2017

A note on non-splitting Z-bent functions

Gangopadhyay, Sugata; Pasalic, Enes; Stnic, Pantelimon; Datta, Saral

Elsevier

S. Gangopadhyay, E. Pasalic, P. Stnica, S. Datta, "A note on non-splitting Z-bent functions,", Information Processing Letters, v.121, (2017), pp. 1-5.
http://hdl.handle.net/10945/55173

Information Processing Letters 121 (2017) 1–5

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

A note on non-splitting $\mathbb{Z}$-bent functions

Sugata Gangopadhyay [a,*], Enes Pasalic [b], Pantelimon Stănică [c], Saral Datta [d]

[a] Department of Computer Science and Engineering, Indian Institute of Technology Roorkee, India
[b] University of Primorska, Faculty of Mathematics, Natural Sciences, and Information Technologies (Famnit), Slovenia
[c] Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943-5216, USA
[d] Department of Mathematics, Brahmananda Keshab Chandra College, Kolkata, India

ARTICLE INFO

Article history:
Received 6 November 2014
Received in revised form 15 September 2016
Accepted 1 January 2017
Available online 9 January 2017
Communicated by A. Tarlecki

Keywords:
Cryptography
$\mathbb{Z}$-bent functions
Fourier spectrum
Walsh–Hadamard spectrum

ABSTRACT

In this note, we find constructions of non-splitting $\mathbb{Z}$-bent functions, thus solving an open problem of Dobbertin and Leander (2008) [4]. Under some technical conditions, we also construct $\mathbb{Z}$-bent functions of level $r+1$ that are not splitting into $\mathbb{Z}$-bent functions of level $r \geq 0$.

1. Introduction

Let $\mathbb{F}_2 = \{0, 1\}$ be the field containing two elements. For any positive integer n, the Cartesian product of n copies of $\mathbb{F}_2$ is $\mathbb{F}_2^n = \{\mathbf{x} = (x_1, \ldots, x_n) : x_i \in \mathbb{F}_2, \text{ for all } i \in \{1, \ldots, n\}\}$. The vectors $\mathbf{0}, \mathbf{1} \in \mathbb{F}_2^n$ are the vectors having each component equal to 0 and 1, respectively. Let the ring of integers be denoted by $\mathbb{Z}$ and, $\mathbb{R}$, $\mathbb{C}$ denote the fields of real and complex numbers, respectively. Addition over $\mathbb{F}_2^n$ is denoted by $\oplus$, whereas additions over $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ are denoted by $+$. Any function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a *Boolean function* on n variables. The set of all Boolean functions on n variables is denoted by $\mathfrak{B}_n$. We associate the *character form* of f (we borrow the notation from [1]), namely $\chi_f : \mathbb{F}_2^n \to \mathbb{F}_2$ defined by $\chi_f(\mathbf{x}) = (-1)^{f(\mathbf{x})}$. For a detailed study of Boolean functions (and their character forms) we refer to Carlet [1,2], and Cusick and Stănică [3].

An inner product (dot product) on $\mathbb{F}_2^n$ is defined by $\mathbf{x} \cdot \mathbf{y} = \bigoplus_{i=1}^n x_i y_i$, where $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n)$. The Hamming weight of $\mathbf{x} \in \mathbb{F}_2^n$ is $wt(\mathbf{x}) = \sum_{i=1}^n x_i$, that is, the number of nonzero components of $\mathbf{x}$.

Definition 1.1. Suppose $g : \mathbb{F}_2^n \to \mathbb{C}$. The Fourier transform of g at $\mathbf{u} \in \mathbb{F}_2^n$ is defined as

$$\widehat{g}(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} g(\mathbf{x})(-1)^{\mathbf{u} \cdot \mathbf{x}}. \tag{1}$$

The multi-set consisting of the values of $\widehat{g}(\mathbf{u})$ for all $\mathbf{u} \in \mathbb{F}_2^n$ is said to be the *Fourier spectrum* of the function g and each $\widehat{g}(\mathbf{u})$ is referred to as a *Fourier coefficient* of g. The set of Fourier coefficients is denoted by $Spec(g)$. The connection between the Fourier transforms of $f \in \mathfrak{B}_n$ and of χ_f is given by the well known identity [3], $\widehat{\chi_f}(\mathbf{x}) = -2\widehat{f}(\mathbf{x}) + 2^{n/2}\delta(\mathbf{x})$, where $\delta(\mathbf{x}) = 1$ if $\mathbf{x} = \mathbf{0}$ and 0, otherwise.

* Corresponding author.
E-mail addresses: gsugata@gmail.com (S. Gangopadhyay), enes.pasalic6@gmail.com (E. Pasalic), pstanica@nps.edu (P. Stănică), saraldatta@yahoo.com (S. Datta).

http://dx.doi.org/10.1016/j.ipl.2017.01.001
0020-0190/

Definition 1.2. A Boolean function $g \in \mathfrak{B}_n$ is said to be bent (notion introduced by Rothaus [6]) if the Fourier coefficients of χ_g are in the set $\{-1, 1\}$.

Bent functions are particular cases of functions having avalanche features: if any collection of the n input bits of f are complemented, the output changes with probability $1/2$. That means that bent functions f do not have what is called a linear structure, which is a vector $\mathbf{a}$ such that $f(\mathbf{x}+\mathbf{a}) + f(\mathbf{x})$ is constant. In fact, this last expression (called a derivative) is always balanced for bent functions. As a consequence, bent functions are resistant to linear and even differential cryptanalysis (albeit, not being balanced). In spite of that, a simple modification of bent functions (flipping some bits to make them balanced, for example) retains many of their good cryptographic properties (for more on this, the reader can consult [1–3] and the references therein).

That being said, as the interest in bent functions is very high, even after extensive study for several decades, the complete characterization of the entire class of bent functions remains elusive. Dobbertin and Leander [4] pointed out that "a main obstacle in the study of bent functions is the lack of recurrence laws", and "it seems that most bent functions appear without any roots to bent functions in lower dimensions, which could explain their existence." In the same paper, they proposed a way to embed bent functions into the framework of more general $\mathbb{Z}$-bent functions. The $\mathbb{Z}$-bent functions are those functions from $\mathbb{F}_2^n$ to $\mathbb{Z}$ whose Fourier transforms are also in $\mathbb{Z}$. The $\mathbb{Z}$-bent functions can be separated in different levels and higher level $\mathbb{Z}$-bent functions can be used to construct lower level $\mathbb{Z}$-bent functions, in a recursive fashion, finally producing $\mathbb{Z}$-bent functions of level 0 which are bent functions. A $\mathbb{Z}$-bent function of level 1 is an integer valued function on $\mathbb{F}_2^n$ which along with its Fourier transforms takes the values from the set $\{-1, 0, 1\}$. It can be checked easily that given any two bent functions on $\mathbb{F}_2^n$, the average of their corresponding character forms at each point of $\mathbb{F}_2^n$ produces a $\mathbb{Z}$-bent function of level 1. These functions are said to be *splitting*. Finding constructions of non-splitting $\mathbb{Z}$-bent functions is stated as an open problem by Dobbertin and Leander [4]. In this note we propose some constructions of non-splitting $\mathbb{Z}$-bent functions, thus answering in the affirmative that open question. Under some technical conditions, we also construct $\mathbb{Z}$-bent functions of level $r+1$ that are not splitting into $\mathbb{Z}$-bent functions of level $r \geq 0$.

2. $\mathbb{Z}$-bent functions

Throughout this paper $n = 2k$ where $k \in \mathbb{Z}$ and $k > 1$. Let

$$W_0 = \{-1, 1\},$$
$$W_r = \{z \in \mathbb{Z} : -2^{r-1} \leq z \leq 2^{r-1}\}, \text{ for } r \geq 1.$$

Definition 2.1. A function $f : \mathbb{F}_2^n \to W_r \subseteq \mathbb{Z}$ is said to be a $\mathbb{Z}$-bent function of size k level r if $\widehat{f}(\mathbf{x}) \in W_r$ for all $\mathbf{x} \in \mathbb{F}_2^n$. The set of all $\mathbb{Z}$-bent functions of size k level r is denoted by $\mathfrak{BF}_r^k$. Any function belonging to $\bigcup_{r\geq 0} \mathfrak{BF}_r^k$ is said to be a $\mathbb{Z}$-bent function of size k.

Dobbertin and Leander [4] observed that given two bent functions $g, h \in \mathfrak{BF}_0^k$ on $n = 2k$ variables, the function

$$f(\mathbf{x}) = \frac{\chi_g(\mathbf{x}) + \chi_h(\mathbf{x})}{2} \in \{-1, 0, 1\}, \tag{2}$$

for all $\mathbf{x} \in \mathbb{F}_2^n$. The Fourier transform of f at $\mathbf{u} \in \mathbb{F}_2^n$ is then

$$\widehat{f}(\mathbf{u}) = \frac{\widehat{\chi}_g(\mathbf{u}) + \widehat{\chi}_h(\mathbf{u})}{2} \in \{-1, 0, 1\}, \tag{3}$$

for all $\mathbf{u} \in \mathbb{F}_2^n$, since $g, h \in \mathfrak{BF}_0^k$. If a $\mathbb{Z}$-bent function of level 1 can be written as in (2) then it is said to be *splitting*, otherwise it is said to be *non-splitting*. The notion of non-splitting $\mathbb{Z}$-bent functions was introduced by Dobbertin and Leander in [4] and the following open problem is proposed:

Problem 2.2 *([4], Problem 4).* Find constructions of non-splitting $\mathbb{Z}$-bent functions f with level $r = 1$.

In Section 3 we provide some constructions of non-splitting $\mathbb{Z}$-bent functions of level 1, thus answering in the affirmative the previous open problem.

3. Non-splitting $\mathbb{Z}$-bent functions

In this section we investigate the possibilities of generating $\mathbb{Z}$-bent functions of level 1 and answer positively the existence problem of so-called non-splitting $\mathbb{Z}$-bent functions of level 1 posed by Dobbertin and Leander in [4].

3.1. Construction from semibent functions with disjoint spectra

The first construction is based on the concept of disjoint spectra functions. Two Boolean functions $f_1, f_2 \in \mathfrak{B}_n$ are called *disjoint spectra* functions if $\widehat{\chi_{f_1}}(\mathbf{u}) \cdot \widehat{\chi_{f_2}}(\mathbf{u}) = 0$, for any $\mathbf{u} \in \mathbb{F}_2^n$. It turns out that one can generate non-splitting $\mathbb{Z}$-bent functions of level 1 from disjoint spectra semibent functions.

Definition 3.1. A function $f \in \mathfrak{B}_n$ is semibent if $\widehat{\chi_f}(\mathbf{u}) \in \{0, \pm 2\}$, when n even, and $\widehat{\chi_f}(\mathbf{u}) \in \{0, \pm\sqrt{2}\}$, when n odd, for all $\mathbf{u} \in \mathbb{F}_2^n$.

Thus, the Fourier spectrum of a semibent function on n variables consists of values from the set $\{0, \pm 2\}$ or $\{0, \pm\sqrt{2}\}$, depending on whether n is even or odd, respectively.

Theorem 3.2. *Let $f_1, f_2 \in \mathfrak{B}_n$ be two disjoint spectra semibent functions with n even number of variables. Then the function, f, defined by*

$$f(\mathbf{x}) = \frac{\chi_{f_1}(\mathbf{x}) + \chi_{f_2}(\mathbf{x})}{2}, \text{ for all } \mathbf{x} \in \mathbb{F}_2^n, \tag{4}$$

is a non-splitting $\mathbb{Z}$-bent function of level 1.

Proof. The Fourier spectra of f_1 and f_2 consist of values from the set $\{-2, 0, 2\}$. The Fourier spectrum of each χ_{f_i} $(i = 1, 2)$ has 2^{n-2} nonzero values, using the Parseval's identity $\sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{\chi_g}(\mathbf{u})^2 = 2^n$, for any $g \in \mathfrak{B}_n$. Since f_1 and f_2 have disjoint Fourier spectra, the number of $\mathbf{x} \in \mathbb{F}_2^n$ for which $\widehat{f}(\mathbf{x}) = \frac{\widehat{\chi_{f_1}}(\mathbf{x})+\widehat{\chi_{f_2}}(\mathbf{x})}{2} \in \{-1, 1\}$ is 2^{n-1}, while at the remaining points of $\mathbb{F}_2^n$ the Fourier transform $\widehat{f}(\mathbf{x}) = 0$. It is clear that f is a $\mathbb{Z}$-bent function of level 1.

Assuming that f splits, then there exist two bent functions g and h say, such that

$$\frac{\chi_g(\mathbf{x}) + \chi_h(\mathbf{x})}{2} = \frac{\chi_{f_1}(\mathbf{x}) + \chi_{f_2}(\mathbf{x})}{2} = f(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{F}_2^n.$$

Therefore for all $\mathbf{x} \in \mathbb{F}_2^n$

$$\begin{aligned}
&\chi_g(\mathbf{x}) + \chi_h(\mathbf{x}) = \chi_{f_1}(\mathbf{x}) + \chi_{f_2}(\mathbf{x})\\
\iff &2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (\chi_g(\mathbf{x}) + \chi_h(\mathbf{x}))(-1)^{\mathbf{u}\cdot\mathbf{x}}\\
&= 2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (\chi_{f_1}(\mathbf{x}) + \chi_{f_2}(\mathbf{x}))(-1)^{\mathbf{u}\cdot\mathbf{x}}\\
\iff &\widehat{\chi_g}(\mathbf{u}) + \widehat{\chi_h}(\mathbf{u}) = \widehat{\chi_{f_1}}(\mathbf{u}) + \widehat{\chi_{f_2}}(\mathbf{u})\\
\implies &(\widehat{\chi_g}(\mathbf{u}) + \widehat{\chi_h}(\mathbf{u}))^2 = (\widehat{\chi_{f_1}}(\mathbf{u}) + \widehat{\chi_{f_2}}(\mathbf{u}))^2\\
\iff &\widehat{\chi_g}(\mathbf{u})^2 + \widehat{\chi_h}(\mathbf{u})^2 + 2\widehat{\chi_g}(\mathbf{u})\widehat{\chi_h}(\mathbf{u})\\
&= \widehat{\chi_{f_1}}(\mathbf{u})^2 + \widehat{\chi_{f_2}}(\mathbf{u})^2 + 2\widehat{\chi_{f_1}}(\mathbf{u})\widehat{\chi_{f_2}}(\mathbf{u})\\
\iff &2 + 2\widehat{\chi_g}(\mathbf{u})\widehat{\chi_h}(\mathbf{u}) = 4 + 2\widehat{\chi_{f_1}}(\mathbf{u})\widehat{\chi_{f_2}}(\mathbf{u})\\
\iff &\widehat{\chi_g}(\mathbf{u})\widehat{\chi_h}(\mathbf{u}) = 1 + \widehat{\chi_{f_1}}(\mathbf{u})\widehat{\chi_{f_2}}(\mathbf{u}) = 1.
\end{aligned}$$

Thus, for all $\mathbf{u} \in \mathbb{F}_2^n$ the Fourier transform values $\widehat{\chi_g}(\mathbf{u})$ and $\widehat{\chi_h}(\mathbf{u})$ have the same sign forcing $\widehat{f}(\mathbf{u}) = \frac{\widehat{\chi_g}(\mathbf{u})+\widehat{\chi_h}(\mathbf{u})}{2} \in \{-1, 1\}$, for all $\mathbf{u} \in \mathbb{F}_2^n$. This contradicts the fact that $\widehat{f}(\mathbf{u})$ is 0 for 2^{n-1} values of $\mathbf{u} \in \mathbb{F}_2^n$. Therefore f is a non-splitting $\mathbb{Z}$-bent of level 1. □

Nevertheless, the existence problem of disjoint spectra semibent functions remains to be resolved. Disjoint spectra functions were used originally in [5], where for instance two disjoint spectra semibent functions in 6-variables were utilized in the construction of (7, 2, 4, 56) functions.[1] However, finding disjoint (semibent) spectra functions appears to be quite trivial using some well known facts regarding functions defined as a direct sum of two functions on different variable spaces.

Theorem 3.3. *Let $f_0, g_0 \in \mathfrak{B}_n$ be a pair of disjoint spectra functions. Then, the functions*

$$f(\mathbf{x}, \mathbf{y}) = f_0(\mathbf{x}) + s(\mathbf{y}) \quad \text{and} \quad g(\mathbf{x}, \mathbf{y}) = g_0(\mathbf{x}) + t(\mathbf{y}),$$

where $s, t \in \mathfrak{B}_k$ are arbitrary disjoint spectra k-variable Boolean functions, are disjoint spectra functions. In particular, if f_0 and g_0 are disjoint spectra semibent (respectively, plateaued – see Section 3.2) functions and s, t are arbitrary bent functions then f and g are disjoint spectra semibent (respectively, plateaued) functions.

Proof. For any $\mathbf{z}_1 \in \mathbb{F}_2^n$, it holds $\widehat{\chi_{f_0}}(\mathbf{z}_1)\widehat{\chi_{g_0}}(\mathbf{z}_1) = 0$. Let $\mathbf{z} = (\mathbf{z}_1, \mathbf{z}_2) \in \mathbb{F}_2^{n+k}$, where $\mathbf{z}_1 \in \mathbb{F}_2^n$ and $\mathbf{z}_2 \in \mathbb{F}_2^k$. Then, we have

$$\begin{aligned}
2^{(n+k)/2}\widehat{\chi_f}(\mathbf{z}) &= \sum_{(\mathbf{x},\mathbf{y})\in\mathbb{F}_2^{n+k}} \chi_f(\mathbf{x}, \mathbf{y})(-1)^{\mathbf{z}\cdot(\mathbf{x},\mathbf{y})}\\
&= \sum_{(\mathbf{x},\mathbf{y})\in\mathbb{F}_2^{n+k}} \chi_{f_0}(\mathbf{x})\chi_s(\mathbf{y})(-1)^{\mathbf{z}_1\cdot\mathbf{x}+\mathbf{z}_2\cdot\mathbf{y}}\\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \chi_{f_0}(\mathbf{x})(-1)^{\mathbf{z}_1\cdot\mathbf{x}} \sum_{\mathbf{y}\in\mathbb{F}_2^k} \chi_s(\mathbf{y})(-1)^{\mathbf{z}_2\cdot\mathbf{y}}\\
&= 2^{(n+k)/2}\widehat{\chi_{f_0}}(\mathbf{z}_1)\widehat{\chi_s}(\mathbf{z}_2). \qquad (5)
\end{aligned}$$

Similarly,

$$\widehat{\chi_g}(\mathbf{z}) = \widehat{\chi_{g_0}}(\mathbf{z}_1)\widehat{\chi_t}(\mathbf{z}_2). \qquad (6)$$

Multiplying (5) and (6), we deduce that $\widehat{\chi_f}(\mathbf{z})\widehat{\chi_g}(\mathbf{z}) = 0$, that is, f and g are disjoint spectra functions.

In particular, if f_0 and g_0 are disjoint spectra semibent functions then $\widehat{\chi_{f_0}}(\mathbf{z}_1)$, $\widehat{\chi_{g_0}}(\mathbf{z}_1) \in \{0, \pm 2\}$, for n even, $\widehat{g_0}(\mathbf{z}_1) \in \{0, \pm\sqrt{2}\}$, for n odd, and furthermore

$$\widehat{\chi_{f_0}}(\mathbf{z}_1)\widehat{\chi_{g_0}}(\mathbf{z}_1) = 0,$$

for any $\mathbf{z}_1 \in \mathbb{F}_2^n$. Then, since s, t are bent we have k is even and $\widehat{\chi_s}(\mathbf{z}_2)$, $\widehat{\chi_t}(\mathbf{z}_2) = \pm 1$. Therefore, using (5) and (6), we have $\widehat{\chi_f}(\mathbf{z})$, $\widehat{\chi_g}(\mathbf{z}) \in \{0, \pm 2\}$, for n even, and $\widehat{\chi_f}(\mathbf{z})$, $\widehat{\chi_g}(\mathbf{z}) \in \{0, \pm\sqrt{2}\}$, for n odd, and thus f and g are disjoint spectra semibent functions. Certainly, the argument can be repeated for plateaued functions. □

Remark 3.4. To obtain a pair of disjoint spectra semibent functions f_0 and g_0 for odd n, the easiest approach is to take a bent function $h \in \mathfrak{B}_{n+1}$ and consider its restrictions to $\mathbb{Z}_2^n$. That is, writing $h(\mathbf{x}, x_{n+1}) = f_0(\mathbf{x})(x_{n+1} + 1) + g_0(\mathbf{x})x_{n+1}$ it can be easily verified (using the fact that h is bent) that f_0 and g_0 are necessarily disjoint spectra semibent functions.

Thus, there are infinitely many examples of non-splitting $\mathbb{Z}$-bent functions of level 1 which completely resolves the problem posed by Dobbertin and Leander in [4].

3.2. Construction from general plateaued functions

A concept which generalizes bent and semibent functions was introduced by Zheng and Zhang [7]. A function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is called *s-plateaued* if $Spec(\chi_f) = \{0, \pm 2^{s/2}\}$, for some $s \in \mathbb{Z}$. If $s = 1$ (thus n must be odd), or $s = 2$ (thus n must be even), then we recover the semibent functions. For any s-plateaued function $f \in \mathfrak{B}_n$, we write $\widehat{\chi_f}(\mathbf{x}) = \epsilon 2^{s/2}$, for some $\epsilon \in \{0, \pm 1\}$ dependent upon $\mathbf{x}$. (Recall that Theorem 3.3 is also true for plateaued functions.)

Theorem 3.5. *Let n be even, and $f_1, f_2 \in \mathfrak{B}_n$ be s_1-, respectively, s_2-plateaued functions that are neither bent nor both*

[1] The notation used here refers to the specification of the function being a 7-variable, 2-resilient, degree 4, with nonlinearity 56 function.

semibent, and so, $Spec(\chi_{f_i}) = \{0, \pm 2^{1+r_i}\}$, $r_i := s_i/2 - 1 \geq 0$ $(i = 1, 2)$. *Let* α, β *be arbitrary nonzero integers with* $\alpha \equiv \beta \pmod 2$. *If* $r_1 = 0$, $r_2 = 1$, $\alpha = \pm 1$ *(or* $r_2 = 0$, $r_1 = 1$, $\beta = \pm 1$*), we assume* $2\beta\epsilon_2 + \alpha\epsilon_1 \notin \{-1, 1\}$ *(respectively,* $2\alpha\epsilon_1 + \beta\epsilon_2 \notin \{-1, 1\}$*), for at least one value of* $\mathbf{x} \in \mathbb{F}_2^n$*; if* $r_1 > 0, r_2 > 0$, *we assume that* $\alpha\widehat{\chi_{f_1}}(\mathbf{x}) + \beta\widehat{\chi_{f_2}}(\mathbf{x}) \notin \{0, \pm 2\}$, *for at least one value* $\mathbf{x} \in \mathbb{F}_2^n$. *Then*

$$f(\mathbf{x}) = \frac{\alpha\, \chi_{f_1}(\mathbf{x}) + \beta\, \chi_{f_2}(\mathbf{x})}{2}, \text{ for all } \mathbf{x} \in \mathbb{F}_2^n, \tag{7}$$

is a $\mathbb{Z}$*-bent function of level* $\ell := \lceil \log_2 M \rceil$, *where* $M = \max_{\mathbf{u} \in \mathbb{F}_2^n} \{|\alpha\widehat{\chi_{f_1}}(\mathbf{u}) + \beta\widehat{\chi_{f_2}}(\mathbf{u})|\}$, *which cannot be split into (that is, it is not the average of) two bent functions.*

Proof. Applying the Fourier transform on (7) and

$$Spec(\chi_{f_i}) = \{0, \pm 2^{1+r_i}\}$$

we have

$$\widehat{f}(\mathbf{x}) = \frac{\alpha\widehat{\chi_{f_1}}(\mathbf{x}) + \beta\widehat{\chi_{f_2}}(\mathbf{x})}{2} = \frac{\alpha\epsilon_1 2^{r_1+1} + \beta\epsilon_2 2^{r_2+1}}{2}$$
$$= \alpha\epsilon_1 2^{r_1} + \beta\epsilon_2 2^{r_2} \in [-2^{\ell-1}, 2^{\ell-1}],$$

(recall that ϵ_i's depend upon $\mathbf{x}$) and so, f is a $\mathbb{Z}$-bent function of level ℓ. If f splits, then there exist two bent functions g, h, such that

$$f(\mathbf{x}) = \frac{\chi_g(\mathbf{x}) + \chi_h(\mathbf{x})}{2} = \frac{\alpha\, \chi_{f_1}(\mathbf{x}) + \beta\, \chi_{f_2}(\mathbf{x})}{2},$$
$$\text{for all } \mathbf{x} \in \mathbb{F}_2^n. \tag{8}$$

Therefore, for a fixed $\mathbf{x} \in \mathbb{F}_2^n$, for easy writing we label $\widehat{\chi_g}(\mathbf{x}) = \eta_1$, $\widehat{\chi_h}(\mathbf{x}) = \eta_2$ (with $\eta_i \in \{\pm 1\}$ dependent upon $\mathbf{x}$), equation (8) implies

$$\chi_g(\mathbf{x}) + \chi_h(\mathbf{x}) = \alpha\, \chi_{f_1}(\mathbf{x}) + \beta\, \chi_{f_2}(\mathbf{x})$$
$$\iff \widehat{\chi_g}(\mathbf{x}) + \widehat{\chi_h}(\mathbf{x}) = \alpha\widehat{\chi_{f_1}}(\mathbf{x}) + \beta\widehat{\chi_{f_2}}(\mathbf{x})$$
$$\implies \left(\widehat{\chi_g}(\mathbf{x}) + \widehat{\chi_h}(\mathbf{x})\right)^2 = \left(\alpha\widehat{\chi_{f_1}}(\mathbf{x}) + \beta\widehat{\chi_{f_2}}(\mathbf{x})\right)^2$$
$$\iff 2 + 2\eta_1\eta_2 = 4(\alpha\epsilon_1 2^{r_1} + \beta\epsilon_2 2^{r_2})^2$$
$$\iff 1 + \eta_1\eta_2 = 2(\alpha\epsilon_1 2^{r_1} + \beta\epsilon_2 2^{r_2})^2. \tag{9}$$

First, we consider the case when both f_1, f_2 are strictly plateaued (thus, not semibent), and so $r_1 > 0$, $r_2 > 0$. Then, for all $\mathbf{x} \in \mathbb{F}_2^n$, equation (9) renders $\alpha\epsilon_1 2^{r_1} + \beta\epsilon_2 2^{r_2} \in \{0, \pm 1\}$, which implies that $\alpha\widehat{\chi_{f_1}}(\mathbf{x}) + \beta\widehat{\chi_{f_2}}(\mathbf{x}) = 2(\alpha\epsilon_1 2^{r_1} + \beta\epsilon_2 2^{r_2}) \in \{0, \pm 2\}$, but this last assertion cannot hold for all $\mathbf{x}$, given our imposed condition.

Next, we assume (without loss of generality) that f_1 is semibent, hence, $r_1 = 0$, and f_2 is strictly plateaued (plateaued, but not semibent), and so, $r_2 > 0$. Then (9) becomes $\{0, 1\} \ni \frac{1+\eta_1\eta_2}{2} = (\alpha\epsilon_1 + \beta\epsilon_2 2^{r_2})^2$, forcing $\alpha\epsilon_1 + \beta\epsilon_2 2^{r_2} \in \{0, \pm 1\}$, for *all* $\mathbf{x} \in \mathbb{F}_2^n$. Consider a value $\mathbf{x}$ such that $\epsilon_1 = 0$, which would force $\beta\epsilon_2 2^{r_2} \in \{0, \pm 1\}$ (recall that $r_2 > 0$), and that is a contradiction, *unless*, $\epsilon_2 = 0$. However, since f_1 is semibent, it is known that there are exactly $2^{n-1} + 2^{n-2}$ values of $\mathbf{x}$ for which $\epsilon_1 = 0$. Also, since f_2 is strictly plateaued, by Parseval's identity, we know that there are fewer than 2^{n-2} nonzero values for ϵ_2, and so more than $2^{n-1} + 2^{n-2}$ values of $\mathbf{x}$ for which $\epsilon_2 = 0$. Take such a value $\mathbf{x}_0$ for which $\epsilon_2 = 0$, $\epsilon_1 \neq 0$. Then, for such $\mathbf{x}_0$, we get $(\alpha\epsilon_1)^2 \in \{0, 1\}$, which forces $\alpha = \pm 1$, and so, $\beta \equiv 1 \pmod 2$. Now take a value of $\mathbf{x}$ such that $\epsilon_2 \neq 0$. Then (9) transforms into $(\alpha\epsilon_1 + \beta\epsilon_2 2^{r_2})^2 \in \{0, 1\}$ (recall that $\alpha = \pm 1$). If $r_2 > 1$, this is obviously false, and if $r_2 = 1$, our condition $2\beta\epsilon_2 + \alpha\epsilon_1 \notin \{-1, 1\}$ (for at least one value of $\mathbf{x}$) shows also that the previous claim cannot hold. □

Remark 3.6. The imposed condition in the above theorem is easily satisfied since, given the spectrum of two plateaued functions f_1, f_2, we can flexibly choose α, β so that the necessary condition is satisfied at an input $\mathbf{x}$, for the considered plateaued functions.

For easy writing, we use the notations

$$c \cdot \{x_1, x_2, \ldots\} := \{cx_1, cx_2, \ldots\} \text{ and}$$
$$c + \{x_1, x_2, \ldots\} := \{c + x_1, c + x_2, \ldots\}.$$

Corollary 3.7. *The level* ℓ *in Theorem 3.5 is*

$$\ell \in 1 + \{0, r_1 + \lceil \log_2(|\alpha|) \rceil, r_2 + \lceil \log_2(|\beta|) \rceil,$$
$$\lceil \log_2(|2^{r_1}\alpha \pm 2^{r_2}\beta|) \rceil\}$$

(with the convention that if the last expression's argument is 0*, then we disregard that set element).*

Proof. First, we observe that

$$\alpha\widehat{\chi_{f_1}}(\mathbf{x}) + \beta\widehat{\chi_{f_2}}(\mathbf{x}) \in 2$$
$$\cdot\{0, \pm 2^{r_1}\alpha, \pm 2^{r_2}\beta, \pm 2^{r_1}\alpha \pm 2^{r_2}\beta\}$$
(any sign combinations),

and so (using the notations of our previous theorem),

$$M \in 2 \cdot \{0, 2^{r_1}|\alpha|, 2^{r_2}|\beta|, |2^{r_1}\alpha + 2^{r_2}\beta|, |2^{r_1}\alpha - 2^{r_2}\beta|\}.$$

It follows that

$$\log_2 M \in 1 + \{0, r_1 + \log_2(|\alpha|), r_2 + \log_2(|\beta|),$$
$$\log_2(|2^{r_1}\alpha \pm 2^{r_2}\beta|\}. \qquad \square$$

Our next result extends our previous Theorem 3.2 by constructing $\mathbb{Z}$-bent functions of level $r + 1$ that are not splitting into $\mathbb{Z}$-bent functions of level r, under some technical conditions. Given two $\mathbb{Z}$-bent functions f, g, we say that they have *unitary spectra quotient* if $|\widehat{f}(\mathbf{x})| = |\widehat{g}(\mathbf{x})|$, for all $\mathbf{x} \in \mathbb{F}_2^n$. Obviously, the two functions have non-unitary spectra quotient if $|\widehat{f}(\mathbf{x}_0)| \neq |\widehat{g}(\mathbf{x}_0)|$, for some $\mathbf{x}_0 \in \mathbb{F}_2^n$.

Theorem 3.8. *Let* n *be even,* $0 \leq r < n/2$ *and* f_1, f_2 *be disjoint spectra plateaued functions with* $Spec(\chi_{f_i}) = \{0, \pm 2^{1+r}\}$ *(obviously, then both* f_1, f_2 *are* $(2r + 2)$*-plateaued functions). Then*

$$f(\mathbf{x}) = \frac{\chi_{f_1}(\mathbf{x}) + \chi_{f_2}(\mathbf{x})}{2}, \text{ for all } \mathbf{x} \in \mathbb{F}_2^n$$

is a $\mathbb{Z}$*-bent function of level* $r + 1$*, which is non-splitting into* $\mathbb{Z}$*-bent functions of level* r*, satisfying the non-unitary spectra quotient if* $r > 0$.

Proof. The level of f (under the disjoint spectra condition) is easily seen to be $r+1$. Now, we assume that f can be split into two level r functions g, h. Writing $\widehat{\chi_{f_i}}(\mathbf{x}) = \epsilon_i 2^{1+r}$, $\widehat{g}(\mathbf{x}) = \eta_1 2^r$, $\widehat{h}(\mathbf{x}) = \eta_2 2^r$ (with $\epsilon_i \in \{0, \pm 1\}$ and *real* $|\eta_i| \leq 1$, all dependent upon $\mathbf{x}$),

$$(\widehat{g}(\mathbf{x}) + \widehat{h}(\mathbf{x}))^2 = (\widehat{\chi_{f_1}}(\mathbf{x}) + \widehat{\chi_{f_2}}(\mathbf{x}))^2$$

$$(\eta_1 + \eta_2)^2 = 4\epsilon, \text{ where } \epsilon \in \{0, 1\} \text{ is dependent on } \mathbf{x}.$$

If $\epsilon = 1$ (which happens if $\epsilon_1 \neq 0$, or $\epsilon_2 \neq 0$, and, since the two sets of such values $\mathbf{x}$ are not overlapping, by our disjoint spectra condition, there are $2 \times 2^{n-2r-2} = 2^{n-2r-1}$ such values of $\mathbf{x}$, all belonging to a set, call it S_1), then $\eta_1 = \eta_2 = \pm 1$. If $\epsilon = 0$ (which happens if $\epsilon_1 = \epsilon_2 = 0$, and so, there are $2^n - 2^{n-2r-1}$ such values of $\mathbf{x}$, all belonging to the set $S_0 = \mathbb{F}_2^n \setminus S_1$), then $\eta_1 = -\eta_2$. Thus, both values $\epsilon = 0, 1$ are attained, forcing $|\eta_1| = |\eta_2|$, for any value of $\mathbf{x}$, but then g, h would have unitary spectra quotient, contradicting our assumption. □

Acknowledgements

This paper was written during an enjoyable visit of S.G. at the Applied Mathematics Department of Naval Postgraduate School in December, 2013. During the preparation of this paper, S.G. was supported in part by VSP award no. N62909-13-1-V105 (Department of the US Navy, ONR-Global).

References

[1] C. Carlet, Boolean functions for cryptography and error correcting codes, Chapter of the monograph: in: Yves Crama, Peter L. Hammer (Eds.), Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge University Press, 2010, pp. 257–397, available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.

[2] C. Carlet, Vectorial Boolean functions for cryptography, in: Y. Crama, P. Hammer (Eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, 2010, pp. 398–469, available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.

[3] T.W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications, Elsevier–Academic Press, 2009.

[4] H. Dobbertin, G. Leander, Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions, Des. Codes Cryptogr. 49 (2008) 3–22.

[5] E. Pasalic, T. Johansson, S. Maitra, P. Sarkar, New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity, in: Workshop on Coding and Cryptography Proceedings, vol. 6, Elsevier Science, 2001, pp. 425–435.

[6] O.S. Rothaus, On bent functions, J. Comb. Theory, Ser. A 20 (1976) 300–305.

[7] Y. Zheng, X.M. Zhang, Plateaued functions, in: Advances in Cryptology–ICICS 1999, in: Lect. Notes Comput. Sci., vol. 1726, Springer-Verlag, 1999, pp. 284–300.