A secondary construction of bent functions, octal gbent functions and their duals

Wilfried Meidl
Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria
Email: meidlwilfried@gmail.com

April 4, 2016

Abstract

We observe that every octal gbent function in even dimension is essentially equivalent to a bent function obtained with Carlet's secondary construction of bent functions from three bent functions with certain properties. We use this strong connection to completely describe octal gbent functions in even dimension and their duals. This is also the first comprehensive treatment of duality for gbent functions. Implementations of this construction of bent functions also enable us to construct infinite classes of octal gbent functions and their duals. We present some examples.

Keywords. Bent function, gbent function, duality, Boolean function, Walsh-Hadamard transform, sequence generation

1 Introduction

Let $\mathbb{V}_n$ be an n-dimensional vector space over $\mathbb{F}_2$. For a Boolean function f from $\mathbb{V}_n$ to $\mathbb{F}_2$ the *Walsh-Hadamard transform* is the complex valued function

$$\mathcal{W}_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{V}_n} (-1)^{f(\mathbf{x})}(-1)^{\langle \mathbf{u},\mathbf{x}\rangle},$$

where $\langle , \rangle$ denotes a nondegenerate inner product on $\mathbb{V}_n$. If $\mathbb{V}_n$ is $\mathbb{F}_2^n$, we can take the dot product $\mathbf{u}\cdot\mathbf{x}$ for $\langle \mathbf{u},\mathbf{x}\rangle$, the standard inner product for $\mathbb{V}_n = \mathbb{F}_{2^n}$ is $\langle \mathbf{u},\mathbf{x}\rangle = \mathrm{Tr}_n(\mathbf{ux})$, where $\mathrm{Tr}_n(\mathbf{z})$ denotes the absolute trace of

$\mathbf{z} \in \mathbb{F}_{2^n}$. A function f for which $|\mathcal{W}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$ is called a *bent* function, [4, 12]. Obviously bent functions only exist if n is even, and then $\mathcal{W}_f(\mathbf{u}) = 2^{n/2}(-1)^{f^*(\mathbf{x})}$ for a Boolean function $f^*(\mathbf{x})$, called the *dual* of f. As is well known, the dual f^* is also a bent function.

For an integer q let $\mathbb{Z}_q$ be the ring of integers modulo q. For a *generalized Boolean function* f from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$, $k \geq 1$, the *generalized Walsh-Hadamard transform* is the complex valued function

$$\mathcal{H}_f^{(k)}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta_{2^k}^{f(\mathbf{x})} (-1)^{\langle \mathbf{u}, \mathbf{x} \rangle}, \quad \zeta_{2^k} = e^{\frac{2\pi i}{2^k}}.$$

Note that $\mathcal{H}_f^{(1)}(\mathbf{u}) = \mathcal{W}_f(\mathbf{u})$. We shall use ζ, respectively, $\mathcal{H}_f$, instead of ζ_{2^k}, respectively, $\mathcal{H}_f^{(k)}$, when k is fixed. If we identify $\mathbb{V}_n$ with $\mathbb{F}_{2^n}$, we will write z rather than $\mathbf{z}$ for elements in $\mathbb{F}_{2^n} = \mathbb{V}_n$. We denote the set of all generalized Boolean functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$ by $\mathcal{GB}_n^{2^k}$ and when $k = 1$, by $\mathcal{B}_n$. A function $f \in \mathcal{GB}_n^{2^k}$ is called *generalized bent* (*gbent*) if $|\mathcal{H}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$. Differently to the case $k = 1$, gbent functions also exist for odd n when $k > 1$. As shown in [6], if f is gbent (and $k \neq 2$ if n is odd), then for every $\mathbf{u} \in \mathbb{V}_n$, we have $\mathcal{H}_f(\mathbf{u}) = 2^{n/2} \zeta_{2^k}^{f^*(\mathbf{u})}$ for some $f^* \in \mathcal{GB}_n^{2^k}$, which is again gbent, see [7]. In consistence with the case $k = 1$, we may call f^* the dual of f.

Bent functions can be used to construct families of binary sequences with pairwise low crosscorrelation, see [11], which has applications in code-division multiple access (CDMA) systems. Attaining highest possible nonlinearity, bent functions play a fundamental role in applications in cryptography, for instance in S-Boxes in block ciphers, or as components for constructing nonlinear Boolean functions in the design of pseudorandom sequences for stream ciphers. For background on Boolean functions in cryptography we refer to [3, 10].

Generalized bent functions were introduced in [13] in connection with CDMA systems, and several constructions of quaternary gbent functions were exploited in connection with algebraic codes over $\mathbb{Z}_4$, to design families of quaternary constant-amplitude codes for multicode CDMA systems. Since then one can observe an increasing interest in gbent functions, see [5, 8, 14, 15].

We start recalling some preliminary results in Section 2. In Section 3, after describing the dual of a gbent function in $\mathcal{GB}_n^4$, n even, we reveal a close connection between a secondary construction of bent functions in [2] and octal gbent functions in even dimension n. We use this connection to completely describe gbent functions in $\mathcal{GB}_n^8$, n even, and their duals. Finally

we present some infinite classes of gbent functions employing the analysis of the construction of bent functions in [2] by Mesnager in [9]. We close this article with some perspectives in Section 4.

2 Preliminaries

Henceforth we write $\oplus$ for the addition modulo 2 respectively the addition in $\mathbb{F}_2$, and $+$ for the addition in $\mathbb{C}$, V_n, $\mathbb{Z}_q$, $q > 2$. Let f be a function from V_n to $\mathbb{Z}_{2^k}$ given as

$$f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{k-1}a_{k-1}(\mathbf{x}),\ a_i \in \mathcal{B}_n, 0 \leq i \leq k-1.$$

As one may expect, one can show relations between the generalized Walsh-Hadamard transform of f and the Walsh-Hadamard transforms of the associated Boolean functions. The following lemma is Lemma 3.1 in [14] and Lemma 17 in [15].

Lemma 1. *The following statements are true:*

(i) Let $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) \in \mathcal{GB}_n^4$ with $a_0, a_1 \in \mathcal{B}_n$. The generalized Walsh-Hadamard transform of f is given by

$$2\mathcal{H}_f^{(4)}(\mathbf{u}) = (\mathcal{W}_{a_1}(\mathbf{u}) + \mathcal{W}_{a_0 \oplus a_1}(\mathbf{u})) + i\,(\mathcal{W}_{a_1}(\mathbf{u}) - \mathcal{W}_{a_0 \oplus a_1}(\mathbf{u}))\,.$$

(ii) Let $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + 4a_2(\mathbf{x}) \in \mathcal{GB}_n^8$ with $a_0, a_1, a_2 \in \mathcal{B}_n$. The generalized Walsh-Hadamard transform of f is given by

$$4\mathcal{H}_f^{(8)}(\mathbf{u}) = \alpha_0\mathcal{W}_{a_2}(\mathbf{u}) + \alpha_1\mathcal{W}_{a_0 \oplus a_2}(\mathbf{u}) + \alpha_2\mathcal{W}_{a_1 \oplus a_2}(\mathbf{u}) + \alpha_{12}\mathcal{W}_{a_0 \oplus a_1 \oplus a_2}(\mathbf{u}),$$

where $\alpha_0 = 1 + (1 + \sqrt{2})i$, $\alpha_1 = 1 + (1 - \sqrt{2})i$, $\alpha_2 = 1 + \sqrt{2} - i$, $\alpha_{12} = 1 - \sqrt{2} - i$.

Whether f is gbent or not is hence strongly related to properties of the Walsh-Hadamard transforms of the associated Boolean functions.

Proposition 1. *Let n be an even integer.*

(i) [14, Theorem 32] The function $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x})$ in $\mathcal{GB}_n^4$ is gbent if and only if a_1 and $a_0 \oplus a_1$ are bent.

(ii) [15, Theorem 19] The function $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + 4a_2(\mathbf{x})$ in $\mathcal{GB}_n^8$ is gbent if and only if a_2, $a_0 \oplus a_2$, $a_1 \oplus a_2$ and $a_0 \oplus a_1 \oplus a_2$ are bent functions, and $\mathcal{W}_{a_0 \oplus a_2}(\mathbf{u})\mathcal{W}_{a_1 \oplus a_2}(\mathbf{u}) = \mathcal{W}_{a_2}(\mathbf{u})\mathcal{W}_{a_0 \oplus a_1 \oplus a_2}(\mathbf{u})$ for all $\mathbf{u} \in V_n$.

(iii) [6, Theorem 18] If $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{k-1}a_{k-1}(\mathbf{x})$ *is a gbent function in* $\mathcal{GB}_n^{2^k}$, $k > 1$, *then all Boolean functions of the form*

$$g_{\mathbf{c}}(\mathbf{x}) = c_0 a_0(\mathbf{x}) \oplus c_1 a_1(\mathbf{x}) \oplus \cdots \oplus c_{k-2} a_{k-2}(\mathbf{x}) \oplus a_{k-1}(\mathbf{x}),$$

$\mathbf{c} = (c_0, c_1, \ldots, c_{k-2}) \in \mathbb{F}_2^{n-1}$, *are bent functions.*

Remark 1. *Sufficient conditions for f to be gbent have been given in [6] also for $k = 3$. We omit those conditions here, apparently sufficient conditions become quite complicated when k increases.*
For odd n, where bent functions do not exist, for $k = 2, 3, 4$ relations between the gbentness of $f \in \mathcal{GB}_n^{2^k}$ and the semibentness of associated Boolean functions have been shown in [6, 14, 15].

Examples for gbent functions in $\mathcal{GB}_n^4$, n even, are easy to construct from a pair of bent functions. For larger k the additional conditions for gbentness become complicated. Trivial examples of gbent functions are some functions with quite reduced value sets, like $f(\mathbf{x}) = 2^{k-1}a(\mathbf{x}) \in \mathcal{GB}_n^{2^k}$, $a(\mathbf{x}) \in \mathcal{B}_n$ bent, for arbitrary $k > 1$, and for $k = 3$, $f_1(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + 4a_2(\mathbf{x}) \in \mathcal{GB}_n^8$ with $a_0 = 0$ (or $a_1 = 0$) and a_2 and $a_1 + a_2$ (or $a_0 + a_2$) are bent, or $f_2(\mathbf{x}) = 1 + 2(g_1(\mathbf{x}) \oplus g_2(\mathbf{x})) + 4g_1(\mathbf{x})$ for some bent functions g_1, g_2, which does not take on the value 0. For further (nontrivial) examples we may refer to [5, 8, 15]. In [7], the class of the partial spread bent functions was generalized to functions in $\mathcal{GB}_n^{2^k}$. This yields a large variety of nontrivial gbent functions in $\mathcal{GB}_n^{2^k}$, n even.

3 Carlet's secondary construction and octal gbent functions

This section contains the main contributions of this paper. We show that bent functions obtained with the secondary construction proposed in [2] are equivalent to octal gbent functions in even dimension. This strong connection yields a simple characterization of gbent functions in $\mathcal{GB}_n^8$, n even. We then employ investigations on the secondary construction of [2] in Mesnager [9], to generate several further (nontrivial) classes of gbent functions and their duals in $\mathcal{GB}_n^8$, n even.

Before we recall Carlet's construction and study gbent functions in $\mathcal{GB}_n^8$ in detail, we give a precise description of the dual of a gbent function $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x})$ in $\mathcal{GB}_n^4$, n even. Recall that we easily obtain a gbent function in $\mathcal{GB}_n^4$ from any two bent functions.

Theorem 1. *Let n be even and let $f(\mathbf{x}) = a_0(\mathbf{x})+2a_1(\mathbf{x})$ be a gbent function in $\mathcal{GB}_n^4$. Then the dual f^* of f is given by*

$$f^*(\mathbf{x}) = a_1^*(\mathbf{x}) \oplus (a_0 \oplus a_1)^*(\mathbf{x}) + 2a_1^*(\mathbf{x}).$$

Proof. Recall that the Boolean functions a_1 and $a_0 \oplus a_1$ are bent if f is gbent. Therefore the expression for f^* makes sense. We put $g_1 = a_1$ and $g_2 = a_0 \oplus a_1$. By Lemma (1)(i), we have

$$2\mathcal{H}_f(\mathbf{u}) = 2^{n/2}[(-1)^{g_1^*(\mathbf{u})} + (-1)^{g_2^*(\mathbf{u})} + i((-1)^{g_1^*(\mathbf{u})} - (-1)^{g_2^*(\mathbf{u})})].$$

By our claim,

$$2\mathcal{H}_f(\mathbf{u}) = 2 \cdot 2^{n/2} i^{g_1^*(\mathbf{u}) \oplus g_2^*(\mathbf{u}) + 2g_1^*(\mathbf{u})}.$$

Comparing the last two equations for all 4 possible values of $g_1^*(\mathbf{u})$, $g_2^*(\mathbf{u})$, we see the correctness of our claim. □

Let us now recall the secondary construction of bent functions proposed by Carlet in [2]. We state a version given by Mesnager in [9].

Proposition 2. *[9, Theorem 4] Let g_1, g_2, g_3 be bent functions over $\mathbb{V}_n$ such that $g_4 = g_1 \oplus g_2 \oplus g_3$ is bent. The Boolean function*

$$h(\mathbf{x}) = g_1(\mathbf{x})g_2(\mathbf{x}) \oplus g_1(\mathbf{x})g_3(\mathbf{x}) \oplus g_2(\mathbf{x})g_3(\mathbf{x})$$

is bent if and only if $g_1^* \oplus g_2^* \oplus g_3^* \oplus g_4^* = 0$.

As a first step in relating the construction in Proposition 2 with octal gbent functions we show the following lemma.

Lemma 2. *Let $f \in \mathcal{GB}_n^8$, n even, be given as*

$$f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + 4a_2(\mathbf{x}),\ a_i \in \mathcal{B}_n, i = 0, 1, 2.$$

Then f is gbent if and only if a_2, $a_0 \oplus a_2$, $a_1 \oplus a_2$ and $a_0 \oplus a_1 \oplus a_2$ are bent functions, and $a_2^* \oplus (a_0 \oplus a_2)^* + (a_1 \oplus a_2)^* + (a_0 \oplus a_1 \oplus a_2)^* = 0$.

Proof. By Proposition 1, f is gbent if and only if a_2, $a_0 \oplus a_2$, $a_1 \oplus a_2$ and $a_0 \oplus a_1 \oplus a_2$ are bent functions, and $\mathcal{W}_{a_0 \oplus a_2}(\mathbf{u})\mathcal{W}_{a_1 \oplus a_2}(\mathbf{u}) = \mathcal{W}_{a_2}(\mathbf{u})\mathcal{W}_{a_0 \oplus a_1 \oplus a_2}(\mathbf{u})$ for all $\mathbf{u} \in V_n$. We show that the second condition is equivalent to $a_2^* \oplus (a_0 \oplus a_2)^* \oplus (a_1 \oplus a_2)^* \oplus (a_0 \oplus a_1 \oplus a_2)^* = 0$. The second condition holds if and only if

$$2^n(-1)^{(a_0 \oplus a_2)^*(\mathbf{u})}(-1)^{(a_1 \oplus a_2)^*(\mathbf{u})} = 2^n(-1)^{a_2^*(\mathbf{u})}(-1)^{(a_0 \oplus a_1 \oplus a_2)^*(\mathbf{u})}$$

or equivalently

$$(-1)^{a_2^*(\mathbf{u})\oplus(a_0\oplus a_2)^*(\mathbf{u})\oplus(a_1\oplus a_2)^*(\mathbf{u})\oplus(a_0\oplus a_1\oplus a_2)^*(\mathbf{u})}=1$$

for all $\mathbf{u}\in V_n$. This holds if and only if $a_2^*\oplus(a_0\oplus a_2)^*\oplus(a_1\oplus a_2)^*\oplus(a_0\oplus a_1\oplus a_2)^*=0$. □

Theorem 2. *For an even integer n let $f\in\mathcal{GB}_n^8$ be given as*

$$f(\mathbf{x})=a_0(\mathbf{x})+2a_1(\mathbf{x})+4a_2(\mathbf{x}),\ a_i\in\mathcal{B}_n, i=0,1,2.$$

Then f is gbent if and only if a_2, $a_0\oplus a_2$, $a_1\oplus a_2$, $a_0\oplus a_1\oplus a_2$ and $a_2\oplus a_0a_1$ are bent functions. The dual f^* of f is then given by

$$f^*(\mathbf{x})=a_2^*(\mathbf{x})\oplus(a_0+a_2)^*(\mathbf{x})+2(a_2^*(\mathbf{x})\oplus(a_1\oplus a_2)^*(\mathbf{x}))+4a_2^*(\mathbf{x}).$$

Proof. Put $a_2=g_1$, $a_0\oplus a_2=g_2$, $a_1\oplus a_2=g_3$, $a_0\oplus a_1\oplus a_2=g_4$, and note that then $g_4=g_1\oplus g_2\oplus g_3$.

$\Rightarrow$: If f is gbent, then g_1,g_2,g_3 and $g_4=g_1\oplus g_2\oplus g_3$ are bent. Moreover, by Lemma 2 we have $g_1^*\oplus g_2^*\oplus g_3^*\oplus g_4^*=0$, and hence by Proposition 2 the function $g_1g_2\oplus g_1g_3\oplus g_2g_3=a_2(a_0\oplus a_2)\oplus a_2(a_1\oplus a_2)\oplus(a_0\oplus a_2)(a_1\oplus a_2)=a_2\oplus a_0a_1$ is bent.

$\Leftarrow$: Suppose g_1,g_2,g_3 and $g_4=g_1\oplus g_2\oplus g_3$ are bent, and additionally $a_2\oplus a_0a_1=g_1g_2\oplus g_1g_3\oplus g_2g_3$ is bent. Then by Proposition 2, $g_1^*\oplus g_2^*\oplus g_3^*\oplus g_4^*=0$. By Lemma 2, f is then gbent.
To show the second part, we observe that by Lemma (1)(ii), we have

$$\begin{aligned}4\mathcal{H}_f(\mathbf{u}) &= 2^{n/2}[(1+(1+\sqrt{2})i)(-1)^{g_1^*(\mathbf{u})}+(1+(1-\sqrt{2})i)(-1)^{g_2^*(\mathbf{u})}\\ &\quad +(1+\sqrt{2}-i)(-1)^{g_3^*(\mathbf{u})}+(1-\sqrt{2}-i)(-1)^{(g_1^*\oplus g_2^*\oplus g_3^*)(\mathbf{u})}].\end{aligned}$$

By our claim,

$$4\mathcal{H}_f(\mathbf{u})=4\cdot 2^{n/2}\zeta^{g_1^*(\mathbf{u})\oplus g_2^*(\mathbf{u})+2(g_1^*(\mathbf{u})\oplus g_3^*(\mathbf{u}))+4g_1^*(\mathbf{u})},$$

where $\zeta=(1+i)/\sqrt{2}$. Comparing the last two equations for all 8 possible values of $g_1^*(\mathbf{u})$, $g_2^*(\mathbf{u})$, $g_3^*(\mathbf{u})$, we see the correctness of our claim. □

We can apply Lemma 2 to construct more non-trivial examples of gbent functions in $\mathcal{GB}_n^8$. We solely require four bent functions g_1,g_2,g_3,g_4 satisfying

(I) $g_1\oplus g_2\oplus g_3\oplus g_4=0$,

(II) $g_1^* \oplus g_2^* \oplus g_3^* \oplus g_4^* = 0$.

The function

$$\begin{aligned} f(\mathbf{x}) &= a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + 4a_2(\mathbf{x}) \\ &= g_1(\mathbf{x}) \oplus g_2(\mathbf{x}) + 2(g_1(\mathbf{x}) \oplus g_3(\mathbf{x})) + 4g_1(\mathbf{x}) \end{aligned} \tag{1}$$

is then gbent. We hereby can take advantage of the discussions in [9], where the construction of bent functions employing Proposition 2 is investigated.

Recall that for a Boolean function $h \in \mathcal{B}_n$ and $\mathbf{u}, \mathbf{v} \in \mathbb{V}_n$, the derivative of h in direction $\mathbf{u}$ is $D_{\mathbf{u}}h(\mathbf{x}) := h(\mathbf{x}) \oplus h(\mathbf{x}+\mathbf{u})$ and the second order derivative of h with respect to $(\mathbf{u}, \mathbf{v})$ is defined as $D_{\mathbf{v}}D_{\mathbf{u}}h(\mathbf{x}) := h(\mathbf{x}) \oplus h(\mathbf{x}+\mathbf{v}) \oplus h(\mathbf{x}+\mathbf{u}) \oplus h(\mathbf{x}+\mathbf{u}+\mathbf{v})$.

An obvious way for at least satisfying condition (I) is to choose $g_1(\mathbf{x}) = h(\mathbf{x})$, $g_2(\mathbf{x}) = h(\mathbf{x}) \oplus \langle \mathbf{u}, \mathbf{x} \rangle$, $g_3(\mathbf{x}) = h(\mathbf{x}) \oplus \langle \mathbf{v}, \mathbf{x} \rangle$ and hence $g_4(\mathbf{x}) = h(\mathbf{x}) \oplus \langle \mathbf{u}+\mathbf{v}, \mathbf{x} \rangle$, for some bent function $h \in \mathcal{B}_n$. Observing that $(h(\mathbf{x}) \oplus \langle \mathbf{w}, \mathbf{x} \rangle)^* = h^*(\mathbf{x}+\mathbf{w})$ (see e.g. [1, Proposition 3]), condition (II) equals

$$h^*(\mathbf{x}) \oplus h^*(\mathbf{x}+\mathbf{u}) \oplus h^*(\mathbf{x}+\mathbf{v}) \oplus h^*(\mathbf{x}+\mathbf{u}+\mathbf{v}) = D_{\mathbf{v}}D_{\mathbf{u}}h^*(\mathbf{x}) = 0. \tag{2}$$

Alternatively one may pick two bent functions $h_1, h_2 \in \mathcal{B}_n$ and put $g_1(\mathbf{x}) = h_1(\mathbf{x})$, $g_2(\mathbf{x}) = h_1(\mathbf{x}) \oplus \langle \mathbf{u}, \mathbf{x} \rangle$, $g_2(\mathbf{x}) = h_2(\mathbf{x})$, and hence $g_4(\mathbf{x}) = h_2(\mathbf{x}) \oplus \langle \mathbf{u}, \mathbf{x} \rangle$. Again with $(h_i(\mathbf{x}) \oplus \langle \mathbf{u}, \mathbf{x} \rangle)^* = h_i^*(\mathbf{x}+\mathbf{u})$, $i = 1, 2$, condition (II) is of the form

$$h_1^*(\mathbf{x}) \oplus h_2^*(\mathbf{x}) \oplus h_1^*(\mathbf{x}+\mathbf{u}) \oplus h_2^*(\mathbf{x}+\mathbf{u}) = D_{\mathbf{u}}h_1^*(\mathbf{x}) \oplus D_{\mathbf{u}}h_2^*(\mathbf{x}) = 0. \tag{3}$$

We summarize our observations in the following corollary (compare with Corollaries 5 and 6 in [9] for the construction of bent functions).

Corollary 1. *Let n be an even integer, let h, h_1, h_2 be bent functions in $\mathcal{B}_n$ and let $\mathbf{u}, \mathbf{v} \in \mathbb{V}_n$.*

(i) The function $f \in \mathcal{GB}_n^8$

$$f(\mathbf{x}) = \langle \mathbf{u}, \mathbf{x} \rangle + 2\langle \mathbf{v}, \mathbf{x} \rangle + 4h(\mathbf{x})$$

is gbent if and only if $D_{\mathbf{v}}D_{\mathbf{u}}h^*(\mathbf{x}) = 0$. The dual of f is then

$$f^*(\mathbf{x}) = D_{\mathbf{u}}h^*(\mathbf{x}) + 2D_{\mathbf{v}}h^*(\mathbf{x}) + 4h^*(\mathbf{x}).$$

(ii) The function $f \in \mathcal{GB}_n^8$

$$f(\mathbf{x}) = \langle \mathbf{u}, \mathbf{x} \rangle + 2(h_1(\mathbf{x}) \oplus h_2(\mathbf{x})) + 4h_1(\mathbf{x})$$

is gbent if and only if $D_{\mathbf{u}}h_1^*(\mathbf{x}) = D_{\mathbf{u}}h_2^*(\mathbf{x})$. The dual of f is then

$$f^*(\mathbf{x}) = D_{\mathbf{u}}h_1^*(\mathbf{x}) + 2(h_1^*(\mathbf{x}) \oplus h_2^*(\mathbf{x})) + 4h_1^*(\mathbf{x}).$$

Proof. By Equation (2) respectively Equation (3), and Lemma 2, we obtain the conditions for the gbentness of f. The expression for the gbent function and for its dual follow then from Equation (1) and Theorem 2. □

Remark 2. *Observe that given bent functions g_1, g_2, g_3, g_4 satisfying (I), (II), we obtain a set of octal gbent functions. Changing the roles of the bent functions g_i, $i = 1, 2, 3, 4$, for instance putting in the second construction in Corollary 1, $g_1(\mathbf{x}) = h_1(\mathbf{x})$, $g_2(\mathbf{x}) = h_2(\mathbf{x}) \oplus \langle \mathbf{u}, \mathbf{x} \rangle$, $g_3(\mathbf{x}) = h_1(\mathbf{x}) \oplus \langle \mathbf{u}, \mathbf{x} \rangle$, and hence $g_4(\mathbf{x}) = h_2(\mathbf{x})$, with Equation (1), we obtain another gbent function,*

$$f(\mathbf{x}) = \langle \mathbf{u}, \mathbf{x} \rangle + 2(h_1(\mathbf{x}) \oplus h_2(\mathbf{x}) \oplus \langle \mathbf{u}, \mathbf{x} \rangle) + 4h_1(\mathbf{x})$$

with the dual

$$f^*(\mathbf{x}) = D_{\mathbf{u}} h_1^*(\mathbf{x}) + 2(h_1^*(\mathbf{x}) \oplus h_2^*(\mathbf{x} + \mathbf{u})) + 4h_1^*(\mathbf{x}).$$

Example 1. *In Theorem 9 in [9], the quadratic Niho bent function $h : \mathbb{F}_{2^n} \to \mathbb{F}_2$, $n = 2m$, given by $h(x) = \mathrm{Tr}_m(\lambda x^{2^m+1})$, $\lambda \in \mathbb{F}_{2^m}^*$, is employed to construct a new bent function applying Proposition 2. It is observed that the dual of h is*

$$h^*(x) = \mathrm{Tr}_m(\lambda^{-1} x^{2^m+1}) \oplus 1,$$

and for $u, v \in \mathbb{F}_{2^n}$ we have

$$D_v h^*(x) = \mathrm{Tr}_n(\lambda^{-1} v^{2^m} x) \oplus \mathrm{Tr}_m(\lambda^{-1} v^{2^m+1}), \quad D_u D_v h^*(x) = \mathrm{Tr}_n(\lambda^{-1} v^{2^m} u).$$

Choosing $u, v \in \mathbb{F}_{2^n}$ such that $\mathrm{Tr}_n(\lambda^{-1} v^{2^m} u) = 0$, with Corollary 1(i) we obtain the gbent function

$$f(x) = \mathrm{Tr}_n(ux) + 2\mathrm{Tr}_n(vx) + 4\mathrm{Tr}_m(\lambda x^{2^m+1})$$

and its dual

$$f^*(x) = \mathrm{Tr}_n(\lambda^{-1} u^{2^m} x) \oplus \mathrm{Tr}_m(\lambda^{-1} u^{2^m+1}) + 2[\mathrm{Tr}_n(\lambda^{-1} v^{2^m} x) \oplus \mathrm{Tr}_m(\lambda^{-1} v^{2^m+1})] + 4(\mathrm{Tr}_m(\lambda^{-1} x^{2^m+1}) \oplus 1).$$

Example 2. *In this example we employ Corollary 1(ii). We assume that $n = 2m = 4k$ and choose for h_1 the Niho bent function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, given as $h_1(x) = \mathrm{Tr}_m(x^{2^m+1})$, for which the dual is $h_1^*(x) = \mathrm{Tr}_m(x^{2^m+1}) \oplus 1$. For h_2 we choose the quadratic bent function*

$$h_2(x) = \mathrm{Tr}_n(\lambda(x + \beta)^{2^k+1}),$$

where $\beta \in \mathbb{F}_{2^n}$ and $\lambda \in \mathbb{F}_{2^n}$ such that $\lambda + \lambda^{2^{2k}} + 1 = 0$. The dual of h_2 is then, see [9, Section IV D],

$$h_2^*(x) = \mathrm{Tr}_n(\lambda(x+\beta)^{2^k+1}) \oplus \mathrm{Tr}_n(\beta x).$$

As observed in [9], for $u \in \mathbb{F}_{2^k}$ we have $D_u h_1^* = D_u h_2^*$ if and only if the conditions

$$\begin{aligned} &\mathrm{Tr}_m(u^{2^{2k}+1}) \oplus \mathrm{Tr}_n(\lambda u^{2^k+1}) = \mathrm{Tr}_n(\beta u), \\ &u^{2^{2k}} + \lambda^{2^{-k}} u^{2^{-k}} + \lambda u^{2^k} = 0 \end{aligned}$$

hold. For simplicity we choose u from $\mathbb{F}_{2^k}$. With $\lambda + \lambda^{2^{2k}} + 1 = 0$, it is then easily verified that these two conditions reduce to the condition

$$\mathrm{Tr}_n(\lambda u^2) = \mathrm{Tr}_n(\beta u). \tag{4}$$

Applying Corollary 1(ii), for $\lambda \in \mathbb{F}_{2^n}$ with $\lambda + \lambda^{2^{2k}} + 1 = 0$, and $u \in \mathbb{F}_{2^k}$, $\beta \in \mathbb{F}_{2^n}$ such that (4) is satisfied, we get the gbent function

$$f(x) = \mathrm{Tr}_n(ux) + 2[\mathrm{Tr}_m(x^{2^m+1}) \oplus \mathrm{Tr}_n(\lambda(x+\beta)^{2^k+1}] + 4\mathrm{Tr}_m(x^{2^m+1}).$$

The dual f^* is obtained straightforward with Corollary 1(ii).

The class of the Maiorana-McFarland bent functions is the class of the functions $g : \mathbb{V}_m \times \mathbb{V}_m \to \mathbb{F}_2$ of the form

$$g(x,y) = \langle x, \pi(y) \rangle \oplus \sigma(y),$$

for a permutation π of $\mathbb{V}_m$ and a Boolean function $\sigma : \mathbb{V}_m \to \mathbb{F}_2$. For simplicity we choose $\sigma = 0$, then the dual of $g(x,y) = \langle x, \pi(y) \rangle$ is

$$g^*(x,y) = \langle y, \pi^{-1}(x) \rangle.$$

Let $g_i(x,y) = \langle x, \pi_i(y) \rangle$, $i = 1,2,3,4$, be Maiorana-McFarland bent functions. As easily observed, g_1, g_2, g_3, g_4 satisfy the conditions (I) and (II) if and only if $\pi_1 + \pi_2 + \pi_3 = \pi_4$ and $\pi_1^{-1} + \pi_2^{-1} + \pi_3^{-1} = \pi_4^{-1}$. In [9, Theorem 14], Maiorana-McFarland functions obtained with power permutations of $\mathbb{F}_{2^m}$ are employed in the construction of Proposition 2. In the subsequent corollary we apply Lemma 2 to the same class of Maiorana-McFarland functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_2$.

Corollary 2. *Let d be a positive integer relatively prime to 2^m-1, let e be the multiplicative inverse of d modulo 2^m-1, and let c_1, c_2, c_3 be nonzero elements of $\mathbb{F}_{2^m}$ such that $c_1+c_2+c_3 \neq 0$ and $c_1^{-e}+c_2^{-e}+c_3^{-e} = (c_1+c_2+c_3)^{-e}$. The function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$*

$$f(x,y) = \mathrm{Tr}_m((c_1+c_2)y^d x) + 2\mathrm{Tr}_m((c_1+c_3)y^d x) + 4\mathrm{Tr}_m(c_1 y^d x)$$

is gbent, and its dual is

$$f^*(x,y) = \mathrm{Tr}_m((c_1^{-e}+c_2^{-e})x^e y) + 2\mathrm{Tr}_m((c_1^{-e}+c_3^{-e})x^e y) + 4\mathrm{Tr}_m(c_1^{-e}x^e y).$$

Proof. Consider the Maiorana-McFarland bent functions $g_i = \mathrm{Tr}_m(x\pi_i(y))$, $i = 1,2,3$, with $\pi_i(y) = c_i y^d$, hence $\pi_i^{-1}(y) = c_i^{-e} y^e$. With the conditions on c_1, c_2, c_3 we have that $\pi_1 + \pi_2 + \pi_3 := \pi_4$ is a permutation and $\pi_1^{-1}+\pi_2^{-1}+\pi_3^{-1} = (\pi_1+\pi_2+\pi_3)^{-1} = \pi_4^{-1}$. Hence conditions (I) and (II) are satisfied. Applying Lemma 2 and Theorem 2 we obtain the gbent function $f(x,y)$ and its dual. Note that in the expressions for f and f^* we use "+" for both, the addition in $\mathbb{F}_{2^m}$ and the addition in $\mathbb{Z}_8$. □

In [9], the existence of exponents e relatively prime to 2^m-1 for which there exists a 3-tuple (c_1, c_2, c_3) of pairwise distinct nonzero elements in $\mathbb{F}_{2^m}$ for which $c_1^{-e} + c_2^{-e} + c_3^{-e} = (c_1+c_2+c_3)^{-e}$ (and $c_1+c_2+c_3 \neq 0$) is discussed. A complete list is given for $4 \leq m \leq 8$, and it is pointed out that d in Corollary 2 cannot be a power of 2. In [9, Proposition 20] it is shown that for every m divisible by 4 but not by 5, the 3-tuple $(c, bc, b^{-1}c)$, $b, c \in \mathbb{F}_{2^m}^*$ and $b^4+b+1 = 0$, is such a 3-tuple for $e = 11$. Accordingly we get the following corollary.

Corollary 3. *Let m be an integer divisible by 4 but not by 5, let $b, c \in \mathbb{F}_{2^m}^*$ with $b^4+b+1 = 0$, and let d be the multiplicative inverse of 11 modulo 2^m-1. Then the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$*

$$f(x,y) = \mathrm{Tr}_m(c(1+b)y^d x) + 2\mathrm{Tr}_m(c(1+b^{-1})y^d x) + 4\mathrm{Tr}_m(cy^d x)$$

is gbent and its dual is

$$f^*(x,y) = \mathrm{Tr}_m(c^{-11}(1+b^{-11})x^{11}y) + 2\mathrm{Tr}_m(c^{-11}(1+b^{11})x^{11}y) + 4\mathrm{Tr}_m(c^{-11}x^{11}y).$$

We finally remark that in [9] some more examples for the construction of bent function with Proposition 2 are given. By the observed equivalence between bent functions obtained in this way and octal gbent functions, one can generate further examples of gbent functions in $\mathcal{GB}_n^8$, n even.

4 Perspectives

In this article we observe a strong connection between a secondary construction of bent functions proposed by Carlet in [2] and octal gbent functions in even dimension. We characterize gbent functions $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + 4a_2(\mathbf{x}) \in \mathcal{GB}_n^8$, n even, as those functions for which a_2, $a_0 \oplus a_2$, $a_1 \oplus a_2$, $a_0 \oplus a_1 \oplus a_2$ and $a_2 \oplus a_0 a_1$ are bent (Theorem 2). We present their duals using the duals of the associated bent functions. Alternatively, we completely describe such gbent functions and their duals in terms of a triple of bent functions g_1, g_2, g_3 satisfying (I) and (II). Our examination is also the first comprehensive treatment of duality for gbent functions.

Octal gbent functions also exist for odd n, where the associated Boolean functions are semibent (and their Walsh transforms must satisfy certain relations), see Theorem 9 in [6]. A general description of their duals hence cannot rely on the duals of these Boolean functions and is still missing.

If $f \in \mathcal{GB}_n^{2^k}$ is gbent, then cf is not necessarily gbent if $1 \leq c \leq 2^k - 1$ is even. However in some cases cf is gbent for every nonzero c. Examples are obtained from some of the partial spread gbent functions analysed in [7], and from the Maiorana-McFarland gbent functions in Corollaries 2 and 3. In those examples a_1, a_2, a_3 form vectorial bent functions in dimension 3 (the same applies to g_1, g_2, g_3). (However vectorial bent functions a_0, a_1, a_2 in general do not induce gbent functions as $a_0 \oplus a_1 a_2$ is not bent in general.) The class of gbent functions f for which cf is gbent for all $1 \leq c \leq 2^k - 1$, may be particularly interesting for future research as they give relative difference sets, see [7].

Acknowledgement. The author is supported by the Austrian Science Fund (FWF) Project no. M 1767-N26.

References

[1] A. Canteaut, P. Charpin, Decomposing bent functions, IEEE Trans. Inf. Theory 49 (2003) 2004–2019.

[2] C. Carlet, in: M.P.C. Fossorier et *al.* (Eds.), On Bent and Highly Nonlinear Balanced/Resilient Functions and their Algebraic Immunities, AAECC, Lecture Notes in Computer Science 3857, Springer-Verlag, New York, 2006, pp. 1–28.

[3] C. Carlet, in: Y. Cramer, P. Hammer (Eds.), Boolean Functions for Cryptography and Error Correcting Codes, Boolean Models and Methods in Mathematics, Computer Science and Engineering, Cambridge University Press, 2010, pp.257–397.

[4] J.F. Dillon, Elementary Hadamard Difference Sets, Ph.D. dissertation, University of Maryland, 1974.

[5] S. Hodžić, E. Pasalic, Generalized bent functions – Some general construction methods and related necessary and sufficient conditions, Cryptogr. Commun. 7 (2015) 469–483.

[6] T. Martinsen, W. Meidl, P. Stănică, Generalized bent functions and their Gray images, manuscript.

[7] T. Martinsen, W. Meidl, P. Stănică, Partial spread and vectorial generalized bent functions, manuscript.

[8] T. Martinsen, P. Stănică, Octal bent Boolean functions, IACR Cryptology ePrint Archive, 2011.

[9] S. Mesnager, Several infinite classes of bent functions and their duals, IEEE Trans. Inf. Theory 60 (2014) 4397–4407.

[10] K. Nyberg, in: D.W. Davies (Ed.), Perfect Nonlinear S-Boxes, Advances in Cryptology, EUROCRYPT '91 (Brighton, 1991), Lecture Notes in Computer Science 547, Springer, Berlin, 1991, pp. 378–386.

[11] J.D. Olsen, R.A. Scholtz, L.R. Welch, Bent-function sequences, IEEE Trans. Inf. Theory 28 (1982) 858–864.

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

[13] K.U. Schmidt, Quaternary constant-amplitude codes for multicode CDMA, IEEE Trans. Inf. Theory 55 (2009) 1824–1832.

[14] P. Solé, N. Tokareva, Connections between quaternary and binary bent functions, http://eprint.iacr.org/2009/544.pdf; see also, Prikl. Diskr. Mat. 1 (2009) 16–18.

[15] P. Stănică, T. Martinsen, S. Gangopadhyay, B.K. Singh, Bent and generalized bent Boolean functions, Des. Codes Cryptography 69 (2013) 77–94.