Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 24, 2018, No. 4, 38–44
DOI: 10.7546/nntdm.2018.24.4.38-44

Results on generalized negabent functions

Rashmeet Kaur and Deepmala Sharma

Department of Mathematics, National Institute of Technology, Raipur
Raipur, 49010, Chhattisgarh, India
e-mails: rashmeetkaur2739@yahoo.com,
deepsha.maths@nitrr.ac.in

Received: 29 January 2018 **Revised:** 18 October 2018 **Accepted:** 22 October 2018

Abstract: In this article, we characterize generalized negabent functions on $\mathbb{Z}_2^n$ with values in $\mathbb{Z}_8$ and $\mathbb{Z}_{16}$. Furthermore, we propose several constructions of generalized negabent functions.

Keywords: Boolean function, Generalized negabent, Nega-Hadamard transform.
2010 Mathematics Subject Classification: 94A60, 94C10, 06E30.

1 Introduction

Boolean Bent functions are the functions having optimal nonlinearity. Bent functions were introduced by Rothaus [3]. Bent function is an important combinatorial object having a wide range of applications in coding theory, difference set theory and cryptography. Although few classes of Bent functions have been analyzed, a complete characterization of Bent functions is still elusive. In recent years, researchers have focused on the generalization of Boolean functions and also examined the effect of Walsh–Hadamard transform on them. In [4] Schmidt considered functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ and due to more natural connection to cyclic codes over rings, these functions have drawn more attention. Later Sole and Tokareva [5] considered functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$ and called these functions as generalized Boolean functions. They also conferred the direct link between Bent functions and generalized Bent functions. In [2] Parker and Pott considered nega-Hadamard transform and introduced negabent functions. Negabent functions are the functions having flat spectra under nega-Hadamard transform. The functions which are both Bent and negabent are called bent-negabent functions. Bent-negabent functions are interesting to study as they possess extreme properties in terms of two different Fourier transform. The generalization of negabent function is called generalized negabent function [1]. Generalized negabent functions have flat spectrum with respect to generalized nega-Hadamard transform.

In this article, we study generalized negabent functions and by using negabent functions, we propose several constructions of generalized negabent functions on $\mathbb{Z}_8$ and $\mathbb{Z}_{16}$.

2 Preliminaries

Boolean function is a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$, where $\mathbb{Z}_2^n$ is an n-dimensional vector space over $\mathbb{Z}_2$. The set of all n-variable Boolean functions is denoted by $\mathcal{B}_n$. Hamming weight of $f \in \mathcal{B}_n$ is defined by the number of elements in the set $|wt(f) = \{x \in \mathbb{Z}_2^n : f(x) = 1\}|$. Hamming distance between two Boolean functions $f, g \in \mathcal{B}_n$ is defined by the number of positions in which the functions differ and is denoted by $d(f, g)$. Every Boolean function has a unique representation called its algebraic normal form

$$f(x_1, x_2, \cdots, x_n) = \oplus_{I \subseteq \{1,2,\cdots,n\}} a_I \prod_{i \in I} x_i,$$

where $a_I \in \mathbb{Z}_2$.

The algebraic degree of $f \in \mathcal{B}_n$ is defined by the degree of highest monomial with non-zero coefficient.

The functions with algebraic degree at most one are called affine Boolean functions. The set of all n-variable affine Boolean functions is denoted by $\mathcal{A}_n$. If the constant term of an affine Boolean function is zero, then it is called linear Boolean function.

The scalar product of two vectors $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$ is defined by $x \cdot y = x_1 y_1 \oplus x_2 y_2 \oplus \cdots \oplus x_n y_n$.

Walsh–Hadamard transform of f at any point $\lambda \in \mathbb{Z}_2^n$ is defined by

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

Nonlinearity and Walsh–Hadamard transform are related as

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{Z}_2^n} |W_f(\lambda)|.$$

By using Parseval's equality

$$\sum_{\lambda \in \mathbb{Z}_2^n} W_f(\lambda)^2 = 2^{2n},$$

we have

$$nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

A Boolean function $f \in \mathcal{B}_n$ is said to be a Bent function if it possesses maximum nonlinearity.

Generalized Boolean function is a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$ ($q \geq 2$, a positive integer). The set of all n-variable generalized Boolean functions is denoted by $\mathcal{GB}_n^q$. Generalized Walsh–Hadamard transform of $f \in \mathcal{GB}_n^q$ at any point u is defined by

$$\mathcal{H}_f(u) = \frac{1}{2^{\frac{n}{2}}} \sum_{x \in \mathbb{Z}_2^n} \zeta^{f(x)} (-1)^{u \cdot x},$$

where $\zeta = e^{\frac{2\pi i}{q}}$ is the q-th primitive root of unity. A function $f \in \mathcal{GB}_n^q$ is said to be a generalized Bent function if and only if $|\mathcal{H}_f(u)| = 1$ for all $u \in \mathbb{Z}_2^n$.

Nega-Hadamard transform of f at $u \in \mathbb{Z}_2^n$ is given by

$$\mathcal{N}_f(u) = \frac{1}{2^{\frac{n}{2}}} \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus u \cdot x} i^{wt(x)}.$$

The nega spectrum of a Boolean function f contains all values $\{\mathcal{N}_f(u) | u \in \mathbb{Z}_2^n\}$. A function is said to be negabent if and only if $|\mathcal{N}_f(u)| = 1$, for all $u \in \mathbb{Z}_2^n$.

Generalized nega-Hadamard transform of f at any point u is defined by

$$\mathcal{N}_f^q(u) = \frac{1}{2^{\frac{n}{2}}} \sum_{x \in \mathbb{Z}_2^n} \zeta^{f(x)} (-1)^{u \cdot x} i^{wt(x)}.$$

A function $f \in \mathcal{B}_n^q$ is said to be a generalized negabent function if $|\mathcal{N}_f^q(u)| = 1$ for all $u \in \mathbb{Z}_2^n$.

3 Construction of generalized negabent function in $\mathbb{Z}_8$

Stanica et al. [6] have presented several classes of generalized Bent functions with values in $\mathbb{Z}_8$. In this section, we define several classes of generalized negabent functions in $\mathbb{Z}_8$.

Theorem 3.1. *Let $f : \mathbb{Z}_2^{n+1} \to \mathbb{Z}_8$ be defined by*

$$f(x, y) = 4g(x) + (4h(x) + 4g(x))y, \tag{1}$$

then f is generalized negabent if g and h are negabent functions.

Moreover, if f_1 is given by

$$f_1(x, y) = 4g(x) + (4h(x) + 2g(x))y, \tag{2}$$

then f_1 is generalized negabent if g, h and $g \oplus h$ are negabent and if $\mathcal{N}_h(u) = \mathcal{N}_{g \oplus h}(u)$.

Proof. We compute generalized nega-Hadamard coefficient

$$\begin{aligned}\mathcal{N}_f^q(u, v) =& \frac{1}{2^{n+1/2}} \sum_{x \in \mathbb{Z}_2^n} \left(\zeta^{4g(x)} (-1)^{u \cdot x} i^{wt(x)} + i \zeta^{4h(x)} (-1)^{u \cdot x} i^{wt(x)} (-1)^v \right) \\ =& \frac{1}{\sqrt{2}} \sum_{x \in \mathbb{Z}_2^n} (-1)^{g(x) \oplus u \cdot x} i^{wt(x)} + i (-1)^{h(x) \oplus u \cdot x} i^{wt(x)} (-1)^v\end{aligned}$$

$$\sqrt{2} \mathcal{N}_f^q(u, v) = \mathcal{N}_g(u) + i(-1)^v \mathcal{N}_h(u).$$

By taking square of norm, we obtain

$$2|\mathcal{N}_f^q(u, v)|^2 = \mathcal{N}_g(u)^2 + \mathcal{N}_h(u)^2.$$

Since g and h are negabent, we have $|\mathcal{N}_g(u)| = |\mathcal{N}_h(u)| = 1$. So $|\mathcal{N}_f^q(u, v)| = 1$, Therefore f is generalized negabent function.

For the second claim, again we compute the generalized nega-Hadamard coefficient

$$\sqrt{2}\mathcal{N}^q_{f_1}(u,v) = \sum_{x\in\mathbb{Z}_2^n} \left((-1)^{g(x)\oplus u\cdot x} i^{wt(x)} + i(-1)^{g(x)\oplus h(x)\oplus u\cdot x} i^{wt(x)}(-1)^v i^{g(x)}\right).$$

Now by putting $i^{g(x)} = \frac{1+(-1)^{g(x)}}{2} + i\frac{1-(-1)^{g(x)}}{2}$, we obtain

$$\sqrt{2}\mathcal{N}^q_{f_1}(u,v) = \mathcal{N}_g(u) + (-1)^v\left(\frac{\mathcal{N}_h(u)}{2} + i\frac{\mathcal{N}_h(u)}{2} - \frac{\mathcal{N}_{g\oplus h}(u)}{2} + i\frac{\mathcal{N}_{g\oplus h}(u)}{2}\right).$$

By taking square of norm, we get

$$\begin{aligned}2|\mathcal{N}^q_{f_1}(u,v)|^2 &= \frac{1}{2}\mathcal{N}_h(u)^2 + \frac{1}{2}\mathcal{N}_{g\oplus h}(u)^2 + \mathcal{N}_g(u)^2 + (-1)^v(\mathcal{N}_h(u)\mathcal{N}_g(u) - \mathcal{N}_{g\oplus h}(u)\mathcal{N}_h(u)) \\ &= \frac{1}{2}(\mathcal{N}_h(u)^2 + \mathcal{N}_{g\oplus h}(u)^2 + 2\mathcal{N}_g(u)^2) + (-1)^v(\mathcal{N}_h(u)\mathcal{N}_g(u) - \mathcal{N}_{g\oplus h}(u)\mathcal{N}_g(u)).\end{aligned}$$

Since g, h and $g\oplus h$ are all negabent functions, so, $|\mathcal{N}_h(u)| = |\mathcal{N}_g(u)| = |\mathcal{N}_{g\oplus h}(u)| = 1$ and by the imposed condition the remaining coefficients become zero.

Hence, we obtain $|\mathcal{N}^q_{f_1}(u,v)| = 1$. So, f_1 is generalized negabent. □

Theorem 3.2. *Let $f : \mathbb{Z}_2^{n+2} \to \mathbb{Z}_8$ be defined by*

$$f(x,y,z) = 4g(x) + (4h(x) + 4g(x) + 1)y + (4k(x) + 4g(x) + 1)z - 2yz, \tag{3}$$

then f is generalized negabent if g, h, k and $g\oplus h\oplus k$ are negabent functions with

$$\mathcal{N}_g(u)\mathcal{N}_h(u) = \mathcal{N}_k(u)\mathcal{N}_{g\oplus h\oplus k}(u). \tag{4}$$

Moreover, if f_1 is given by

$$f_1(x,y,z) = 4g(x) + (4h(x) + 2g(x) + 1)y + (4k(x) + 2g(x) + 1)z - 2yz, \tag{5}$$

then f_1 is generalized negabent if g, h, k, $g\oplus h$, $k\oplus g$ and $h\oplus k$ are all negabent functions and

$$\mathcal{N}_h(u)\mathcal{N}_k(u) + \mathcal{N}_{g\oplus h}(u)\mathcal{N}_{k\oplus g(u)} = 2\mathcal{N}_g(u)\mathcal{N}_{h\oplus k}(u). \tag{6}$$

Proof. We compute generalized nega-Hadamard coefficient

$$\begin{aligned}\mathcal{N}^q_f(u,v,w) =& \frac{1}{2^{n+2/2}}\sum_{x\in\mathbb{Z}_2^n}\left(\zeta^{4g(x)}(-1)^{u\cdot x}i^{wt(x)} + i\zeta^{4h(x)+1}(-1)^{u\cdot x}i^{wt(x)}(-1)^v\right. \\ &\left. + i\zeta^{4k(x)+1}(-1)^{u\cdot x}i^{wt(x)}(-1)^w + i^2\zeta^{4g(x)+4h(x)+4k(x)}(-1)^{u\cdot x}i^{wt(x)}(-1)^{v\oplus w}\right) \\ =& \frac{1}{2}\sum_{x\in\mathbb{Z}_2^n}\left((-1)^{g(x)\oplus u\cdot x}i^{wt(x)} + i(-1)^{h(x)\oplus u\cdot x}\zeta(-1)^v i^{wt(x)}\right. \\ &\left. + i(-1)^{k(x)\oplus u\cdot x}\zeta(-1)^w i^{wt(x)} - (-1)^{g(x)\oplus h(x)\oplus k(x)\oplus u\cdot x}(-1)^{v\oplus w}i^{wt(x)}\right) \\ =& \frac{1}{2}(\mathcal{N}_g(u) + i(-1)^v\mathcal{N}_h(u)\zeta + i(-1)^w\mathcal{N}_k(u)\zeta - (-1)^{v\oplus w}\mathcal{N}_{g\oplus h\oplus k}(u)).\end{aligned}$$

Now putting $\zeta = \frac{1+i}{\sqrt{2}}$, we obtain

$$\begin{aligned}2\mathcal{N}_f^q(u,v,w) &= \mathcal{N}_g(u) + (-1)^v \left(\frac{i\mathcal{N}_h(u) - \mathcal{N}_h(u)}{\sqrt{2}}\right)\\ &\quad + (-1)^w \left(\frac{i\mathcal{N}_k(u) - \mathcal{N}_k(u)}{\sqrt{2}}\right) - (-1)^{v\oplus w}\mathcal{N}_{g\oplus h\oplus k}(u).\end{aligned}$$

Now, by taking square of norm, we obtain

$$\begin{aligned}4|\mathcal{N}_f^q(u,v,w)|^2 &= \mathcal{N}_g(u)^2 + \mathcal{N}_h(u)^2 + \mathcal{N}_k(u)^2 + \mathcal{N}_{g\oplus h\oplus k}(u)^2\\ &\quad + 2(-1)^{v\oplus w}(\mathcal{N}_g(u)\mathcal{N}_h(u) - \mathcal{N}_k(u)\mathcal{N}_{g\oplus h\oplus k}(u))\\ &\quad + \sqrt{2}(-1)^v(\mathcal{N}_g(u)\mathcal{N}_k(u) - \mathcal{N}_h(u)\mathcal{N}_{g\oplus h\oplus k}(u))\\ &\quad + \sqrt{2}(-1)^w(\mathcal{N}_h(u)\mathcal{N}_k(u) - \mathcal{N}_g(u)\mathcal{N}_{g\oplus h\oplus k}(u)).\end{aligned}$$

Since g, h, k and $g \oplus h \oplus k$ are all negabent functions. So

$$|\mathcal{N}_g(u)| = |\mathcal{N}_h(u)| = |\mathcal{N}_g(u)| = |\mathcal{N}_{g\oplus h\oplus k}(u)| = 1.$$

By using the imposed conditions, the remaining coefficients are all zero.
Hence, $|\mathcal{N}_f^q(u,v,w)| = 1$. So, f is a generalized negabent function.
For the second claim, we compute the generalized nega-Hadamard coefficient

$$\begin{aligned}2\mathcal{N}_{f_1}^q(u,v,w) = \sum_{x\in\mathbb{Z}_2^n} &\big((-1)^{g(x)\oplus u\cdot x} i^{wt(x)} + i(-1)^{g(x)\oplus k(x)\oplus u\cdot x} i^{g(x)}\zeta(-1)^v i^{wt(x)}\\ &+ i(-1)^{g(x)\oplus h(x)\oplus u\cdot x} i^{g(x)}\zeta(-1)^w i^{wt(x)} - (-1)^{h(x)\oplus k(x)\oplus u\cdot x}(-1)^{v\oplus w} i^{wt(x)}\big)\\ &= \mathcal{N}_g(u) + \frac{(-1)^v\zeta}{2}\big(i\mathcal{N}_{g\oplus k}(u) + i\mathcal{N}_k(u) - \mathcal{N}_{g\oplus k}(u) + \mathcal{N}_k(u)\big)\\ &+ \frac{(-1)^w\zeta}{2}\big(i\mathcal{N}_{g\oplus h}(u) + i\mathcal{N}_h(u) - \mathcal{N}_{g\oplus h}(u) + \mathcal{N}_h(u)) - (-1)^{v\oplus w}\mathcal{N}_{h\oplus k}(u)\big)\\ &= \mathcal{N}_g(u) + \frac{(-1)^v}{\sqrt{2}}\big(i\mathcal{N}_h(u) - \mathcal{N}_{g\oplus h}(u)\big)\\ &+ \frac{(-1)^w}{\sqrt{2}}\big(i\mathcal{N}_k(u) - \mathcal{N}_{g\oplus k}(u)\big) - (-1)^{v\oplus w}\mathcal{N}_{h\oplus k}(u).\end{aligned}$$

By taking square of the norm, we obtain

$$\begin{aligned}4|\mathcal{N}_{f_1}^q(u,v,w)|^2 =& \frac{1}{2}\mathcal{N}_h(u)^2 + \frac{1}{2}\mathcal{N}_k(u)^2 + \frac{1}{2}\mathcal{N}_{g\oplus h}(u)^2 + \frac{1}{2}\mathcal{N}_{g\oplus k}(u)^2 + \mathcal{N}_g(u)^2 + \mathcal{N}_{h\oplus k}(u)^2\\ &+ (-1)^v\sqrt{2}(\mathcal{N}_{g\oplus k}(u)\mathcal{N}_{h\oplus k}(u) - \mathcal{N}_g(u)\mathcal{N}_{g\oplus h}(u))\\ &+ (-1)^w\sqrt{2}(\mathcal{N}_{g\oplus h}(u)\mathcal{N}_{h\oplus k}(u) - \mathcal{N}_g(u)\mathcal{N}_{g\oplus k}(u))\\ &+ (-1)^{v\oplus w}(\mathcal{N}_h(u)\mathcal{N}_k(u) + \mathcal{N}_{g\oplus h}(u)\mathcal{N}_{k\oplus g}(u) - 2\mathcal{N}_g(u)\mathcal{N}_{h\oplus k}(u)).\end{aligned}$$

Since g, h, k, $g \oplus h$, $k \oplus g$ and $h \oplus k$ are all negabent. So

$$|\mathcal{N}_g(u)| = |\mathcal{N}_h(u)| = |\mathcal{N}_k(u)| = |\mathcal{N}_{g\oplus h}(u)| = |\mathcal{N}_{k\oplus g}(u)| = |\mathcal{N}_{h\oplus k}(u)| = 1.$$

The remaining coefficients become zero by applying the imposed condition. Hence, we obtain $|\mathcal{N}_{f_1}^q(u,v,w)| = 1$. So f_1 is a generalized negabent function. □

4 Construction of generalized negabent function in $\mathbb{Z}_{16}$

Theorem 4.1. *Let $f : \mathbb{Z}_2^{n+1} \to \mathbb{Z}_{16}$ be defined by*

$$f(x, y) = 8g(x) + (8h(x) + 8k(x) + 8g(x))y, \tag{7}$$

then f is generalized negabent if and only if g and $h \oplus k$ are negabent functions.

Moreover, if f_1 is given by

$$f_1(x, y) = 8g(x) + (8h(x) + 8k(x) + 4g(x))y, \tag{8}$$

then f_1 is generalized negabent if g, $h \oplus k$ and $g \oplus h \oplus k$ are negabent and if $\mathcal{N}_{h\oplus k}(u) = \mathcal{N}_{g\oplus h\oplus k}(u)$.

Further if $f_2 : \mathbb{Z}_2^{n+2} \to \mathbb{Z}_{16}$ is given by

$$f_2(x, y, z) = 8g(x) + (8h(x) + 4)y + (8k(x) + 4)z + (8l(x) + 4)(1 + y)(1 + z) - 4yz, \tag{9}$$

then f_2 is generalized negabent if $g \oplus l$, $g \oplus k$, $g \oplus h$ and $g \oplus h \oplus k$ are negabent and if

$$\mathcal{N}_{g\oplus k}(u)\mathcal{N}_{g\oplus h}(u) = \mathcal{N}_{g\oplus l}(u)\mathcal{N}_{g\oplus h\oplus k}(u). \tag{10}$$

Proof. We shall only show the third claim, since the proof of remaining ones are same as that of Theorem 3.1. The generalized nega-Hadamard coefficient is given by

$$2\mathcal{N}^q_{f_2}(u, v, w) = i\mathcal{N}_{g\oplus l}(u) - (-1)^v\mathcal{N}_{g\oplus h}(u) - (-1)^w\mathcal{N}_{g\oplus k}(u) - i(-1)^{v\oplus w}\mathcal{N}_{g\oplus h\oplus k}(u).$$

By taking square of norm, we get

$$\begin{aligned} 4|\mathcal{N}^q_{f_2}(u, v, w)|^2 &= \mathcal{N}_{g\oplus l}(u)^2 + \mathcal{N}_{g\oplus h}(u)^2 + \mathcal{N}_{g\oplus k}(u)^2 + \mathcal{N}_{g\oplus h\oplus k}(u)^2 \\ &\quad + 2(-1)^{v\oplus w}(\mathcal{N}_{g\oplus k}(u)\mathcal{N}_{g\oplus h}(u) - \mathcal{N}_{g\oplus l}(u)\mathcal{N}_{g\oplus h\oplus k}(u)), \end{aligned}$$

since $g \oplus l$, $g \oplus k$, $g \oplus h$ and $g \oplus h \oplus k$ are all negabent functions. Using the imposed condition the remaining coefficients become zero. Hence $|\mathcal{N}^q_{f_2}(u, v, w)| = 1$. □

References

[1] Chaturvedi, A., & Gangopadhyay, A. K. (2013) On Generalized NegaHadamard Transform, In: Singh K., Awasthi A.K. (eds) Quality, Reliability, Security and Robustness in Heterogeneous Networks. QShine 2013. *Lectures Notes of the Institute for Computer Sciences, Social Informatics and Telecommunication Engineering*, Vol. 115, Springer, Berlin, 771–777.

[2] Parker, M. G., & Pott, A. (2007) On Boolean Functions Which Are Bent and Negabent, Sequences, Subsequences and consequences, *Lecture Notes in Computer Science*, Vol. 4893, Springer, Berlin, 9–23.

[3] Rothaus, O. S. (1976) On Bent functions, *Journal of Combinatorial Theory, Series A*, 20 (3), 300–305.

[4] Schmidt, K. U. (2009) Quaternary Constant-Amplitude Codes for Multicode CDMA, *IEEE Transactions on Information Theory*, 55 (4), 1824–1832.

[5] Sole, P., & Tokareva, N. (2009) Connections between Quaternary and Binary Bent Functions, In: *Cryptology ePrint Archives*, `http://eprint.iacr.org/2009/544.pdf`.

[6] Stanica, P., Martin, T., Gangopadhyay S., & Singh, B. K. (2013) Bent and generalized bent Boolean functions, *Designs Codes and Cryptography*, 69 (1), 77–94.