IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

DOI:10.1587/transfun.2024EAP1008

Publicized:2024/06/14

This advance publication article will be replaced by the finalized version after proofreading.

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY

The Institute of Electronics, Information and Communication Engineers

Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER

Boolean Functions with Two Distinct Nega-Hadamard Coefficients*

Jinfeng CHONG[†a)], **Niu JIANG**[††], **Zepeng ZHUO**[†], *Nonmembers*, *and* **Weiyu ZHANG**[†], *Student Member*

SUMMARY In this paper, we consider the spectra of Boolean functions with respect to the nega-Hadamard transform. Based on the properties of the nega-Hadamard transform and the solutions of the Diophantine equations, we investigate all possibilities of the nega-Hadamard transform of Boolean functions with exactly two distinct nega-Hadamard coefficients.

key words: *Boolean function; Nega-Hadamard coefficient; Negabent function*

1. Introduction

Boolean functions are widely used in cryptography, error correcting coding and signal sequence design. The Walsh-Hadamard transform of Boolean functions is an important tool to study the properties of cryptographic functions, since many cryptographic properties of Boolean functions are characterized by their Walsh coefficients. A value of the Walsh-Hadamard transform of a Boolean function is called a Walsh coefficient, and the set of all Walsh coefficients is called the Walsh spectrum. In 1976, Rothaus [1] introduced the class of bent functions, which have the maximum nonlinearity in the sense that their Hamming distances to all the affine Boolean functions are optimal. A Boolean function is bent if and only if its spectrum with respect to the Walsh-Hadamard transform is flat, but bent functions exist only in an even number of variables and are not balanced.

To get Boolean functions with good properties in an odd or even number of variables. Riera and Parker [2] extended the concept of a bent function to some generalized bent criteria for a Boolean function, where they required that a Boolean function has a 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 matrix, the Walsh-Hadamard matrix and the nega-Hadamard matrix, respectively

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, N = \begin{pmatrix} 1 & \mathrm{i} \\ 1 & -\mathrm{i} \end{pmatrix},$$

where $\mathrm{i}^2 = -1$. 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 $N's$. 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.

Chee et al. [3] and Zhang [4] generalized the bent functions to semi-bent and plateaued functions, respectively. Pei et al. [5] studied the Boolean functions having at most eight nonzero Walsh coefficients. Boolean functions with exactly four or five different Walsh coefficients have not been extensively studied except in a few works like [6]–[9]. In [10], Tu et al. characterized all Boolean functions with exactly two distinct Walsh coefficients in terms of their spectrum, and they pointed out that the Boolean functions with exactly two distinct Walsh coefficients were close to bent functions and affine functions.

In [11], Schmidt shows that the nega spectrum of a negabent function has at most four values, and the nega spectrum distribution of negabent functions has been presented in [12]. Parker and Pott [13] showed that for even n, every negabent function over $\mathbb{F}_2^n$ can be constructed from a bent one over $\mathbb{F}_2^n$ and vice versa. Furthermore, when $n>1$ is odd, Su[12] showed that every negabent function over $\mathbb{F}_2^n$ can also be obtained from a bent one over $\mathbb{F}_2^{n-1}$ and vice versa. Therefore, the construction of negabent functions and bent functions may be equivalent. However, this equivalence does not reduce the importance to construct and classify the negabent functions. One of our motivations comes from Boolean functions with exactly two distinct Walsh coefficients present in [10]. In order to investigate all possibilities of nega-Hadamard spectra of Boolean functions with exactly two distinct nega-Hadamard coefficients. We prove that such Boolean functions have exactly three possible choices of Walsh spectra if the number of variables $n \geq 3$ is odd, and exactly two possible choices if n is even.

2. Preliminaries

Throughout this paper, $\mathbb{F}_2^n$ denotes the n-dimensional vector space over $\mathbb{F}_2$. Let $\mathcal{B}_n$ be the set of all n-variable Boolean functions. 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 binary addition over $\mathbb{F}_2$ is denoted by "$\oplus$". Let $a \cdot b$ denotes the inner product of $a, b \in \mathbb{F}_2^n$. If $z = a + b\mathrm{i} \in \mathbb{C}$, then $|z| = \sqrt{a^2 + b^2}$ denotes the absolute value of z, and $\bar{z} = a - b\mathrm{i}$ denotes the complex

[†]The author is with School of Mathematics and Statistics, Huaibei Normal University, Huaibei, Anhui 235000, China

[††]The author is with School of Mathematics Science College of Shanghai Normal University, Shanghai, 200234, China

*This paper was supported by Huaibei Normal University natural science surplus funds supported projects (No.2023ZK032, No.RE230438)

a) E-mail: cjf791009@163.com

conjugate of z, where $\mathrm{i}^2 = -1$, $a, b \in \mathbb{R}$.

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

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

Let n be an even positive integer, a function $f \in \mathcal{B}_n$ is a bent function if $W_f(u) = \pm 2^{\frac{n}{2}}$ for all $u \in \mathbb{F}_2^n$. The value $W_f(u)$ is called a Walsh-Hadamard coefficient of f at $u \in \mathbb{F}_2^n$. The multiset

$$\mathrm{Spec}(f) = \{W_f(u) : u \in \mathbb{F}_2^n\}$$

is said to be the Walsh-Hadamard spectrum of f.

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

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

where $\mathrm{i}^2 = -1$. A function f is called negabent function if $\mathcal{N}_f(\mathbf{u}) = \pm 2^{\frac{n}{2}}$ for all $u \in \mathbb{F}_2^n$. In contrast to bent functions, negabent functions also exist if n is odd. For an even number of variables, a bent function f is said to be bent-negabent if f is negabent. For example, all affine functions (both with an even and an odd numbers of variables) are negabent. The value $\mathcal{N}_f(\mathbf{u})$ is called a nega-Hadamard coefficient of f at $u \in \mathbb{F}_2^n$. The multiset

$$\mathrm{nega-Spec}(f) = \{\mathcal{N}_f(\mathbf{u}) : u \in \mathbb{F}_2^n\}$$

is said to be the nega-Hadamard spectrum of f. It is clear that $\mathrm{nega-Spec}(f)$ is a finite subset of $\mathbb{C}$. From the formula (1), we can verify

$$\sum_{u \in \mathbb{F}_2^n} \mathcal{N}_f(\mathbf{u}) = 2^n (-1)^{f(0)}. \tag{2}$$

The Nega-Parseval's Identity is given in [14] as follows

$$\sum_{u \in \mathbb{F}_2^n} |\mathcal{N}_f(\mathbf{u})|^2 = 2^{2n}. \tag{3}$$

3. Boolean functions with two distinct nega coefficients

The cardinality of the spectrum of a Boolean function is always greater than or equal to 2. It is known that an n-variable affine Boolean function has the Walsh spectrum $\{0, 2^n\}$ or $\{0, -2^n\}$, and an n-variable bent Boolean function has the Walsh spectrum $\{\pm 2^{\frac{n}{2}}\}$. In [10], the modification of affine and bent functions are obtained, by changing their values at $x = 0$. The corresponding functions are near affine functions with Walsh spectrum $\{2, -2^n + 2\}$ or $\{-2, 2^n - 2\}$, and near bent function with Walsh spectrum $\{\pm 2^{\frac{n}{2}} + 2\}$ or $\{\pm 2^{\frac{n}{2}} - 2\}$.

In this section we investigate all possibilities of nega-Hadamard spectra of Boolean functions with exactly two distinct nega-Hadamard coefficients. Let $f \in \mathcal{B}_n$ and $\mathrm{nega-Spec}(f) = \{\alpha, \beta\}$, where α and β are distinct complex numbers with the real parts and the imaginary parts are all integer. Denote by N_1 and N_2 the number of $u \in \mathbb{F}_2^n$ such that $\mathcal{N}_f(\mathbf{u})$ equals α and β, respectively. By (2) and (3) we have

$$\begin{cases} N_1 + N_2 = 2^n, \\ N_1\alpha + N_2\beta = 2^n(-1)^{f(0)}, \\ N_1|\alpha|^2 + N_2|\beta|^2 = 2^{2n}. \end{cases} \tag{4}$$

But for the case on nega-Hadamard transform, we prove the following statement.

Lemma 1. *Let $f \in \mathcal{B}_n$ with two distinct nega-Hadamard coefficients $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$. Then $|\alpha - \beta|^2 \mid 2^{2n}$.*

Proof. It is known that an n-variable Boolean function f can be written as

$$f(\mathbf{x}_{n-1}, x') = g(\mathbf{x}_{n-1})(1 \oplus x') \oplus x' \cdot h(\mathbf{x}_{n-1}),$$

where $g, h \in \mathcal{B}_{n-1}$, $(\mathbf{x}_{n-1}, x') \in \mathbb{F}_2^{n-1} \times \mathbb{F}_2$. The nega-Hadamard transform of f at $(\mathbf{u}_{n-1}, u') \in \mathbb{F}_2^{n-1} \times \mathbb{F}_2$ is

$$\begin{aligned} \mathcal{N}_f(\mathbf{u}_{n-1}, u') &= \sum_{\substack{(\mathbf{x}_{n-1}, x') \\ \in \mathbb{F}_2^{n-1} \times \mathbb{F}_2}} (-1)^{f(\mathbf{x}_{n-1}, x') \oplus \mathbf{u}_{n-1} \cdot \mathbf{x}_{n-1} \oplus u' x'} \mathrm{i}^{\mathrm{wt}(\mathbf{x}_{n-1}, x')} \\ &= \sum_{\mathbf{x}_{n-1} \in \mathbb{F}_2^{n-1}} (-1)^{g(\mathbf{x}_{n-1}) \oplus \mathbf{u}_{n-1} \cdot \mathbf{x}_{n-1}} \mathrm{i}^{\mathrm{wt}(\mathbf{x}_{n-1})} \\ &\quad + \sum_{\mathbf{x}_{n-1} \in \mathbb{F}_2^{n-1}} (-1)^{h(\mathbf{x}_{n-1}) \oplus \mathbf{u}_{n-1} \cdot \mathbf{x}_{n-1} \oplus u'} \mathrm{i}^{\mathrm{wt}(\mathbf{x}_{n-1}) + 1} \\ &= \mathcal{N}_g(\mathbf{u}_{n-1}) + \mathrm{i}(-1)^{u'} \mathcal{N}_h(\mathbf{u}_{n-1}). \end{aligned}$$

Thus

$$\begin{cases} \mathcal{N}_f(\mathbf{u}_{n-1}, 0) = \mathcal{N}_g(\mathbf{u}_{n-1}) + \mathrm{i}\mathcal{N}_h(\mathbf{u}_{n-1}), \\ \mathcal{N}_f(\mathbf{u}_{n-1}, 1) = \mathcal{N}_g(\mathbf{u}_{n-1}) - \mathrm{i}\mathcal{N}_h(\mathbf{u}_{n-1}). \end{cases} \tag{5}$$

From (5), we have

$$\mathcal{N}_h(\mathbf{u}_{n-1}) = \frac{\mathcal{N}_f(\mathbf{u}_{n-1}, 1) - \mathcal{N}_f(\mathbf{u}_{n-1}, 0)}{2} \mathrm{i} \in \left\{0, \pm \frac{\alpha - \beta}{2} \mathrm{i}\right\},$$

for all $\mathbf{u}_{n-1} \in \mathbb{F}_2^{n-1}$. Using Nega-Parseval's Identity to h, we have

$$\left(\left|\frac{\alpha - \beta}{2}\right|^2\right) \Big| 2^{2(n-1)},$$

therefore $|\alpha - \beta|^2 \mid 2^{2n}$. □

Lemma 2. *Let $f \in \mathcal{B}_n$ with two distinct nega-Hadamard coefficients $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$. Then, we have*

$$(\alpha - 1)(1 - \overline{\beta}) = 2^n - 1 \text{ and } \alpha - 1 = t(1 - \beta)$$

for some real number $t > 0$.

Proof. Since the proofs for the two cases of $f(0) = 0$ and $f(0) = 1$ are similar, we only prove the results when $f(0) = 0$. From the second and third equations of (4) we get

$$N_1\overline{\alpha} + N_2\overline{\beta} = 2^n \text{ and } N_1\alpha\overline{\alpha} + N_2\beta\overline{\beta} = 2^{2n}. \tag{6}$$

Solving (4) and (6) we have

$$N_2 = 2^n \frac{\alpha - 1}{\alpha - \beta} \text{ and } N_2 = 2^n \frac{\alpha - 2^n}{\alpha\overline{\beta} - \beta\overline{\beta}}.$$

Thus,

$$(\alpha - 1)(1 - \overline{\beta}) = 2^n - 1. \tag{7}$$

From (6), we get

$$(\alpha - 1)\overline{(1 - \beta)} = \overline{(\alpha - 1)}(1 - \beta),$$

that is,

$$\frac{\alpha - 1}{1 - \beta} = \frac{\overline{\alpha - 1}}{\overline{1 - \beta}} = \overline{\left(\frac{\alpha - 1}{1 - \beta}\right)}.$$

This proves that $\frac{\alpha-1}{1-\beta}$ is a real number, that is,

$$\alpha - 1 = t(1 - \beta)$$

for some $t \in \mathbb{R}$. Moreover, from

$$(\alpha - 1)\overline{(1 - \beta)} = t|1 - \beta|^2 = 2^n - 1,$$

we have $t > 0$. □

Lemma 3. *Let s and t be two positive integers, such that $st = 2^n - 1$ and $(s + t) \mid 2^n$. Without loss of generality, assume that $s \le t$, then*
(1) *If $n = 1$, then $s = t = 1$.*
(2) *If $n = 2k$, then $s = 1,\ t = 2^n - 1$ or $s = 2^k - 1,\ t = 2^k + 1$.*
(3) *If $n \ge 3$ is odd, then $s = 1,\ t = 2^n - 1$.*

Proof. The result of (1) is obviously. Now we prove (2) and (3). Without loss of generality, assume that $n \ge 2$. If $s = t$, then

$$s^2 + 1 = 2^n \equiv 0 \pmod 4,$$

this is a contradiction, since

$$s^2 + 1 \equiv 2 \pmod 4.$$

Since, $st = 2^n - 1$, then $s,\ t$ are two odd numbers and $\frac{s+t}{2}$, st are two positive integers. Based on the fact that

$$\left(\frac{s + t}{2}\right)^2 > st,$$

we have

$$\left(\frac{s + t}{2}\right)^2 \ge st + 1,$$

that is,

$$\frac{s + t}{2} \ge 2^{\frac{n}{2}}.$$

Let

$$\frac{s + t}{2} = 2^k,\ k \ge \frac{n}{2} \ge 1,$$

where k is positive integer. Let

$$s = 2^k - u,\ t = 2^k + u,$$

where u is positive odd number and $u < 2^k$. Since, $st = 2^n - 1$, then

$$2^{2k} - u^2 = 2^n - 1,$$

that is,

$$2^{2k} - 2^n = u^2 - 1 = (u + 1)(u - 1),$$

thus $2^n \mid (u + 1)(u - 1)$. From the fact that

$$(u + 1, u - 1) = (u + 1, 2) = 2,$$

we have

$$4 \nmid (u + 1) \text{ or } 4 \nmid (u - 1).$$

Therefore, $2^{n-1} \mid (u + 1)$ or $2^{n-1} \mid (u - 1)$.

In the case of $2^{n-1} \mid (u + 1)$, we have

$$u + 1 \ge 2^{n-1},\ u \ge 2^{n-1} - 1,$$

that is,

$$t \ge 2u = 2^n - 2,$$

then $s = 1, t = 2^n - 1$.

The case of $2^{n-1} \mid (u - 1)$ implies that $u - 1 \ge 2^{n-1}$, it is impossible. Therefore, $u - 1 = 0$, $u = 1$, that is, $s = 2^k - 1$, $t = 2^k + 1$, where $n = 2k$. □

Lemma 4. *Let n be a positive integer and $\omega_1, \omega_2 \in \mathbb{Z}[\mathrm{i}]$ with*

$$\omega_1\overline{\omega_2} = 2^n - 1 \text{ and } |\omega_1 + \omega_2|^2 \mid 2^{2n}, \tag{8}$$

where $\omega_1 \ne \omega_2$. Then all solutions of (8) are

$$(1, 2^n - 1),\ (2^n - 1, 1),\ (-1, -2^n + 1),\ (-2^n + 1, -1),$$

$$(\mathrm{i}, \mathrm{i}(2^n - 1)),\ (\mathrm{i}(2^n - 1), \mathrm{i}),\ (-\mathrm{i}, -\mathrm{i}(2^n - 1)),\ (-\mathrm{i}(2^n - 1), -\mathrm{i}),$$

if $n \ge 3$ is odd, and all solutions of (8) are

$$(2^k - 1, 2^k + 1),\ (2^k + 1, 2^k - 1),\ (-2^k + 1, -2^k - 1),\ (-2^k - 1, -2^k + 1)),$$

$$(\mathrm{i}(2^k - 1), \mathrm{i}(2^k + 1)),\ (\mathrm{i}(2^k + 1), \mathrm{i}(2^k - 1)),\ (-\mathrm{i}(2^k - 1), -\mathrm{i}(2^k + 1)),$$

$$(-\mathrm{i}(2^k + 1), -\mathrm{i}(2^k - 1)),$$

if $n = 2k$ is even.

Proof. Let $\omega_1 = s(a + b\mathrm{i})$, $\omega_2 = c + d\mathrm{i}$, where s is a positive integer, $(a, b) = 1$ and a, b is not all zero. Since, $\omega_1\overline{\omega_2}$ is a real number, then $bc = ad$. Therefore, $a|c$, $b|d$.

If $a \ne 0$. Let $c = at$. Then, $d = bt$. If $b \ne 0$, let $d = bt$. Then, $c = at$, where $t \in \mathbb{Z}$. Therefore,

$$\omega_2 = c + d\mathrm{i} = t(a + b\mathrm{i}) \text{ and } \omega_1\bar{\omega_2} = st(a^2 + b^2) = 2^n - 1,$$

where $t > 0$. Since,

$$|\omega_1 + \omega_2|^2 = (s + t)^2(a^2 + b^2) \mid 2^{2n},$$

then

$$(a^2 + b^2) \mid (2^n - 1, 2^{2n}) = 1,$$

thus $a^2 + b^2 = 1$.

Hence, all solutions of (8) is equivalent to all solutions of the following Eq.(9)

$$st = 2^n - 1 \text{ and } (s + t) \mid 2^n, \tag{9}$$

Based on Lemma 3, we obtain all solutions of (9) are

$$\omega_1 = \varepsilon,\ \omega_2 = (2^n - 1)\varepsilon,$$

if $n \geq 3$ is odd, and all solutions of (9) are

$$\omega_1 = (2^k - 1)\varepsilon,\ \omega_2 = (2^k + 1)\varepsilon,$$

if $n = 2k$, where ε is one of 1, -1, i and $-$i. □

Proposition 1. *In the case of the Boolean functions with two distinct nega-Hadamard coefficients, there is no such case with $a \in \mathbb{Z}$, $ta \in \mathbb{Z}$ for some real number $t > 0$ and $t \neq 1$.*

Proof. We suppose that $f \in \mathcal{B}_n$ has two distinct nega-Hadamard coefficients $a \in \mathbb{Z}$ and $ta \in \mathbb{Z}$ for some real number $t > 0$ and $t \neq 1$. Now using the second equation of (4), we have

$$N_1 + tN_2 = 2^n \frac{(-1)^{f(0)}}{a}.$$

Since $t > 0$, then

$$2^n \frac{(-1)^{f(0)}}{a} > 0.$$

On the one hand, if $a = (-1)^{f(0)}$ we have

$$N_1 + tN_2 = 2^n \frac{(-1)^{f(0)}}{a} = 2^n = N_1 + N_2,$$

which leads to $t = 1$, a contradiction. If $a \neq (-1)^{f(0)}$, we have

$$0 < 2^n \frac{(-1)^{f(0)}}{a} < 2^n$$

and

$$N_1 + tN_2 = 2^n \frac{(-1)^{f(0)}}{a} < 2^n = N_1 + N_2,$$

which leads to $t < 1$. Then we have $0 < t < 1$.

On the other hand, from the second and third equations of (4), since

$$0 < 2^n \frac{(-1)^{f(0)}}{a} \leq \left(2^n \frac{(-1)^{f(0)}}{a}\right)^2 = \left(\frac{2^n}{a}\right)^2,$$

we have

$$N_1 + tN_2 = 2^n \frac{(-1)^{f(0)}}{a} \leq \left(\frac{2^n}{a}\right)^2 = N_1 + t^2 N_2,$$

which leads to $t > 1$, a contradiction. □

From the known results above, we can obtain the following Theorem 1.

Theorem 1. *For any non-constant Boolean functions f with two distinct nega-Hadamard coefficients. If $f(0) = 0$, then all the possible nega-Hadamard spectrum of f are*

$$\begin{aligned}\text{nega} - \text{Spec}(f) =& \{2, -2^n + 2\} \text{ or } \{2^n, 0\} \\ & \text{or } \{1 + \text{i}, 1 - \text{i}(2^n - 1)\} \\ & \text{or } \{1 - \text{i}, 1 + \text{i}(2^n - 1)\},\end{aligned}$$

when $n \geq 3$ is odd, and

$$\begin{aligned}\text{nega} - \text{Spec}(f) =& \{2^k, -2^k\} \text{ or } \{2^k + 2, -2^k + 2\} \\ & \text{or } \{1 + \text{i}(2^k - 1), 1 - \text{i}(2^k + 1)\} \\ & \text{or } \{1 + \text{i}(2^k + 1), 1 - \text{i}(2^k - 1)\},\end{aligned}$$

when $n = 2k$ is even. If $f(0) = 1$, then all the possible nega-Hadamard spectrum of f are

$$\begin{aligned}\text{nega} - \text{Spec}(f) =& \{-2, 2^n - 2\} \text{ or } \{-2^n, 0\} \\ & \text{or } \{-1 - \text{i}, -1 + \text{i}(2^n - 1)\} \\ & \text{or } \{-1 + \text{i}, -1 - \text{i}(2^n - 1)\},\end{aligned}$$

when $n \geq 3$ is odd, and

$$\begin{aligned}\text{nega} - \text{Spec}(f) =& \{-2^k, 2^k\} \text{ or } \{-2^k - 2, 2^k - 2\} \\ & \text{or } \{-1 - \text{i}(2^k - 1), -1 + \text{i}(2^k + 1)\} \\ & \text{or } \{-1 - \text{i}(2^k + 1), -1 + \text{i}(2^k - 1)\},\end{aligned}$$

when $n = 2k$ is even.

Proof. By Lemma 2 we know that, if $\alpha, \beta \in \mathbb{Z}[\text{i}]$ are two distinct nega-Hadamard coefficients of $f \in \mathcal{B}_n$, then

$$(\alpha - 1)(1 - \bar{\beta}) = 2^n - 1.$$

Together with the fact that

$$|\alpha - 1 + 1 - \beta|^2 = |\alpha - \beta|^2 \mid 2^{2n},$$

using the result in Lemma 1.

Without loss of generality, we may assume that $\alpha - 1 > 0$ and $1 - \bar{\beta} > 0$. Using Lemma 4, we solve the Diophantine equation (7) to get all the possible nega-Hadamard spectrum of f , that is, when $n \geq 3$ is odd, we have

$$\begin{aligned}\text{nega} - \text{Spec}(f) =& \{2, -2^n + 2\} \text{ or } \{2^n, 0\} \\ & \text{or } \{1 + \text{i}, 1 - (2^n - 1)\text{i}\} \\ & \text{or } \{1 - \text{i}, 1 + (2^n - 1)\text{i}\},\end{aligned}$$

and when $n = 2k$ is even we have

$$\begin{aligned}\text{nega} - \text{Spec}(f) =& \{2^k, -2^k\} \text{ or } \{2^k, -2^k + 2\} \\ & \text{or } \{1 + \text{i}(2^k - 1), 1 + \text{i}(2^k + 1)\} \\ & \text{or } \{1 + \text{i}(2^k + 1), 1 + \text{i}(2^k - 1)\}.\end{aligned}$$

From Proposition 1, we know that all forms of nega-Hadamard spectra of the Boolean function with two distinct nega-Hadamard coefficients obtained in Theorem 1 exist.

In [12], it was shown that the relationship between negabent functions and bent functions, which is an important tool to analyze the properties of negabent functions. If n is even, necessary and sufficient conditions for a Boolean function $f \in \mathcal{B}_n$ to be negabent have been given in [11], that is, the Boolean function f is negabent if and only if $f + \sigma_2$ is bent.

Lemma 5. *[12] Let $f \in \mathcal{B}_n$. Between the nega-Hadamard transform and the Walsh-Hadamard transform, there is the*

relation

$$\mathcal{N}_f(u) = \frac{\mathcal{W}_{f\oplus\sigma_2}(u) + \mathcal{W}_{f\oplus\sigma_2}(\overline{u})}{2} + \mathrm{i}\frac{\mathcal{W}_{f\oplus\sigma_2}(u) - \mathcal{W}_{f\oplus\sigma_2}(\overline{u})}{2}.$$

With Lemma 5, we can present the following proposition.

Proposition 2. *When $n = 2k$ is even, the relationships between the Boolean functions with two distinct Walsh coefficients and the Boolean functions with two distinct nega-Hadamard coefficients are*

Case 1. *If* $\mathcal{W}_{f\oplus\sigma_2}(u) = 2^{\frac{n}{2}}, \mathcal{W}_{f\oplus\sigma_2}(\overline{u}) = -2^{\frac{n}{2}} + 2$ and $\mathcal{W}_{f\oplus\sigma_2}(u) = -2^{\frac{n}{2}}, \mathcal{W}_{f\oplus\sigma_2}(\overline{u}) = 2^{\frac{n}{2}} + 2$, *then*

$$\mathrm{Nega-spec}(f) = \{1 + \mathrm{i}(2^k - 1), 1 - \mathrm{i}(2^k + 1)\}.$$

Case 2. *If* $\mathcal{W}_{f\oplus\sigma_2}(u) = 2^{\frac{n}{2}} + 2$, $\mathcal{W}_{f\oplus\sigma_2}(\overline{u}) = -2^{\frac{n}{2}}$ *and* $\mathcal{W}_{f\oplus\sigma_2}(u) = -2^{\frac{n}{2}} + 2$, $\mathcal{W}_{f\oplus\sigma_2}(\overline{u}) = 2^{\frac{n}{2}}$, *then*

$$\mathrm{Nega-spec}(f) = \{1 + \mathrm{i}(2^k + 1), 1 - \mathrm{i}(2^k - 1)\}.$$

Case 3. *If* $\mathcal{W}_{f\oplus\sigma_2}(u) = -2^{\frac{n}{2}}$, $\mathcal{W}_{f\oplus\sigma_2}(\overline{u}) = 2^{\frac{n}{2}} - 2$ *and* $\mathcal{W}_{f\oplus\sigma_2}(u) = 2^{\frac{n}{2}}$, $\mathcal{W}_{f\oplus\sigma_2}(\overline{u}) = -2^{\frac{n}{2}} - 2$, *then*

$$\mathrm{Nega-spec}(f) = \{-1 - \mathrm{i}(2^k - 1), -1 + \mathrm{i}(2^k + 1)\}.$$

Case 4. *If* $\mathcal{W}_{f\oplus\sigma_2}(u) = -2^{\frac{n}{2}} - 2$, $\mathcal{W}_{f\oplus\sigma_2}(\overline{u}) = 2^{\frac{n}{2}}$ *and* $\mathcal{W}_{f\oplus\sigma_2}(u) = 2^{\frac{n}{2}} - 2$, $\mathcal{W}_{f\oplus\sigma_2}(\overline{u}) = -2^{\frac{n}{2}}$, *then*

$$\mathrm{Nega-spec}(f) = \{-1 - \mathrm{i}(2^k + 1), -1 + \mathrm{i}(2^k - 1)\}.$$

The above cases indicate that the two distinct nega-Hadamard coefficients of f at $u \in \mathbb{F}_2^n$, can be obtained by selecting the appropriate value of the two distinct Walsh coefficients of $f \oplus \sigma_2$ at $u, \overline{u} \in \mathbb{F}_2^n$, where $n = 2k$ is even.

4. Conclusion

We have presented all possibilities of nega-Hadamard spectra of Boolean functions with exactly two distinct nega-Hadamard coefficients. Furthermore, it is interesting to construct specific Boolean function with two distinct nega-Hadamard coefficients.

References

[1] O.S. Rothaus, "On "bent" functions," Journal of Combinatorial Theory Series A, vol.20, no.3, pp.300-305, 1976. DOI:10.1016/0097-3165(76)90024-8

[2] C. Riera and M.G. Parker, "Generalized bent criteria for Boolean functions," IEEE Transactions on Information Theory, vol.52, no.9, pp.4142-4159, 2006. DOI:10.1109/TIT.2006.880069

[3] S. Chee, S. Lee and K. Kim, "Semi-bent functions," Advances in Cryptology-ASIACRYPT'94, LNCS, vol.917, pp.105-118, Springer, 1995. DOI:10.1007/BFb0000428

[4] Y.L. Zheng and X.M. Zhang, "Plateaued functions," Advances in Cryptology ICICS'99, LNCS 1726, vol.1726, pp.284-300, Springer, 1999. DOI:10.1007/978-3-540-47942-0_24

[5] D.Y. Pei and W.L. Qin, "The correlation of a Boolean function with its variables," Progress in Cryptology-INDOCRYPT 2000, LNCS 1977, vol.1977, pp.1-8, 2000. DOI:10.1007/3-540-44495-5_1

[6] Z.Q. Sun and L. Hu, "Several classes of boolean functions with four-Valued walsh spectra," International Journal of Foundations of Computer Science, vol.28, no.4, pp.357-377, 2017. DOI:10.1142/S0129054117500228

[7] X.W. Cao and L. Hu, "Two Boolean functions with five valued Walsh spectra and high nonlinearity," International Journal of Foundations of Computer Science, vol.26, no.5, pp.537-556, 2015. DOI:10.1142/S0129054115500306

[8] S. Mesnager and F.R. Zhang, "On constructions of bent, semi-bent and five valued spectrum functions from old bent functions," Advances in Mathematics of Communications, vol.11, no.2, pp.339-345, 2017. DOI:10.3934/amc.2017026

[9] S. Maitra and P. Sarkar, "Cryptographically significant Boolean functions with five valued Walsh spectra," Theoretical Computer Science, vol.276, no.1-2, pp.133-146, 2002. DOI:10.1016/S0304-3975(01)00196-7

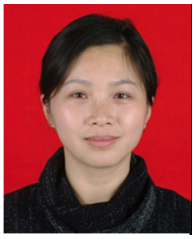
[10] Z.R. Tu, D.B. Zheng, X.Y. Zeng, et al, "Boolean functions with two distinct Walsh coefficients," Applicable Algebra in Engineering, Communication and Computing, vol.22, pp.359-366, 2011. DOI:10.1007/s00200-011-0155-3

[11] K.U Schmidt, M.G. Parker and A. Pott, "Negabent functions in the Maiorana-McFarland class," Sequences and Their Applications-SETA 2008, LNCS, vol.5203, pp.390-402, Springer, 2008. DOI:10.1007/978-3-540-85912-3_34

[12] W. Su, A. Pott and X.H. Tang, "Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree," IEEE Transactions on Information Theory, vol.59, no.6, pp.3387-3395, 2013. DOI:https:10.1109/TIT.2013.2245938

[13] M.G. Parker and A. Pott, "On Boolean functions which are bent and negabent," Sequences, Subsequences, and Consequences, 2007, LNSC, vol.4893, pp.9-23. DOI:10.1007/978-3-540-77404-4_2

[14] P. Stănică, S. Gangopadhyay, A. Chaturvedi, et al, "Investigations on bent and negabent functions via the nega-Hadamard transforms," IEEE Transactions on Information Theory, vol.58, no.6, pp.4064-4072, 2012. DOI:10.1109/TIT.2012.2186785



Jinfeng CHONG received the M.S. degree from Huaibei Normal University in 2007. Since 2002, she has been with the School of Mathematical Science, Huaibei Normal University, where she is currently an associate professor. Her research interests include cryptography and information theory.

Niu JIANG received the M.S. degree in applied mathematics from Huaibei Normal University in 2023. She is now a Ph.D. candidate of Shanghai Normal University. Her research interests include cryptography and information theory.

Zepeng ZHUO received the M.S. degree from Huaibei Normal University in 2007, and the Ph.D. degree from Xidian University in 2012. Since 2002, he has been with the School of Mathematical Science, Huaibei Normal University, where he is now a professor. His research interests include cryptography and information theory.

Weiyu ZHANG received the B.S. degrees in 2022 from the School of Mathematical Sciences, Huainan Normal University. She is currently a master course student at the School of Mathematical Sciences, Huaibei Normal University. Her research interests include cryptography and information theory.