mathbf{y}) \in E^0_{\mathbf{1},\bar{\mathbf{b}}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} \\
&\quad = \sum_{\mathbf{y} \in E^0_{\mathbf{b}}} \sum_{\mathbf{x} \in E^0_{\mathbf{1}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} + \sum_{\mathbf{y} \in E^1_{\mathbf{b}}} \sum_{\mathbf{x} \in E^1_{\mathbf{1}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} \\
&\quad = \sum_{\mathbf{y} \in E^0_{\mathbf{b}}} \sum_{\mathbf{x} \in E^0_{\mathbf{1}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} + \sum_{\mathbf{y} \in E^1_{\mathbf{b}}} \sum_{\mathbf{x} \in \mathbb{F}_2^m} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} \\
&\qquad - \sum_{\mathbf{y} \in E^1_{\bar{\mathbf{b}}}} \sum_{\mathbf{x} \in E^0_{\mathbf{1}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} \\
&\quad = \sum_{\mathbf{y} \in E^0_{\mathbf{b}}} \sum_{\mathbf{x} \in E^0_{\mathbf{1}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} - \sum_{\mathbf{y} \in E^1_{\mathbf{b}}} \sum_{\mathbf{x} \in E^0_{\mathbf{1}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} \\
&\quad = 2^{m-1}(|E^0_{\mathbf{b}} \cap \delta_\pi(\mathbf{b}, \mathbf{1})| - |E^1_{\mathbf{b}} \cap \delta_\pi(\mathbf{b}, \mathbf{1})|),
\end{aligned}$$

as $\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}) \in E^{0\perp}_{\mathbf{1}} = \{\mathbf{0}, \mathbf{1}\}$ implies $\mathbf{y} \in \delta_\pi(\mathbf{b}, \mathbf{1})$, which is equal to 0 if and only if $|E^0_{\mathbf{b}} \cap \delta_\pi(\mathbf{b}, \mathbf{1})| = |E^1_{\mathbf{b}} \cap \delta_\pi(\mathbf{b}, \mathbf{1})|$, for all nonzero odd weight $\mathbf{b} \in \mathbb{F}_2^m$.
Case (iii): Let $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ and $wt(\mathbf{a}, \mathbf{b})$ be even. Then,

$$\begin{aligned}
&\sum_{(\mathbf{x},\mathbf{y}) \in E^0_{\mathbf{a},\mathbf{b}}} (-1)^{f(\mathbf{x},\mathbf{y}) \oplus f(\mathbf{x} \oplus \mathbf{a}, \mathbf{y} \oplus \mathbf{b})} = \sum_{(\mathbf{x},\mathbf{y}) \in E^0_{\mathbf{a},\mathbf{b}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b})) \oplus \mathbf{a} \cdot \pi(\mathbf{y} \oplus \mathbf{b})} \\
&= \sum_{\mathbf{y} \in E^0_{\mathbf{b}}} (-1)^{\mathbf{a} \cdot \pi(\mathbf{y} \oplus \mathbf{b})} \sum_{\mathbf{x} \in E^0_{\mathbf{a}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} + \sum_{\mathbf{y} \in E^1_{\mathbf{b}}} (-1)^{\mathbf{a} \cdot \pi(\mathbf{y} \oplus \mathbf{b})} \\
&\cdot \sum_{\mathbf{x} \in E^1_{\mathbf{a}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} \\
&\sum_{\mathbf{y} \in E^1_{\mathbf{b}}} (-1)^{\mathbf{a} \cdot \pi(\mathbf{y} \oplus \mathbf{b})} \sum_{\mathbf{x} \in E^1_{\mathbf{a}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} \\
&= \sum_{\mathbf{y} \in E^1_{\mathbf{b}}} (-1)^{\mathbf{a} \cdot \pi(\mathbf{y} \oplus \mathbf{b})} \left(\sum_{\mathbf{x} \in \mathbb{F}_2^m} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} - \sum_{\mathbf{x} \in E^0_{\mathbf{a}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))} \right) \\
&= - \sum_{\mathbf{y} \in E^1_{\mathbf{b}}} (-1)^{\mathbf{a} \cdot \pi(\mathbf{y} \oplus \mathbf{b})} \sum_{\mathbf{x} \in E^0_{\mathbf{a}}} (-1)^{\mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}))},
\end{aligned}$$

as $\mathbf{b} \neq \mathbf{0}$ implies $\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}) \neq \mathbf{0}$ for all $\mathbf{y} \in \mathbb{F}_2^m$, and so,

$$\sum_{(\mathbf{x},\mathbf{y}) \in E^0_{\mathbf{a},\mathbf{b}}} (-1)^{f(\mathbf{x},\mathbf{y}) \oplus f(\mathbf{x} \oplus \mathbf{a}, \mathbf{y} \oplus \mathbf{b})}$$

$$= \left(\sum_{\mathbf{y} \in E_{\mathbf{b}}^0} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} - \sum_{\mathbf{y} \in E_{\mathbf{b}}^1} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} \right) \sum_{\mathbf{x} \in E_{\mathbf{a}}^0} (-1)^{\mathbf{x}\cdot(\pi(\mathbf{y})\oplus\pi(\mathbf{y}\oplus\mathbf{b}))}$$

$$= |E_{\mathbf{a}}^0| \left(\sum_{\mathbf{y} \in E_{\mathbf{b}}^0 \cap \delta_\pi(\mathbf{b},\mathbf{a})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} - \sum_{\mathbf{y} \in E_{\mathbf{b}}^1 \cap \delta_\pi(\mathbf{b},\mathbf{a})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} \right)$$

$$= 2^{m-1}(-1)^{wt(\mathbf{a})} \left(\sum_{\mathbf{y} \in E_{\mathbf{b}}^0 \cap \delta_\pi(\mathbf{b},\mathbf{a})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} - \sum_{\mathbf{y} \in E_{\mathbf{b}}^1 \cap \delta_\pi(\mathbf{b},\mathbf{a})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} \right),$$

as $\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}) = \mathbf{a}$, which is equal to 0 if and only if

$$\sum_{\mathbf{y} \in E_{\mathbf{b}}^0 \cap \delta_\pi(\mathbf{b},\mathbf{a})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} = \sum_{\mathbf{y} \in E_{\mathbf{b}}^1 \cap \delta_\pi(\mathbf{b},\mathbf{a})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})},$$

for all nonzero $\mathbf{a}, \mathbf{b}$ with even $wt(\mathbf{a}, \mathbf{b})$.
Case (iv): Let $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ and and $wt(\mathbf{a}, \mathbf{b})$ be odd. Then,

$$\sum_{(\mathbf{x},\mathbf{y}) \in E_{\bar{\mathbf{a}},\bar{\mathbf{b}}}^0} (-1)^{f(\mathbf{x},\mathbf{y})\oplus f(\mathbf{x}\oplus\mathbf{a},\mathbf{y}\oplus\mathbf{b})} = \sum_{(\mathbf{x},\mathbf{y}) \in E_{\bar{\mathbf{a}},\bar{\mathbf{b}}}^0} (-1)^{\mathbf{x}\cdot(\pi(\mathbf{y})\oplus\pi(\mathbf{y}\oplus\mathbf{b}))\oplus\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})}$$

$$= \sum_{\mathbf{y} \in E_{\bar{\mathbf{b}}}^0} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} \sum_{\mathbf{x} \in E_{\bar{\mathbf{a}}}^0} (-1)^{\mathbf{x}\cdot(\pi(\mathbf{y})\oplus\pi(\mathbf{y}\oplus\mathbf{b}))} + \sum_{\mathbf{y} \in E_{\bar{\mathbf{b}}}^1} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} \sum_{\mathbf{x} \in E_{\bar{\mathbf{a}}}^1} (-1)^{\mathbf{x}\cdot(\pi(\mathbf{y})\oplus\pi(\mathbf{y}\oplus\mathbf{b}))},$$

$$\sum_{\mathbf{y} \in E_{\bar{\mathbf{b}}}^1} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} \sum_{\mathbf{x} \in E_{\bar{\mathbf{a}}}^1} (-1)^{\mathbf{x}\cdot(\pi(\mathbf{y})\oplus\pi(\mathbf{y}\oplus\mathbf{b}))}$$

$$= \sum_{\mathbf{y} \in E_{\bar{\mathbf{b}}}^1} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} \left(\sum_{\mathbf{x} \in \mathbb{F}_2^m} (-1)^{\mathbf{x}\cdot(\pi(\mathbf{y})\oplus\pi(\mathbf{y}\oplus\mathbf{b}))} - \sum_{\mathbf{x} \in E_{\bar{\mathbf{a}}}^0} (-1)^{\mathbf{x}\cdot(\pi(\mathbf{y})\oplus\pi(\mathbf{y}\oplus\mathbf{b}))} \right)$$

$$= - \sum_{\mathbf{y} \in E_{\bar{\mathbf{b}}}^1} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} \sum_{\mathbf{x} \in E_{\bar{\mathbf{a}}}^0} (-1)^{\mathbf{x}\cdot(\pi(\mathbf{y})\oplus\pi(\mathbf{y}\oplus\mathbf{b}))},$$

as $\mathbf{b} \neq \mathbf{0}$ implies $\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}) \neq \mathbf{0}$ for all $\mathbf{y} \in \mathbb{F}_2^m$, and so,

$$\sum_{(\mathbf{x},\mathbf{y}) \in E_{\bar{\mathbf{a}},\bar{\mathbf{b}}}^0} (-1)^{f(\mathbf{x},\mathbf{y})\oplus f(\mathbf{x}\oplus\mathbf{a},\mathbf{y}\oplus\mathbf{b})}$$

$$= \left(\sum_{\mathbf{y} \in E_{\mathbf{b}}^0} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} - \sum_{\mathbf{y} \in E_{\mathbf{b}}^1} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} \right) \sum_{\mathbf{x} \in E_{\bar{\mathbf{a}}}^0} (-1)^{\mathbf{x}\cdot(\pi(\mathbf{y})\oplus\pi(\mathbf{y}\oplus\mathbf{b}))}$$

$$= |E_{\bar{\mathbf{a}}}^0| \left(\sum_{\mathbf{y} \in E_{\mathbf{b}}^0 \cap \delta_\pi(\mathbf{b},\bar{\mathbf{a}})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} - \sum_{\mathbf{y} \in E_{\bar{\mathbf{b}}}^1 \cap \delta_\pi(\mathbf{b},\bar{\mathbf{a}})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y}\oplus\mathbf{b})} \right)$$

$$= 2^{m-1} \left(\sum_{\mathbf{y} \in E_{\mathbf{b}}^0 \cap \delta_\pi(\mathbf{b},\bar{\mathbf{a}})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} - \sum_{\mathbf{y} \in E_{\mathbf{b}}^1 \cap \delta_\pi(\mathbf{b},\bar{\mathbf{a}})} (-1)^{\mathbf{a}\cdot\pi(\mathbf{y})} \right),$$

as $\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b}) = \bar{\mathbf{a}}$, and which is equal to 0 if and only if

$$\sum_{\mathbf{y} \in E_{\mathbf{b}}^0 \cap \delta_\pi(\mathbf{b}, \bar{\mathbf{a}})} (-1)^{\mathbf{a} \cdot \pi(\mathbf{y})} = \sum_{\mathbf{y} \in E_{\mathbf{b}}^1 \cap \delta_\pi(\mathbf{b}, \bar{\mathbf{a}})} (-1)^{\mathbf{a} \cdot \pi(\mathbf{y})}$$

for all nonzero $\mathbf{a}, \mathbf{b}$ with odd $wt(\mathbf{a}, \mathbf{b})$. □

Suppose $f \in \mathcal{B}_n$ is defined as in (2) with $h \neq 0$. For any $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m$, we have

$$D_{(\mathbf{a},\mathbf{b})} f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot (\pi(\mathbf{y}) \oplus \pi(\mathbf{y} \oplus \mathbf{b})) \oplus \mathbf{a} \cdot \pi(\mathbf{y} \oplus \mathbf{b}) \oplus h(\mathbf{y}) \oplus h(\mathbf{y} \oplus \mathbf{b}),$$

so, $D_{\mathbf{b}}(\mathbf{y}) = h(\mathbf{y}) \oplus h(\mathbf{y} \oplus \mathbf{b})$ depends only on $\mathbf{b}$ and on the variable $\mathbf{y}$. The next result follows from Theorem 4.

Corollary 5. *Let $n = 2m$ and f be defined as in (2). The function f is bent-negabent if and only if the following conditions are satisfied for any nonzero $(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$:*

1. *If $\mathbf{a} = \mathbf{0}$ and $wt(\mathbf{b})$ is odd, then*

$$\sum_{\mathbf{y} \in E_{\mathbf{b}}^0 \cap \delta_\pi(\mathbf{b}, \mathbf{1})} (-1)^{D_{\mathbf{b}} h(\mathbf{y})} = \sum_{\mathbf{y} \in E_{\mathbf{b}}^1 \cap \delta_\pi(\mathbf{b}, \mathbf{1})} (-1)^{D_{\mathbf{b}} h(\mathbf{y})}.$$

2. *If $wt(\mathbf{a}, \mathbf{b})$ is even, then*

$$\sum_{\mathbf{y} \in E_{\mathbf{b}}^0 \cap \delta_\pi(\mathbf{b}, \mathbf{a})} (-1)^{\mathbf{a} \cdot \pi(\mathbf{y}) \oplus D_{\mathbf{b}} h(\mathbf{y})} = \sum_{\mathbf{y} \in E_{\mathbf{b}}^1 \cap \delta_\pi(\mathbf{b}, \mathbf{a})} (-1)^{\mathbf{a} \cdot \pi(\mathbf{y}) \oplus D_{\mathbf{b}} h(\mathbf{y})}.$$

3. *If $wt(\mathbf{a}, \mathbf{b})$ is odd, then*

$$\sum_{\mathbf{y} \in E_{\mathbf{b}}^0 \cap \delta_\pi(\mathbf{b}, \bar{\mathbf{a}})} (-1)^{\mathbf{a} \cdot \pi(\mathbf{y}) \oplus D_{\mathbf{b}} h(\mathbf{y})} = \sum_{\mathbf{y} \in E_{\mathbf{b}}^1 \cap \delta_\pi(\mathbf{b}, \bar{\mathbf{a}})} (-1)^{\mathbf{a} \cdot \pi(\mathbf{y}) \oplus D_{\mathbf{b}} h(\mathbf{y})}.$$

4.1 Existence of bent-negabent functions in $\mathcal{M}$ class

By the previous analysis, it is possible to construct bent-negabent functions in $\mathcal{M}$ when the permutations are either complete mapping polynomials or satisfy the weight-sum-invariant property. For example, let $n = 4t \geq 12$ and $1 \leq i < t$ be an integer such that $\gcd(2^i + 1, 2^t - 1) = 1$. Then $(y', y'') \longmapsto (y'', y' + y''^{2^i+1})$ is a complete mapping permutation, and the Boolean function $\mathrm{Tr}_1^t(x'y'' + x''y' + x''y''^{2^i+1})$ is bent-negabent in $\mathcal{M}$, where $x', x'', y', y'' \in \mathbb{F}_{2^t}$.

Is there a bent-negabent function in $\mathcal{M}$ such that the corresponding permutation is not a complete mapping or does not satisfy the weight-sum-invariant property? We identify two bent-negabent functions in 6 variables in Maiorana–McFarland class where one permutation is a complete mapping but not weight-sum-invariant, and other one is not complete mapping and not weight-sum-invariant. We define the corresponding permutations and the functions h.

- Let $\pi(y_1, y_2, y_3) = (y_1 \oplus y_3, y_1, y_2)$ and $h(y_1, y_2, y_3) = (y_1 \oplus y_2)y_3$. It is clear that π is a complete mapping polynomial but not weight-sum-invariant. The function $x_1(y_1 \oplus y_3) \oplus x_2 y_1 \oplus x_3 y_2 \oplus (y_1 \oplus y_2)y_3$ is bent-negabent. So, the function is not obtained via [20, Theorem 6].

- Let $\pi(y_1, y_2, y_3) = (y_1 \oplus y_3, y_2, y_1)$ and $h(y_1, y_2, y_3) = (y_1 \oplus y_2)y_3$. It is clear that π is not a complete mapping polynomial and not weight-sum-invariant. The function $x_1(y_1 \oplus y_3) \oplus x_2y_2 \oplus x_3y_1 \oplus (y_1 \oplus y_2)y_3$ is bent-negabent. Thus, the function is not obtained via [20, Theorem 6] or [22, Theorem 17].

Also, it is clear that the second function is not used in [22, Theorem 22] and [25, Theorem 5] to construct a new bent-negabent function as the permutation $\pi(y_1, y_2, y_3) = (y_1 \oplus y_3, y_2, y_1)$ is not a complete mapping permutation. However, the second function may or may not be constructed using [25, Theorem 5]. We display in Figure 2 a Venn diagram of existing constructions in the $\mathcal{M}$ class.

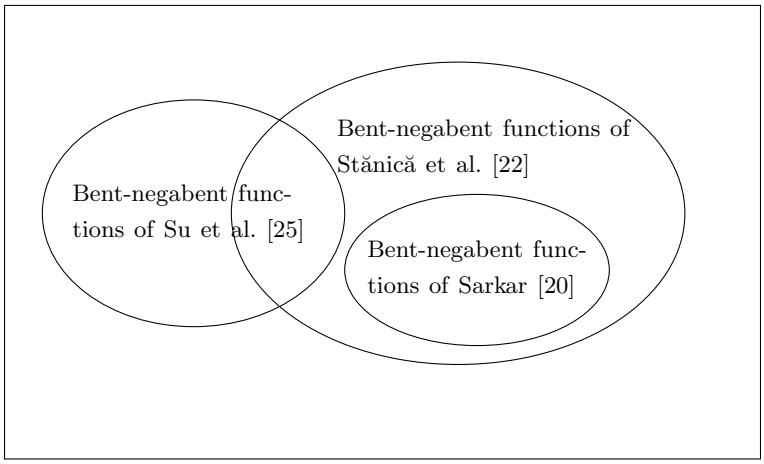

Figure 2: The set of bent-negabent functions in Maiorana–McFarland class

4.2 Non-existence of bent-negabent functions in $\mathcal{M}$ class

We also can infer the non-existence of bent-negabent functions $f \in \mathcal{B}_n$ defined as in (2) from Theorem 4.

Corollary 6. *Let $f \in \mathcal{B}_n$ be defined as in (2) with $h = 0$ and let π be a permutation over $\mathbb{F}_2^m$ such that there exists $\mathbf{b} \in \mathbb{F}_2^m$ with odd $wt(\mathbf{b})$, $|\delta_\pi(\mathbf{b}, \mathbf{1})| = 2$, where $\delta_\pi(\mathbf{b}, \mathbf{1})$ is defined as in (3). Then f is not a bent-negabent function.*

Proof. Let $\mathbf{y}_0, \mathbf{y}_0 \oplus \mathbf{b} \in \delta_\pi(\mathbf{b}, \mathbf{1})$. Since $\bar{\mathbf{b}} \cdot (\mathbf{y}_0 \oplus \mathbf{b}) = \bar{\mathbf{b}} \cdot \mathbf{y}_0 \oplus \bar{\mathbf{b}} \cdot \mathbf{b} = \bar{\mathbf{b}} \cdot \mathbf{y}_0$, then $\mathbf{y}_0 \in E_{\bar{\mathbf{b}}}^0$ (or $E_{\bar{\mathbf{b}}}^1$) if and only if $\mathbf{y}_0 \oplus \mathbf{b} \in E_{\bar{\mathbf{b}}}^0$ (or $E_{\bar{\mathbf{b}}}^1$, respectively). From Theorem 4, we infer that f is not a bent-negabent function. □

For example, let $m = 4$ and π be the GIFT Sbox [1] defined as in Table 1. It is known that $|\delta_\pi(0001, 1111)| = 2$, where $1 = 0001$ and $f = 15 = 1111$. Thus, the Maiorana–McFarland bent function corresponding to GIFT Sbox is not bent-negabent.

From [20, Theorem 5] and using the permutation π over $\mathbb{F}_2^4$ used in the GIFT Sbox, we have

$$\sum_{\mathbf{y} \in \delta_\pi(\mathbf{b}, \mathbf{1})} (-1)^{\mathbf{1} \cdot \pi(\mathbf{y}) \oplus \mathbf{b} \cdot \mathbf{y}} = (-1)^{\mathbf{1} \cdot \pi(\mathbf{y}_0) \oplus \mathbf{b} \cdot \mathbf{y}_0} + (-1)^{\mathbf{1} \cdot \pi(\mathbf{y}_0 \oplus \mathbf{b}) \oplus \mathbf{b} \cdot (\mathbf{y}_0 \oplus \mathbf{b})} = 0$$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\pi(\mathbf{x})$	1	a	4	c	6	f	3	9	2	d	b	7	5	0	8	e

Table 1: GIFT Sbox in hexadecimal notation

if and only if $wt(\mathbf{b})$ is odd. Further, if $wt(\mathbf{b})$ is odd, by using Theorem 4, we conclude that the corresponding function is not bent-negabent.

Let $n = 6$ and $f \in \mathcal{B}_6$ be defined as in (2), where $\pi(y_3, y_2, y_1) = (y_1y_3 \oplus y_2 \oplus y_3, y_2y_3 \oplus y_2 \oplus y_1, y_1y_2 \oplus y_1 \oplus y_3)$, for all $(y_3, y_2, y_1) \in \mathbb{F}_2^3$ and $h = 0$. It is clear that π is not a complete mapping since $(\pi \oplus I_3)(000) = (\pi \oplus I_3)(111)$, where I_3 is an identity mapping over $\mathbb{F}_2^3$ (we customarily write an element $(y_3, y_2, y_1) \in \mathbb{F}_2^3$ as $y_3y_2y_1$). Moreover, $\delta_\pi(001, 111) = \{100, 101\} \subset E_{110}^1 = E_{\overline{001}}^1$. Thus, f is not a bent-negabent function.

In [27], Zhang et al. constructed a class of bent-negabent functions outside the complete Maiorana–McFarland class, by using the concept of indirect sums, which had been proposed by Carlet [4]. Here, we look at the behavior of the derivative of a particular type of Maiorana–McFarland bent functions, and then prove the non-existence of bent-negabent functions defined as in (4), below. These are as in [12, Lemma 23], where Mesnager constructed a set of self dual quadratic bent functions.

Lemma 7. [12] *Let $k \geq 2$, $\lambda \in \mathbb{F}_{2^{4k}} \setminus \{0\}$, with $\lambda \oplus \lambda^{2^{3k}} = 1$, or $\lambda^{(2^k+1)^2(2^k-1)} = 1$. Then*

$$f(x) = \mathrm{Tr}_1^{4k}(\lambda x^{2^k+1}), \tag{4}$$

for all $x \in \mathbb{F}_{2^{4k}}$, is a self dual bent function.

It is not difficult to show that the bent function f defined as in (4) is not negabent. In the next theorem, we consider a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

Theorem 8. *The function f defined as in* (4) *is not bent-negabent.*

Proof. Let $a \in \mathbb{F}_{2^k}$ and $wt(a)$ be even, i.e., $\mathrm{Tr}_1^{4k}(a) = 0$. Then $a^{2^k-1} = 1$ and

$$\begin{aligned} f(x) \oplus f(x \oplus a) &= \mathrm{Tr}_1^{4k}(\lambda(x^{2^k+1} \oplus (x \oplus a)^{2^k+1})) \\ &= \mathrm{Tr}_1^{4k}(\lambda(x^{2^k}a \oplus xa^{2^k})) \oplus \mathrm{Tr}_1^{4k}(\lambda a^{2^k+1}) \\ &= \mathrm{Tr}_1^{4k}((\lambda^{2^{3k}}a \oplus \lambda a)x) \oplus \mathrm{Tr}_1^{4k}(\lambda a^2) = \mathrm{Tr}_1^{4k}(ax) \oplus \mathrm{Tr}_1^{4k}(\lambda a^2). \end{aligned}$$

Thus,

$$\sum_{x \in \mathbb{F}_{2^{4k}} : \mathrm{Tr}_1^{4k}(ax)=0} (-1)^{f(x)\oplus f(x\oplus a)} = (-1)^{\mathrm{Tr}_1^{4k}(\lambda a^2)} \sum_{x \in \mathbb{F}_{2^{4k}} : \mathrm{Tr}_1^{4k}(ax)=0} (-1)^{\mathrm{Tr}_1^{4k}(ax)} \neq 0. \tag{5}$$

From [11, Theorem 10], we infer that f is not bent-negabent. □

5 Non-existence of rotation symmetric bent-negabent functions

In this section, we discuss a special class of Boolean functions, called rotation symmetric Boolean functions. First, we give some basic definitions and results on orbits counts, which will be used

later. Let $E_O = \{\mathbf{x} \in \mathbb{F}_2^n : wt(\mathbf{x}) \text{ is odd}\}$, $E_E = \{\mathbf{x} \in \mathbb{F}_2^n : wt(\mathbf{x}) \text{ is even}\}$ and $E_i = \{\mathbf{x} \in \mathbb{F}_2^n : wt(\mathbf{x}) = i\}$, $i \in \{0, 1, \ldots, n\}$. Here, $E_O = E_{\mathbf{1}}^1$ and $E_E = E_{\mathbf{1}}^0$. Let the set $\{1, 2, \ldots, n\}$ be denoted by $[1, n]$ for any positive integer $n \geq 2$. We define (identify $x_0 := x_n$)

$$\rho_n^k(x_j) = x_{(j+k) \bmod n} = \begin{cases} x_{j+k}, & \text{if } j+k \leq n; \\ x_{j+k-n}, & \text{if } j+k > n, \end{cases}$$

where $x_j \in \mathbb{F}_2$ for $j \in \{1, 2, \ldots, n\}$. Let $O_n = \{\rho_n^1, \rho_n^2, \ldots, \rho_n^n\}$ be the permutation (cyclic) group, which extends the previous definition to n-tuples,

$$\rho_n^i(\mathbf{x}) = \rho_n^i(x_1, x_2, \ldots, x_n) = (x_{(1+i) \bmod n}, x_{(2+i) \bmod n}, \ldots, x_{(n+i) \bmod n}). \tag{6}$$

An n-variable Boolean function f is said to be *rotation symmetric* (RotS) if and only if for any $\mathbf{x} \in \mathbb{F}_2^n$,

$$f(\rho_n^k(\mathbf{x})) = f(\mathbf{x}), \text{ for all } k \in [1, n].$$

Let

$$Orb(\mathbf{x}) = \{\rho_n^k(\mathbf{x}) : k \in [1, n]\}$$

be the orbit of $\mathbf{x} \in \mathbb{F}_2^n$ under the action of ρ_n^k, $k \in [1, n]$. Using Burnside's Lemma, Stănică and Maitra [23] counted the total number of orbits, showing that the number of orbits induced by the action of O_n on $\mathbb{F}_2^n$, as described in (6), is

$$g_n = \frac{1}{n} \sum_{t|n} \phi(t) 2^{\frac{n}{t}},$$

where ϕ is Euler's phi-function. Let $g_{n,k}$ be the total number of orbits of an n-bit binary strings of weight k and $g_{n,k}^l$ be the total number of orbits of n-bit binary strings of weight k such that $|Orb(\mathbf{x})| = n$. Here, the superscript l of $g_{n,k}^l$ stands for long length (or full length n) orbits. In the same paper, Stănică and Maitra [23, Theorem 9] showed ($k_1 | k$ means that k_1 divides k):

1. $g_{n,k} = \frac{1}{n}\binom{n}{k}$, if $\gcd(k, n) = 1$. Also $g_{n,0} = g_{n,n} = 1$.

2. $g_{n,k} = \frac{1}{n}\left(\binom{n}{k} - \sum_{k_1 | \gcd(n,k);\ k_1 \neq 1} (n/k_1) g_{n/k_1, k/k_1}^l\right) + \sum_{k_1 | \gcd(n,k);\ k_1 \neq 1} g_{n/k_1, k/k_1}^l$, if $k < n$.

Let $\{R_E, R_O\}$ be a partition of $\{1, 2, \ldots, g_n\}$ such that if $i \in R_E$ then $wt(\wedge_i)$ is even and if $j \in R_O$ then $wt(\wedge_j)$ is odd ($\wedge_i$ is a representative of the i-th orbit $Orb(\wedge_i)$ in some random but fixed ordering of all orbits).

Using [11, Theorem 5 and Corollary 8], Mandal et al. proved the following theorem.

Theorem 9. [11, Theorem 10] *There is no rotation symmetric bent-negabent function in $2p^k$ variables, where p is an odd prime and k is any positive integer*

In this direction, we discuss further results related to non-existence of various classes of rotation symmetric bent-negabent functions by using the necessary and sufficient condition given in [11, Theorem 5]. These are additional results over what had been discussed in [11]. Here, we mainly focus on counting the orbits of certain types to show the non-existence of. One important result here is to show non-existence of rotation symmetric bent-negabent function in $4p^k$ variables, where p is an odd prime and k is any positive integer.

5.1 The case of $n = 2^k$, where k is a positive integer

Let $f \in \mathcal{B}_n$, and $1 \leq i \leq n-1$, be an odd integer. Then $\gcd(i, n) = 1$ and all the orbits are of length n and odd weight. Thus,

$$\sum_{j \in R_O} (-1)^{f(\wedge_j) \oplus f(\wedge_j \oplus \mathbf{1})} |Orb(\wedge_j)| = 2^{k+1} t_{2^k},$$

where t_{2^k} is equal to the sum of $(-1)^{f(\wedge_r) \oplus f(\wedge_r \oplus \mathbf{1})}$ with $|Orb(\wedge_r)| = 2^k$ and the weight of $\wedge_r$ is less than or equal to $2^{k-1} - 1$. From [11, Corollary 8], we know that if $f \in \mathcal{B}_{2^k}$ is a RotS bent-negabent function then

$$2^{k+1} t_{2^k} = 0 \quad \Leftrightarrow \quad t_{2^k} = 0, \tag{7}$$

where t_{2^k} is defined as above. The number of odd weight orbits with weight less than or equal to $2^{k-1} - 1$ is

$$2^{-k} \left(\binom{2^k}{1} + \binom{2^k}{3} + \cdots + \binom{2^k}{2^{k-1} - 1} \right).$$

If $k = 2$ then $g_{1,4} = 1$, and so, the left hand side of (7) in this case is nonzero, which is a contradiction. Consequently, there is no rotation symmetric bent-negabent function in 4 variables.

5.2 The case of $n = 2m$, where m is an even integer, not a power of 2

Let $n = 2^{e_1+1} p_2^{e_2} \dots p_k^{e_k}$, with $p_1 = 2$, and $1 \leq i \leq n-1$ be an odd integer, $e_1 \geq 1$. Then $\gcd(i, n) = p_2^{r_2} \dots p_k^{r_k}$, where $0 \leq r_i \leq e_i$, $2 \leq i \leq k$, and all possible lengths of the orbits in E_i (i is odd) are of the form $2^{e_1+1} p_2^{r_2} \dots p_k^{r_k}$, where $0 \leq r_s \leq e_s$, $2 \leq s \leq k$. Thus,

$$\sum_{j \in R_O} (-1)^{f(\wedge_j) \oplus f(\wedge_j \oplus \mathbf{1})} |Orb(\wedge_j)| = 2^{e_1+2} \sum_{r_2=0}^{e_2} \dots \sum_{r_k=0}^{e_k} p_2^{r_2} \dots p_k^{r_k} t_{2 p_1^{e_1} p_2^{r_2} \dots p_k^{r_k}}, \tag{8}$$

where t_r is an integer equal to the sum of $(-1)^{f(\wedge_r) \oplus f(\wedge_r \oplus \mathbf{1})}$ with $|Orb(\wedge_r)| = r$ and $wt(\wedge_r) \leq 2^{n-1} - 1$, $r \in \{2^{e_1+1} p_2^{r_2} \dots p_k^{r_k} : 0 \leq r_s \leq e_s, 2 \leq s \leq k\}$. Thus, we get the next theorem.

Theorem 10. *Let $n = 2^{e'_1} p_2^{e_2} \dots p_k^{e_k}$ be the prime decomposition of n with $e'_1 \geq 2$. If*

$$\sum_{\substack{0 \leq r_i \leq e_i \\ 2 \leq i \leq k}} p_2^{r_2} \dots p_k^{r_k} t_{2^{e'_1} p_2^{r_2} \dots p_k^{r_k}} \neq 0$$

for a rotation symmetric function $f \in \mathcal{B}_n$, then f is not bent-negabent.

5.2.1 The case of $n = 4p^k$, where p is an odd primes and k is a positive integer

Let us consider $e_1 = 1$, $e_2 = k$ and $e_i = 0$, $3 \leq i \leq k$, and $p_2 = p$ be an odd prime. Then we get the following corollary.

Corollary 11. *There is no rotation symmetric bent-negabent function in $4p^k$ variables, where p is an odd prime and k is a positive integer.*

Proof. Let $n = 4p^k$ where p is an odd prime and k is any positive integer, and i, $1 \leq i \leq n-1$, be an odd integer. Then

$$\gcd(i,n) = \begin{cases} 1, & \text{if } i \not\equiv 0 \pmod{p}; \\ p^r, & \text{if } i \equiv 0 \pmod{p^r} \text{ but } i \not\equiv 0 \pmod{p^{r+1}}, 1 \leq r \leq k-1; \\ p^k, & \text{if } i \equiv 0 \pmod{p^k}. \end{cases}$$

Notice that if $\gcd(i,n) = p^k$, where $1 \leq i \leq n-1$ is an odd integer, then i is equal to either p^k or $3p^k$ and $g^l_{4,1} = 1 = g^l_{4,3}$. Thus, the possible lengths of an odd weight orbit are of the form $4p^{k-j}$, where $0 \leq j \leq k$. There is exactly one orbit of length 4 in E_{p^k} and exactly one orbit of length 4 in E_{3p^k}, and they are the complement of each other. We know that if $f \in \mathcal{B}_n$ is a rotation symmetric bent-negabent, then

$$\sum_{j \in R_O} (-1)^{f(\wedge_j) \oplus f(\wedge_j \oplus \mathbf{1})} |Orb(\wedge_j)| = 0.$$

From (8) we get

$$\sum_{j \in R_O} (-1)^{f(\wedge_j) \oplus f(\wedge_j \oplus \mathbf{1})} |Orb(\wedge_j)| = 8 \sum_{t=0}^{k-1} p^{k-t} t_{4p^{k-t}} + 8t_4,$$

where $t_{4p^{k-t}}$ is an integer such that $t_{4p^{k-t}}$ is equal to the sum of $(-1)^{f(\wedge_r) \oplus f(\wedge_r \oplus \mathbf{1})}$ with $|Orb(\wedge_r)| = 4p^{k-t}$, $0 \leq t \leq k-1$, $wt(\wedge_r) \leq 2p^k - 1$, and $t_4 = (-1)^{f(\wedge) \oplus f(\wedge \oplus \mathbf{1})}$ with $|Orb(\wedge)| = 4$. Note that

$$8 \sum_{t=0}^{k-1} p^{k-t} t_{4p^{k-t}} + 8t_4 = 8 \left(p \sum_{t=0}^{k-1} p^{k-1-t} t_{4p^{k-t}} + t_4 \right) \neq 0,$$

and so, we get the result. □

5.2.2 The case of $n = 2^k p$, where p is an odd primes and $k \geq 3$ is any positive integer

Let us consider $e_1 = k-1 \geq 2$, $e_2 = 1$ and $e_i = 0$, $3 \leq i \leq k$, and $p_2 = p$ be an odd prime. Then we get the following corollary.

Corollary 12. *Let $n = 2^k p$, where p is an odd prime and $k \geq 3$ is any positive integer. If $f \in \mathcal{B}_n$ is a rotation symmetric bent-negabent function, then*

$$\sum_{j \in R_{O_{2^k}}} (-1)^{f(\wedge_j) \oplus f(\wedge_j \oplus \mathbf{1})} \equiv 0 \pmod{p},$$

where $R_{O_{2^k}} \subset R_O$, and $j \in R_{O_{2^k}}$ means that $|Orb(\wedge_j)| = 2^k$ and $wt(\wedge_j) \leq 2^{k-1}p - 1$.

Proof. Let $n = 2^k p$, where p is an odd prime and $k \geq 3$ is a positive integer, and let $1 \leq i \leq n-1$ be an odd integer. Then

$$\gcd(i,n) = \begin{cases} 1, & \text{if } i \not\equiv 0 \pmod{p}; \\ p, & \text{if } i \equiv 0 \pmod{p}. \end{cases}$$

Here $\gcd(2^k, i/p) = 1$ and the possible length of an odd weight orbit is either $2^k p$ or 2^k. We know that if $f \in \mathcal{B}_n$ is a rotation symmetric bent-negabent, then

$$\sum_{j \in R_O} (-1)^{f(\wedge_j) \oplus f(\wedge_j \oplus \mathbf{1})} |Orb(\wedge_j)| = 0.$$

From (8) we get

$$\sum_{j \in R_O} (-1)^{f(\wedge_j) \oplus f(\wedge_j \oplus \mathbf{1})} |Orb(\wedge_j)| = 2^{k+1} p t_{2^k p} + 2^{k+1} t_{2^k},$$

where $t_{2^k p}$ is an integer such that $t_{2^k p}$ is equal to the sum of $(-1)^{f(\wedge_r) \oplus f(\wedge_r \oplus \mathbf{1})}$ with $|Orb(\wedge_r)| = 2^k p$ and t_{2^k} is equal to the sum of $(-1)^{f(\wedge_l) \oplus f(\wedge_l \oplus \mathbf{1})}$ with $|Orb(\wedge_l)| = 2^k$, and the weights of $\wedge_r$ and $\wedge_l$ are less than or equal to $2^{k-1} p - 1$. Thus, if f is bent-negabent then

$$2^{k+1} p t_{2^k p} + 2^{k+1} t_{2^k} = 0 \Longrightarrow p t_{2^k p} + t_{2^k} = 0 \Longrightarrow t_{2^k} \equiv 0 \pmod{p},$$

and the claim is shown. □

5.3 The case of $n = 2m$, where m is an odd integer

Let $f \in \mathcal{B}_n$, and $n = 2m = 2p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, m odd, be the prime power decomposition of $2m$, and $1 \le i \le n-1$ be an odd integer. Then $\gcd(i, n) = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, where $0 \le r_i \le e_i$, $1 \le i \le k$. Thus, all possible lengths of the orbits in E_i, i is odd, are some of the even divisors $2p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ (where $0 \le r_i \le e_i$, $1 \le i \le k$) of n. Since $\gcd(p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}, n) = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, the possible lengths of the orbits in $E_{p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}}$ are all the even divisors $2p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ (where $0 \le r_i \le e_i$, $1 \le i \le k$) of n. There is a single orbit of length 2 in $E_{p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}}$, which contains the concatenation of $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ copies of the block 01 (or 10) such that $(0,1,0,1,\dots,0,1) \oplus (1,1,1,1,\dots,1,1) = (1,0,1,0,\dots,1,0) \in Orb(0,1,0,1,\dots,0,1)$. Thus,

$$\sum_{j \in R_O} (-1)^{f(\wedge_j) \oplus f(\wedge_j \oplus \mathbf{1})} |Orb(\wedge_j)| = 2 \sum_{r_1=0}^{e_1} \sum_{r_2=0}^{e_2} \cdots \sum_{r_k=0}^{e_k} p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} t_{2p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}}, \tag{9}$$

where t_r is an integer equal to the sum of $(-1)^{f(\wedge_r) \oplus f(\wedge_r \oplus \mathbf{1})}$ with $|Orb(\wedge_r)| = r$, $r \in \{2p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} : 0 \le r_s \le e_s, s = 1, 2, \dots, k\}$ and $t_2 = 1$. Thus, we have the next result.

Theorem 13. *Let m be an odd integer and $n = 2m = 2p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ be its prime power decomposition, and let $f \in \mathcal{B}_n$ be a rotation symmetric Boolean function. If*

$$\sum_{\substack{0 \le r_i \le e_i \\ 1 \le i \le k}} p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} t_{2p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}} \neq 0,$$

then f is not bent-negabent.

Let $n = 2pq$, where p and q are distinct odd primes (thus, $e_1 = e_2 = 1$ and $e_i = 0$, $3 \le i \le k$, and $p_1 = p, p_2 = q$). Then, all possible lengths of the orbits in E_i (i is odd) are $n, 2p, 2q$ and 2. There is a single orbit of length 2 in E_{pq} and contains the concatenation of pq copies of

the block 01 (or 10) such that $(0,1,0,1,\ldots,0,1) \oplus (1,1,1,1,\ldots,1,1) = (1,0,1,0,\ldots,1,0) \in Orb(0,1,0,1,\ldots,0,1)$. From (9) we get

$$\sum_{j \in R_O} (-1)^{f(\wedge_j) \oplus f(\wedge_j \oplus \mathbf{1})} |Orb(\wedge_j)| = 2pqt_{2pq} + 2pt_{2p} + 2qt_{2q} + 2,$$

where t_r is an integer such that t_r is equal to the sum of $(-1)^{f(\wedge_r) \oplus f(\wedge_r \oplus \mathbf{1})}$ with $|Orb(\wedge_r)| = r$, $r \in \{2pq, 2p, 2q\}$. Thus, we get the next corollary.

Corollary 14. *Let $n = 2pq$ where p and q are distinct odd primes and $f \in \mathcal{B}_n$ be a rotation symmetric Boolean function. If $pqt_{2pq} + pt_{2p} + qt_{2q} + 1 \neq 0$, then f is not bent-negabent.*

Thus, using [11, Theorem 10] and Corollary 11 we infer that there is no rotation symmetric bent-negabent function in n variables $n \leq 100$ except for $16, 24, 30, 32, 40, 42, 48, 56, 64, 66, 70, 78, 80, 88, 96$. For these exceptions, the necessary condition for which a rotation symmetric Boolean function is bent-negabent is given in Table 2. We now summarize the necessary condition for which a rotation symmetric Boolean function in $n \in \{24, 30, 40, 42, 48, 56, 66, 70, 78, 80, 88, 96\}$ variables is bent-negabent. Here $t_i = \sum_{\wedge_r, |Orb(\wedge_r)|=i} (-1)^{f(\wedge_r) \oplus f(\wedge_r \oplus \mathbf{1})}$, as already defined.

n	**Corollary**	**Condition**
$24 = 2^3 \times 3$	4	$3t_{24} + t_8 = 0$
$40 = 2^3 \times 5$	4	$5t_{40} + t_8 = 0$
$56 = 2^3 \times 7$	4	$7t_{56} + t_8 = 0$
$88 = 2^3 \times 11$	4	$11t_{88} + t_8 = 0$
$48 = 2^4 \times 3$	4	$3t_{48} + t_{16} = 0$
$80 = 2^4 \times 5$	4	$5t_{80} + t_{16} = 0$
$96 = 2^5 \times 3$	4	$3t_{96} + t_{32} = 0$
$30 = 2 \times 3 \times 5$	2	$30t_{30} + 10t_{10} + 6t_6 + 2 = 0$
$66 = 2 \times 3 \times 11$	2	$66t_{66} + 22t_{22} + 6t_6 + 2 = 0$
$78 = 2 \times 3 \times 13$	2	$78t_{78} + 26t_{26} + 6t_6 + 2 = 0$
$70 = 2 \times 5 \times 7$	2	$70t_{70} + 14t_{14} + 10t_{10} + 2 = 0$

Table 2: Some necessary conditions for existence of rotation symmetric bent-negabent functions.

5.4 Non-existence of bent-negabent functions via rotation symmetry

Let p be an odd prime and let k be a positive integer. Mandal et al. [11, Theorem 10] showed that there is no rotation symmetric bent-negabent function in $2p^k$ variables. In Corollary 11, we proved that there is no rotation symmetric bent-negabent function in $4p^k$ variables. In Theorem 17 we identify a class of Boolean functions in $2p^k$ or $4p^k$ variables, not necessarily rotation symmetric, which are not bent-negabent. Let $E^0_{\mathbf{a}} = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{a} \cdot \mathbf{x} = 0\}$ be the orthogonal complement of $\mathbf{a} \in \mathbb{F}_2^n \setminus \{0\}$.

Theorem 15. [2, Theorem 3] *Let $f \in \mathcal{B}_n$ be a bent function and $E^0_{\mathbf{a}}$ defined as above. Then, for any $\mathbf{b} \notin E^0_{\mathbf{a}}$,*

$$\sum_{\mathbf{x} \in E^0_{\mathbf{a}}} (-1)^{f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{b})} = \sum_{\mathbf{x} \in \mathbb{F}_2^n \setminus E^0_{\mathbf{a}}} (-1)^{f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{b})} = 0.$$

Let $f \in \mathcal{B}_n$ be a bent-negabent function. Thus, from Theorem 15, for each hyperplane $E^0_{\mathbf{a}}$ and $\mathbf{b} \notin E^0_{\mathbf{a}}$, the derivative $D_{\mathbf{b}} f$ is balanced over $E^0_{\mathbf{a}}$, as well as over $\mathbb{F}_2^n \setminus E^0_{\mathbf{a}}$. From [11, Theorem

5], if $wt(\mathbf{b})$ is even, then $D_{\mathbf{b}}f$ is balanced over $E_{\mathbf{b}}^0$ and also $\mathbb{F}_2^n \setminus E_{\mathbf{b}}^0$ (notice that $\mathbf{b} \in E_{\mathbf{b}}^0$), and if $wt(\mathbf{b})$ is odd, then $D_{\mathbf{b}}f$ is balanced over $E_{\mathbf{b}}^0$, as well as over $\mathbb{F}_2^n \setminus E_{\mathbf{b}}^0$ (notice that $\mathbf{b} \in E_{\mathbf{b}}^0$).

Lemma 16. *For any nonzero $\mathbf{a} \in \mathbb{F}_2^n$, and $\varepsilon \in \{0,1\}$, let $E_{\mathbf{a}}^{\varepsilon} = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{a} \cdot \mathbf{x} = \varepsilon\}$. Then $\mathbf{x} \in E_{\mathbf{a}}^{\varepsilon}$ if and only if $\mathbf{x} \oplus \mathbf{a} \in E_{\mathbf{a}}^{\varepsilon}$ if $wt(\mathbf{a})$ is even, and when $wt(\mathbf{a})$ is odd, $\mathbf{x} \oplus \bar{\mathbf{a}} \in E_{\mathbf{a}}^{\varepsilon}$.*

Proof. Let $\mathbf{a}$ be a nonzero element of $\mathbb{F}_2^n$ such that $wt(\mathbf{a})$ is even. Then $\mathbf{a} \cdot \mathbf{a} \equiv wt(\mathbf{a}) \equiv 0 \pmod 2$, and so, $(\mathbf{x} \oplus \mathbf{a}) \cdot \mathbf{a} = \mathbf{x} \cdot \mathbf{a}$. If $wt(\mathbf{a})$ is odd, then $\bar{\mathbf{a}} \cdot \mathbf{a} = \mathbf{a} \cdot \mathbf{a} \oplus \mathbf{1} \cdot \mathbf{a} \equiv 2wt(\mathbf{a}) \equiv 0 \pmod 2$, and so, $(\mathbf{x} \oplus \bar{\mathbf{a}}) \cdot \mathbf{a} = \mathbf{x} \cdot \mathbf{a}$, and the claim is shown. □

Theorem 17. *Let $n = 2p^k$ or $4p^k$, where p is an odd prime and k is a positive integer, and let $f \in \mathcal{B}_n$ be a rotation symmetric Boolean function. Let $g(\mathbf{x}) = f(\mathbf{x}A)$, where $A \in GL(n, \mathbb{F}_2)$. Then:*

(i) If A maps odd weight elements to odd weight elements, and $\mathbf{1}A = \mathbf{1}$, then g is not a bent-negabent function.

(ii) Let $E_O' = \{\mathbf{x}A^{-1} : \mathbf{x} \in E_O\}$, $\mathbf{c} = \mathbf{1}A^{-1} \in \mathbb{F}_2^n$. If A maps a hyperplane to another hyperplane with $\mathbf{c} \notin \mathbb{F}_2^n \setminus E_O'$, then g is not a bent-negabent function.

Proof. Since $A \in GL(n, \mathbb{F}_2)$ maps odd weight elements to odd weight elements, if $\mathbf{x} \in E_O$ then $\mathbf{x}A^{-1} \in E_O$. If g is also a rotation symmetric Boolean function, then from [11, Theorem 10] and Corollary 11, g is not bent-negabent. Next, if g is not rotation symmetric, again from [11, Theorem 10] and Corollary 11, we get

$$\begin{aligned} 0 \neq \sum_{j \in R_O} (-1)^{f(\wedge_j) \oplus f(\wedge_j \oplus \mathbf{1})} |Orb(\wedge_j)| &= \sum_{\mathbf{x} \in E_O} (-1)^{f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{1})} \\ = \sum_{\mathbf{x} \in E_O} (-1)^{g(\mathbf{x}A^{-1}) \oplus g(\mathbf{x}A^{-1} \oplus \mathbf{1})} &= \sum_{\mathbf{x} \in E_O} (-1)^{g(\mathbf{x}) \oplus g(\mathbf{x} \oplus \mathbf{1})}, \end{aligned}$$

so, g is not bent-negabent.

We now show the second claim. From [11, Theorem 10] and Corollary 11, we get

$$\begin{aligned} 0 \neq \sum_{j \in R_O} (-1)^{f(\wedge_j) \oplus f(\wedge_j \oplus \mathbf{1})} |Orb(\wedge_j)| &= \sum_{\mathbf{x} \in E_O} (-1)^{g(\mathbf{x}A^{-1}) \oplus g(\mathbf{x}A^{-1} \oplus \mathbf{c})} \\ &= \sum_{\mathbf{x} \in E_O'} (-1)^{g(\mathbf{x}) \oplus g(\mathbf{x} \oplus \mathbf{c})}. \end{aligned}$$

From Theorem 15, we get that g is not bent-negabent. □

6 Conclusion

In this paper, we investigate several questions related to bent-negabent functions. First we revisit a few existing claims, point out some errors and fix certain technical issues in this direction. Further, a necessary and sufficient condition is derived for which a Boolean function of the form $\mathbf{x} \cdot \pi(\mathbf{y}) \oplus h(\mathbf{y})$ in the $2m$ variables is bent-negabent. We also prove the non-existence of a particular class of Maiorana–McFarland bent-negabent functions. Next, we study the bent-negabent conditions which are given in [11, Theorem 5] and prove that there is no rotation symmetric bent-negabent function under some conditions.

Acknowledgments. The authors are grateful to the reviewers for their helpful comments and suggestions which have highly improved the manuscript. The work was started during an enjoyable visit of the third-named author to ISI-Kolkata in the Spring of 2019. This author would like to thank the host institution for the excellent working conditions.

References

[1] S. Banik, S. K. Pandey, T. Peyrin, Y. Sasaki, S. Sim, M Siang, Y. Todo, *GIFT: A Small Present Towards Reaching the Limit of Lightweight Encryption*, CHES 2017, LNCS 10529 (2017), 321–345.

[2] A. Canteaut, P. Charpin, *Decomposing bent functions*, IEEE Trans. Inf. Theory 49(8) (2003), 2004–2019.

[3] C. Carlet, *Boolean functions for cryptography and error correcting codes*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge (2010), 257–397.

[4] C. Carlet, *On the secondary constructions of resilient and bent functions*, Coding, Crypt. and Combinatorics 23 (2004), 3–28.

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

[6] T. W. Cusick, P. Stănică, *Cryptographic Boolean Functions and Applications* (Ed. 2), Academic Press, San Diego, CA (2017).

[7] D. K. Dalai, S. Maitra, S. Sarkar, *Results on rotation symmetric bent functions*, Disc. Math. 309(8) (2009), 2398–2409.

[8] J. F. Dillon, *A survey of bent functions*, NSA Technical Journal (Special Issue) (1972).

[9] S. Kavut, S. Maitra, M. D. Yücel, *Search for Boolean functions with excellent profiles in the rotation symmetric class*, IEEE Trans. Inf. Theory 53(5) (2007), 1743–1751.

[10] R. L. McFarland, *A family of noncyclic difference sets*, J. Combinatorial Theory, Ser. A 15 (1973), 1–10.

[11] B. Mandal, B. Singh, S. Gangopadhyay, S. Maitra, V. Vetrivel, *On non-existence of bent-negabent rotation symmetric Boolean functions*, Discr. Appl. Math. 236 (2018), 1–6.

[12] S. Mesnager, *Several new infinite families of bent functions and their duals*, IEEE Trans. Inf. Theory 60(7) (2014), 4397–4407.

[13] S. Mesnager, *Bent Functions–Fundamentals and Results*, Springer, Switzerland, ISBN 978-3-319-32593-4 (2016), 1–544.

[14] M. G. Parker, *The constabent properties of Goley-Devis-Jedwab sequences*, Int. Symp. Information Theory, Sorrento, Italy (2000), http://www.ii.uib.no/ matthew/mattweb.html.

[15] M. G. Parker, A. Pott, *On Boolean functions which are bent and negabent*, In S. W. Golomb, G. Gong, T. Helleseth and H. Y. Song, Sequences, Subsequences, and Consequences, SSC 2007 LNCS 4893 (2007), 9–23.

[16] J. Pieprzyk, C. X. Qu, *Fast hashing and rotation-symmetric functions*, J. Univ. Comp. Sci. 5(1) (1999), 20–31.

[17] O. S. Rothaus, *On bent functions*, J. Combin. Theory – Ser. A 20 (1976), 300–305.

[18] C. Riera and M. G. Parker, *Generalized bent criteria for Boolean functions*, IEEE Trans. Inf. Theory 52(9) (2006), 4142–4159.

[19] K.-U. Schmidt, M. G. Parker, A. Pott, *Negabent functions in Maiorana–McFarland class*, In: SETA (2008) LNCS 5203 (2008), 390–402 (2008)

[20] S. Sarkar, *Characterizing negabent Boolean functions over finite fields*, In Proc. SETA 2012, LNCS 7280 (2012), 77–88.

[21] S. Sarkar, T. W. Cusick, *Initial results on the rotation symmetric bent-negabent functions*, 7th Int. Work. on Signal Design & Appl. in Communic. (IWSDA) (2015), 80–84.

[22] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. Kar Gangopadhyay, S. Maitra, *Investigations on bent and negabent functions via the nega-Hadamard transform*, IEEE Trans. Inf. Theory 58(6) (2012), 4064–4072.

[23] P. Stănică, S. Maitra, *Rotation symmetric Boolean functions – count and cryptographic properties*, Disc. Appl. Math. 156 (2008), 1567–1580.

[24] P. Stănică, B. Mandal, S. Maitra, *The connection between quadratic bent-negabent functions and the Kerdock code*, Applicable Algebra in Engineering, Communication and Computing 30:5 (2019), 387–401.

[25] W. Su, A. Pott, X. Tang, *Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree*, IEEE Trans. Inf. Theory 59(6) (2013), 3387–3395.

[26] T. Xia, J. Seberry, J. Pieprzyk, C. Charnes, *Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$*, Disc. Appl. Math. 142 (1–3) (2004), 127–132.

[27] F. Zhang, Y. Wei, E. Pasalic, *Constructions of Bent-Negabent Functions and Their Relation to the Completed Maiorana–McFarland Class*, IEEE Trans. Inf. Theory 61(3) (2015), 1496–1506.