International Journal of Hybrid Information Technology
Vol.8, No. 5 (2015), pp. 91-96
http://dx.doi.org/10.14257/ijhit.2015.8.5.09

Constructions of Generalized Bent Boolean Functions on Odd Number of Variables

Yong-Bin Zhao[1, 2*], Feng-Rong Zhang[3] and Yu-Pu Hu[1]

[1]State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China
[2]School of Information Science and Technology, Shijiazhuang Tiedao University, Shijiazhuang 050043, China
[3]School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu 221116, China;
zhaoyungbin@163.com

Abstract

In this paper, we investigate the constructions of generalized bent Boolean functions defined on with values in Z4. We first present a construction of generalized bent Boolean functions defined on with values in Z4. The main technique is to utilize bent functions to derive generalized bent functions on odd number of variables. In addition, by using Boolean permutations, we provide a specific method to construct generalized bent functions on odd number of variables.

Keywords: *Boolean functions, Generalized Boolean functions, Generalized bent functions, bent functions*

1. Introduction

Bent functions have optimal nonlinearity [5]. They were introduced by Rothaus in 1976 as an interesting combinatorial object [16]. Bent functions have been extensively studied during the thirty last years [1-4, 6-9, 10,12] since bent functions have many applications in sequence design, cryptography and algebraic coding [13,15].

In the recent years, generalizations of Boolean functions [11, 17-21, and 22] were proposed. In 2009, Schmidt [17] considered functions from Z_2^n to Z_q from the viewpoint of cyclic codes over rings. Latter, Solé and Tokareva [18] called these functions from Z_2^n to Z_q generalized Boolean functions and presented the direct links between Boolean bent functions and generalized bent functions. More recently, Stănică *et al.*, [22] investigated the properties of generalized bent functions and presented several constructions of such generalized bent functions for both n even and n odd.

In this paper, we concentrate on constructions of generalized bent Boolean functions on odd number of variables. We first present a construction of generalized bent Boolean functions defined on Z_2^n with values in Z_4. The main technique is to utilize the links between bent functions and semi-bent functions to derive generalized bent functions on odd number of variables. In addition, by using Boolean permutations and special Boolean functions g , we provide a specific method to construct generalized bent functions on odd number of variables.

2. Preliminaries

The following notations will be used throughout the paper. Let us denote the set of integers, real numbers and complex numbers by Z, R and C , respectively and let the ring

ISSN: 1738-9968 IJHIT

of integers modulo r be denoted by Z_r. We denote the addition over Z, R and C by '+'. Moreover, addition modulo q ($\neq 2$) is also denoted by '+' and it is understood from the context. Let Z_2^n be the n-dimensional vector space over Z_2. We denote the addition over Z_2^n and Z_2 by '$\oplus$'. Let $\omega = (\omega_1, \cdots, \omega_n)$ and $x = (x_1, \cdots, x_n) \in Z_2^n$, we define the inner (or scalar) product by $\omega \cdot x = \omega_1 x_1 \oplus \ldots \oplus \omega_n x_n$. If $z = a + bi \in C, a, b \in R$, then $|z| = \sqrt{a^2 + b^2}$ denotes the absolute value of z, where $i^2 = -1$. We denote the vectors $(0, 0, \cdots, 0) \in Z_2^n$ by 0_n.

A function from Z_2^n to Z_q ($q \geq 2$ a positive integer) is called a *generalized Boolean function* in n variables [18]. Let GB_n^q be the set of all n-variable generalized Boolean functions from Z_2^n to Z_q. If $q = 2$, we obtain the classical Boolean functions in n variables, whose set will be denoted by B_n. The *Hamming weight* wt (u) of a vector $u \in Z_2^n$ is the weight of the binary string.

The *(generalized) Walsh-Hadamard transform* of $f \in GB_n^q$ is the complex valued function over Z_2^n which is defined as

$$H_f(\omega) = \sum_{x \in Z_2^n} \zeta^{f(x)} (-1)^{\omega \cdot x},$$

where $\zeta (= e^{2\pi i/q})$ is the complex q-primitive root of unity. When $q = 2$, we obtain the Walsh transform of $f \in B_n$, which will be denoted by W_f. A generalized Boolean function $f \in GB_n^q$ is *generalized bent Boolean* function if and only if $|H_f(\omega)| = 2^{n/2}$ for all $\omega \in Z_2^n$. In this article, we shall call these functions *gbent* functions. Note that when $q = 2$, Boolean bent functions exists only if the number of variables, n, is even. For $q > 2$, if f is a gbent function in n variables, it does not follow that n must be even. Such functions for $q = 4$ were investigated by Schmidt [17], Solé and Tokareva[18], Stănică, Martinsen, Gangopadhyay, and Singh[22], *etc*.

If $2^{h-1} < q \leq 2^h$, for any $f \in GB_n^q$ we associate a unique sequence of Boolean functions $\upsilon_i \in B_n$ $(i = 0, 1, \cdots, h-1)$ such that

$$f(x) = \upsilon_0(x) + 2\upsilon_1(x) + \cdots + 2^{h-1}\upsilon_{h-1}(x), \ for \ all \ x \in Z_2^n. \tag{1}$$

If $q = 4$, then for $f \in GB_n^4$ as in (1) we define the Gray map $\psi(f): GB_n^4 \to B_n$ by

$$\psi(f)(z, x) = \upsilon_0(x) z \oplus \upsilon_1(x), \ for \ all \ (z, x) \in Z_2 \times Z_2^n.$$

The function $\psi(f)$ is referred to as the Gray image of f [22].

We call the functions, from Z_2^n to Z_2^m, (n, m)-functions. Such function F being given, the Boolean functions $f_1, \ldots, f_m$ defined, at every $x \in Z_2^n$, by $F(x) = (f_1(x), \cdots, f_m(x))$, are called the *coordinate functions* of F. For a nonzero vector $u \in Z_2^n$, the function $F_u = u_0 f_1 \oplus \cdots \oplus u_m f_m$ is a called a *component function* of F. Obviously, these functions include the (single-output) Boolean functions which correspond to the case $m = 1$. Furthermore, for $m = n$, the function $F = (f_1, \cdots, f_n)$ is called a Boolean permutation if F is a bijective mapping from Z_2^n to Z_2^m.

The original Maiorana-McFarland's (M-M) class of bent functions [14] is the set of all the (bent) Boolean functions on $Z_2^{2n} = \{(x,y) \mid x, y \in Z_2^n\}$ of the form:

$$f(x,y) = x \cdot \varphi(y) \oplus g(y) \quad (2)$$

where φ is any permutation on Z_2^n and $g \in B_n$.

2.1. Definition [23] Let $f \in B_n$. If there exists an even integer r, $0 \le r \le n$, such that $\|\{\omega \mid W_f(\omega) \ne 0, \omega \in F_2^n\}\| = 2^r$, where $\|\cdot\|$ denotes the size of a set, and $(W_f(\omega))^2$ equals 2^{2n-r} or 0, for every $\omega \in F_2^n$, then f is called an r th-order plateaued function in n variables. If f is a $2\lceil \frac{n-2}{2} \rceil$ th-order plateaued function in n variables, where $\lceil n/2 \rceil$ denotes the smallest integer exceeding $n/2$, then f is also called a semi-bent function.

3. Main Results

In this section, we present two constructions of generalized bent Boolean functions on odd number of variables.

We first recall a lemma which plays an important role in the part.

3.1. Lemma [18, 22] Let n be a positive odd integer and $f \in GB_n^4$, $\upsilon_0, \upsilon_1 \in B_n$ such that $f(x) = \upsilon_0(x) + 2\upsilon_1(x)$ for all $x \in Z_2^n$. Then the following statements are equivalent:

(1)The generalized Boolean function $f \in GB_n^4$ is gbent;

(2)$\psi(f)$ $(i.e., \psi(f)(z,x) = \upsilon_0(x)z \oplus \upsilon_1(x),\ for\ all (z,x) \in Z_2 \times Z_2^n)$ is bent.

From the above lemma, we have the following theorem.

3.2. Theorem Let n be a positive even number and $\theta \in B_n$. Let $X = (x_1, x_2, \cdots, x_n) \in Z_2^n$ and $x^{(j_i)} = (x_1, \cdots, x_{j-1}, i, x_{j+1}, \cdots, x_n) \in Z_2^n$, where $j \in \{1, 2, \cdots, n\}, i = 0,1$. Set

$$\upsilon_1(x^{(j_0)}) = \theta(x^{(j_0)}),\ for\ all\ x^{(j_0)} \in Z_2^n \quad (1)$$

and

$$\upsilon_0(x^{(j_0)}) = \theta(x^{(j_1)}) \oplus \theta(x^{(j_0)}),\ for\ all\ x^{(j_0)}, x^{(j_1)} \in Z_2^n. \quad (2)$$

If $\theta \in B_n$ is a bent function, then $f \in GB_n^4$, defined as $f(x^{(j_0)}) = \upsilon_0(x^{(j_0)}) + 2\upsilon_1(x^{(j_0)})$, is gbent.

Proof. Let $\psi(f)$ be Gray image of f. Then

$$\psi(f)(x_j, x^{(j_0)}) = x_j \upsilon_0(x^{(j_0)}) \oplus \upsilon_1(x^{(j_0)}).$$

Further, from Equations (1) and (2), we have

$$\psi(f)(x_j, x^{(j_0)}) = x_j \theta(x^{(j_0)}) \oplus (x_j \oplus 1)\theta(x^{(j_0)}),$$

that is, $\psi(f) = \theta$. Thus, if θ is bent, then from Lemma 1, f is gbent.

Remark 1. From the above theorem, we know for any bent function, a gbent function in GB_n^4 can be obtained.

In the following, we present a new method to construct gbent functions in GB_n^4 on odd number of variables.

3.3. Theorem Let σ be a permutation on Z_2^n, and let $g \in B_n$ be an function satisfying $g(\sigma^{(-1)}(\alpha)) = g(\sigma^{(-1)}(\alpha \oplus (1,0,\cdots,0))) \oplus 1$, where $\alpha \in Z_2^n$. Let $Y \in Z_2^n$ and $X = (x_1, x_2, \cdots, x_n) \in Z_2^n$, $x^{(j_i)} = (x_1, \cdots, x_{j-1}, i, x_{j+1}, \cdots, x_n) \in Z_2^n$, where $j \in \{1, 2, \cdots, n\}, i = 0,1$. Let the function $f: Z_2^n \to Z_2$ be defined as

$$f'(x^{(j_i)}, Y) = g(Y) + 2\sigma(Y) \cdot x^{(j_i)},\ for\ all\ x^{(j_i)}, Y \in Z_2^n,$$

is a gbent function in $2n-1$ variables.

Proof. Without lose of generality, we set $j = 1$ and $i = 0$.

Compute

$$\begin{aligned} H_{f'}(\alpha,\beta) &= \sum_{Y \in Z_2^n} \sum_{x^{(1_0)} \in Z_2^n} \zeta^{f'(x^{(1_0)},Y)} (-1)^{\alpha \cdot x^{(1_0)} \oplus \beta \cdot Y} \\ &= \sum_{Y \in Z_2^n} \zeta^{g(Y)} (-1)^{\beta \cdot Y} \sum_{x^{(1_0)} \in Z_2^n} (-1)^{(\sigma(Y) \oplus \alpha) \cdot x^{(1_0)}} \\ &= 2^{n-1} \sum_{Y \in Z_2^n} \zeta^{g(Y)} (-1)^{\beta \cdot Y} \varphi_{\{0_n\}}(\sigma(Y) \oplus \alpha) \\ &+ 2^{n-1} \sum_{Y \in Z_2^n} \zeta^{g(Y)} (-1)^{\beta \cdot Y} \varphi_{\{0_n\}}(\sigma(Y) \oplus \alpha \oplus (1,0,\cdots,0)). \qquad (3) \\ &= 2^{n-1} \zeta^{g(\sigma^{(-1)}(\alpha)) + 2\beta \cdot \sigma^{(-1)}(\alpha)} \\ &+ 2^{n-1} \zeta^{g\left(\sigma^{(-1)}(\alpha \oplus (1,0,\cdots,0))\right) + 2\beta \cdot \sigma^{(-1)}(\alpha \oplus (1,0,\cdots,0))} \\ &= 2^{n-1} \zeta^{g(\sigma^{(-1)}(\alpha)) + 2\beta \cdot \sigma^{(-1)}(\alpha)} \\ &+ 2^{n-1} \zeta^{1 + g\left(\sigma^{(-1)}(\alpha)\right) + 2\beta \cdot \sigma^{(-1)}(\alpha \oplus (1,0,\cdots,0))} \end{aligned}$$

From the above relationship, there are four cases to be considered.

(1)For $\beta \cdot \sigma^{(-1)}(\alpha) = 0$ and $\beta \cdot \sigma^{(-1)}\left(\alpha \oplus (1,0,\cdots,0)\right) = 0$, we have

$$H_{f'}(\alpha,\beta) = 2^{n-1} \zeta^{g(\sigma^{(-1)}(\alpha))} (1 + \zeta), \qquad (4)$$

Further, $|H_{f'}(\alpha,\beta)| = 2^{\frac{2n-1}{2}}$.

(2) For $\beta \cdot \sigma^{(-1)}(\alpha) = 1$ and $\beta \cdot \sigma^{(-1)}\left(\alpha \oplus (1,0,\cdots,0)\right) = 0$, we have

$$H_{f'}(\alpha,\beta) = 2^{n-1} \zeta^{g(\sigma^{(-1)}(\alpha))} (-1 + \zeta), \qquad (5)$$

Further, $|H_{f'}(\alpha,\beta)| = 2^{\frac{2n-1}{2}}$.

(3) For $\beta \cdot \sigma^{(-1)}(\alpha) = 0$ and $\beta \cdot \sigma^{(-1)}\left(\alpha \oplus (1,0,\cdots,0)\right) = 1$, we have

$$H_{f'}(\alpha,\beta) = 2^{n-1} \zeta^{g(\sigma^{(-1)}(\alpha))} (1 - \zeta), \qquad (6)$$

Further, $|H_{f'}(\alpha,\beta)| = 2^{\frac{2n-1}{2}}$.

(4) For $\beta \cdot \sigma^{(-1)}(\alpha) = 1$ and $\beta \cdot \sigma^{(-1)}\left(\alpha \oplus (1,0,\cdots,0)\right) = 1$, we have

$$H_{f'}(\alpha,\beta) = -2^{n-1} \zeta^{g(\sigma^{(-1)}(\alpha))} (1 + \zeta), \qquad (7)$$

Further, $|H_{f'}(\alpha,\beta)| = 2^{\frac{2n-1}{2}}$.

Remark 2. For any Boolean permutation σ, the function g is easy to be obtained.

4. Conclusion

In this note we have developed further construction method concerning the design of generalized bent Boolean functions on odd number of variables. We first proposed a construction of generalized bent Boolean functions with values in Z_4. Further, we utilized

Boolean permutations and special functions g to characterize a class of generalized bent Boolean functions on odd number of variables.

Acknowledgements

This work was supported in part by National Science Foundation of China (61303263, 61272254), in part by the Fundamental Research Funds for the Central Universities (2013QNA26), and in part by the Jiangsu Planned Projects for Postdoctoral Research Funds (1401056B)

References

[1] A. Canteaut, M. Daum, H. Dobbertin and G. Leander, "Normal and Non-Normal Bent Functions", Proceedings of the Workshop on Coding and Cryptography 2003, **(2003)** March 24-28; Versailles, France, pp.910-100.
[2] C. Carlet, "Two new classes of bent functions", Advances in EUROCRYPT'93, **(1993)** May 23–27; Lofthus, Norway, pp. 77–101.
[3] C. Carlet, "Generalized partial spreads", IEEE Trans. Inf. Theory, 41, **(1995)**, pp. 1482–1487.
[4] C. Carlet, "On bent and highly nonlinear balanced/resilient functions and their algebraic immunities", 16th International Symposium, AAECC-16, **(2006)**, February 20-24; Las Vegas, NV, USA, pp. 1–28.
[5] C. Carlet, "Boolean functions for cryptography and error correcting codes", in Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Edits Y. Crama , P. Hammer, Cambridge University Press, **(2010)**, pp. 257–397.
[6] C. Carlet, H. Dobbertin and G. Leander, "Normal extensions of bent functions, IEEE Trans. Inf. Theory, vol. 50, **(2004)**, pp. 2880–2885.
[7] C. Carlet, F. Zhang and Y. Hu, "Secondary constructions of bent functions and their enforcement", Advances in Mathematics of Communications, vol. 6, **(2012)**, pp. 305–314.
[8] J. Dillon, "Elementary Hadamard difference sets", Ph.D. dissertation, Univ. Maryland, College Park, **(1974)**.
[9] H. Dobbertin and G. Leander, "Bent functions embedded into the recursive framework of [Trial mode]-bent functions", Des. Codes Cryptogr., vol. 49, **(2008)**, pp. 3–22.
[10] P. Guillot, "Completed GPS Covers All Bent Functions", Combin. Theory Ser. A, vol. 93, **(2001)**, pp. 242–260.
[11] P. V. Kumar, R. A. Scholtz, L. R. Welch, "Generalized bent functions and their properties", Combin. Theory Ser. A, vol. 40, **(1985)**, pp. 90–107.
[12] G. Leander and G. McGuire, "Construction of bent functions from near-bent functions", Combin. Theory Ser. A, vol. 116, **(2009)**, pp. 960–970.
[13] F. J. Mac Williams and N. J. A. Sloane, in "The theory of Error-Correcting Codes", North Holland Publishing Co., North-Holland, Amsterdam **(1977)**, chapter 14, pp.406-431.
[14] R. I. McFarland, "A family of difference sets in non-cyclic groups", Comb. Theory, Ser. A., vol. 15, **(1973)**, pp. 1–10.
[15] J. D. Olsen, R. A. Scholtz and L. R. Welch, "Bent-function sequence", IEEE Trans. Inf. Theory, vol. 28, **(2003)**, pp. 1769–1780.
[16] O. S. Rothaus, "on 'bent' functions", Combin. Theory ser. A, vol. 20, **(1976)**, pp. 300–305.
[17] K.-U. Schmidt, "Quaternary constant-amplitude codes for multimode CDMA, IEEE Trans. Inf. Theory, vol. 55, **(2009)**, pp. 1824–1832.
[18] P. Solé, N. Tokareva, "Connections Between Quaternary and Binary Bent Functions", Available at http://eprint.iacr.org/2009/544.pdf.
[19] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. Kar Gangopadhyay, S. Maitra, "Nega-Hadamard transform, bent and negabent functions", 6th International Conference, Sequences and Their Applications—SETA 2010, **(2010)** September 13-17; Paris, France, pp. 359–372.
[20] P. Stănică, S. Gangopadhyay, B. K. Singh, "Some Results Concerning Generalized Bent Functions". Available at http:// eprint.iacr.org/2011/290.pdf.
[21] P. Stănică, T. Martinsen, "Octal Bent Generalized Boolean Functions". Available at http://eprint.iacr.org/2011/089.pdf.
[22] P. Stănică, T. Martinsen, S. Gangopadhyay, B. K. Singh, "Bent and generalized bent Boolean functions", Des. Codes Cryptogr., vol. 69, **(2013)**, pp. 77–94.
[23] Y. Zheng, Zhang, X. M, "Relationships between bent functions and complementary plateaued functions". Proceedings Second International Conference, Information Security and Cryptology (ICISC'99), **(1999)** December 9-10; Seoul, Korea, pp. 60–75.

Author

Yong-Bin Zhao received the MS degrees in cryptology from Xidian University, China. Currently, he is an associate professor in College of Information Science and Technology at Shijiazhuang Tiedao University. His research interests in Bioinformatics, stream cipher and Boolean functions.