Constructing Boolean functions with four-valued and five-valued spectra by modifying the Maiorana-McFarland class of bent functions *

Fei Guo and Zilong Wang

State Key Laboratory of Integrated Service Networks, School of Cyber Engineering, Xidian University, Xi'an, 710071, China

Abstract

Construction and analysis of bent functions (i.e., Boolean functions with two-valued spectrum $\{\pm 2^{\frac{n}{2}}\}$) and plateaued functions (i.e., Boolean functions with three-valued spectrum $\{0, \pm 2^{\frac{n+s}{2}}\}$) have been active research fields for the last several decades and a large number of results have emerged. Nevertheless, only a few studies consider the design of Boolean functions with four-valued and five-valued spectra. In this paper, by modifying the Maiorana-McFarland class of bent functions, we present a construction of even-variable Boolean functions with four-valued spectrum $\{0, \pm 2^{\frac{n}{2}}, 2^{\frac{n}{2}+1}\}$ or $\{0, \pm 2^{\frac{n}{2}}, -2^{\frac{n}{2}+1}\}$ and five-valued spectrum $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n}{2}+1}\}$. These functions have any possible algebraic degree ranging from 3 to theoretical upper bound $\frac{n}{2}+1$ and nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$, which is as good as that of semi-bent functions. The spectral distribution of these functions is analyzed as well. Moreover, we investigate a special case of the construction, which is shown to consist of Boolean functions lacking non-trivial linear structures and having five-valued spectra and algebraic degree $\frac{n}{2}+1$, which is as high as it can possibly be for n-variable Boolean functions that have Walsh spectrum $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n}{2}+1}\}$.

1 Introduction

The Walsh spectrum has a central role in studying Boolean functions [2], and many cryptographic properties can be characterized with it, such as nonlinearity, balancedness, algebraic degree and correlation immunity. Researches show that Boolean functions with four-valued and five-valued spectra may possess good cryptographic properties, such as balancedness, resiliency, high nonlinearity and algebraic degree [7,8,10]. Nevertheless, there only exist a few methods to construct Boolean functions with four-valued and five-valued spectra, including constructions via some trace representations [1,10,12], and constructions on the basis of bent functions [8,9]. Recently in [6, 7], several characterizations and constructions of Boolean functions with five-valued spectra were presented in the spectral domain, which provide a new sight into this family of functions.

Unlike previous perspectives, this paper proposes a method to construct Boolean functions with four-valued and five-valued spectra by modifying the Maiorana-McFarland class of bent functions. Let $n = 2m \geq 4$, $\mathbf{x}' = (x_1, \cdots, x_{m-1}) \in \mathbb{F}_2^{m-1}, \mathbf{y}' = (y_1, \cdots, y_{m-1}) \in \mathbb{F}_2^{m-1}$, $\mathbf{x} = (\mathbf{x}', x_m) \in \mathbb{F}_2^m$, and $\mathbf{y} = (\mathbf{y}', y_m) \in \mathbb{F}_2^m$. The proposed functions are defined as the form

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \big(\pi(\mathbf{y}'),\ y_m t(\mathbf{y}')\big) \oplus g(\mathbf{y}'), \tag{1}$$

where π is a permutation over $\mathbb{F}_2^{m-1}$, and t and g are arbitrary $(m-1)$-variable Boolean functions. It is not hard to see that, if t is the constant zero function, then $\big(\pi(\mathbf{y}'), 0\big)$ is a two-to-one mapping

*The work was supported by National Natural Science Foundation of China (No. U19B2021), Natural Science Basic Research Program of Shaanxi (No. 2021JQ-192), the Fundamental Research Funds for the Central Universities and the Innovation Fund of Xidian University.

over $\mathbb{F}_2^m$, and further f is a semi-bent function by [3, Lemma 1]; if t is the constant one function, then $\big(\pi(\mathbf{y}'), y_m\big)$ is a permutation over $\mathbb{F}_2^m$, and further f is a bent function in the Maiorana-McFarland class. Inspired by the cases $t = 0$ and $t = 1$, we investigate the property of f with $\deg(t) \geq 1$, and prove f to have Walsh spectrum containing at most five values (Theorem 3.1). The Walsh spectral distribution of f is determined as well (Theorem 3.2). We further explain that these functions have four-valued spectrum $\{0, \pm 2^m, 2^{m+1}\}$ or $\{0, \pm 2^m, -2^{m+1}\}$, or five-valued spectrum $\{0, \pm 2^m, \pm 2^{m+1}\}$ (Corollary 3.3). The nonlinearity of these functions is $2^{n-1} - 2^m$, which is as good as semi-bent functions. Besides, we show that the algebraic degree of f can reach any value ranging from 3 to $\frac{n}{2} + 1$, which is as high as possible for Boolean functions whose Walsh spectrum consists of $0, \pm 2^m$, and at least one of $\pm 2^{m+1}$ (Corollary 3.5). Moreover, we study a special subclass of f with $\pi = id$, $t(\mathbf{y}') = y_1 y_2 \cdots y_{m-1}$, $g(\mathbf{y}') = 0$, and prove that it has five-valued spectrum and algebraic degree $\frac{n}{2} + 1$, and lack non-trivial linear structures (Theorem 4.1). Finally, we modify it to be balanced with other properties preserved (Corollary 4.2).

The extended abstract is organized as follows. Section 2 introduces some basic knowledge of the Boolean function and the Walsh spectrum. Section 3 investigates the Walsh spectral characterization, algebraic degree and nonlinearity of f defined in (1). Section 4 studies a special case of the construction in (1), which produces Boolean functions with five-valued spectra, theoretical maximum algebraic degree and without non-trivial linear structures.

2 Preliminaries

A Boolean function on n variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let $\mathcal{B}_n$ be the set of all n-variable Boolean functions. For $f \in \mathcal{B}_n$, it can be expressed as the algebraic normal form (ANF)

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

where $\lambda_{\mathbf{u}} \in \mathbb{F}_2$. f is called balanced if $|\{\mathbf{x} \in \mathbb{F}_2^n \mid f(\mathbf{x}) = 1\}| = 2^{n-1}$. The algebraic degree of f is defined as $\deg(f) = \max\{\mathrm{w_H}(\mathbf{u}) \mid \lambda_{\mathbf{u}} \neq 0\}$, where $\mathrm{w_H}(\mathbf{u}) = \sum_{i=1}^{n} u_i$ is the Hamming weight of $\mathbf{u}$.

The Walsh-Hadamard transform of $f \in \mathcal{B}_n$ is defined as

$$\mathrm{W}_f(\boldsymbol{\omega}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\boldsymbol{\omega}\cdot\mathbf{x}}, \boldsymbol{\omega} \in \mathbb{F}_2^n.$$

Obviously, $\mathrm{W}_f(\mathbf{0}_n) = 0$ if and only if f is balanced, where $\mathbf{0}_n$ is the zero vector in $\mathbb{F}_2^n$. The sequence of all Walsh-Hadamard transforms with inputs in lexicographic order is called the Walsh spectrum, i.e.,

$$\left[\mathrm{W}_f(0, \cdots, 0, 0), \mathrm{W}_f(0, \cdots, 0, 1), \cdots, \mathrm{W}_f(1, \cdots, 1, 1)\right].$$

The nonlinearity of $f \in \mathcal{B}_n$, denoted by N_f, which measures the minimum distance between f and all affine functions, has the following relation with the Walsh-Hadamard transform:

$$\mathrm{N}_f = 2^{n-1} - \frac{1}{2} \max_{\boldsymbol{\omega}\in\mathbb{F}_2^n} |\mathrm{W}_f(\boldsymbol{\omega})|. \tag{2}$$

A Boolean function $f \in \mathcal{B}_n$ is called bent if $\mathrm{W}_f(\boldsymbol{\omega}) = \pm 2^{\frac{n}{2}}$ for all $\boldsymbol{\omega} \in \mathbb{F}_2^n$, where n is even. A Boolean function $f \in \mathcal{B}_n$ is called s-plateaued if its Walsh spectrum takes three values $0, \pm 2^{\frac{n+s}{2}}$, where $s \geq 1$ for odd n while $s \geq 2$ for even n, and s has the same parity as n. In particular, 1-plateaued odd-variable functions and 2-plateaued even-variable functions are called semi-bent.

The autocorrelation function of $f \in \mathcal{B}_n$ is defined as

$$\Delta_f(\boldsymbol{\alpha}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\boldsymbol{\alpha})}, \boldsymbol{\alpha} \in \mathbb{F}_2^n.$$

The vector $\boldsymbol{\alpha}$ is called a linear structure of f if $\Delta_f(\boldsymbol{\alpha}) = \pm 2^n$. Obviously, $\Delta_f(\mathbf{0}_n) = 2^n$ always holds and $\mathbf{0}_n$ is called the trivial linear structure of f. A Boolean function with any non-trivial linear structure has very bad performance when applied in cryptosystems [4, 5].

3 Construction of Boolean functions with four-valued and five-valued spectra

In this section, let $\mathbf{u}' = (u_1, \cdots, u_{m-1}) \in \mathbb{F}_2^{m-1}$, $\mathbf{v}' = (v_1, \cdots, v_{m-1}) \in \mathbb{F}_2^{m-1}$, $\mathbf{u} = (\mathbf{u}', u_m) \in \mathbb{F}_2^m$, and $\mathbf{v} = (\mathbf{v}', v_m) \in \mathbb{F}_2^m$. Recall the function f defined in (1), its spectrum is given in the following theorem.

Theorem 3.1 The spectrum of f in (1) contains at most five possible values, all of which lie in $\{0, \pm 2^m, \pm 2^{m+1}\}$.

The spectral distribution of f in (1) is given in the following theorem.

Theorem 3.2 Let f be defined in (1) with $\deg(t) \geq 1$, and Γ_i express the number of i's in the Walsh spectrum of f, where $i \in \{0, \pm 2^m, \pm 2^{m+1}\}$. Then

$$\begin{cases} \Gamma_0 = 3|N| + 3|M|, \\ \Gamma_{2^m} = 3 \cdot 2^{n-2} - 2|S| - 3|N| - |M|, \\ \Gamma_{-2^m} = 2^{n-2} + 2|S| - |N| - 3|M|, \\ \Gamma_{2^{m+1}} = |N|, \\ \Gamma_{-2^{m+1}} = |M|, \end{cases}$$

where

$$\begin{aligned} M &= \{(\mathbf{u}', \mathbf{v}') \in \mathbb{F}_2^{n-2} \mid t(\mathbf{u}') = 0, \mathbf{u}' \cdot \mathbf{v}' \oplus g(\mathbf{u}') = 1\}, \\ N &= \{(\mathbf{u}', \mathbf{v}') \in \mathbb{F}_2^{n-2} \mid t(\mathbf{u}') = 0, \mathbf{u}' \cdot \mathbf{v}' \oplus g(\mathbf{u}') = 0\}, \\ S &= \{(\mathbf{u}', \mathbf{v}') \in \mathbb{F}_2^{n-2} \mid \mathbf{u}' \cdot \mathbf{v}' \oplus g(\mathbf{u}') = 1\}. \end{aligned}$$

By Theorem 3.1 and Theorem 3.2, we show that f defined in (1) has a four-valued or five-valued spectrum in the following corollary.

Corollary 3.3 With the notations in Theorem 3.2,

1) if $|M| = 0$, then f has a four-valued spectrum $\{0, \pm 2^m, 2^{m+1}\}$, and $\Gamma_{2^m} = \Gamma_{-2^m}$;

2) if $|N| = 0$, then f has a four-valued spectrum $\{0, \pm 2^m, -2^{m+1}\}$, and $\Gamma_{2^m} = \Gamma_{-2^m}$;

3) if $|M| \neq 0, |N| \neq 0$, then f has a five-valued spectrum $\{0, \pm 2^m, \pm 2^{m+1}\}$, and either $\Gamma_{2^m} = \Gamma_{-2^m}$ or $\Gamma_{2^{m+1}} = \Gamma_{-2^{m+1}}$.

By Corollary 3.3, it is obvious that $\max_{\boldsymbol{\omega} \in \mathbb{F}_2^n} |\mathrm{W}_f(\boldsymbol{\omega})| = 2^{m+1}$. Thus, from (2), we have $\mathrm{N}_f = 2^{n-1} - 2^m$, which is as good as the nonlinearity of semi-bent functions.

Proposition 3.4 Let $g \in \mathcal{B}_n$ with $n = 2m \geq 4$. If the Walsh spectrum of g only contains $0, \pm 2^m$ and at least one of $\pm 2^{m+1}$, then $3 \leq \deg(g) \leq m + 1$.

The algebraic degree of f in (1) is given in the following corollary.

Corollary 3.5 Let f be defined in (1) with $\deg(t) \geq 1$ and $\pi = (\pi_1, \cdots, \pi_{m-1})$, where $\pi_i \in \mathcal{B}_{m-1}$ for all $1 \leq i \leq m-1$. Then

$$\deg(f) = \max\{\max_{1 \leq i \leq m-1} \deg(\pi_i) + 1, \deg(t) + 2, \deg(g)\}.$$

Since $\deg(t) \geq 1$, by using different π, t and g, it is obvious that $\deg(f)$ can reach any value in range of 3 to theoretical upper bound $m + 1$ by Proposition 3.4.

Remark 3.6 Considering the expression of M and N in Theorem 3.2, we know

$$\begin{cases} |M| \neq 0 \iff (t(\mathbf{x}') \oplus 1)(\mathbf{x}' \cdot \mathbf{y}' \oplus g(\mathbf{x}')) \neq 0, \\ |N| \neq 0 \iff (t(\mathbf{x}') \oplus 1)(\mathbf{x}' \cdot \mathbf{y}' \oplus g(\mathbf{x}') \oplus 1) \neq 0. \end{cases} \tag{3}$$

On the other hand, it is proved in [11, Corollary 1] that the $(2m-2)$-variable Maiorana-McFarland class of bent functions $\mathbf{x}' \cdot \mathbf{y}' \oplus g(\mathbf{x}')$ have algebraic immunity no more than $\lceil \frac{m-1}{2} \rceil + 2$, where algebraic immunity of a function $f \in \mathcal{B}_n$ is defined as the number $\min\{\deg(g) | g \in \mathcal{B}_n, g \neq 0, fg = 0 \text{ or } (f \oplus 1)g = 0\}$. Thus, we know f and $f \oplus 1$ have the same algebraic immunity. Therefore, by (3), if the function t is chosen with algebraic degree strictly greater than $\lceil \frac{m-1}{2} \rceil + 2$, then neither $|N|$ nor $|M|$ equals 0. That is to say, plenty of Boolean functions with five-valued spectra can be obtained by using t with $\deg(t) > \lceil \frac{m-1}{2} \rceil + 2$. Especially, for $m \geq 7$, if $\deg(t) = m-1$, then f in (1) is a function with five-valued spectrum and maximum algebraic degree $m+1$.

4 Boolean functions with five-valued spectra, theoretical maximum algebraic degree and without non-trivial linear structures

Let $\pi = id, t(\mathbf{y}') = y_1 y_2 \cdots y_{m-1}$ and $g(\mathbf{y}') = 0$. Then f in (1) reads

$$f(x_1, \cdots, x_m, y_1, \cdots, y_m) = \bigoplus_{i=1}^{m-1} x_i y_i \oplus x_m \prod_{i=1}^{m} y_i. \tag{4}$$

Theorem 4.1 Let $m \geq 3$ be a positive integer. The function f defined in (4) has a five-valued spectrum and theoretical maximum algebraic degree $(m+1)$, and lack non-trivial linear structures. Moreover, its Wlash spectral distribution is given by

$$\begin{cases} \Gamma_0 = 3 \cdot (2^{n-2} - 2^{m-1}), \\ \Gamma_{2^m} = \Gamma_{-2^m} = 2^m, \\ \Gamma_{2^{m+1}} = 2^{n-3}, \\ \Gamma_{-2^{m+1}} = 2^{n-3} - 2^{m-1}, \end{cases} \tag{5}$$

where Γ_i expresses the number of i's in the Walsh spectrum of f.

One may notice that f in (4) is unbalanced since $\mathrm{W}_f(\mathbf{0}_n) \neq 0$ can be easily verified. In next corollary, by adding affine terms to f, we modify it to be balanced with other properties preserved.

Corollary 4.2 Let $m \geq 3$ be a positive integer and f defined in (4). Then $f_1(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}, \mathbf{y}) \oplus y_m$ and $f_2(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}, \mathbf{y}) \oplus y_1 \oplus \bigoplus_{i=2}^{m}(x_i \oplus y_i)$ are balanced functions with five-valued spectrum $\{0, \pm 2^m, \pm 2^{m+1}\}$ and algebraic degree $(m+1)$, and without non-trivial linear structures. And their Walsh spectral distributions are given by (5) as well.

References

[1] X. Cao, and L. Hu, Two Boolean functions with five-valued Walsh spectra and high nonlinearity, Int. J. Found. Comput. Sci., vol. 26, no. 5, pp. 537–556, 2015.

[2] C. Carlet, Boolean functions for cryptography and error correcting codes, Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Y. Crama and P. L. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 257–397.

[3] C. Carlet, G. Gao, and W. Liu, Results on constructions of rotation symmetric bent and semi-bent functions, in Sequences and Their Applications-SETA 2014, pp. 21–33, Springer, 2014.

[4] S. Dubuc, Linear structures of Boolean functions, in Proceedings 1998 IEEE International Symposium on Information Theory (Cat. No.98CH36252), Cambridge, MA, vol. 440, 1998.

[5] J. H. Evertse, Linear structures in block ciphers, in Advances in Cryptology-EUROCRYPT'87, LNCS, vol. 304, pp. 249–266, Springer-Verlag, 1988.

[6] S. Hodžić, P. Horak, and E. Pasalic, Characterization of basic 5-value spectrum functions through Walsh-Hadamard transform, IEEE Trans. Inf. Theory, vol. 67, no. 2, pp. 1038–1053, 2021.

[7] S. Hodžić, E. Pasalic, and W. Zhang, Generic constructions of 5-valued spectra Boolean functions, IEEE Trans. Inf. Theory, vol. 65, no. 11, pp. 7554–7565, 2019.

[8] S. Maitra, and P. Sarkar, Cryptographically significant Boolean functions with five valued Walsh spectra, Theor. Comput. Sci., vol. 276, no. 1–2, pp. 133–146, 2002.

[9] S. Mesnager, and F. Zhang, On constructions of bent, semi-bent and five valued spectrum functions from old bent functions, Adv. Math. Commun., vol. 11, pp. 2, pp. 339–345, 2017.

[10] Z. Sun, and L. Hu, Boolean functions with four-valued Walsh spectra, J. Syst. Sci. Complex., vol. 28, no. 3, pp. 743–754, 2015.

[11] Q. Wang, and C. Tan, A note on the algebraic immunity of the Maiorana-McFarland class of bent functions, Inf. Process. Lett., vol. 112, pp. 22, pp. 869–871, 2012.

[12] G. Xu, X. Cao, and S. Xu, Several classes of Boolean functions with few Walsh transform values, Appl. Algebra Eng. Commun. Comput., vol. 28, no. 2, pp. 155–176, 2017.