Further Results on Bent–Negabent Boolean Functions

Sihem Mesnager, Bachir ben Moussat, and Zepeng Zhuo

1 Introduction

Bent functions are Boolean functions with the highest possible nonlinearity in an even number of variables. They were introduced by Rothaus [19] and already studied first by Dillon [9] and next by many researchers for more than three decades ago. Since 1974, bent functions have been extensively developed for their own sake as interesting combinatorial objects but also due to their significantly important role in cryptography (design of stream ciphers, see, e.g., [3]), coding theory (Reed–Muller codes, Kerdock codes (see, e.g., [7]), two-weight codes [1], codes with a few weights [12], association schemes [17]), sequences (see, e.g., [13]), and graph theory (see, e.g., [16]). The classification of bent functions is still elusive, and therefore not only their characterization, but also their generation is a challenging problem.

A number of recent research works in the theory of bent functions have been devoted to the construction of bent functions. One distinguishes two kinds of con-

S. Mesnager (✉) · B. ben Moussat
Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis, France
e-mail: smesnager@univ-paris8.fr

B. ben Moussat
e-mail: bachir.benmoussat@etud.univ-paris8.fr

S. Mesnager
Laboratory Geometry, Analysis and Applications, LAGA, University Sorbonne Paris Nord, CNRS, UMR 7539, Villetaneuse, F-93430, 91120 Palaiseau, Telecom Paris, France

B. ben Moussat
Laboratory Geometry, Analysis and Applications, LAGA, University Sorbonne Paris Nord, CNRS, UMR 7539, Villetaneuse, France

Z. Zhuo
School of Mathematical Science, Huaibei Normal University, Anhui 235000, Huaibei, China
e-mail: zzp781021@sohu.com

P. Stănică et al. (eds.), *Security and Privacy*, Lecture Notes in Electrical Engineering 744,
https://doi.org/10.1007/978-981-33-6781-4_5

structions of bent functions: primary constructions, which do not need to use previously constructed functions for designing new ones and secondary constructions (of new functions from two or several already known ones). A book devoted to bent functions is [11] and a jubilee survey on bent functions is [4].

The Walsh–Hadamard transform has been exploited extensively for the analysis of Boolean functions and used in coding theory and cryptology [3]. A Boolean function on an even number of variables is bent if and only if the magnitude of all the values in its Walsh–Hadamard spectrum is the same (flat Walsh–Hadamard spectrum). The Walsh–Hadamard transform is an example of a unitary transformation on the space of all Boolean functions. Riera and Parker [18] extended the concept of a bent function to some generalized bent criteria for a Boolean function, where they required that a Boolean function has flat spectrum with respect to one or more transforms from a specified set of unitary transforms. The set of transforms they chose is not arbitrary but is motivated by a choice of local unitary transforms that are central to the structural analysis of pure n-qubit stabilizer quantum states. The transforms they applied are n-fold tensor products of the identity $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the Walsh–Hadamard matrix $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and the nega-Hadamard matrix $N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, where $i^2 = -1$. The Walsh–Hadamard transform can be described as the tensor product of several H's, and the nega-Hadamard transform is constructed from the tensor product of several N's. The nega-Hadamard transform of Boolean functions was first proposed by Parker [14]. As in the case of the Walsh–Hadamard transform, a Boolean function is called negabent if the spectrum under the nega-Hadamard transform is flat. There are some papers about negabent functions in the last few years [10, 20–24, 26–28]. Many bent functions are known, and also some negabent functions are known. For an even number of variables, a function is bent–negabent if it is both bent and negabent. An interesting topic is to investigate the intersection of these two sets, i.e., to construct Boolean functions which are both bent and negabent. The bent–negabent functions were first introduced by Riera and Parker [18]. Some quite interesting results have been found in this topic by the authors mentioned above but there is still a gap between our interest and the results on the literature. The goal of this paper is to push further the study of negabent and bent–negabent by deriving results which help to design more such functions.

The paper is organized as follows. Section 2 aims to bring a background on the notions related to Boolean function needed in the paper. In Sect. 3, we discuss secondary constructions of bent–negabent functions and exhibit one construction based on the well-known indirect construction of bent functions. In Sect. 4, a secondary construction of bent function is revisited and a new method to design secondary construction is exhibited. Section 5 shows how one can design bent–negabent functions from quadratic Boolean functions. In Sect. 6, we provide a characterization of bent–negabent functions in terms of their second-order derivatives. In Sect. 7, we study the sum-of-squares indicator and derive tight lower and upper bounds. Negabent are those whose lower bound on the sum-of-squares indicator is reached.

2 Preliminaries

Let $\mathbb{F}_2$ denote the finite field with two elements. We denote by $\mathcal{B}_n$ the set of all Boolean functions of n-variable, i.e., of all the functions from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. The set of integers, real numbers, and complex numbers are denoted by $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$, respectively. The addition over $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$ is denoted by $+$. The addition over $\mathbb{F}_2^n$ for all $n \geq 1$ is denoted by $\oplus$ (or $+$ if there is no ambiguity). If $z = a + bi \in \mathbb{C}$, then $|z| = \sqrt{a^2 + b^2}$ denotes the absolute value of z, and $\overline{z} = a - bi$ denotes the complex conjugate of z, where $i^2 = -1$, $a, b \in \mathbb{R}$.

The Hamming weight $wt(x)$ of an element $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ is the number of ones in x, i.e., $wt(x) = \sum_{i=1}^{n} x_i$. We say that a Boolean function is balanced if its truth table contains an equal number of 0's and 1's, that is, if its Hamming weight equals $wt(f) = 2^{n-1}$. The Hamming distance between two functions $f(x)$ and $g(x)$, denoted by $d(f, g)$, is the Hamming weight of $f \oplus g$, i.e., $d(f, g) = wt(f \oplus g)$.

Any Boolean function, $f \in \mathcal{B}_n$, is generally represented by its algebraic normal form (ANF)

$$f(x_1, \cdots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u \left(\prod_{i=1}^{n} x_i^{u_i} \right),$$

where $\lambda_u \in \mathbb{F}_2$ and $u = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_2^n$. The algebraic degree of f, denoted by $deg(f)$, is the maximal value of $wt(u)$ such that $\lambda_u \neq 0$. A Boolean function is affine if there exists no term of degree strictly greater than 1 in the ANF and the set of all affine functions is denoted by A_n. An affine function with constant term equal to zero is called a linear function. Any linear function on $\mathbb{F}_2^n$ is denoted by $x \cdot \omega = x_1\omega_1 \oplus x_2\omega_2 \oplus \cdots \oplus x_n\omega_n$, where $x, \omega \in \mathbb{F}_2^n$. The nonlinearity of an n-variable function $f(x)$ is $nl(f) = min_{g \in A_n}(d(f, g))$, i.e., the distance from the set of all n-variable affine functions.

The derivative of $f \in \mathcal{B}_n$ at $\beta \in \mathbb{F}_2^n$, denoted as $D_\beta f$, is defined as $D_\beta f(x) = f(x) + f(x + \beta)$ for all $x \in \mathbb{F}_2^n$. The second-order derivatives $D_\alpha D_\beta f$ at $(\alpha, \beta) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ of a Boolean function f are defined by $D_\alpha D_\beta f(x) = f(x + \alpha + \beta) - f(x + \alpha) - f(x + \beta) + f(x)$.

The Walsh–Hadamard transform of $f \in \mathcal{B}_n$ at $u \in \mathbb{F}_2^n$ is defined by

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

The nega-Hadamard transform of $f \in \mathcal{B}_n$ at $u \in \mathbb{F}_2^n$ is the complex-valued function:

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

Let n be an even positive integer, a function $f \in \mathcal{B}_n$ is a bent function if $|W_f(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$. Similarly, f is called negabent function if $|N_f(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$. If f is both bent and negabent, we say that f is *bent–negabent*.

The concept of a dual bent function is well known. If $f \in \mathcal{B}_n$ is bent, then the dual function $\widetilde{f}$ of f, defined on $\mathbb{F}_2^n$ by $W_f(x) = 2^{n/2}(-1)^{\widetilde{f}(x)}$, is also bent and its own dual is f itself. If f is bent–negabent, then the dual has the same property. We refer to Carlet [3], and Cusick and Stănică [6] for more on cryptographic Boolean functions and to [11] for more about bent functions.

The nega-cross-correlation of f and g at $u \in \mathbb{F}_2^n$ is denoted by

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

In case $f = g$, then the nega-cross-correlation is called the nega-autocorrelation of f at u and denoted by $C_f(u)$. A Boolean function $f \in \mathcal{B}_n$ is negabent if and only if $C_f(u) = 0$ for all $u \neq \mathbf{0}$. If $f(x)$ is an affine function, then for all $u \neq \mathbf{0}$ the nega-autocorrelation $C_f(u) = 0$. This implies that any affine function is negabent.

Definition 1 ([28]) Let $f, g \in \mathcal{B}_n$, the *sum-of-squares* indicator of the nega-cross-correlation between f and g is defined by

$$\sigma_{f,g} = \sum_{u \in \mathbb{F}_2^n} C_{f,g}^2(u).$$

If $f = g$ then $\sigma_{f,f}$ is called the *sum-of-squares* indicator of the nega-autocorrelation of f and denoted by σ_f, i.e.,

$$\sigma_f = \sum_{u \in \mathbb{F}_2^n} C_f^2(u).$$

Note that $C_f(\mathbf{0}) = 2^n$. Thus, $\sigma_f \geq C_f^2(\mathbf{0}) = 2^{2n}$. A Boolean function $f \in \mathcal{B}_n$ is negabent if and only if $C_f(u) = 0$ for all $u \in \mathbb{F}_2^n \setminus \{0\}$. Hence, $\sigma_f \geq 2^{2n}$, where the equality holds if and only if f is negabent function.

3 Secondary Constructions of Bent–Negabent Functions

A secondary construction of bent functions is due to Carlet [2] and is commonly referred to as the indirect sum construction.

Theorem 1 *([2]) Let $f_1(x)$ and $f_2(x)$ be two r-variable bent functions (r even) and let $g_1(y)$ and $g_2(y)$ be two s-variable bent functions (s even). Let $(x, y) \in \mathbb{F}_2^r \times \mathbb{F}_2^s$. Then the function $h(x, y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y)$ is bent and its dual $\widetilde{h(x, y)}$ is obtained from $\widetilde{f_1(x)}$, $\widetilde{f_2(x)}$, $\widetilde{g_1(y)}$ and $\widetilde{g_2(y)}$ by the same formula as $h(x, y)$ is obtained from $f_1(x)$, $f_2(x)$, $g_1(y)$ and $g_2(y)$.*

In this section, we use $h(x, y)$ to construct bent–negabent function. Here we first analyze the nega-Hadamard transform of the function $h(x, y)$.

Lemma 1 *Let* $f_1(x), f_2(x) \in \mathcal{B}_r, g_1(y), g_2(y) \in \mathcal{B}_s$. *Define* $h(x, y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y)$. *Then the nega-Hadamard transform of* $h(x, y)$ *at* $(u, v) \in \mathbb{F}_2^{r+s}$ *is given by*

$$N_h(u, v) = \frac{1}{2}N_{f_1}(u)[N_{g_1}(v) + N_{g_2}(v)] + \frac{1}{2}N_{f_2}(u)[N_{g_1}(v) - N_{g_2}(v)]. \quad (1)$$

Proof By definition, we have

$$\begin{aligned}
N_h(u, v) &= \sum_{(x,y)\in\mathbb{F}_2^{r+s}} (-1)^{h(x,y)\oplus u\cdot x\oplus v\cdot y} i^{wt(x)+wt(y)} \\
&= \sum_{(x,y)\in\mathbb{F}_2^{r+s}:(g_1\oplus g_2)(y)=0} (-1)^{f_1(x)\oplus g_1(y)\oplus u\cdot x\oplus v\cdot y} i^{wt(x)+wt(y)} \\
&+ \sum_{(x,y)\in\mathbb{F}_2^{r+s}:(g_1\oplus g_2)(y)=1} (-1)^{f_2(x)\oplus g_1(y)\oplus u\cdot x\oplus v\cdot y} i^{wt(x)+wt(y)} \\
&= \sum_{y\in\mathbb{F}_2^s:(g_1\oplus g_2)(y)=0} (-1)^{g_1(y)\oplus v\cdot y} i^{wt(y)} \left(\sum_{x\in\mathbb{F}_2^r} (-1)^{f_1(x)\oplus u\cdot x} i^{wt(x)}\right) \\
&+ \sum_{y\in\mathbb{F}_2^s:(g_1\oplus g_2)(y)=1} (-1)^{g_1(y)\oplus v\cdot y} i^{wt(y)} \left(\sum_{x\in\mathbb{F}_2^r} (-1)^{f_2(x)\oplus u\cdot x} i^{wt(x)}\right) \\
&= N_{f_1}(u) \sum_{y\in\mathbb{F}_2^s:(g_1\oplus g_2)(y)=0} (-1)^{g_1(y)\oplus v\cdot y} i^{wt(y)} \\
&+ N_{f_2}(u) \sum_{y\in\mathbb{F}_2^s:(g_1\oplus g_2)(y)=1} (-1)^{g_1(y)\oplus v\cdot y} i^{wt(y)} \\
&= N_{f_1}(u) \sum_{y\in\mathbb{F}_2^s} (-1)^{g_1(y)\oplus v\cdot y} \left(\frac{1 + (-1)^{(g_1\oplus g_2)(y)}}{2}\right) i^{wt(y)} \\
&+ N_{f_2}(u) \sum_{y\in\mathbb{F}_2^s} (-1)^{g_1(y)\oplus v\cdot y} \left(\frac{1 - (-1)^{(g_1\oplus g_2)(y)}}{2}\right) i^{wt(y)} \\
&= \frac{1}{2}\Bigg[N_{f_1}(u) \left(\sum_{y\in\mathbb{F}_2^s} (-1)^{g_1(y)\oplus v\cdot y} i^{wt(y)} + \sum_{y\in\mathbb{F}_2^s} (-1)^{g_2(y)\oplus v\cdot y} i^{wt(y)}\right) \\
&+ N_{f_2}(u) \left(\sum_{y\in\mathbb{F}_2^s} (-1)^{g_1(y)\oplus v\cdot y} i^{wt(y)} - \sum_{y\in\mathbb{F}_2^s} (-1)^{g_2(y)\oplus v\cdot y} i^{wt(y)}\right)\Bigg]
\end{aligned}$$

$$= \frac{1}{2}N_{f_1}(u)[N_{g_1}(v) + N_{g_2}(v)] + \frac{1}{2}N_{f_2}(u)[N_{g_1}(v) - N_{g_2}(v)].$$

This completes the proof. □

In (1), if $f_1(x) = f_2(x)$ or $g_1(y) = g_2(y)$, then $N_h(u, v) = N_{f_1}(u)N_{g_1}(v)$.

Corollary 1 *Let r and s be two even positive integers. Let $f_1(x) \in \mathcal{B}_r$ and $g_1(y) \in \mathcal{B}_s$ be two bent–negabent functions. Then $h(x, y) = f_1(x) \oplus g_1(y)$ is also a bent–negabent function.*

In the following, we propose a necessary and sufficient condition so that the indirect sum construction generates bent–negabent functions in $r + s$ variables, using r and s variable bent–negabent functions as the input functions.

Theorem 2 *Let $f_1(x)$, $f_2(x)$ be two r-variable bent–negabent functions (r even) and let $g_1(y)$, $g_2(y)$ be two s-variable bent–negabent functions (s even). Let $(x, y) \in \mathbb{F}_2^r \times \mathbb{F}_2^s$. Define*

$$h(x, y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y).$$

Then $h(x, y)$ is bent–negabent if and only if $\frac{N_{f_1}(u)}{N_{f_2}(u)} = \pm 1$ or $\frac{N_{g_1}(v)}{N_{g_2}(v)} = \pm 1$, for all $(u, v) \in \mathbb{F}_2^r \times \mathbb{F}_2^s$.

Proof From Theorem 1, we know that $h(x, y)$ is bent. Thus, we need to prove that $\frac{N_{f_1}(u)}{N_{f_2}(u)} = \pm 1$ or $\frac{N_{g_1}(v)}{N_{g_2}(v)} = \pm 1$ if and only if $h(x, y)$ is negabent, that is, $|N_h(u, v)| = 2^{(r+s)/2}$ for all $(u, v) \in \mathbb{F}_2^r \times \mathbb{F}_2^s$.

For simplicity, set $z = N_h(u, v)$, $z_1 = N_{f_1}(u)$, $z_2 = N_{f_2}(u)$, $z_3 = N_{g_1}(v)$, and $z_4 = N_{g_2}(v)$. By Lemma 1, for all $(u, v) \in \mathbb{F}_2^r \times \mathbb{F}_2^s$, we have

$$2z = z_1(z_3 + z_4) + z_2(z_3 - z_4), \tag{2}$$

and

$$2\overline{z} = \overline{z_1}(\overline{z_3} + \overline{z_4}) + \overline{z_2}(\overline{z_3} - \overline{z_4}). \tag{3}$$

Combining (2) and (3), we have

$$\begin{aligned}
4|z|^2 = 4z\overline{z} &= [z_1(z_3 + z_4) + z_2(z_3 - z_4)][\overline{z_1}(\overline{z_3} + \overline{z_4}) + \overline{z_2}(\overline{z_3} - \overline{z_4})] \\
&= z_1\overline{z_1}(z_3\overline{z_3} + z_3\overline{z_4} + \overline{z_3}z_4 + z_4\overline{z_4}) + z_1\overline{z_2}(z_3\overline{z_3} - z_3\overline{z_4} + \overline{z_3}z_4 - z_4\overline{z_4}) \\
&+ \overline{z_1}z_2(z_3\overline{z_3} + z_3\overline{z_4} - \overline{z_3}z_4 - z_4\overline{z_4}) + z_2\overline{z_2}(z_3\overline{z_3} - z_3\overline{z_4} - \overline{z_3}z_4 + z_4\overline{z_4}) \\
&= |z_1|^2(|z_3|^2 + z_3\overline{z_4} + \overline{z_3}z_4 + |z_4|^2) + z_1\overline{z_2}(|z_3|^2 - z_3\overline{z_4} + \overline{z_3}z_4 - |z_4|^2) \\
&+ \overline{z_1}z_2(|z_3|^2 + z_3\overline{z_4} - \overline{z_3}z_4 - |z_4|^2) + |z_2|^2(|z_3|^2 - z_3\overline{z_4} - \overline{z_3}z_4 + |z_4|^2).
\end{aligned}$$

Suppose $h(x, y)$ is negabent $|N_h(u, v)| = 2^{(r+s)/2}$ for all $(u, v) \in \mathbb{F}_2^r \times \mathbb{F}_2^s$ and $|z_1| = |z_2| = 2^{r/2}$, $|z_3| = |z_4| = 2^{s/2}$, we obtain

$$(z_1\overline{z_2} - \overline{z_1}z_2)(z_3\overline{z_4} - \overline{z_3}z_4) = 0,$$

that is, $z_1\overline{z_2} = \overline{z_1}z_2$ or $z_3\overline{z_4} = \overline{z_3}z_4$. Therefore, we have

$$N_{f_1}(u)\overline{N_{f_2}(u)} = \overline{N_{f_1}(u)}N_{f_2}(u)$$

or

$$N_{g_1}(v)\overline{N_{g_2}(v)} = \overline{N_{g_1}(v)}N_{g_2}(v),$$

that is,

$$\frac{N_{f_1}(u)}{N_{f_2}(u)} = \frac{\overline{N_{f_1}(u)}}{\overline{N_{f_2}(u)}} = \overline{\left(\frac{N_{f_1}(u)}{N_{f_2}(u)}\right)}$$

or

$$\frac{N_{g_1}(v)}{N_{g_2}(v)} = \frac{\overline{N_{g_1}(v)}}{\overline{N_{g_2}(v)}} = \overline{\left(\frac{N_{g_1}(v)}{N_{g_2}(v)}\right)},$$

then $\frac{N_{f_1}(u)}{N_{f_2}(u)}$ or $\frac{N_{g_1}(v)}{N_{g_2}(v)}$ is a real number. Since $|N_{f_1}(u)| = |N_{f_2}(u)| = 2^{r/2}$, $|N_{g_1}(v)| = |N_{g_2}(v)| = 2^{s/2}$, we obtain $\frac{N_{f_1}(u)}{N_{f_2}(u)} = \pm 1$ or $\frac{N_{g_1}(v)}{N_{g_2}(v)} = \pm 1$.

Conversely, since $|z_1| = |z_2| = 2^{r/2}$, $|z_3| = |z_4| = 2^{s/2}$, and $\frac{z_1}{z_2} = \pm 1$ or $\frac{z_3}{z_4} = \pm 1$, which implies that $4|z|^2 = 2^{(r+s+2)}$, that is, $|z| = 2^{(r+s)/2}$. Therefore, we have $|N_h(u, v)| = 2^{(r+s)/2}$. This implies that $h(x, y)$ is a negabent function. □

The sufficient condition for the function $h(x, y)$ to be bent–negabent has been given in [26].

Theorem 3 *([26]) Let $f_1(x)$, $f_2(x)$ be two n-variable bent–negabent functions (n even) and let $g_1(y)$, $g_2(y)$ be two m-variable bent–negabent functions (m even). Let $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$. Define $h(x, y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y)$. If $D_{\mathbf{1}}(\widetilde{f_1 \oplus \sigma_2})(x) = D_{\mathbf{1}}(\widetilde{f_2 \oplus \sigma_2})(x)$, then $h(x, y)$ is bent–negabent.*

In the following, we show that the condition $D_{\mathbf{1}}(\widetilde{f_1 \oplus \sigma_2})(x) = D_{\mathbf{1}}(\widetilde{f_2 \oplus \sigma_2})(x)$ is equivalent to the condition $\frac{N_{f_1}(u)}{N_{f_2}(u)} = \pm 1$. We also need the following lemmas.

Lemma 2 *([15])Let n be even and $f(x) \in \mathcal{B}_n$. Then, $f(x)$ is negabent if and only if $f(x) \oplus s_2(x)$ is bent, where $s_2(x) = \bigoplus_{1 \le i < j \le n} x_i x_j$.*

Lemma 2 provides a connection between bent and negabent.

Lemma 3 *([24]) Let $f(x) \in \mathcal{B}_n$, then*

$$N_f(u) = \frac{W_{f \oplus s_2}(u) + W_{f \oplus s_2}(\overline{u})}{2} + i \cdot \frac{W_{f \oplus s_2}(u) - W_{f \oplus s_2}(\overline{u})}{2}.$$

Lemma 3 explores a direct link between the Walsh–Hadamard transform and the nega-Hadamard transform. These properties are an important tool to analyze the properties of negabent functions.

Theorem 4 *Let $f_1(x)$ and $f_2(x)$ be two r-variable negabent functions (r even). Then $\frac{N_{f_1}(u)}{N_{f_2}(u)} = \pm 1$ if and only if $D_{\mathbf{1}}(\widetilde{f_1 \oplus s_2})(u) = D_{\mathbf{1}}(\widetilde{f_2 \oplus s_2})(u)$, $u \in \mathbb{F}_2^r$.*

Proof Since $\frac{N_{f_1}(u)}{N_{f_2}(u)} = \pm 1$, then $N_{f_1}(u) = \pm N_{f_2}(u)$. By Lemma 3, we have

$$\begin{aligned}&\frac{W_{f_1\oplus s_2}(u) + W_{f_1\oplus s_2}(\overline{u})}{2} + i \cdot \frac{W_{f_1\oplus s_2}(u) - W_{f_1\oplus s_2}(\overline{u})}{2}\\ &= \pm\frac{W_{f_2\oplus s_2}(u) + W_{f_2\oplus s_2}(\overline{u})}{2} \pm i \cdot \frac{W_{f_2\oplus s_2}(u) - W_{f_2\oplus s_2}(\overline{u})}{2}.\end{aligned}$$

Hence

$$\frac{W_{f_1\oplus s_2}(u) + W_{f_1\oplus s_2}(\overline{u})}{2} = \pm\frac{W_{f_2\oplus s_2}(u) + W_{f_2\oplus s_2}(\overline{u})}{2},$$

$$\frac{W_{f_1\oplus s_2}(u) - W_{f_1\oplus s_2}(\overline{u})}{2} = \pm\frac{W_{f_2\oplus s_2}(u) - W_{f_2\oplus s_2}(\overline{u})}{2},$$

then

$$W_{f_1\oplus s_2}(u) = \pm W_{f_2\oplus s_2}(u),\ W_{f_1\oplus s_2}(\overline{u}) = \pm W_{f_2\oplus s_2}(\overline{u}).$$

Recall that $W_f(u) = 2^{r/2}(-1)^{\widetilde{f}(u)}$, we get

$$(-1)^{\widetilde{f_1\oplus s_2}(u)\oplus\widetilde{f_1\oplus s_2}(\overline{u})} = (-1)^{\widetilde{f_2\oplus s_2}(u)\oplus\widetilde{f_2\oplus s_2}(\overline{u})}.$$

Thus, $D_{\mathbf{1}}(\widetilde{f_1 \oplus s_2})(u) = D_{\mathbf{1}}(\widetilde{f_2 \oplus s_2})(u)$.

Conversely, since $D_{\mathbf{1}}(\widetilde{f_1 \oplus s_2})(u) = D_{\mathbf{1}}(\widetilde{f_2 \oplus s_2})(u)$, then

$$\widetilde{f_1 \oplus s_2}(u) \oplus \widetilde{f_2 \oplus s_2}(\overline{u}) = \widetilde{f_1 \oplus s_2}(\overline{u}) \oplus \widetilde{f_2 \oplus s_2}(u).$$

Hence

$$W_{f_1\oplus s_2}(u)W_{f_2\oplus s_2}(\overline{u}) = W_{f_1\oplus s_2}(\overline{u})W_{f_2\oplus s_2}(u).$$

Since $f_1 \oplus s_2$, $f_2 \oplus s_2$ are bent functions, we have $|W_{f_1\oplus s_2}(u)| = |W_{f_2\oplus s_2}(u)| = 2^{r/2}$, then $W_{f_1\oplus s_2}(u) = \pm W_{f_2\oplus s_2}(u)$, $W_{f_1\oplus s_2}(\overline{u}) = \pm W_{f_2\oplus s_2}(\overline{u})$. Thus, according to the similar discussion above, we obtain $\frac{N_{f_1}(u)}{N_{f_2}(u)} = \pm 1$. □

The functions $f(x)$ and $g(x)$ are said to have *complementary nega-autocorrelation* if for all nonzero $u \in \mathbb{F}_2^n$, $C_f(u) + C_g(u) = 0$. The relationship between the nega-autocorrelations of $f(x)$, $g(x)$ and their nega-Hadamard transforms has been given in [22] as follows.

Lemma 4 *([22]) The functions $f(x), g(x) \in \mathcal{B}_n$ have complementary nega-autocorrelations if and only if*

$$|N_f(u)|^2 + |N_g(u)|^2 = 2^{n+1}.$$

The following corollary is a direct consequence from Definition 1, Theorem 2, and Lemma 4.

Corollary 2 *Let $f_1(x), f_2(x) \in \mathcal{B}_n$. If $\frac{N_{f_1}(u)}{N_{f_2}(u)} = 1$ for all $u \in \mathbb{F}_2^n$, then the following statements are equivalent.*

1. *$f_1(x), f_2(x)$ are negabent functions.*
2. *$|N_{f_1}(u)|^2 + |N_{f_2}(u)|^2 = 2^{n+1}$.*
3. *$f_1(x)$ and $f_2(x)$ have complementary nega-autocorrelations.*

4 A Secondary Construction Revisited

Recently, a secondary construction of bent functions whose duals satisfy a certain property [25] [Theorem 5.1] has been proposed:

Theorem 5 *Let f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ be bent. Let $\beta_1, \ldots, \beta_r$ be points of $\mathbb{F}_2^n$. Let F be a Boolean function from $\mathbb{F}_2^r$ to $\mathbb{F}_2$. Suppose that its dual $\tilde{f}$ satisfies: there exists Boolean functions $g_1, \ldots, g_r$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ such that*

$$\tilde{f}(u + \sum_{i=1}^{r} w_i \beta_i) = \tilde{f}(u) + \sum_{i=1}^{r} w_i g_i(u) \tag{4}$$

for every $u \in \mathbb{F}_2^n$ and $(w_1, \ldots, w_r) \in \mathbb{F}_2^r$. Then, the Boolean function h from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ defined at any point $x \in \mathbb{F}_2^n$ as

$$h(x) = f(x) + F(\beta_1 \cdot x, \ldots, \beta_r \cdot x)$$

is bent and its dual is at any point $x \in \mathbb{F}_2^n$ equal to

$$\tilde{h}(x) = \tilde{f}(x) + F(g_1(x), \ldots, g_r(x)).$$

Let us now show that Condition (4) of the above theorem can be rewritten in terms of derivatives of the dual function of f. Recall that the derivative at point $\beta \in \mathbb{F}_2^n$ of a Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, denoted as $D_\beta f$, is defined at any point $x \in \mathbb{F}_2^n$ as $D_\beta f(x) = f(x) + f(x + \beta)$. We introduce now a notation to denote derivatives of higher order. Let k be a positive integer and $\beta_1, \cdots, \beta_k$ be k elements of $\mathbb{F}_2^n$. Then, the kth-derivative of f at $(\beta_1, \ldots, \beta_k) \in \left(\mathbb{F}_2^n\right)^k$ is denoted by $D^k_{\beta_1, \ldots, \beta_k} f = D_{\beta_1} \cdots D_{\beta_k} f$. Now, note that, for $w \in \mathbb{F}_2$,

$$f(x+w\beta) = f(x) + D_{w\beta}f(x) = f(x) + wD_\beta f(x).$$

If we iterate the above identity, we get that, for $(w_1, \ldots, w_r) \in \mathbb{F}_2^r$,

$$f(x+\sum_{i=1}^{r} w_i\beta_i) = f(x) + \sum_{i=1}^{r} w_i D_{\beta_i} f(x) + \sum_{k=2}^{r} \sum_{a\in\mathbb{F}_2^r, wt(a)=k} w^a D_{\beta_a}^k f(x),$$

where $w^a = \prod_{i=1}^{r} w_i^{a_i}$ and $\beta_a = (\beta_{a_{i_1}}, \ldots, \beta_{a_{i_k}}) \in \mathbb{F}_2^k$ where $1 \le i_1 < \cdots < i_k \le r$ are the indexes such that $a_i = 1$. Therefore, Condition (4) is equivalent to say that, for $k \ge 2$, any kth-derivative with respect to any subset of $\{\beta_1, \ldots, \beta_r\}$ of the dual function $\tilde{f}$ of f vanishes on $\mathbb{F}_2^n$. Therefore, Theorem 5 can be rewritten as follows.

Theorem 6 *Let f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ be a Boolean bent function. Let $\beta_1, \ldots, \beta_r$ be points of $\mathbb{F}_2^n$. Suppose that, for any positive integer $2 \le k \le r$, all the kth-order derivatives of the dual of f relatively to subsets of $\{\beta_1, \ldots, \beta_r\}$ of size k vanish on $\mathbb{F}_2^n$. Let F be a Boolean function from $\mathbb{F}_2^r$ to $\mathbb{F}_2$. Then, the Boolean function h from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ defined at any point $x \in \mathbb{F}_2^n$ as*

$$h(x) = f(x) + F(\beta_1 \cdot x, \ldots, \beta_r \cdot x)$$

is bent and its dual is

$$\tilde{h}(x) = \tilde{f}(x) + F(D_{\beta_1}\tilde{f}(x), \ldots, D_{\beta_r}\tilde{f}(x)).$$

5 Bent–Negabent Functions From Quadratic Functions

5.1 Generalities

Let f be a quadratic Boolean function whose algebraic normal form

$$f(x) = \sum_{1\le i<j\le n} a_{ij}x_ix_j + \sum_{i=1}^{n} b_ix_i + c = x\cdot(\mathbf{M}x) + b\cdot x + c, \tag{5}$$

where $\mathbf{M} = (a_{ij})_{1\le i,j\le n}$ is a square matrix of size n whose entries are in $\mathbb{F}_2$ and whose entries are equal to 0 if $i \ge j$, $b \in \mathbb{F}_2^n$, and $c \in \mathbb{F}_2$. We denote $\mathbf{B}^\star$ the transpose matrix of $\mathbf{B}$ and $\mathbf{B}^{-1}$ the inverse of $\mathbf{B}$ (if $\mathbf{B}$ is of full rank). Finally, we denote $\mathbf{I}$ the identity matrix of size n. Define a symmetric square matrix of size n as $\mathbf{A} = \mathbf{M} + \mathbf{M}^\star$. Then, one has

Theorem 7 *([15]) f is bent if and only if $\mathbf{A}$ is of maximal rank.*

One can compute explicitly the dual of f.

Proposition 1 *A quadratic Boolean function f of the form (5) is bent if and only if $\mathbf{A} = \mathbf{M} + \mathbf{M}^\star$ is of full rank and the dual of f is $\tilde{f}(x) = f(\mathbf{A}^{-1}x) + f(0) + \varepsilon_f$ at any point $x \in \mathbb{F}_2^n$ where $\varepsilon_f = 0$ if $wt(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ and 1 if $wt(f) = 2^{n-1} + 2^{\frac{n}{2}-1}$.*

Proof The necessary and sufficient condition for bentness of f is a well-known result ([15]). We now show that the dual of f can be explicitly computed. Indeed,

$$\begin{aligned}
W_f(u) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+u\cdot x} \\
&= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x+\mathbf{A}^{-1}u)+u\cdot(x+\mathbf{A}^{-1}u)} \\
&= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+f(\mathbf{A}^{-1}u)+(\mathbf{A}\mathbf{A}^{-1}u)\cdot x+f(0)+u\cdot x+u\cdot\mathbf{A}^{-1}u} \\
&= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+f(\mathbf{A}^{-1}u)+u\cdot\mathbf{A}^{-1}u+f(0)} \quad (\text{since } (\mathbf{A}\mathbf{A}^{-1}u)\cdot x = u\cdot x) \\
&= (-1)^{f(\mathbf{A}^{-1}u)+u\cdot\mathbf{A}^{-1}u+f(0)} \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)} \\
&= (-1)^{f(\mathbf{A}^{-1}u)+u\cdot\mathbf{A}^{-1}u+f(0)} \widehat{\chi_f}(0) \\
&= (-1)^{(\mathbf{A}^{-1}u)\cdot(\mathbf{M}\mathbf{A}^{-1}u)+b\cdot(\mathbf{A}^{-1}u)+(\mathbf{A}\mathbf{A}^{-1}u)\cdot\mathbf{A}^{-1}u} \times 2^{\frac{n}{2}}(-1)^{\varepsilon_f} \\
&= 2^{\frac{n}{2}}(-1)^{(\mathbf{A}^{-1}u)\cdot((\mathbf{M}+\mathbf{A})\mathbf{A}^{-1}u)+b\cdot(\mathbf{A}^{-1}u)+\varepsilon_f} \\
&= 2^{\frac{n}{2}}(-1)^{(\mathbf{A}^{-1}u)\cdot(\mathbf{M}^\star\mathbf{A}^{-1}u)+b\cdot(\mathbf{A}^{-1}u)+\varepsilon_f} \\
&= 2^{\frac{n}{2}}(-1)^{(\mathbf{M}\mathbf{A}^{-1}u)\cdot(\mathbf{A}^{-1}u)+b\cdot(\mathbf{A}^{-1}u)+\varepsilon_f} \\
&= 2^{\frac{n}{2}}(-1)^{f(\mathbf{A}^{-1}u)+f(0)+\varepsilon_f}.
\end{aligned}$$

□

Note that one can associate likewise the symmetric square matrix $\mathbf{I} + \mathbf{J}$ of size n to the quadratic function s_2 where $\mathbf{I}$ is the identity matrix of size n and $\mathbf{J}$ the square matrix of size n whose all entries are equal to 1. The polar form of s_2 is then $x \cdot ((\mathbf{I} + \mathbf{J})y)$. Then one has

Theorem 8 *([15]) f is bent–negabent if and only if $\mathbf{A}$ and $\mathbf{A} + \mathbf{I} + \mathbf{J}$ are both of maximal rank.*

5.2 Secondary Constructions of Bent and Negabent Functions

5.2.1 Symplectic Forms

Let V be a symplectic vector space over a field F. A mapping σ from $V \times V$ to F is said to be a symplectic form if it is

1 symmetric: $\sigma(x, y) = -\sigma(y, x)$ for any $(x, y) \in V \times V$ (in characteristic two, skew symmetry and symmetry coincides);
2 totally isotropic: $\sigma(x, x) = 0$ for any $x \in V$;
3 non-degenerate: if $\sigma(u, v) = 0$ for any $v \in V$ then $u = 0$.

Then, (V, σ) denotes the vector space V equipped with a symplectic form. Let δ_{ij} be the Kronecker index: $\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ii} = 1$. Suppose that $\dim(V) = 2n$.

Definition 2 A *symplectic basis* for (V, σ) is a basis $v_1, \cdots, v_n, w_1, \ldots, w_n$ such that

$$\sigma(v_i, w_j) = \delta_{ij}, \sigma(v_i, v_j) = \sigma(w_i, w_j) = 0$$

for any $1 \leq i, j \leq r$ (where $\delta_{ij} = 1$ if $i = j$ and 0 otherwise).

5.2.2 Secondary Constructions

A Boolean function f is said to be quadratic if and only if

$$\phi(x, y) = f(x + y) + f(x) + f(y) + f(0)$$

is bilinear, symmetric, and symplectic. The bilinear map ϕ is called the polar form of f. Write f as (5). Observe that

$$\begin{aligned} \phi(x, y) &= x \cdot (\mathbf{M}y) + (\mathbf{M}x) \cdot y \\ &= x \cdot (\mathbf{M}y) + x \cdot (\mathbf{M}^{\star}y) \\ &= x \cdot (\mathbf{A}y). \end{aligned} \tag{6}$$

The dual of a quadratic bent function is again a quadratic bent function (see Proposition 1). On the other hand, notice that the polar form at point (a, b) coincides with the second-order derivative $D_a D_b f$. Then, Theorem 6 is rewritten as

Corollary 3 *Let f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ be a quadratic bent function. Denote $\tilde{\phi}$ the polar form of the quadratic part of the dual of f. Let $\beta_1, \ldots, \beta_r$ be points of $\mathbb{F}_2^n$ such that $\tilde{\phi}(\beta_i, \beta_j) = 0$ for $1 \leq i < j \leq r$. Let F be a Boolean function from $\mathbb{F}_2^r$ to $\mathbb{F}_2$. Then, the Boolean function h from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ defined at any point $x \in \mathbb{F}_2^n$ as*

$$h(x) = f(x) + F(\beta_1 \cdot x, \ldots, \beta_r \cdot x)$$

is bent.

Now, according to Proposition 1, the polar form associated to the dual of f is

$$\tilde{\phi}(x, y) = \phi(\mathbf{A}^{-1}x, \mathbf{A}^{-1}y) = (\mathbf{A}^{-1}x) \cdot y = x \cdot (\mathbf{A}^{-1}y). \tag{7}$$

Therefore,

Corollary 4 *Let f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ be a quadratic bent function of the form (5). Let $\beta_1, \ldots, \beta_r$ be points of $\mathbb{F}_2^n$ such that $\beta_i \cdot (\mathbf{A}^{-1})\beta_j = 0$ for $1 \leq i < j \leq r$. Let F be a Boolean function from $\mathbb{F}_2^r$ to $\mathbb{F}_2$. Then, the Boolean function h from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ defined at any point $x \in \mathbb{F}_2^n$ as*

$$h(x) = f(x) + F(\beta_1 \cdot x, \ldots, \beta_r \cdot x)$$

is bent.

Remark 1 Let $n = 2k$. Observe that ϕ is a symplectic form over $\mathbb{F}_2^n$. Thus, if $\{e_1, \ldots, e_k, f_1, \ldots, f_k\}$ is a symplectic basis of $(\mathbb{F}_2^n, \phi)$ then one can take $\{\beta_1, \ldots, \beta_r\} = \{\mathbf{A}e_i, i \in I\} \cup \{\mathbf{A}f_j, j \in J\}$ with $I \cap J = \emptyset$ and $I \cup J \subset \{1, \ldots, k\}$. The so-constructed bent function is then of algebraic degree r.

Next, observe that the polar form associated to $f + s_2$ is

$$\psi(x, y) = x \cdot ((\mathbf{A} + \mathbf{I} + \mathbf{J})y) \tag{8}$$

and thus, by the same calculation as for f, we get that the polar form of its dual is

$$\tilde{\psi}(x, y) = x \cdot ((\mathbf{A} + \mathbf{I} + \mathbf{J})^{-1}y). \tag{9}$$

Therefore,

Corollary 5 *Let f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ be a quadratic negabent function of the form (5). Let $\gamma_1, \ldots, \gamma_r$ be points of $\mathbb{F}_2^n$ such that $\gamma_i \cdot ((\mathbf{A} + \mathbf{I} + \mathbf{J})^{-1}\gamma_j) = 0$ for $1 \leq i < j \leq r$. Let F be a Boolean function from $\mathbb{F}_2^r$ to $\mathbb{F}_2$. Then, the Boolean function h from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ defined at any point $x \in \mathbb{F}_2^n$ as*

$$h(x) = f(x) + F(\gamma_1 \cdot x, \ldots, \gamma_r \cdot x)$$

is negabent.

Remark 2 Like in Remark 1, one can deduce from a symplectic basis of $(\mathbb{F}_2^n, \psi)$ a set $\{\gamma_1, \ldots, \gamma_r\}$ which satisfies the condition of the above corollary.

6 A Characterization of Bent–Negabent Functions Through Their Second-Order Derivatives

A useful tool to study a Boolean function $f(x)$ is derivative. The derivatives play an important role in cryptography, related to the differential attack. They are also naturally involved in the definition of the strict avalanche criterion and the propagation

criterion. These criteria evaluate some kind of diffusion of the function. Carlet and Prouff [5] gave a characterization of bent functions via their second-order derivatives as follows.

Lemma 5 *([5])A Boolean function $f(x)$ defined on $\mathbb{F}_2^n$ is bent if and only if*

$$\forall x \in \mathbb{F}_2^n, \sum_{a,b\in\mathbb{F}_2^n} (-1)^{D_a D_b f(x)} = 2^n.$$

Inspired by the work of [10], we present a characterization of bent–negabent functions, which is related to the second-order derivatives in the following.

Theorem 9 *Let $f(x)$ be n-variable bent function (n even). Then $f(x)$ is bent–negabent if and only if for all $b \in \mathbb{F}_2^n$*

$$\sum_{a\in\mathbb{F}_2^n : a\cdot b=0} (-1)^{D_a D_b f(x)} = 2^n, \quad \sum_{a\in\mathbb{F}_2^n : a\cdot b=1} (-1)^{D_a D_b f(x)} = 0$$

when $wt(b)$ is even, and

$$\sum_{a\in\mathbb{F}_2^n : a\cdot \bar{b}=0} (-1)^{D_a D_b f(x)} = 2^n, \quad \sum_{a\in\mathbb{F}_2^n : a\cdot \bar{b}=1} (-1)^{D_a D_b f(x)} = 0$$

when $wt(b)$ is odd.

Proof By Lemma 2, $f(x)$ is bent–negabent if and only if $f(x)$ and $f(x) \oplus s_2(x)$ are both bent, i.e., for $\forall x \in \mathbb{F}_2^n$,

$$\sum_{a,b\in\mathbb{F}_2^n} (-1)^{D_a D_b f(x)} = 2^n \text{ and } \sum_{a,b\in\mathbb{F}_2^n} (-1)^{D_a D_b (f(x)\oplus s_2(x))} = 2^n. \tag{10}$$

Since

$$\begin{aligned} D_a D_b \sigma_2(x) &= s_2(x) \oplus s_2(x \oplus a) \oplus s_2(x \oplus b) \oplus s_2(x \oplus a \oplus b) \\ &= \bigoplus_{1\le i\le n} a_i \Big(\bigoplus_{1\le j\le n, j\neq i} b_j \Big), \end{aligned}$$

so

$$D_a D_b s_2(x) = \begin{cases} a \cdot b, & \text{if } wt(b) \text{ is even}, \\ a \cdot \bar{b}, & \text{if } wt(b) \text{ is odd}. \end{cases}$$

From the second part of (10), we get

$$\sum_{a,b\in\mathbb{F}_2^n} (-1)^{D_a D_b f(x)} (-1)^{D_a D_b s_2(x)} = 2^n.$$

If $wt(b)$ is even, then

$$\sum_{a\in\mathbb{F}_2^n:a\cdot b=0}(-1)^{D_aD_bf(x)}-\sum_{a\in\mathbb{F}_2^n:a\cdot b=1}(-1)^{D_aD_bf(x)}=2^n. \tag{11}$$

If $wt(b)$ is odd, then

$$\sum_{a\in\mathbb{F}_2^n:a\cdot \bar{b}=0}(-1)^{D_aD_bf(x)}-\sum_{a\in\mathbb{F}_2^n:a\cdot \bar{b}=1}(-1)^{D_aD_bf(x)}=2^n. \tag{12}$$

From the first part of (10), we obtain

$$\sum_{a\in\mathbb{F}_2^n:a\cdot b=0}(-1)^{D_aD_bf(x)}+\sum_{a\in\mathbb{F}_2^n:a\cdot b=1}(-1)^{D_aD_bf(x)}=2^n, \tag{13}$$

for all $b\in\mathbb{F}_2^n$. By (11)–(13), we have

$$\sum_{a\in\mathbb{F}_2^n:a\cdot b=0}(-1)^{D_aD_bf(x)}=2^n,\quad \sum_{a\in\mathbb{F}_2^n:a\cdot b=1}(-1)^{D_aD_bf(x)}=0$$

when $wt(b)$ is even, and

$$\sum_{a\in\mathbb{F}_2^n:a\cdot \bar{b}=0}(-1)^{D_aD_bf(x)}=2^n,\quad \sum_{a\in\mathbb{F}_2^n:a\cdot \bar{b}=1}(-1)^{D_aD_bf(x)}=0$$

when $wt(b)$ is odd. This completes the proof. □

7 An Upper Bound on the Sum-of-Squares Indicator $\sigma_{f,g}$

In order to find the upper bound on the sum-of-squares indicator $\sigma_{f,g}$ for a given two n-variable Boolean functions f and g, we study some properties of the cross-correlation function. We firstly give the sum-of-squares indicators σ_f of $s_2(x)=\bigoplus_{1\le i<j\le n}x_ix_j$ in the following.

Proposition 2 *Let $s_2(x)=\bigoplus_{1\le i<j\le n}x_ix_j$ be the elementary symmetric Boolean function in n variables of degree 2. Then*

$$C_{s_2}(u)=\begin{cases}\pm 2^n, & \text{if } wt(u) \text{ is even,}\\ 0, & \text{if } wt(u) \text{is odd}\end{cases}$$

and $\sigma_f=2^{3n-1}$.

Proof Since

$$\begin{aligned} s_2(x) \oplus s_2(x \oplus u) &= \bigoplus_{1 \le i < j \le n} x_i x_j \oplus \bigoplus_{1 \le i < j \le n} (x_i \oplus u_i)(x_j \oplus u_j) \\ &= \bigoplus_{1 \le i < j \le n} (x_i u_j \oplus x_j u_i \oplus u_i u_j) \\ &= \bigoplus_{1 \le i < j \le n} (x_i u_j \oplus x_j u_i) \oplus \bigoplus_{1 \le i < j \le n} u_i u_j \\ &= \bigoplus_{1 \le i \le n} \left(x_i \bigoplus_{1 \le j \le n, j \ne i} u_j \right) \oplus s_2(u), \end{aligned}$$

thus,

$$s_2(x) \oplus s_2(x \oplus u) = \begin{cases} u \cdot x \oplus s_2(u), \text{ if } wt(u) \text{is even}, \\ \overline{u} \cdot x \oplus s_2(u), \text{ if } wt(u) \text{ is odd}. \end{cases}$$

According to the definitions of the nega-autocorrelation and sum-of-squares indicator, we have

$$C_{s_2}(u) = \begin{cases} \sum_{x \in \mathbb{F}_2^n} (-1)^{s_2(u)} = \pm 2^n, \text{ if } wt(u) \text{ is even}, \\ \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathbf{1} \cdot x + s_2(u)} = 0, \text{ if } wt(u) \text{ is odd} \end{cases}$$

and

$$\sigma_f = \sum_{u \in \mathbb{F}_2^n : wt(u) \text{ even}} C_f^2(u) + \sum_{u \in \mathbb{F}_2^n : wt(u) \text{ odd}} C_f^2(u) = 2^{3n-1}.$$

This proves the result. □

Lemma 6 *([28]) Let $f(x), g(x) \in \mathcal{B}_n$. Then*

$$\sigma_{f,g} = \sum_{u \in \mathbb{F}_2^n} C_{f,g}^2(u) = \sum_{v \in \mathbb{F}_2^n} C_f(v) C_g(v). \tag{14}$$

Remark 3 If we use *Cauchy's inequality* $(\sum_i a_i b_i)^2 \le \sum_i a_i^2 \sum_i b_i^2$ to the sum on the right-hand side of (8), we get

$$\begin{aligned} \sigma_{f,g} &= \sum_{u \in \mathbb{F}_2^n} C_{f,g}^2(u) = \sum_{v \in \mathbb{F}_2^n} C_f(v) C_g(v) \\ &\le \left(\sum_{v \in \mathbb{F}_2^n} C_f^2(v) \right)^{\frac{1}{2}} \left(\sum_{v \in F_2^n} C_g^2(v) \right)^{\frac{1}{2}} \\ &= \sigma_f^{\frac{1}{2}} \sigma_g^{\frac{1}{2}} = \sqrt{\sigma_f \sigma_g}, \end{aligned}$$

i.e., $\sigma_{f,g} \leq \sqrt{\sigma_f \sigma_g}$. Furthermore, for n-variable negabent functions $f(x)$ and $g(x)$, $\sigma_{f,g} = 2^{2n}$.

In order to give the upper bound on $\sigma_{f,g}$, we need the following important results.

Lemma 7 *([22]) Let $f(x), g(x) \in \mathcal{B}_n$. Then*

$$C_{f,g}(v) = 2^{-n} i^{wt(v)} \sum_{u \in \mathbb{F}_2^n} N_f(u) \overline{N_g(u)} (-1)^{u \cdot v}.$$

Lemma 8 *Let $f(x), g(x) \in \mathcal{B}_n$. Then*

$$\sum_{u \in \mathbb{F}_2^n} |N_f(u)|^2 |N_g(u)|^2 = 2^n \sum_{v \in \mathbb{F}_2^n} C_{f,g}^2(v).$$

Proof By Lemma 7, we have

$$\overline{N_f(u)} N_g(u) = \sum_{v \in \mathbb{F}_2^n} C_{f,g}(v) (-1)^{u \cdot v} i^{wt(v)}$$

and

$$\begin{aligned} |N_f(u)|^2 |N_g(u)|^2 &= \left(\sum_{v \in \mathbb{F}_2^n} C_{f,g}(v) (-1)^{u \cdot v} i^{-wt(v)} \right) \cdot \left(\sum_{w \in \mathbb{F}_2^n} C_{f,g}(w) (-1)^{u \cdot w} i^{wt(w)} \right) \\ &= \sum_{v,w \in \mathbb{F}_2^n} C_{f,g}(v) C_{f,g}(w) (-1)^{u \cdot (v \oplus w)} i^{wt(w) - wt(v)} \\ &= \sum_{v \in \mathbb{F}_2^n} C_{f,g}^2(v) + \sum_{v,w \in \mathbb{F}_2^n : v \neq w} C_{f,g}(v) C_{f,g}(w) (-1)^{u \cdot (v \oplus w)} i^{wt(w) - wt(v)}. \end{aligned}$$

Thus

$$\begin{aligned} \sum_{u \in \mathbb{F}_2^n} |N_f(u)|^2 |N_g(u)|^2 &= \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^n} C_{f,g}^2(v) \\ &\quad + \sum_{u \in \mathbb{F}_2^n} \sum_{v,w \in \mathbb{F}_2^n : v \neq w} C_{f,g}(v) C_{f,g}(w) (-1)^{u \cdot (v \oplus w)} i^{wt(w) - wt(v)} \\ &= 2^n \sum_{v \in \mathbb{F}_2^n} C_{f,g}^2(v) \\ &\quad + \sum_{v,w \in \mathbb{F}_2^n : v \neq w} C_{f,g}(v) C_{f,g}(w) \sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot (v \oplus w)} i^{wt(w) - wt(v)}, \end{aligned}$$

since $v \neq w$, $\sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot (v \oplus w)} = 0$, thus

$$\sum_{u\in\mathbb{F}_2^n} |N_f(u)|^2|N_g(u)|^2 = 2^n \sum_{v\in\mathbb{F}_2^n} C_{f,g}^2(v).$$

This proves the result. □

If we take $f(x) = g(x)$ in the previous lemma, then we have

$$\sum_{u\in\mathbb{F}_2^n} |N_f(u)|^4 = 2^n \sum_{v\in\mathbb{F}_2^n} C_f^2(v). \tag{15}$$

Theorem 10 *Let $f(x), g(x) \in \mathcal{B}_n$. Then $\sigma_{f,g} \leq 2^{3n}$, with equality if and only if there exists $u_0 \in \mathbb{F}_2^n$ such that $|N_f(u_0)| = |N_g(u_0)| = 2^n$.*

Proof By Lemma 8 and *Nega-Parseval's Identity* $\sum_{u\in\mathbb{F}_2^n} |N_f(u)|^2 = 2^{2n}$, we have

$$\begin{aligned}\sigma_{f,g} &= \frac{1}{2^n} \sum_{u\in\mathbb{F}_2^n} |N_f(u)|^2|N_g(u)|^2 \\ &\leq \frac{1}{2^n} \left[\sum_{u\in\mathbb{F}_2^n} |N_f(u)|^2\right] \cdot \left[\sum_{u\in\mathbb{F}_2^n} |N_g(u)|^2\right] = 2^{3n}.\end{aligned}$$

We know $\sigma_{f,g} = 2^{3n}$ if and only if

$$\sum_{u\in\mathbb{F}_2^n} |N_f(u)|^2|N_g(u)|^2 = \sum_{u\in\mathbb{F}_2^n} |N_f(u)|^2 \sum_{u\in\mathbb{F}_2^n} |N_g(u)|^2,$$

that is,

$$\sum_{u,v\in\mathbb{F}_2^n, u\neq v} |N_f(u)|^2|N_g(v)|^2 = 0$$

if and only if $|N_f(u)|^2|N_g(v)|^2 = 0$ for any $u \neq v$. There are three cases:

(i) If there does not exist $u_0 \in \mathbb{F}_2^n$ such that $|N_f(u_0)|^2 \neq 0$, then $|N_f(u)|^2 = 0$ for all $u \in \mathbb{F}_2^n$, which leads to a contradiction with *Nega-Parseval's Identity*.

(ii) If there exists only one $u_0 \in \mathbb{F}_2^n$ such that $|N_f(u_0)|^2 \neq 0$, then $|N_g(v)|^2 = 0$ for all $v \neq u_0$. According to *Nega-Parseval's Identity*, we have $|N_f(u_0)|^2 = 2^{2n}$, i.e., $|N_f(u_0)| = 2^n$. On the other hand, we have $|N_g(u_0)|^2 = 2^{2n}$, i.e., $|N_g(u_0)| = 2^n$.

(iii) If there exist only two $u_1, u_2 \in \mathbb{F}_2^n (u_1 \neq u_2)$ such that $|N_f(u_1)|^2 \neq 0$ and $|N_f(u_2)|^2 \neq 0$, then we have $|N_g(v)|^2 = 0$ for all $v \neq u_1$ and $|N_g(v)|^2 = 0$ for all $v \neq u_2$. It implies that $|N_g(v)|^2 = 0$ for all $v \in \mathbb{F}_2^n$, which is in contradiction with *Nega-Parseval's Identity*. By the same way, we know that there does not exist only $k (3 \leq k \leq 2^n)$ different elements $u_i \in \mathbb{F}_2^n (1 \leq i \leq k)$ such that $|N_f(u_0)|^2 \neq 0$. □

Based on Theorem 10, we give tight lower and upper bounds on σ_f.

Corollary 6 *Let $f(x) \in \mathcal{B}_n$. Then*

(1) $2^{2n} \leq \sigma_f \leq 2^{3n}$;
(2) $\sigma_f = 2^{2n}$ *if and only if f is a negabent function;*
(3) $\sigma_f = 2^{3n}$ *if and only if there exists* $u_0 \in \mathbb{F}_2^n$ *such that* $|N_f(u_0)| = 2^n$.

Remark 4 Let $\Re(N_f(u_0))$ be the *real part* and $\Im(N_f(u_0))$ be the *imaginary part* of $N_f(u_0)$. Then $\Re(N_f(u_0))$ or $\Im(N_f(u_0))$ must be integer and $|N_f(u_0)|^2 = 2^{2n}$ must be a sum of two squares. From *Jacobi's Two-Squares Theorem* we know that $(2^n)^2 + 0^2 = 2^{2n}$. Thus, $(|\Re(N_f(u_0))|, |\Im(N_f(u_0))|) = (2^n, 0)$ or $(0, 2^n)$, i.e., either $\Re(N_f(u_0))$ or $\Im(N_f(u_0))$ must be zero.

8 Conclusion

In this paper, we have pushed further the theory of the so-called negabent and bent–negabent functions and derived results, which included methods of secondary constructions and characterizations.

References

1. Calderbank R, Kantor WM (1986) The geometry of two-weight codes. Bull Lond Math Soc 18(2):97–122
2. Carlet C (2004) On the secondary constructions of resilient and bent functions. In: Coding, Cryptography and combinatorics (Progress in computer science and applied logic), 18 vol 23, Basel, Switzerland, Birkhäuser, Verlag, , pp 3–28
3. Carlet C (2010) Boolean functions for cryptography and error correcting codes. chapter of the monography. In: Crama Y and Hammer P (eds) Boolean models and methods in mathematics, computer science, and engineering. Cambridge University Press, pp 257–397
4. Carlet C, Mesnager S (2016) Four decades of research on bent Functions. J Des Codes Cryptogr 78(1):5–50
5. Carlet C, Prouff E (2003) On plateaued functions and their constructions. In: Proceedings of fast software encryption FSE 2003, Lecture Notes in Computer Science 2887, pp 54–73
6. Cusick TW, Stănică P (2009) Cryptographic Boolean functions and applications. Elsevier-Academic Press
7. Cohen G, Honkala I, Litsyn S, Lobstein A (1997) Covering codes, North Holland
8. Dillon JF (1972) A survey of bent functions. NSA Tech J Spec Issue 191–215
9. Dillon JF (1974) Elementary Hadamard difference sets. Ph.D. dissertation. University of Maryland
10. Mandal B, Singh B, Gangopadhyay S, Maitra S, Vetrivel V (2018) On non-existence of bent-negabent rotation symmetric Boolean functions. Discret Appl Math 236:1–6
11. Mesnager S (2016) Bent functions: fundamentals and results. Springer, Switzerland
12. Mesnager S, Linear codes from functions. A concise encyclopedia of coding theory. To appear
13. Olsen JD, Scholtz RA, Welch LR (1982) Bent-function sequences. IEEE Transform Inf Theory 28(6):858–864

14. Parker MG (2000) The constant properties of Goley-Devis-Jedwab sequences. In: International symposium on information theory, Sorrento, Italy.http://www.ii.uib.no/matthew/mattweb.html
15. Parker MG, Pott A (2007) On Boolean functions which are bent and negabent. SSC 2007, LNCS 4893. Springer, Heidelberg, pp 9–23
16. Pott A, Tan Y, Feng T (2010) Strongly regular graphs associated with ternary bent functions. J Comb Theory Ser A 117:668–682
17. Pott A, Tan Y, Feng T, Ling S (2011) Association schemes arising from bent functions. J. Des Codes Cryptogr 59:319–331
18. Riera C, Parker MG (2006) Generalized bent criteria for Boolean functions. IEEE Transform Inform Theory 52(9):4142–4159
19. Rothaus O (1976) On bent functions. J Comb Theory Ser A 20:300–305
20. Sarkar S (2012) Characterizing negabent Boolean functions over finite fields. SETA 2012, vol 7280, LNCS, Springer, Berlin, Heidelberg, 2, pp 77–88
21. Schmidt KU, Parker MG, Pott A (2008) Negabent functions in the Maiorana-McFarland Class. SETA 390–402
22. Stănică P, Gangopadhyay S, Chaturvedi A, Gangopadhyay AK, Maitra S (2012) Investigations on bent and negabent functions via the Nega-Hadamard transform. IEEE Transform Inf Theory 58(6):4064–4072
23. Stănică P, Mandal B, Maitra S (2019) The connection between quadratic bent-negabent functions and the Kerdock code. Appl Algebra Eng Commun Comput 30(5):387–401
24. Su W, Pott A, Tang X (2013) Investigations on bent and negabent functions via the nega-Hadamard transform. IEEE Transform Inf Theory 59(6):3387–3395
25. Tang C, Zhou Z, Qi Y, Zhang X, Fan C, Helleseth T (2017) Generic construction of bent functions and bent idempotents with any possible algebraic degrees. IEEE Trans Inf Theory 63(10):6149–6157
26. Zhang F, Wei Y, Pasalic E (2015) Constructions of bent-negabent functions and their relation to the completed Maiorana-McFarland class. IEEE Trans Inf Theory 61(3):1496–1506
27. Zhou Y, Qu L (2017) Constructions of negabent functions over finite fields. Cryptogr Commun 9:165–180
28. Zhuo Z, Chong J (2015) On negabent functions and nega-Hadamard transform. Math Problems Eng Article ID 959617. https://doi.org/10.1155/2015/959617