Journal of Applied Mathematics and Computing
https://doi.org/10.1007/s12190-023-01887-3

ORIGINAL RESEARCH

Stability of the Walsh–Hadamard spectrum of cryptographic Boolean functions with biased inputs

Aditi Kar Gangopadhyay[1] · Vikas Kumar[1] · Pantelimon Stănică[2] · Sugata Gangopadhyay[3]

Received: 2 March 2023 / Revised: 2 March 2023 / Accepted: 7 June 2023

Abstract

We propose a notion of stability of the Walsh–Hadamard spectrum of Boolean functions when inputs are independent and identically distributed Bernoulli random variables. We study the stability spectrum of bent Boolean functions and obtain a bound for it. We also derive the formula for the stability transform of Maiorana–McFarland type bent functions. We analyze the stability spectrum of symmetric Boolean functions and characterize it for symmetric bent Boolean functions and symmetric Boolean functions in an odd number of variables with maximum nonlinearity. We show that the stability spectrum is not, in general, invariant under extended affine transformations. Further, we display some non-bent symmetric Boolean functions whose stability spectra are flatter than that of symmetric bent Boolean functions.

Keywords Boolean function · Bias · Walsh–Hadamard transform (WHT) · Nonlinearity · Bent · Symmetric

Mathematics Subject Classification 05A10 · 11B65 · 33C05 · 06E30 · 94D10

✉ Aditi Kar Gangopadhyay
aditi.gangopadhyay@ma.iitr.ac.in

Vikas Kumar
v_kumar@ma.iitr.ac.in

Pantelimon Stănică
pstanica@nps.edu

Sugata Gangopadhyay
sugata.gangopadhyay@cs.iitr.ac.in

1 Department of Mathematics, IITR, Roorkee, Uttarakhand 247667, India

2 Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93955, USA

3 Department of Computer Science and Engineering, IITR, Roorkee, Uttarakhand 247667, India

Published online: 17 June 2023

1 Introduction

An n-variable Boolean function f is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $\mathbb{F}_2$ is the finite field with two elements and $\mathbb{F}_2^n$ is the cartesian product of n copies of $\mathbb{F}_2$. The set of all such functions is denoted by $\mathfrak{B}_n$. Let $f, g \in \mathfrak{B}_n$ be two such Boolean functions. The Hamming distance between f and g is the count of the number of input vectors for which outputs of f and g differ. The Hamming distance when divided by 2^n, i.e., the cardinality of the domain of f and g, is the probability that f and g return different outputs for an input chosen uniformly at random from their domain. The probability associated with the Hamming distance is the measure of closeness of two Boolean functions f and g when the input vectors are chosen uniformly at random. If this probability is small, the function f is equal to the function g for most of the points in their domain. Furthermore, if g is an affine function, it is said to be an affine approximation of f.

Let $\mu(p_1, \ldots, p_k)$ denote a probability distribution over $\mathbb{F}_2^n$ with parameters $p_1, \ldots, p_k$ such that the input vectors of f and g satisfy this probability distribution. In that case, the probability that their outputs differ, in general, deviates from the Hamming distance between f and g divided by 2^n. This new probability measure that depends on $\mu(p_1, \ldots, p_k)$ indicates how well f can be approximated by g. We consider the particular case where the distribution of the n coordinates of the input vectors are i.i.d. Bernoulli, each with parameter p. Therefore, the input vectors with n coordinates satisfy the binomial distribution with parameters n and p. When value of the parameter $p = 1/2$, input vectors are chosen uniformly at random.

O'Donnell [9] discussed Boolean functions with biased inputs in detail. For cryptographic Boolean functions, Gangopadhyay et al. [5, 6] investigated functions whose inputs satisfy binomial distributions. This paper considers affine approximations of Boolean functions in n variables with inputs following binomial distribution with parameters n and $p = 1/2 + \delta$. We call them Boolean functions with δ-biased (or simply, biased) inputs. If $\delta = 0$, the inputs are distributed uniformly at random. One should observe that if $|\delta| \to \frac{1}{2}$, then the distribution on $\mathbb{F}_2^n$ approaches a constant distribution and the input vector is either zero vector or all one vector. Consequently, the functions defined on $\mathbb{F}_2^n$ behave almost like constant functions, therefore, we consider the values of $|\delta| << \frac{1}{2}$. For such values of $|\delta|$, we demonstrate that the ease of affine approximation varies among different classes of Boolean functions. In this paper, we quantify this idea and study it for Boolean functions.

2 Preliminaries

Let $\mathbb{Z}$ be the ring of integers, $\mathbb{R}$ and $\mathbb{C}$ be the fields of real and complex numbers, respectively. Let us define $[n] = \{i \in \mathbb{Z} : 1 \leq i \leq n\}$. Let $\mathbb{F}_2^n = \{\mathbf{x} = (x_1, \ldots, x_n) : x_i \in \mathbb{F}_2, \text{ for all } i \in [n]\}$. Let $\sum$ and $\oplus$ denote addition over integers and $\mathbb{F}_2$, respectively. The addition and scalar multiplication over $\mathbb{F}_2^n$ is defined coordinatewise, as usual. The intersection of two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ is defined by $\mathbf{x} * \mathbf{y} = (x_1 y_1, \ldots, x_n y_n)$.

The character form of a Boolean function $f \in \mathfrak{B}_n$ is $\chi_f : \mathbb{F}_2^n \to \mathbb{R}$ defined as $\chi_f(\mathbf{x}) = (-1)^{f(\mathbf{x})}$, for all $\mathbf{x} \in \mathbb{F}_2^n$.

The support set of a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ is $\mathrm{supp}(\mathbf{x}) = \{i \in [n] : x_i \neq 0\}$. The (Hamming) weight of the vector $\mathbf{x} \in \mathbb{F}_2^n$ is $\mathrm{wt}(\mathbf{x}) = |\mathrm{supp}(\mathbf{x})|$, and the weight of the function $f \in \mathfrak{B}_n$ is $\mathrm{wt}(f) = |\{\mathbf{x} \in \mathbb{F}_2^n : f(\mathbf{x}) \neq 0\}| = |\mathrm{supp}(f)|$. Alternatively, for $\mathbf{x} \in \mathbb{F}_2^n$, $\mathrm{wt}(\mathbf{x}) = \sum_{i \in [n]} x_i$, and for $f \in \mathfrak{B}_n$, $\mathrm{wt}(f) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} f(\mathbf{x})$. The Hamming distance between two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ is defined by $\mathrm{dist}_H(\mathbf{x}, \mathbf{y}) = |\{i \in [n] : x_i \neq y_i\}| = \mathrm{wt}(\mathbf{x} \oplus \mathbf{y})$. The Hamming distance between two functions $f, g \in \mathfrak{B}_n$ is defined by $\mathrm{dist}_H(f, g) = |\{\mathbf{x} \in \mathbb{F}_2^n : f(\mathbf{x}) \neq g(\mathbf{x})\}|$. We define an inner product on $\mathbb{F}_2^n$ by

$$\mathbf{x} \cdot \mathbf{y} = (x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = \bigoplus_{i \in [n]} x_i y_i.$$

For every $(\mathbf{u}, b) \in \mathbb{F}_2^n \times \mathbb{F}_2$ and $\mathbf{x} \in \mathbb{F}_2^n$, the function

$$\ell_{\mathbf{u},b}(\mathbf{x}) = \mathbf{u} \cdot \mathbf{x} \oplus b$$

is called an affine function. We denote $\ell_{\mathbf{u},0}$ by $\ell_{\mathbf{u}}$. Let $\mathfrak{A}_n$ denote the set of affine functions, and $\mathfrak{L}_n$ denote the set of linear functions.

Symmetric cryptographic primitives employ Boolean functions in abundance. We call such functions *Cryptographic Boolean functions*. The monographs of Carlet [2], and Cusick and Stănică [3] have extensive discussions on the properties of cryptographic Boolean functions. In this paper, we focus on approximations of Boolean functions by affine functions and their stability under biased variables. In what follows, we provide the necessary background needed to study affine approximations of Boolean functions.

2.1 The Walsh–Hadamard transform (WHT)

The Walsh–Hadamard transform of the function $f \in \mathfrak{B}_n$ at $\mathbf{u} \in \mathbb{F}_2^n$ is

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

The inverse Walsh–Hadamard transform is the expansion of character form of the function f as a linear combination of character forms of linear functions, i.e.,

$$\chi_f(\mathbf{x}) = 2^{-n} \sum_{\mathbf{u} \in \mathbb{F}_2^n} W_f(\mathbf{u}) \chi_{\ell_{\mathbf{u}}}(\mathbf{x}). \tag{2}$$

$W_f(\mathbf{u})$ are the Walsh–Hadamard coefficient, and the multiset of all such coefficients is said to be the Walsh–Hadamard spectrum of f. We have the following well-known

result

$$\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{(\mathbf{u}\oplus\mathbf{v})\cdot\mathbf{x}} = \begin{cases} 0 & \text{if } \mathbf{u}\neq\mathbf{v} \\ 2^n & \text{if } \mathbf{u}=\mathbf{v} \end{cases}. \tag{3}$$

Equation (3) has the following equivalent form, in terms of character forms of linear functions, demonstrating that the character forms are orthogonal to each other.

$$\sum_{\mathbf{x}\in\mathbb{F}_2^n}\chi_{\ell_\mathbf{u}}(\mathbf{x})\chi_{\ell_\mathbf{v}}(\mathbf{x}) = \begin{cases} 0 & \text{if } \mathbf{u}\neq\mathbf{v} \\ 2^n & \text{if } \mathbf{u}=\mathbf{v} \end{cases}. \tag{4}$$

One more interesting formula is

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n}\chi_{\ell_\mathbf{u}}(\mathbf{x})\chi_{\ell_\mathbf{u}}(\mathbf{y}) = \begin{cases} 0 & \text{if } \mathbf{x}\neq\mathbf{y} \\ 2^n & \text{if } \mathbf{x}=\mathbf{y} \end{cases}. \tag{5}$$

In general, for any function $g : \mathbb{F}_2^n \to \mathbb{R}$, we have the expansion

$$g(\mathbf{x}) = \sum_{\mathbf{u}\in\mathbb{F}_2^n}\hat{g}(\mathbf{u})\chi_{\ell_\mathbf{u}}(\mathbf{x}) \text{ where } \hat{g}(\mathbf{u}) = 2^{-n}\sum_{\mathbf{x}\in\mathbb{F}_2^n} g(\mathbf{x})\chi_{\ell_\mathbf{u}}(\mathbf{x}), \tag{6}$$

for all $\mathbf{u} \in \mathbb{F}_2^n$. Such an expansion is said to be the Fourier expansion of g and $\hat{g}(\mathbf{u})$ are said to be Fourier coefficients of g. The inversion is achieved by using (4).

2.2 Nonlinearity of a Boolean function

The nonlinearity of a Boolean function $f \in \mathfrak{B}_n$, denoted by $\mathcal{N}_f$, is the distance of f from the set of affine functions $\mathfrak{A}_n$, i.e., it is the minimum of the Hamming distances of f and the affine functions.

$$\mathcal{N}_f = \min\{\text{dist}_H(f, g) : g \in \mathfrak{A}_n\} = \min\{\text{dist}_H(f, \ell_{\mathbf{u},b}) : (\mathbf{u}, b) \in \mathbb{F}_2^n \times \mathbb{F}_2\}.$$

The Hamming distance between two Boolean functions $f, \ell_{\mathbf{u},b} \in \mathfrak{B}_n$ is

$$\text{dist}_H(f, \ell_{\mathbf{u},b}) = 2^{n-1} - \frac{1}{2}(-1)^b W_f(\mathbf{u}).$$

The formula that connects the nonlinearity and Walsh–Hadamard spectrum of f is

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2}\max_{\mathbf{u}\in\mathbb{F}_2^n}|W_f(\mathbf{u})|.$$

The Parseval's identity in this context takes the form

$$\sum_{\mathbf{x}\in\mathbb{F}_2^n} W_f(\mathbf{x})^2 = 2^{2n}.$$

Parseval's identity tells us that the Walsh–Hadamard coefficients of a Boolean function cannot all be zero, in fact, for any function $f \in \mathfrak{B}_n$, $\max_{\mathbf{x}\in\mathbb{F}_2^n} |W_f(\mathbf{x})| \geq 2^{\frac{n}{2}}$, therefore $\mathcal{N}_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.

Definition 1 A function $f \in \mathfrak{B}_n$ is said to be a bent function if $W_f(\mathbf{x}) \in \{-2^{\frac{n}{2}}, 2^{\frac{n}{2}}\}$, for all $\mathbf{x} \in \mathbb{F}_2^n$.

Definition 2 Dual of a bent function $f \in \mathfrak{B}_n$ is a Boolean function in n variables denoted by $\tilde{f}$ and is defined by the relation $W_f(\mathbf{x}) = (-1)^{\tilde{f}(\mathbf{x})} 2^{\frac{n}{2}}$, for all $\mathbf{x} \in \mathbb{F}_2^n$.

The dual of bent function $f \in \mathfrak{B}_n$ is also a bent function that satisfies $\tilde{\tilde{f}} = f$, therefore $W_{\tilde{f}}(\mathbf{x}) = (-1)^{f(\mathbf{x})} 2^{\frac{n}{2}}$ for all $\mathbf{x} \in \mathbb{F}_2^n$. Bent functions exist only in even number of variables, i.e., when the number of variables $n = 2m$. A bent function has the maximum possible nonlinearity $2^{n-1} - 2^{\frac{n}{2}-1}$.

2.3 Walsh–Hadamard transform of Boolean functions with biased inputs

A random variable $\mathbf{X} = (X_1, \ldots, X_n)$, defined on $\mathbb{F}_2^n$, is realized as a sequence of random variables X_i defined on $\mathbb{F}_2$ for each $i \in [n]$. If $\mathbf{X}$ is uniformly distributed over $\mathbb{F}_2^n$ we write $\mathbf{X} \sim \mathbb{F}_2^n$. If $\mu(p_1, \ldots, p_k)$ is a probability distribution with parameters p_i with $i \in [k]$, we write $\mathbf{X} \sim \mu(p_1, \ldots, p_k)$ to denote that $\mathbf{X}$ has the probability distribution $\mu(p_1, \ldots, p_k)$. Let us suppose that we have oracle access to the Boolean functions $f, g \in \mathfrak{B}_n$ and we choose their inputs, $\mathbf{X}$, uniformly at random from $\mathbb{F}_2^n$, i.e., $\mathbf{X} \sim \mathbb{F}_2^n$. Then

$$\Pr_{\mathbf{X}\sim\mathbb{F}_2^n}[f(\mathbf{X}) \neq g(\mathbf{X})] = 2^{-n}\mathrm{dist}_H(f, g). \tag{7}$$

Equation (7) demonstrates the probabilistic interpretation of the Hamming distance. Setting $g = \ell_{\mathbf{u}}$

$$\Pr_{\mathbf{X}\sim\mathbb{F}_2^n}[f(\mathbf{X}) \neq \ell_{\mathbf{u}}(\mathbf{X})] = \frac{1}{2} - \frac{1}{2^{n+1}} W_f(\mathbf{u}). \tag{8}$$

Equation (8) shows that the Walsh–Hadamard coefficient at $\mathbf{u}$ is the bias of the event $\{f(\mathbf{X}) \neq \ell_{\mathbf{u}}(\mathbf{X})\}$ up to a constant factor. Suppose that, for all $i \in [n]$, the random variables X_i's are independent and identically distributed, each having Bernoulli distribution with parameter p (and so, 1 is taken with probability p and 0 with probability $(1-p)$). Their joint distribution is denoted by $\mu(p)$, and the random variable is then $\mathbf{X} \sim \mu(p)$. Therefore, the probability $\Pr[\mathbf{X} = \mathbf{x}] = (1-p)^n \rho^{\mathrm{wt}(\mathbf{x})}$ where $\rho = \frac{p}{1-p}$, for all $\mathbf{x} \in \mathbb{F}_2^n$. Gangopadhyay et al. [5] showed that

$$\Pr_{\mathbf{X}\sim\mu(p)}[f(\mathbf{X}) \neq \ell_{\mathbf{u}}(\mathbf{X})] = \frac{1}{2} - \frac{(1-p)^n}{2} W_f^{(\rho)}(\mathbf{u}) \tag{9}$$

where

$$W_f^{(\rho)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}. \tag{10}$$

We write $W_f^{(\rho)}(\mathbf{u})$ instead of $W_f^{(p)}(\mathbf{u})$ as in [5], for notational convenience.

3 Cryptographic properties of biased functions

Let $f \in \mathfrak{B}_n$ with input $\mathbf{X} \sim \mu(p)$. If $p = \frac{1}{2}$, that is $\rho = 1$, then f is a usual n variable Boolean function having $W_f(\mathbf{u})$ as the Walsh–Hadamard transform at $\mathbf{u} \in \mathbb{F}_2^n$. When p deviates from $\frac{1}{2}$ by a small amount δ, say, $p = \frac{1}{2} + \delta$, then $\rho = \frac{p}{1-p}$ deviates from 1 to $1 + \epsilon$, where $\epsilon = \frac{2\delta}{\frac{1}{2}-\delta}$. Then $W_f^{\rho}(\mathbf{u})$ is

$$\begin{aligned} W_f^{(1+\epsilon)}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \sum_{i=0}^{\mathrm{wt}(\mathbf{x})} \binom{\mathrm{wt}(\mathbf{x})}{i} \epsilon^i (-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}} \\ &\approx \sum_{\mathbf{x}\in\mathbb{F}_2^n} (1 + \mathrm{wt}(\mathbf{x})\epsilon)(-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}}, \text{ for small } \epsilon, \\ &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}} + \epsilon \sum_{\mathbf{x}\in\mathbb{F}_2^n} \mathrm{wt}(\mathbf{x})(-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}}. \end{aligned}$$

Therefore, for small ϵ, we have the following:

$$W_f^{(1+\epsilon)}(\mathbf{u}) - W_f(\mathbf{u}) \approx \epsilon\, \mathcal{S}_f(\mathbf{u}) \tag{11}$$

where the first-order fluctuations of the WHT-values of $f \in \mathfrak{B}_n$ are given by the *stability transform* ($\mathcal{S}$-transform, for short)

$$\mathcal{S}_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \mathrm{wt}(\mathbf{x})(-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}}. \tag{12}$$

We call the multiset of values $[\mathcal{S}_f(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_2^n]$, the *stability spectrum* ($\mathcal{S}$-spectrum, for short). The sum (12) appears in different places in literature such as [3, Lemma 2.11] and [7, Theorem 2]. However, its interpretation as the stability of the WHT spectra of Boolean functions seems to be novel. In what follows, we explore these spectra for special classes of Boolean functions.

The sum

$$\begin{aligned} \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathcal{S}_f(\mathbf{u})^2 &= \sum_{\mathbf{u}\in\mathbb{F}_2^n} \left(\sum_{\mathbf{x}\in\mathbb{F}_2^n} \mathrm{wt}(\mathbf{x})(-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}} \right)^2 \\ &= 2^n \sum_{\mathbf{x}\in\mathbb{F}_2^n} \mathrm{wt}(\mathbf{x})^2 = 2^n \sum_{i=0}^{n} \binom{n}{i} i^2 = 2^{2(n-1)} n(n+1). \end{aligned}$$

Therefore, we obtain a Parseval-like identity (see also [7, Theorem 2]).

Proposition 1 *The $\mathcal{S}$-spectrum of a function $f \in \mathfrak{B}_n$ satisfies*

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathcal{S}_f(\mathbf{u})^2 = 2^{2(n-1)} n(n+1). \tag{13}$$

We will give below another connection between our approach and the Walsh–Hadamard transform of a Boolean function in a restricted domain $E_{n,k} = \{\mathbf{x} \in \mathbb{F}_2^n : \mathrm{wt}(\mathbf{x}) = k\}$, $0 \le k \le n$ (see [7] and the references therein), which was useful in analyzing the FLIP [4] family of ciphers. Precisely, the (unnormalized) restricted transform was defined (we slightly change the notation so it does not clash with ours) as

$$W_{f,k}(\mathbf{u}) = \sum_{\mathbf{x}\in E_{n,k}} (-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}}.$$

Thus,

$$\begin{aligned} W_f^{(1+\epsilon)}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \sum_{i=0}^{\mathrm{wt}(\mathbf{x})} \binom{\mathrm{wt}(\mathbf{x})}{i} \epsilon^i (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \\ &= \sum_{k=0}^{n} \sum_{\mathbf{x}\in\mathbb{E}_{n,k}} \sum_{i=0}^{k} \binom{k}{i} \epsilon^i (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \\ &= \sum_{k=0}^{n} \sum_{i=0}^{k} \binom{k}{i} \epsilon^i \sum_{\mathbf{x}\in E_{n,k}} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \\ &= \sum_{k=0}^{n} (1+\epsilon)^k W_{f,k}(\mathbf{u}), \end{aligned}$$

and so, our (biased) transform is a weighted sum of restricted transforms.

4 Properties of the $\mathcal{S}$-transform

The vector $\mathbf{0}_n = (0,\ldots,0) \in \mathbb{F}_2^n$ is the all zero vector, and $\mathbf{1}_n = (1,\ldots,1) \in \mathbb{F}_2^n$ is the all one vector in $\mathbb{F}_2^n$. When there is no confusion for n, we write $\mathbf{0}_n = \mathbf{0}$ and $\mathbf{1}_n = \mathbf{1}$, otherwise we will specify n.

The zero function in $\mathfrak{B}_n$ is

$$\ell_{\mathbf{0}_n}(\mathbf{x}) = \mathbf{0}_n \cdot \mathbf{x} = 0, \text{ for all } \mathbf{x} \in \mathbb{F}_2^n.$$

When there is no chance of confusion, like in the theorem below, we simply write $\ell_{\mathbf{0}}$, for notational convenience. Though, the theorem below (and its proof) can be found in [3, Lemma 2.11], we provide an alternate proof that avoids Krawtchouk polynomials.

Theorem 2 *For the function $\ell_{\mathbf{0}}(\mathbf{x}) = \mathbf{0} \cdot \mathbf{x} = 0$, for all $\mathbf{x} \in \mathbb{F}_2^n$,*

$$\mathcal{S}_{\ell_{\mathbf{0}}}(\mathbf{u}) = \begin{cases} n2^{n-1} & \text{if } \mathbf{u} = \mathbf{0} \\ -2^{n-1} & \text{if } \mathrm{wt}(\mathbf{u}) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Proof

$$\mathcal{S}_{\ell_{\mathbf{0}}}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \mathrm{wt}(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}}.$$

Substituting $\mathbf{u} = \mathbf{0}$, we have

$$\mathcal{S}_{\ell_{\mathbf{0}}}(\mathbf{0}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \mathrm{wt}(\mathbf{x}) = \sum_{i=0}^{n} i \binom{n}{i} = n \sum_{j=0}^{n-1} \binom{n-1}{j} = n2^{n-1}.$$

Let $\mathbf{u} \in \mathbb{F}_2^n$ be such that $\mathrm{wt}(\mathbf{u}) = 1$. Without loss of generality, we can assume that $\mathbf{u} = (1, 0, \ldots, 0)$.

$$\mathcal{S}_{\ell_{\mathbf{0}}}(1, 0, \ldots, 0) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \mathrm{wt}(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}}.$$

If $\mathbf{x} = (\mathbf{x}', \mathbf{x}'') \in \mathbb{F}_2 \times \mathbb{F}_2^{n-1}$, $\mathrm{wt}(\mathbf{x}) = \mathrm{wt}(\mathbf{x}') + \mathrm{wt}(\mathbf{x}'')$,

$$\begin{aligned} \mathcal{S}_{\ell_{\mathbf{0}}}(1, 0, \ldots, 0) &= \sum_{\mathbf{x}'' \in \mathbb{F}_2^{n-1}} \sum_{\mathbf{x}' \in \mathbb{F}_2} \mathrm{wt}(\mathbf{x}')(-1)^{\mathbf{x}'} + \sum_{\mathbf{x}'' \in \mathbb{F}_2^{n-1}} \sum_{\mathbf{x}' \in \mathbb{F}_2} \mathrm{wt}(\mathbf{x}'')(-1)^{\mathbf{x}'} \\ &= \sum_{\mathbf{x}'' \in \mathbb{F}_2^{n-1}} (-1) + \sum_{\mathbf{x}'' \in \mathbb{F}_2^{n-1}} \mathrm{wt}(\mathbf{x}'') \sum_{\mathbf{x}' \in \mathbb{F}_2} (-1)^{\mathbf{x}'} = -2^{n-1}. \end{aligned}$$

Finally, let $\mathrm{wt}(\mathbf{u}) = k \geq 2$. Without loss of generality, we assume $\mathbf{u} = (\mathbf{1}_k, \mathbf{0}_{n-k})$ where $\mathbf{1}_k = (1, \ldots, 1) \in \mathbb{F}_2^k$, $\mathbf{0}_{n-k} = (0, \ldots, 0) \in \mathbb{F}_2^{n-k}$, and $\mathbf{x} = (\mathbf{x}', \mathbf{x}'') \in \mathbb{F}_2^k \times \mathbb{F}_2^{n-k}$.

$$\begin{aligned} \mathcal{S}_{\ell_{\mathbf{0}}}(\mathbf{1}_k, \mathbf{0}_{n-k}) &= \sum_{\mathbf{x}'' \in \mathbb{F}_2^{n-k}} \sum_{\mathbf{x}' \in \mathbb{F}_2^k} \mathrm{wt}(\mathbf{x}')(-1)^{\mathbf{1}_k \cdot \mathbf{x}'} + \sum_{\mathbf{x}'' \in \mathbb{F}_2^{n-k}} \mathrm{wt}(\mathbf{x}'') \sum_{\mathbf{x}' \in \mathbb{F}_2^k} (-1)^{\mathbf{1}_k \cdot \mathbf{x}'} \\ &= 2^{n-k} \sum_{\mathbf{x}' \in \mathbb{F}_2^k} \mathrm{wt}(\mathbf{x}')(-1)^{\mathrm{wt}(\mathbf{x}')} \\ &= 2^{n-k} \sum_{i=0}^{k} i \binom{k}{i} (-1)^i = 2^{n-k} k \sum_{i=1}^{k} \binom{k-1}{i-1} (-1)^i \\ &= 2^{n-k} k(-1) \sum_{j=0}^{k-1} \binom{k-1}{j} (-1)^j = 2^{n-k} k(-1)(1 + (-1))^{k-1} = 0. \end{aligned}$$

Collecting all these cases together, we obtain

$$\mathcal{S}_{\ell_{\mathbf{0}}}(\mathbf{u}) = \begin{cases} n2^{n-1} & \text{if } \mathbf{u} = \mathbf{0} \\ -2^{n-1} & \text{if } \mathrm{wt}(\mathbf{u}) = 1 \\ 0 & \text{if } \mathrm{wt}(\mathbf{u}) \geq 2. \end{cases}$$

□

Corollary 1 *Let $l_{\mathbf{u},b}(\mathbf{x}) = \mathbf{u} \cdot \mathbf{x} \oplus b$ where $\mathbf{u} \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$ be an affine function. Then for any $\mathbf{a} \in \mathbb{F}_2^n$, we have*

$$\mathcal{S}_{l_{\mathbf{u},b}}(\mathbf{a}) = \begin{cases} n2^{n-1}(-1)^b & \textit{if } \mathbf{u} = \mathbf{a} \\ 2^{n-1}(-1)^{b+1} & \textit{if } \mathrm{wt}(\mathbf{u} \oplus \mathbf{a}) = 1 \\ 0 & \textit{if } \mathrm{wt}(\mathbf{u} \oplus \mathbf{a}) \geq 2. \end{cases}$$

Proof We have

$$\begin{aligned} \mathcal{S}_{l_{\mathbf{u},b}}(\mathbf{a}) &= \sum_{\mathbf{x} \in \mathbb{F}_2^n} \mathrm{wt}(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x} \oplus b \oplus \mathbf{a}\cdot\mathbf{x}} \\ &= (-1)^b \mathcal{S}_{\ell_{\mathbf{0}_n}}(\mathbf{u} \oplus \mathbf{a}) \\ &= \begin{cases} n2^{n-1}(-1)^b & \text{if } \mathbf{u} = \mathbf{a} \\ 2^{n-1}(-1)^{b+1} & \text{if } \mathrm{wt}(\mathbf{u} \oplus \mathbf{a}) = 1 \\ 0 & \text{if } \mathrm{wt}(\mathbf{u} \oplus \mathbf{a}) \geq 2. \end{cases} \end{aligned}$$

□

Theorem 3 *Suppose that n, m are positive integers. Let $f \in \mathfrak{B}_n$, $g \in \mathfrak{B}_m$, and for any $\mathbf{a} \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$, we have the affine function $\ell_{\mathbf{a},b} \in \mathfrak{B}_n$. Then for $\mathbf{u} \in \mathbb{F}_2^n$ and $\mathbf{v} \in \mathbb{F}_2^m$, the following statements are true:*

1. $\mathcal{S}_{f \oplus \ell_{\mathbf{a},b}}(\mathbf{u}) = (-1)^b \mathcal{S}_f(\mathbf{a} \oplus \mathbf{u})$.
2. $h(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}) \oplus g(\mathbf{y})$ *implies* $\mathcal{S}_h(\mathbf{u}, \mathbf{v}) = \mathcal{S}_f(\mathbf{u}) W_g(\mathbf{v}) + \mathcal{S}_g(\mathbf{v}) W_f(\mathbf{u})$.
3. $h(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}) g(\mathbf{y})$ *implies*

$$\begin{aligned} \mathcal{S}_h(\mathbf{u}, \mathbf{v}) = {} & 2^m \mathcal{S}_{\ell_{\mathbf{0}_n}}(\mathbf{u}) \delta_{\mathbf{0}_m}(\mathbf{v}) - \frac{1}{2}(\mathcal{S}_{\ell_{\mathbf{0}_n}}(\mathbf{u}) - \mathcal{S}_f(\mathbf{u}))(2^m \delta_{\mathbf{0}_m}(\mathbf{v}) - W_g(\mathbf{v})) \\ & + 2^n \mathcal{S}_{\ell_{\mathbf{0}_m}}(\mathbf{v}) \delta_{\mathbf{0}_n}(\mathbf{u}) - \frac{1}{2}(\mathcal{S}_{\ell_{\mathbf{0}_m}}(\mathbf{v}) - \mathcal{S}_g(\mathbf{v}))(2^n \delta_{\mathbf{0}_n}(\mathbf{u}) - W_f(\mathbf{u})). \end{aligned}$$

where $\delta_{\mathbf{0}_n}(\mathbf{a}) = 1$, if $\mathbf{a} = \mathbf{0} \in \mathbb{F}_2^n$, otherwise $\delta_{\mathbf{0}_n}(\mathbf{a}) = 0$ if $\mathbf{a} \in \mathbb{F}_2^n - \{\mathbf{0}\}$, and is called the Dirac (or Kronecker) function at $\{\mathbf{0}\}$ over $\mathbb{F}_2^n$.

Proof First two statements are trivial to prove. So, we consider $h(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}) g(\mathbf{y})$. The stability spectrum of such an $h \in \mathfrak{B}_{(n+m)}$ is

$$
\begin{aligned}
\mathcal{S}_h(\mathbf{u},\mathbf{v}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{y}\in\mathbb{F}_2^m} \mathrm{wt}(\mathbf{x},\mathbf{y})(-1)^{f(\mathbf{x})g(\mathbf{y})} \times (-1)^{\mathbf{u}\cdot\mathbf{x}\oplus\mathbf{v}\cdot\mathbf{y}} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{y}\in\mathbb{F}_2^m} \mathrm{wt}(\mathbf{x})(1-2f(\mathbf{x})g(\mathbf{y}))(-1)^{\mathbf{u}\cdot\mathbf{x}\oplus\mathbf{v}\cdot\mathbf{y}} \\
&\quad + \sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{y}\in\mathbb{F}_2^m} \mathrm{wt}(\mathbf{y})(1-2f(\mathbf{x})g(\mathbf{y}))(-1)^{\mathbf{u}\cdot\mathbf{x}\oplus\mathbf{v}\cdot\mathbf{y}} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \mathrm{wt}(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}} \sum_{\mathbf{y}\in\mathbb{F}_2^m}(-1)^{\mathbf{v}\cdot\mathbf{y}} - 2\Bigg(\sum_{\mathbf{x}\in\mathbb{F}_2^n} \mathrm{wt}(\mathbf{x}) f(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&\quad \sum_{\mathbf{y}\in\mathbb{F}_2^m} g(\mathbf{y})(-1)^{\mathbf{v}\cdot\mathbf{y}}\Bigg) + \sum_{\mathbf{y}\in\mathbb{F}_2^m} \mathrm{wt}(\mathbf{y})(-1)^{\mathbf{v}\cdot\mathbf{y}} \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&\quad - 2\sum_{\mathbf{y}\in\mathbb{F}_2^m} \mathrm{wt}(\mathbf{y}) g(\mathbf{y})(-1)^{\mathbf{v}\cdot\mathbf{y}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} f(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= 2^m \mathcal{S}_{\ell_{\mathbf{0}_n}}(\mathbf{u})\delta_{\mathbf{0}_m}(\mathbf{v}) - \frac{1}{2}(\mathcal{S}_{\ell_{\mathbf{0}_n}}(\mathbf{u}) - \mathcal{S}_f(\mathbf{u}))(2^m\delta_{\mathbf{0}_m}(\mathbf{v}) - W_g(\mathbf{v})) \\
&\quad + 2^n \mathcal{S}_{\ell_{\mathbf{0}_m}}(\mathbf{v})\delta_{\mathbf{0}_n}(\mathbf{u}) - \frac{1}{2}(\mathcal{S}_{\ell_{\mathbf{0}_m}}(\mathbf{v}) - \mathcal{S}_g(\mathbf{v}))(2^n\delta_{\mathbf{0}_n}(\mathbf{u}) - W_f(\mathbf{u})).
\end{aligned}
$$

Therefore, the theorem is proved. □

5 $\mathcal{S}$-spectrum of bent Boolean functions

Theorem 4 *Let $f \in \mathfrak{B}_n$ where n is positive even integer. Then $|\mathcal{S}_f(\mathbf{u})| \le n2^{\frac{n}{2}}$ for all $\mathbf{u} \in \mathbb{F}_2^n$.*

Proof For $i \in [n]$, let $\mathbf{e}_i \in \mathbb{F}_2^n$ denotes the vector whose ith coordinate is the only nonzero coordinate. Since f is bent, we have $(-1)^{f(\mathbf{x})} = 2^{-\frac{n}{2}} W_{\tilde{f}}(\mathbf{x})$ for $\mathbf{x} \in \mathbb{F}_2^n$, where $\tilde{f}$ is the dual of f. Consider, for $\mathbf{u} \in \mathbb{F}_2^n$

$$
\begin{aligned}
\mathcal{S}_f(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \mathrm{wt}(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}} \left(\frac{1}{2^{\frac{n}{2}}} W_{\tilde{f}}(\mathbf{x})\right) \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \mathrm{wt}(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}} \sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{\tilde{f}(\mathbf{y})\oplus\mathbf{x}\cdot\mathbf{y}} \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{\tilde{f}(\mathbf{y})} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \mathrm{wt}(\mathbf{x})(-1)^{\mathbf{x}\cdot(\mathbf{u}\oplus\mathbf{y})} \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{\tilde{f}(\mathbf{y})} \mathcal{S}_{\ell_{\mathbf{0}_n}}(\mathbf{u}\oplus\mathbf{y})
\end{aligned}
$$

$$= \frac{1}{2^{\frac{n}{2}}} \left(n2^{n-1}(-1)^{\tilde{f}(\mathbf{u})} - 2^{n-1} \sum_{i\in[n]} (-1)^{\tilde{f}(\mathbf{u}\oplus\mathbf{e}_i)} \right)$$

$$= 2^{\frac{n}{2}-1} \left(n(-1)^{\tilde{f}(\mathbf{u})} \right) - 2^{\frac{n}{2}-1} \left(\sum_{i\in[n]} (-1)^{\tilde{f}(\mathbf{u}\oplus\mathbf{e}_i)} \right).$$

Therefore, $|\mathcal{S}_f(\mathbf{u})| \leq n2^{\frac{n}{2}}$. □

Corollary 2 *Let $n = 2m$, $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be a permutation and g be any Boolean function on $\mathbb{F}_2^m$. Let $f : \mathbb{F}_2^n = \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ be a Maiorana–McFarland type bent function defined as $f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus g(\mathbf{y})$. Then for any $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^m$, we have*

$$\mathcal{S}_f(\mathbf{u}, \mathbf{v}) = 2^m \mathrm{wt}(\pi^{-1}(\mathbf{u}))(-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u})\oplus g(\pi^{-1}(\mathbf{u}))} + m2^{m-1}(-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u})\oplus g(\pi^{-1}(\mathbf{u}))} - 2^{m-1} \sum_{i=1}^{m} (-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u}\oplus\mathbf{e}_i)\oplus g(\pi^{-1}(\mathbf{u}\oplus\mathbf{e}_i))},$$

where $\mathbf{e}_i \in \mathbb{F}_2^m$ for all $i \in [m]$ is as taken in proof of Theorem 4.

Proof We know that for $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^m$, $\tilde{f}(\mathbf{u}, \mathbf{v}) = \mathbf{v}\cdot\pi^{-1}(\mathbf{u})\oplus g(\pi^{-1}(\mathbf{u}))$. Using Theorem 4, we get

$$\begin{aligned}
\mathcal{S}_f(\mathbf{u}, \mathbf{v}) &= 2^{m-1}\Big(n(-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u})\oplus g(\pi^{-1}(\mathbf{u}))} - \sum_{i=1}^{m} (-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u}\oplus\mathbf{e}_i)\oplus g(\pi^{-1}(\mathbf{u}\oplus\mathbf{e}_i))} \\
&\quad - \sum_{i=1}^{m} (-1)^{(\mathbf{v}\oplus\mathbf{e}_i)\cdot\pi^{-1}(\mathbf{u})\oplus g(\pi^{-1}(\mathbf{u}))} \Big) \\
&= 2^{m-1}\Big(n(-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u})\oplus g(\pi^{-1}(\mathbf{u}))} - \sum_{i=1}^{m} (-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u}\oplus\mathbf{e}_i)\oplus g(\pi^{-1}(\mathbf{u}\oplus\mathbf{e}_i))} \\
&\quad - (-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u})\oplus g(\pi^{-1}(\mathbf{u}))} \sum_{i=1}^{m} (-1)^{\mathbf{e}_i\cdot\pi^{-1}(\mathbf{u})} \Big) \\
&= 2^{m-1}\Big(n(-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u})\oplus g(\pi^{-1}(\mathbf{u}))} - \sum_{i=1}^{m} (-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u}\oplus\mathbf{e}_i)\oplus g(\pi^{-1}(\mathbf{u}\oplus\mathbf{e}_i))} \\
&\quad - (-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u})\oplus g(\pi^{-1}(\mathbf{u}))}(m - 2\mathrm{wt}(\pi^{-1}(\mathbf{u}))) \Big) \\
&= 2^m \mathrm{wt}(\pi^{-1}(\mathbf{u}))(-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u})\oplus g(\pi^{-1}(\mathbf{u}))} + m2^{m-1}(-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u})\oplus g(\pi^{-1}(\mathbf{u}))} \\
&\quad - 2^{m-1} \sum_{i=1}^{m} (-1)^{\mathbf{v}\cdot\pi^{-1}(\mathbf{u}\oplus\mathbf{e}_i)\oplus g(\pi^{-1}(\mathbf{u}\oplus\mathbf{e}_i))}.
\end{aligned}$$

In particular, if $\pi(\mathbf{y}) = \mathbf{y}$ and $g \equiv 0$, i.e. $f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$, then $\mathcal{S}_f(\mathbf{u}, \mathbf{v}) = 2^{\frac{n}{2}} \mathrm{wt}(\mathbf{u}, \mathbf{v})(-1)^{\mathbf{u}\cdot\mathbf{v}}$. □

Remark 1 The equality of the bound in Theorem 4 is not always attained. For example, take $\pi : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ to be the permutation defined as follows using the hexadecimal representations of the elements of $\mathbb{F}_2^n$:

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \\ 5 & 6 & C & 8 & 4 & 0 & F & 2 & 3 & A & 1 & E & D & B & 9 & 7 \end{pmatrix}.$$

We define $f : \mathbb{F}_2^4 \times \mathbb{F}_2^4 \to \mathbb{F}_2$ as $f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y})$ for $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^4$. Then, $\max_{(\mathbf{u},\mathbf{v}) \in \mathbb{F}_2^4 \times \mathbb{F}_2^4} |\mathcal{S}_f(\mathbf{u}, \mathbf{v})| = 112 < 128 (= 8 \cdot 2^4)$.

6 Characterization of the $\mathcal{S}$-spectrum for symmetric Boolean functions

Definition 3 A Boolean function $f \in \mathfrak{B}_n$ is said to be symmetric, if for every $\mathbf{x} \in \mathbb{F}_2^n$, the value $f(\mathbf{x})$ is exclusively a function of $\mathrm{wt}(\mathbf{x})$.

In other words, suppose $\mathfrak{S}_n$ is the symmetric group acting on $[n]$. The function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is said to be symmetric if and only if $f(\mathbf{x}) = f(\sigma(\mathbf{x}))$, for all $\mathbf{x} \in \mathbb{F}_2^n$ and $\sigma \in \mathfrak{S}_n$.
Let $Sym(n)$ denote the set of symmetric Boolean functions in n variables.

Definition 4 A symmetric Boolean function f in n variables can be uniquely represented by an $(n + 1)$ length bitstring denoted by $re(f) = c_0 c_1 \dots c_n$, where $f(\mathbf{x}) = c_i \in \mathbb{F}_2$, whenever $\mathrm{wt}(\mathbf{x}) = i \in \{0, 1, \dots, n\}$.

For example, suppose f is a symmetric Boolean function in 4 variables with $f(\mathbf{x}) = 1$ when $\mathrm{wt}(\mathbf{x}) = 0$, $f(\mathbf{x}) = 0$ when $\mathrm{wt}(\mathbf{x}) = 1$, $f(\mathbf{x}) = 1$ when $\mathrm{wt}(\mathbf{x}) = 2$, $f(\mathbf{x}) = 1$ when $\mathrm{wt}(\mathbf{x}) = 3$, and $f(\mathbf{x}) = 0$ when $\mathrm{wt}(\mathbf{x}) = 4$, then, $re(f) = 10110$.

The Krawtchouk polynomial $P_k(x, n)$ is:

$$P_k(x, n) = \sum_{i=0}^{k} (-1)^i \binom{x}{i} \binom{n-x}{k-i}, \tag{14}$$

where $k \geq 0$ and $0 \leq x \leq n$ are integers. The generating function of $P_k(x, n)$ is

$$\sum_{k=0}^{n} \mathcal{P}_k(x, n) z^k = (1 - z)^x (1 + z)^{n-x} \tag{15}$$

and the relation between Krawtchouk polynomials and partial character sums corresponding to linear functions is

$$\sum_{\substack{\mathrm{wt}(\mathbf{x})=k \\ \mathbf{x} \in \mathbb{F}_2^n}} (-1)^{\mathbf{u}\cdot\mathbf{x}} = P_k(\mathrm{wt}(\mathbf{u}), n), \quad \text{for all } \mathbf{u} \in \mathbb{F}_2^n. \tag{16}$$

Refer to [3] for more on Krawtchouk polynomials. Though not needed, one can use Gauss' hypergeometric function ${}_2F_1(a, b, c; z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n} \frac{z^n}{n!}$, where $(a)_n = a(a+1)\cdots(a+n-1)$ is the rising factorial, to rewrite the sum below. See ([1], section 18.5) for details on hypergeometric functions.

Theorem 5 *Let $f \in \mathfrak{B}_n$ be symmetric Boolean function such that for each $\mathbf{x} \in \mathbb{F}_2^n$, $f(\mathbf{x}) = c_{\mathrm{wt}(\mathbf{x})} \in \mathbb{F}_2$. Then for all $\mathbf{u} \in \mathbb{F}_2^n$*

$$\begin{aligned} \mathcal{S}_f(\mathbf{u}) &= \sum_{k=1}^{n} \sum_{j=0}^{k} \binom{\mathrm{wt}(\mathbf{u})}{j} \binom{n-\mathrm{wt}(\mathbf{u})}{k-j} k(-1)^{c_k+j} \\ &= \sum_{k=1}^{n} k(-1)^{c_k} {}_2F_1(-k, -\mathrm{wt}(\mathbf{u}), 1-k+n-\mathrm{wt}(\mathbf{u}); -1). \end{aligned} \tag{17}$$

Proof Let f be a symmetric Boolean function such that $f(\mathbf{x}) = c_{\mathrm{wt}(\mathbf{x})} \in \mathbb{F}_2$. For $\mathbf{u} \in \mathbb{F}_2^n$

$$\begin{aligned} \mathcal{S}_f(\mathbf{u}) &= \sum_{k=1}^{n} k(-1)^{c_k} \sum_{\mathrm{wt}(\mathbf{x})=k} (-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &= \sum_{k=1}^{n} k(-1)^{c_k} P_k(\mathrm{wt}(\mathbf{u}), n) \\ &= \sum_{k=1}^{n} k(-1)^{c_k} \sum_{j=0}^{k} \binom{\mathrm{wt}(\mathbf{u})}{j} \binom{n-\mathrm{wt}(\mathbf{u})}{k-j} (-1)^{j} \\ &= \sum_{k=1}^{n} \sum_{j=0}^{k} \binom{\mathrm{wt}(\mathbf{u})}{j} \binom{n-\mathrm{wt}(\mathbf{u})}{k-j} k(-1)^{c_k+j} \\ &= \sum_{k=1}^{n} k(-1)^{c_k} {}_2F_1(-k, -\mathrm{wt}(\mathbf{u}), 1-k+n-\mathrm{wt}(\mathbf{u}); -1), \end{aligned}$$

and the result follows. □

Corollary 3 *For a symmetric Boolean function $f \in \mathfrak{B}_n$, $\mathcal{S}_f : \mathbb{F}_2^n \to \mathbb{R}$ is symmetric, i.e., $\mathcal{S}_f(\mathbf{u}) = \mathcal{S}_f(\mathbf{v})$, whenever $\mathrm{wt}(\mathbf{u}) = \mathrm{wt}(\mathbf{v})$, for $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^n$.*

Let $\mathbf{u}_n^{(i)} = (\underbrace{0, \ldots, 0}_{(n-i)\text{-times}}, \underbrace{1, \ldots, 1}_{i\text{-times}})$ for $i = 0, 1, \ldots, n$. Then, for a symmetric Boolean function $f \in \mathfrak{B}_n$,

$$\mathcal{S}_f\left(\mathbf{u}_n^{(i)}\right) = \sum_{j=0}^{n} (-1)^{f\left(\mathbf{u}_n^{(j)}\right)} \left(j \sum_{wt(\mathbf{x})=j} (-1)^{\mathbf{u}_n^{(i)}\cdot\mathbf{x}} \right)$$

$$= \sum_{j=0}^{n} j P_j(i,n) \chi_f\left(\mathbf{u}_n^{(j)}\right)$$
$$= \sum_{j=0}^{n} M_j\left(\mathbf{u}_n^{(i)}\right) \chi_f\left(\mathbf{u}_n^{(j)}\right),$$

where $M_j\left(\mathbf{u}_n^{(i)}\right) = j P_j(i,n) = j \sum_{r=0}^{j} (-1)^r \binom{i}{r}\binom{n-i}{j-r}$. The values of $M_j(\mathbf{u}_n^{(i)})$ are independent of the function f. Let $\mathbf{M}_{n+1} = \left(M_j(\mathbf{u}_n^{(i)})\right)_{(n+1)\times(n+1)}$, where $i, j = 0, \ldots, n$, and let $\chi_f = \left(\chi_f(\mathbf{u}_n^{(0)}), \ldots, \chi_f(\mathbf{u}_n^{(n)})\right)^T$. Then

$$\mathbf{S}_f = \mathbf{M}_{n+1}\, \chi_f,$$

where $\mathbf{S}_f = [\mathcal{S}_f(\mathbf{u}_n^{(0)}), \mathcal{S}_f(\mathbf{u}_n^{(1)}), \ldots, \mathcal{S}_f(\mathbf{u}_n^{(n)})]$.

6.1 $\mathcal{S}$-spectrum for symmetric bent functions

In Sect. 5 we have derived an upper bound of the $\mathcal{S}$-transform values for bent functions. In this section we provide a complete characterization of $\mathcal{S}$-spectra of symmetric bent Boolean function and symmetric Boolean functions on odd number of variables having maximum nonlinearity.

Symmetric bent functions are characterized by the following well-known theorem.

Theorem 6 (Savicky, [10]) *For any given even positive integer n, there are only four symmetric bent functions in n variables (as usual,* $\mathbf{x} = (x_1, \ldots, x_n)$*):*

1. $f(\mathbf{x})$
2. $f(\mathbf{x}) \oplus 1$
3. $f(\mathbf{x}) \oplus \bigoplus_{i=1}^{n} x_i$
4. $f(\mathbf{x}) \oplus \bigoplus_{i=1}^{n} x_i \oplus 1$,

where

$$f(\mathbf{x}) = \bigoplus_{i=1}^{n} \bigoplus_{j=i+1}^{n} x_i x_j. \tag{18}$$

Let $g(\mathbf{x}) = f(\mathbf{x}) \oplus a\left(\bigoplus_{i=1}^{n} x_i\right) \oplus b = c_{\mathrm{wt}(\mathbf{x})} \in \mathbb{F}_2$ where the function f is same as in (18) and $a, b \in \mathbb{F}_2$. One can see that $re(g)$ is a contiguous $(n+1)$ length substring of $(0011)^*$. The notation $(0011)^*$ denotes the one way infinite string $001100110011\cdots$ formed by repeatedly concatenating the string 0011. Let $\alpha = (-1)^{c_0} - \iota(-1)^{c_1}$, then, for all $k = 0, 1, \ldots, n$, we have $(-1)^{c_k} = \Re(\alpha \iota^k)$ where $\Re$ denotes the real part of a complex number and $\iota = \sqrt{-1}$ is the imaginary unit. For further clarification on $re(f)$ of symmetric bent functions, one can refer to [10, Theorem 3.3].

Theorem 7 *Let $n = 2m \in \mathbb{Z}$, and $g(\mathbf{x}) = f(\mathbf{x}) \oplus a\left(\bigoplus_{i=1}^{n} x_i\right) \oplus b = c_{\mathrm{wt}(\mathbf{x})}$, where $a, b \in \mathbb{F}_2$ and f is as in Eq. (18). Then for all $\mathbf{u} \in \mathbb{F}_2^n$, $|\mathcal{S}_g(\mathbf{u})|$ belongs to the set*

$$\left\{2^{\frac{n}{2}-1}\left|\left((-1)^{c_0}(n-2\mathrm{wt}(\mathbf{u}))-(-1)^{c_1}n\right)\right|, 2^{\frac{n}{2}-1}\left|\left((-1)^{c_0}n+(-1)^{c_1}(n-2\mathrm{wt}(\mathbf{u}))\right)\right|\right\}$$

with either $|\mathcal{S}_g(\mathbf{0})| = n2^{\frac{n}{2}}$ or $|\mathcal{S}_g(\mathbf{1})| = n2^{\frac{n}{2}}$, and for $\mathbf{u} \in \mathbb{F}_2^n$ such that $\mathrm{wt}(\mathbf{u}) = \frac{n}{2}$, $|\mathcal{S}_g(\mathbf{u})| = n2^{\frac{n}{2}-1}$.

Proof To prove the theorem, we use the relation in (16), and $\alpha = (-1)^{c_0} - \imath(-1)^{c_1}$. For $\mathbf{u} \in \mathbb{F}_2^n$, we have

$$\mathcal{S}_g(\mathbf{u}) = \sum_{k=1}^{n} k(-1)^{c_k} \sum_{\mathrm{wt}(\mathbf{x})=k} (-1)^{\mathbf{u}\cdot\mathbf{x}} = \Re\left(\alpha\imath \sum_{k=1}^{n} k P_k(\mathrm{wt}(\mathbf{u}), n)\imath^{k-1}\right).$$

We know that

$$(1-z)^{\mathrm{wt}(\mathbf{u})}(1+z)^{n-\mathrm{wt}(\mathbf{u})} = \sum_{k=0}^{n} P_k(\mathrm{wt}(\mathbf{u}), n)z^k.$$

Differentiating both sides with respect to z

$$\begin{aligned}(n-\mathrm{wt}(\mathbf{u}))(1-z)^{\mathrm{wt}(\mathbf{u})}(1+z)^{n-\mathrm{wt}(\mathbf{u})-1} - \mathrm{wt}(\mathbf{u})(1-z)^{\mathrm{wt}(\mathbf{u})-1}(1+z)^{n-\mathrm{wt}(\mathbf{u})} \\ = \sum_{k=1}^{n} k P_k(\mathrm{wt}(\mathbf{u}), n)z^{k-1}.\end{aligned}$$

Substituting $z = \imath$ and $\mathrm{wt}(\mathbf{u}) = t$, we get

$$(n-t)(1-\imath)^t(1+\imath)^{n-t-1} - t(1-\imath)^{t-1}(1+\imath)^{n-t} = \sum_{k=1}^{n} k P_k(t, n)\imath^{k-1},$$

that is,

$$(1-\imath)^{t-1}(1+\imath)^{n-t-1}(n-2t-n\imath) = \sum_{k=1}^{n} k P_k(t, n)\imath^{k-1}.$$

Then, the $\mathcal{S}$-transform of g at $\mathbf{u} \in \mathbb{F}_2^n$ is therefore

$$\mathcal{S}_g(\mathbf{u}) = \Re\left(\alpha\imath(1-\imath)^{t-1}(1+\imath)^{n-t-1}(n-2t-n\imath)\right).$$

We consider the case when $0 \le t = \mathrm{wt}(\mathbf{u}) \le \frac{n}{2} = m$. Then

$$\mathcal{S}_g(\mathbf{u}) = \Re\left(\alpha\imath(1-\imath)^{t-1}(1+\imath)^{t-1}(1+\imath)^{n-2t}(n-2t-n\imath)\right)$$

$$
\begin{aligned}
&= 2^{t-1}\Re\left(\alpha\imath(1+\imath)^{n-2t}(n-2t-n\imath)\right)\\
&= 2^{t-1}\Re\left(\alpha\imath(1+\imath)^{2(m-t)}(n-2t-n\imath)\right)\\
&= 2^{t-1}\Re\left(\alpha\imath(2\imath)^{m-t}(n-2t-n\imath)\right)\\
&= 2^{m-1}\Re\left(\alpha\imath^{m-t+1}(n-2t-n\imath)\right)\\
&= 2^{m-1}\Re\left(((-1)^{c_0}-\imath(-1)^{c_1})\imath^{m-t+1}(n-2t-n\imath)\right)\\
&= 2^{m-1}\Re\Big((n-2t)(-1)^{c_0}\imath^{m-t+1}-(n-2t)(-1)^{c_1}\imath^{m-t+2}\\
&\qquad\qquad -n(-1)^{c_0}\imath^{m-t+2}+n(-1)^{c_1}\imath^{m-t+3}\Big).
\end{aligned}
$$

We have the following cases:

1. If $m-t\equiv 0 \pmod 4$, $\mathcal{S}_g(\mathbf{u}) = 2^{m-1}((-1)^{c_0}n+(-1)^{c_1}(n-2t))$.
2. If $m-t\equiv 1 \pmod 4$, $\mathcal{S}_g(\mathbf{u}) = -2^{m-1}((-1)^{c_0}(n-2t)-(-1)^{c_1}n)$.
3. If $m-t\equiv 2 \pmod 4$, $\mathcal{S}_g(\mathbf{u}) = -2^{m-1}((-1)^{c_0}n+(-1)^{c_1}(n-2t))$.
4. If $m-t\equiv 3 \pmod 4$, $\mathcal{S}_g(\mathbf{u}) = 2^{m-1}((-1)^{c_0}(n-2t)-(-1)^{c_1}n)$.

Similarly, for the case when $m=\frac{n}{2}\le t=\mathrm{wt}(\mathbf{u})\le n$, one can prove that

1. If $t-m\equiv 0 \pmod 4$, $\mathcal{S}_g(\mathbf{u}) = (-1)^{t-m}2^{m-1}((-1)^{c_0}n+(-1)^{c_1}(n-2t))$.
2. If $t-m\equiv 1 \pmod 4$, $\mathcal{S}_g(\mathbf{u}) = (-1)^{t-m+1}2^{m-1}((-1)^{c_0}(n-2t)-(-1)^{c_1}n)$.
3. If $t-m\equiv 2 \pmod 4$, $\mathcal{S}_g(\mathbf{u}) = (-1)^{t-m+1}2^{m-1}((-1)^{c_0}n+(-1)^{c_1}(n-2t))$.
4. If $t-m\equiv 3 \pmod 4$, $\mathcal{S}_g(\mathbf{u}) = (-1)^{t-m}2^{m-1}((-1)^{c_0}(n-2t)-(-1)^{c_1}n)$.

Now, it is straightforward to check that either $|\mathcal{S}_g(\mathbf{0})| = n2^{\frac{n}{2}}$ or $|\mathcal{S}_g(\mathbf{1})| = n2^{\frac{n}{2}}$, and if we put $t=\mathrm{wt}(\mathbf{u})=\frac{n}{2}$, then we will get $|\mathcal{S}_g(\mathbf{u})| = n2^{\frac{n}{2}-1}$. □

6.2 $\mathcal{S}$-spectrum for odd variable symmetric Boolean functions having maximum

We recall that for odd $n\ge 3$ of variables:

Theorem 8 [8, Theorem 5] *Let $n\ge 3$ be odd and f be a symmetric Boolean function in n variables, then $\mathcal{N}_f \le 2^{n-1}-2^{\frac{n-1}{2}}$ and the equality holds if and only if $re(f)$ is a contiguous $(n+1)$ length substring of $(0011)^*$.*

Theorem 9 *Let $n\ge 3$ be odd and f be a symmetric Boolean function in n variables such that $\mathcal{N}_f = 2^{n-1}-2^{\frac{n-1}{2}}$ then $\max_{\mathbf{u}\in\mathbb{F}_2^n}|\mathcal{S}_f(\mathbf{u})| = n2^{\frac{n-1}{2}}$ with either $|\mathcal{S}_g(\mathbf{0})| = n2^{\frac{n-1}{2}}$ or $|\mathcal{S}_g(\mathbf{1})| = n2^{\frac{n-1}{2}}$.*

Proof Let f be a Boolean function satisfying the hypothesis of the theorem. By Theorem 8, $re(f)=c_0c_1\ldots c_n$ has one of the following forms

1. $re(f) = 00110011\ldots b$
2. $re(f) = 11001100\ldots 1-b$
3. $re(f) = 01100110\ldots 1-b$

4. $re(f) = 10011001\ldots b$,

where $b = \frac{(n-1) \pmod 4}{2}$. Let $\alpha = (-1)^{c_0} - \imath(-1)^{c_1}$ then, for all $k = 0, 1, \ldots, n$, we have $(-1)^{c_k} = \Re(\alpha \imath^k)$. Therefore, by using the similar steps taken in Theorem 7, one can show that

1. If $n \equiv 1 \pmod 4$, then $\mathcal{S}_f(\mathbf{0}) = (-1)^{\frac{n-1}{4}} n 2^{\frac{n-1}{2}} (-1)^{c_1}$ and $\mathcal{S}_f(\mathbf{1}) = (-1)^{\frac{n+3}{4}} n 2^{\frac{n-1}{2}} (-1)^{c_1}$.
2. If $n \equiv 3 \pmod 4$ then $\mathcal{S}_f(\mathbf{0}) = \mathcal{S}_f(\mathbf{1}) = (-1)^{\frac{n+1}{4}} n 2^{\frac{n-1}{2}} (-1)^{c_0}$.
3. If $\mathbf{u} \in \mathbb{F}_2^n$ such that $0 < \mathrm{wt}(\mathbf{u}) < n$, it is easy to check that $|\mathcal{S}_f(\mathbf{u})| \leq n 2^{\frac{n-1}{2}}$. □

7 The effect of extended affine transformations on the $\mathcal{S}$-spectra

Definition 5 Two functions $f, g \in \mathfrak{B}_n$ are said to be extended affine equivalent to each other if there exists matrix $A \in GL_n(\mathbb{F}_2)$(set of $n \times n$ invertible matrices over $\mathbb{F}_2$), $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$, and $c \in \mathbb{F}_2$ such that $g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{a}) \oplus \mathbf{x} \cdot \mathbf{b} \oplus c$ for all $\mathbf{x} \in \mathbb{F}_2^n$.

Theorem 10 *Let $A \in O_n(\mathbb{F}_2)$ (set of $n \times n$ orthogonal matrices over $\mathbb{F}_2$) preserving the weight of each vector, i.e., $wt(\mathbf{x}) = wt(\mathbf{x}A)$ for all $\mathbf{x} \in \mathbb{F}_2^n$ and $h(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{a})$ where $\mathbf{a} \in \mathbb{F}_2^n$. Then for all $\mathbf{u} \in \mathbb{F}_2^n$*

$$\mathcal{S}_h(\mathbf{u}) = (-1)^{\mathbf{u}A \cdot \mathbf{a}} \left(\mathcal{S}_f(\mathbf{u}A) + \mathrm{wt}(\mathbf{a}) W_f(\mathbf{u}A) - 2 \sum_{\mathbf{z} \in \mathbb{F}_2^n} \mathrm{wt}(\mathbf{a} * \mathbf{z}) (-1)^{f(\mathbf{z}) \oplus \mathbf{u}A \cdot \mathbf{z}} \right)$$

and if $\mathbf{a} = \mathbf{0}$ then $\mathcal{S}_h(\mathbf{u}) = \mathcal{S}_f(\mathbf{u}A)$.

Proof Let $\mathbf{z} = \mathbf{x}A \oplus \mathbf{a}$, if $\mathbf{x}$ varies over $\mathbb{F}_2^n$, so does $\mathbf{z} = \mathbf{x}A \oplus \mathbf{a}$, and $\mathrm{wt}(\mathbf{x}) = \mathrm{wt}(\mathbf{x}A)$ gives that $\mathrm{wt}(\mathbf{x}) = \mathrm{wt}(\mathbf{x}A^{-1})$ for all $\mathbf{x} \in \mathbb{F}_2^n$. The $\mathcal{S}$-transform of h at $\mathbf{u} \in \mathbb{F}_2^n$ is

$$\begin{aligned}
\mathcal{S}_h(\mathbf{u}) &= (-1)^{\mathbf{u} \cdot \mathbf{a} A^{-1}} \sum_{\mathbf{z} \in \mathbb{F}_2^n} \mathrm{wt}((\mathbf{z} \oplus \mathbf{a}) A^{-1}) (-1)^{f(\mathbf{z}) \oplus \mathbf{u} \cdot \mathbf{z} A^{-1}} \\
&= (-1)^{\mathbf{u}A \cdot \mathbf{a}} \sum_{\mathbf{z} \in \mathbb{F}_2^n} (\mathrm{wt}(\mathbf{z}) + \mathrm{wt}(\mathbf{a}) - 2\mathrm{wt}(\mathbf{z} * \mathbf{a})) (-1)^{f(\mathbf{z}) \oplus \mathbf{u}A \cdot \mathbf{z}} \\
&= (-1)^{\mathbf{u}A \cdot \mathbf{a}} \left(\mathcal{S}_f(\mathbf{u}A) + \mathrm{wt}(\mathbf{a}) W_f(\mathbf{u}A) - 2 \sum_{\mathbf{z} \in \mathbb{F}_2^n} \mathrm{wt}(\mathbf{a} * \mathbf{z}) (-1)^{f(\mathbf{z}) \oplus \mathbf{u}A \cdot \mathbf{z}} \right).
\end{aligned}$$

For the second equality, $\mathbf{u} \cdot \mathbf{z}A^{-1} = \mathbf{u}(A^{-1})^T \cdot \mathbf{z} = \mathbf{u}A \cdot \mathbf{z}$ as A is orthogonal, i.e., $AA^T = A^T A = I_n$, where the matrix multiplication is done over the field $\mathbb{F}_2$, A^T, I_n denote the transpose the matrix A, and the identity matrix, respectively.

Now, putting $\mathbf{a} = \mathbf{0}$ gives $\mathcal{S}_h(\mathbf{u}) = \mathcal{S}_f(\mathbf{u}A)$ for all $\mathbf{u} \in \mathbb{F}_2^n$. □

We present a concrete example to show that the stability spectrum is not preserved under the extended affine equivalence. Let us consider the matrix,

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

One can easily check that A is orthogonal over $\mathbb{F}_2$, i.e., $AA^T = A^TA = I_6$, where the matrix multiplication is done over the field $\mathbb{F}_2$. We now let $f \in \mathfrak{B}_6$ be a symmetric Boolean function with $re(f) = 0000100$, and define $g \in \mathfrak{B}_6$ as $g(\mathbf{x}) = f(\mathbf{x}A)$ for all $\mathbf{x} \in \mathbb{F}_2^6$. Then, $\max_{\mathbf{u}\in\mathbb{F}_2^6} |\mathcal{S}_f(\mathbf{u})| = 120$, while $\max_{\mathbf{u}\in\mathbb{F}_2^6} |\mathcal{S}_g(\mathbf{u})| = 104$. This shows that the stability spectrum is not invariant under the extended affine transformation.

8 Experimental results

We know that for any Boolean function $f \in \mathfrak{B}_n$, $\max_{\mathbf{u}\in\mathbb{F}_2^n} |W_f(\mathbf{u})| \geq 2^{\frac{n}{2}}$, and the equality holds for only bent functions, i.e., $W_f(\mathbf{u}) \in \{-2^{\frac{n}{2}}, 2^{\frac{n}{2}}\}$ for all $\mathbf{u} \in \mathbb{F}_2^n$ if and only if f is bent. Further, for the first order fluctuations of the Walsh–Hadamard transform of symmetric bent Boolean functions, we proved that $\max_{\mathbf{u}\in\mathbb{F}_2^n} |\mathcal{S}_f(\mathbf{u})| = n2^{\frac{n}{2}}$. However, there are symmetric Boolean functions satisfying $\max_{\mathbf{u}\in\mathbb{F}_2^n} |\mathcal{S}_f(\mathbf{u})| < n2^{\frac{n}{2}}$.

Here, we present a list of $re(f)$ of non-bent symmetric Boolean functions f such that $\max_{\mathbf{u}\in\mathbb{F}_2^n} |\mathcal{S}_f(\mathbf{u})| = \min_{g\in Sym(n)} \left(\max_{\mathbf{u}\in\mathbb{F}_2^n} |\mathcal{S}_g(\mathbf{u})| \right) < n2^{\frac{n}{2}}$, where g varies over all symmetric Boolean functions in n variables. Since we have performed experiments over the set of symmetric Boolean function in n variables, for $n = 4, 6, 8, \ldots, 20$, the cardinality of the space under consideration is reduced to 2^{n+1}, which is significantly smaller than 2^{2^n}, the cardinality of the space of all Boolean functions in n variables. We then used the formula (17) for efficient computation of the stability spectra of symmetric Boolean functions.

1. For $n = 8$, $\min\limits_{f\in Sym(8)} \left(\max\limits_{\mathbf{u}\in\mathbb{F}_2^8} |\mathcal{S}_f(\mathbf{u})| \right) = 124 < 128 = n2^{\frac{n}{2}}$,

$re(f)$	$\mathcal{N}_f$
001001100, 110110011, 011100110, 100011001	112
000011001, 111100110, 010110011, 101001100	113

2. For $n = 10$, $\min\limits_{f\in Sym(10)} \left(\max\limits_{\mathbf{u}\in\mathbb{F}_2^{10}} |\mathcal{S}_f(\mathbf{u})| \right) = 288 < 320 = n2^{\frac{n}{2}}$,

$re(f)$	$\mathcal{N}_f$
00100110010, 11011001101, 01110011000, 10001100111	489
00001100111, 11110011000, 01011001101, 10100110010	490

3. For $n = 12$, $\min\limits_{f\in Sym(12)}\left(\max\limits_{\mathbf{u}\in\mathbb{F}_2^{12}}|\mathcal{S}_f(\mathbf{u})|\right) = 704 < 768 = n2^{\frac{n}{2}}$,

$re(f)$	$\mathcal{N}_f$
0000011001101, 1111100110010, 0101001100111 1010110011000	1981
0010110011000, 1101001100111, 0111100110010 1000011001101	1982

4. For $n = 16$, $\min\limits_{f\in Sym(16)}\left(\max\limits_{\mathbf{u}\in\mathbb{F}_2^{16}}|\mathcal{S}_f(\mathbf{u})|\right) = 4032 < 4096 = n2^{\frac{n}{2}}$,

$re(f)$	$\mathcal{N}_f$
00100110011001101, 11011001100110010 01110011001100111, 10001100110011000	32625
00001100110011000, 11110011001100111 01011001100110010, 10100110011001101	32626

5. For $n = 18$, $\min\limits_{f\in Sym(18)}\left(\max\limits_{\mathbf{u}\in\mathbb{F}_2^{18}}|\mathcal{S}_f(\mathbf{u})|\right) = 9112 < 9216 = n2^{\frac{n}{2}}$,

$re(f)$	$\mathcal{N}_f$
0000011001100110010, 1111100110011001101 0101001100110011000, 1010110011001100111	130680
0010110011001100111, 0101001100110011000 0111100110011001101, 1000011001100110010	130681

6. For $n = 20$, $\min\limits_{f\in Sym(20)}\left(\max\limits_{\mathbf{u}\in\mathbb{F}_2^{20}}|\mathcal{S}_f(\mathbf{u})|\right) = 19440 < 20480 = n2^{\frac{n}{2}}$,

$re(f)$	$\mathcal{N}_f$
00000110011001100111111, 11111001100110011000 0101001100110011001101, 1010110011001100111010	523659
10000110011001100111111, 01111001100110011000 1101001100110011001101, 0010110011001100111010	523660

7. For $n = 4$, 6 and 14, $\min_{f \in Sym(n)} \left(\max_{\mathbf{u} \in \mathbb{F}_2^n} |\mathcal{S}_f(\mathbf{u})| \right) = n2^{\frac{n}{2}}$, but 4 out of 8 such functions are non-bent and the table below gives their $re(f)$.

n	$re(f)$	$n2^{\frac{n}{2}}$	$\mathcal{N}_f$
4	11100, 00011, 10110, 01001	16	5
6	1110011, 0001100, 1011001, 0100110	48	27
14	111001100110011, 000110011001100 101100110011001, 010011001100110	1792	8127

9 Conclusion

In the recent past, several teams of researchers have studied Boolean functions with biased inputs, from a cryptographic perspective. We have introduced the notion of stability of linear approximations of Boolean functions when the inputs are slightly biased from the uniform distribution. We propose the related concept of $\mathcal{S}$-spectrum and first analyze it for affine and bent functions, in particular, we simplify it for Maiorana–McFarland bent functions. We further characterize it for symmetric bent functions, symmetric Boolean functions on an odd number of variables with maximum nonlinearity. As a consequence, we observe that the bent functions may not have the best possible $\mathcal{S}$-spectrum. We also show its behaviour under extended affine transformation. The present investigation is a step towards increased understanding of their properties.

Funding Not applicable.

Declarations

Conflict of interest The authors declared that they have no conflict of interest.

References

1. Arfken, G.B., Weber, H.J., Harris, F.E.: Mathematical Methods for Physicists. Elsevier, Amsterdam (2012)
2. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2021)
3. Cusick, T., Stănică, P.: Cryptographic Boolean Functions and Applications, 2nd edn. Elsevier, Amsterdam (2017)
4. Carlet, C., Méaux, P., Rotella, Y.: Boolean functions with restricted input and their robustness; application to the FLIP cipher. IACR Trans. Symmetric Cryptol. **3**, 192–227 (2017). https://doi.org/10.13154/tosc.v2017.i3.192-227
5. Gangopadhyay, S., Gangopadhyay, A.K., Pollatos, S., Stănică, P.: Cryptographic Boolean functions with biased inputs. Cryptogr. Commun. **9**(2), 301–314 (2017). https://doi.org/10.1007/s12095-015-0174-1
6. Gangopadhyay, S., Paul, G., Sinha, N., Stănică, P.: Generalized nonlinearity of S-boxes. Adv. Math. Commun. **12**(1), 115–122 (2018). https://doi.org/10.3934/amc.2018007

7. Maitra, S., Mandal, B., Martinsen, T., Roy, D., Stănică, P.: Analysis on Boolean function in a restricted (biased) domain. IEEE Trans. Inf. Theory **66**(2), 1219–1231 (2020). https://doi.org/10.1109/TIT.2019.2932739
8. Maitra, S., Sarkar, P.: Maximum nonlinearity of symmetric Boolean functions on odd number of variables. IEEE Trans. Inf. Theory **48**(9), 2626–2630 (2002). https://doi.org/10.1109/TIT.2002.801482
9. O'Donnell, R.: Analysis of Boolean Functions. Cambridge University Press, Cambridge (2014)
10. Savický, P.: On the bent Boolean functions that are symmetric. Eur. J. Comb. **15**(4), 407–410 (1994). https://doi.org/10.1006/eujc.1994.1044