Negabent Functions in the Maiorana–McFarland Class

Kai-Uwe Schmidt[1], Matthew G. Parker[2], and Alexander Pott[3]

[1] Department of Mathematics, Simon Fraser University
Burnaby, BC V5A 1S6, Canada
kuschmidt@sfu.ca
[2] The Selmer Center, Department of Informatics, University of Bergen
N-5020 Bergen, Norway
matthew.parker@ii.uib.no
[3] Institute for Algebra and Geometry, Faculty of Mathematics,
Otto-von-Guericke-University Magdeburg,
D-39016 Magdeburg, Germany
alexander.pott@ovgu.de

Abstract. Boolean functions which are simultaneously bent and negabent are studied. Transformations that leave the bent-negabent property invariant are presented. A construction for infinitely many bent-negabent Boolean functions in $2mn$ variables ($m > 1$) and of algebraic degree at most n is described, this being a subclass of the Maiorana–McFarland class of bent functions. Finally it is shown that a bent-negabent function in $2n$ variables from the Maiorona–McFarland class has algebraic degree at most $n - 1$.

1 Introduction

Bent Boolean functions are the class of Boolean functions whose spectral values have equal magnitude with respect to the *Hadamard transform* [1]. The construction and classification of bent functions is of significant and active interest to designers of cryptographic primitives [2], as such functions have maximum distance to the set of affine functions and, therefore, are not well-approximated by affine functions. It is natural also to consider spectral values with respect to the *nega-Hadamard transform.* If these spectral values of a Boolean function are all equal in magnitude, then we call the function *negabent.*

In this paper we consider how to construct Boolean functions that are simultaneously bent and negabent. Such a problem has been previously considered in [3], providing constructions for quadratic functions. Here we present a new and infinite construction for functions of more general algebraic degree, thereby answering and generalizing a conjecture made in [3]. More precisely, we construct a subclass of the Maiorana–McFarland class of bent functions in which all functions are also negabent. This construction generalizes the construction of quadratic bent-negabent functions described in [4, 5]. These functions are in $2mn$ variables and have algebraic degree at most n, where $m > 1$.

We also enlarge the class of symmetry operations over which the bent-negabent property of a Boolean function is preserved. In particular, we show that the bent-negabent property is an invariant with respect to the action of the orthogonal group on the input vector space. Finally we provide an upper bound on the algebraic degree of any bent-negabent Boolean function from the Maiorana-McFarland class.

2 Notation

Let V_n be an n-dimensional vector space over $\mathbb{F}_2$. Let $f : V_n \to \mathbb{F}_2$ be a Boolean function. The *Hadamard transform* of f is defined to be

$$\mathcal{H}(f)(u) := (-1)^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x)+u \cdot x}, \quad u \in V_n.$$

The *nega-Hadamard transform* of f is defined to be

$$\mathcal{N}(f)(u) := (-1)^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x)+u \cdot x} i^{\mathrm{wt}(x)}, \quad u \in V_n,$$

where $i := \sqrt{-1}$ and wt(.) denotes the Hamming weight. The function f is called *bent* if

$$|\mathcal{H}(f)(u)| = 1 \quad \text{for all} \quad u \in V_n.$$

Similarly, f is called *negabent* if

$$|\mathcal{N}(f)(u)| = 1 \quad \text{for all} \quad u \in V_n.$$

If f is both bent and negabent, we say that f is *bent-negabent.*

Now let $f : V_n \oplus V_n \to \mathbb{F}_2$ be a Boolean function of the form

$$f(x, y) = \sigma(x) \cdot y + g(x),$$

where $\sigma : V_n \to V_n$ and $g : V_n \to \mathbb{F}_2$. It is well known that this function is bent if and only if σ is a permutation. The whole set of such bent functions forms the *Maiorana–McFarland class.*

In the remainder of this section we will introduce some further notation and a useful lemma. Write $V_n = U \oplus W$, where $\dim W = k$ and $k \leq n$, so that $\dim U = n - k$. Let $f : V_n \to \mathbb{F}_2$ be a Boolean function. For each fixed $x \in U$ we may view $f(x, \cdot)$ as a Boolean function on W. We define the *partial Hadamard transform* of f with respect to W as

$$\mathcal{H}_W(f)(x, v) := 2^{-\frac{k}{2}} \sum_{y \in W} (-1)^{f(x,y)+v \cdot y}, \quad v \in W.$$

We say that f is *bent with respect to W* if

$$|\mathcal{H}_W(f)(x, v)| = 1 \quad \text{for each} \quad x \in U, v \in W.$$

If f is bent with respect to W, the *partial dual* $\tilde{f}_W$ of f with respect to W is defined by the relation

$$\mathcal{H}_W(f)(x,v) = (-1)^{\tilde{f}_W(x,v)}.$$

Note that in the special case where $n = k$, $\tilde{f}_W$ is the usual dual of f, which we will denote by $\tilde{f}$.

In the remainder if this paper we shall make frequent use of the following lemma.

Lemma 1. *For any $u \in V_n$ we have*

$$\sum_{x \in V_n} (-1)^{u \cdot x} i^{\mathrm{wt}(x)} = 2^{\frac{n}{2}} \omega^n i^{-\mathrm{wt}(u)},$$

where $\omega = (1+i)/\sqrt{2}$ is a primitive 8th root of unity.

Proof. Write $u = (u_1, u_2, \ldots, u_n)$. By successively factoring out terms, we obtain

$$\begin{aligned}\sum_{x \in V_n} (-1)^{u \cdot x} i^{\mathrm{wt}(x)} &= \prod_{k=1}^{n} (1 + i(-1)^{u_k}) \\ &= 2^{\frac{n}{2}} \prod_{k=1}^{n} \omega^{(-1)^{u_k}} \\ &= 2^{\frac{n}{2}} \omega^{n-2\,\mathrm{wt}(u)} \\ &= 2^{\frac{n}{2}} \omega^n i^{-\mathrm{wt}(u)}.\end{aligned}$$

□

Note that the preceding lemma shows that all affine functions $f : V_n \to \mathbb{F}_2$ are negabent (see also [3, Prop. 1]).

3 Transformations Preserving Bent-Negabentness

Several transformations that preserve the bent-negabent property have been presented in [3]. Here we provide two new transformations.

It is known that, if $f : V_n \to \mathbb{F}_2$ is a bent function, then the function given by

$$f(Ax + b) + c \cdot x + d, \quad \text{where} \quad A \in GL(2,n),\ b, c \in V_n,\ d \in V_1,$$

is also bent. Here, $GL(2,n)$ is the general linear group of $n \times n$ matrices over $\mathbb{F}_2$. These operations define a group whose action on f leaves the bent property of f invariant. Counterexamples show that these operations generally do not preserve the negabent property of a Boolean function. It is therefore interesting to find a subgroup of the bent-preserving operations that preserves also the negabent property. The following theorem shows that, if we replace $GL(2,n)$ by $O(2,n)$, the orthogonal group of $n \times n$ matrices over $\mathbb{F}_2$, we obtain such a subgroup.

Theorem 2. *Let $f, g : V_n \to \mathbb{F}_2$ be two Boolean functions. Suppose that f and g are related by*

$$g(x) = f(Ax + b) + c \cdot x + d, \quad \textit{where} \quad A \in O(2, n),\ b, c \in V_n,\ d \in V_1.$$

Then, if f is bent-negabent, g is also bent-negabent.

Proof. As discussed above, g is bent if f is bent. It remains to show that g is negabent. From [3, Lem. 2] we know that, if $f(Ax)$ is negabent, so is $f(Ax + b) + c \cdot x + d$. It is therefore sufficient to assume that b and c are all-zero vectors and $d = 0$. Observe that

$$\mathrm{wt}(x) = x^T I x,$$

where I is the $n \times n$ identity matrix and the matrix operations are over $\mathbb{Z}$. We therefore have

$$\mathcal{N}(g)(u) = 2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(Ax)+u\cdot x} i^{x^T I x}.$$

Now, since A is invertible by assumption, there exists B such that $AB = I$. Moreover, when x ranges over V_n, so does Bx. Thus,

$$\mathcal{N}(g)(u) = 2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x)+u\cdot Bx} i^{(Bx)^T I (Bx)}.$$

Since $A \in O(2, n)$, we have $B \in O(2, n)$ and so $B^T I B = I$. Hence,

$$(Bx)^T I (Bx) = x^T (B^T I B) x = x^T I x.$$

We conclude

$$\begin{aligned} \mathcal{N}(g)(u) &= 2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x)+u\cdot Bx} i^{x^T I x} \\ &= 2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x)+B^T u\cdot x} i^{\mathrm{wt}(x)} \\ &= \mathcal{N}(f)(B^T u), \end{aligned}$$

which proves the theorem. □

It is known that the dual of a bent function is again a bent function, and it was proved in [3, Thm. 11] that the dual of a bent-negabent function is also bent-negabent. The following theorem generalizes this concept by showing that, if a bent-negabent function is bent with respect to certain subspaces, then the corresponding partial duals are also bent-negabent.

Theorem 3. *Write $V_n = U \oplus W$, where* $\dim W = k$ *and $k \le n$, so that* $\dim U = n - k$. *Let $f : V_n \to \mathbb{F}_2$ be a bent-negabent function that is bent with respect to U and bent with respect to W. Then $\tilde{f}_W$ is also bent-negabent.*

Proof. We first prove that $\tilde{f}_W$ is bent. By direct calculation,

$$\begin{aligned}\mathcal{H}(\tilde{f}_W)(u,w) &= 2^{-\frac{n}{2}}\sum_{x\in U}\sum_{v\in W}(-1)^{\tilde{f}_W(x,v)+u\cdot x+v\cdot w}\\ &= 2^{-\frac{n+k}{2}}\sum_{x\in U}\sum_{v\in W}\sum_{y\in W}(-1)^{f(x,y)+v\cdot y+u\cdot x+v\cdot w}\\ &= 2^{-\frac{n+k}{2}}\sum_{x\in U}\sum_{y\in W}(-1)^{f(x,y)+u\cdot x}\sum_{v\in W}(-1)^{v\cdot(y+w)}.\end{aligned}$$

The inner sum is zero unless $y = w$, in which case it is 2^k. Hence,

$$\begin{aligned}\mathcal{H}(\tilde{f}_W)(u,w) &= 2^{-\frac{n-k}{2}}\sum_{x\in U}(-1)^{f(x,w)+u\cdot x}\\ &= \mathcal{H}_U(f)(u,w).\end{aligned}$$

By assumption, $|\mathcal{H}_U(f)(u,w)| = 1$ for each $u \in U$ and each $w \in W$. Therefore, $\tilde{f}_W$ is bent.

Next we prove that $\tilde{f}_W$ is negabent. We have

$$\begin{aligned}\mathcal{N}(\tilde{f}_W)(u,w) &= 2^{-\frac{n}{2}}\sum_{x\in U}\sum_{v\in W}(-1)^{\tilde{f}_W(x,v)+u\cdot x+v\cdot w}i^{\mathrm{wt}(v)+\mathrm{wt}(x)}\\ &= 2^{-\frac{n+k}{2}}\sum_{x\in U}\sum_{v\in W}\sum_{y\in W}(-1)^{f(x,y)+v\cdot y+u\cdot x+v\cdot w}i^{\mathrm{wt}(v)+\mathrm{wt}(x)}\\ &= 2^{-\frac{n+k}{2}}\sum_{x\in U}\sum_{y\in W}(-1)^{f(x,y)+u\cdot x}i^{\mathrm{wt}(x)}\sum_{v\in W}(-1)^{v\cdot(y+w)}i^{\mathrm{wt}(v)}.\end{aligned}$$

The inner sum can be computed with Lemma 1. We therefore obtain

$$\begin{aligned}\mathcal{N}(\tilde{f}_W)(u,w) &= 2^{-\frac{n}{2}}\omega^k\sum_{x\in U}\sum_{y\in W}(-1)^{f(x,y)+u\cdot x}i^{\mathrm{wt}(x)}i^{-\,\mathrm{wt}(y+w)}\\ &= 2^{-\frac{n}{2}}\omega^k i^{-\,\mathrm{wt}(w)}\sum_{x\in U}\sum_{y\in W}(-1)^{f(x,y)+u\cdot x+y\cdot w}i^{\mathrm{wt}(x)-\mathrm{wt}(y)}\\ &= \omega^k i^{-\,\mathrm{wt}(w)}\mathcal{N}(f)(u,\bar{w}),\end{aligned}$$

where $\omega = (1+i)/\sqrt{2}$ and $\bar{w}$ is the complement of w. Since f is negabent, this shows that $\tilde{f}_W$ is also negabent. □

4 Constructions

Throughout this section we use the following notation. Define V to be an mn-dimensional vector space over $\mathbb{F}_2$, so that

$$V = \underbrace{V_n \oplus V_n \oplus \cdots \oplus V_n}_{m\text{ times}}.$$

Let the Boolean function $f : V \oplus V \to \mathbb{F}_2$ be given by

$$f(x_1, \ldots, x_m, y_1, \ldots, y_m) = \sigma(x_1, \ldots, x_m) \cdot (y_1, \ldots, y_m) + g(x_1, \ldots, x_m), \quad (1)$$

where $\sigma : V \to V$ is of the form

$$\sigma(x_1, \ldots, x_m) = (\psi_1(x_1), \phi_1(x_1) + \psi_2(x_2), \ldots, \phi_{m-1}(x_{m-1}) + \psi_m(x_m))$$

and $g : V \to \mathbb{F}_2$ is defined by

$$g(x_1, \ldots, x_m) = h_1(x_1) + h_2(x_2) + \cdots + h_m(x_m).$$

Here, $\psi_1, \ldots, \psi_m, \phi_1, \ldots, \phi_{m-1}$ are permutations on V_n and $h_1, \ldots, h_m : V_n \to \mathbb{F}_2$ are arbitrary Boolean functions. Explicitly, f reads

$$\begin{aligned} &f(x_1, \ldots, x_m, y_1, \ldots, y_m) \\ &\qquad = \psi_1(x_1) \cdot y_1 + h_1(x_1) + \sum_{j=2}^{m} (y_j \cdot [\phi_{j-1}(x_{j-1}) + \psi_j(x_j)] + h_j(x_j)). \end{aligned}$$

Since σ is a permutation, f belongs to the Maiorana–McFarland class, and is therefore bent. In the next theorem, we will identify configurations of σ and g so that f is also negabent.

Theorem 4. *Let m be a positive integer satisfying $m \not\equiv 1 \pmod 3$, and let k be an integer satisfying $0 < k < m$ and $k \equiv 0 \pmod 3$ or $(m - k) \equiv 1 \pmod 3$. Let f be as in (1), where*

$$\begin{aligned} \sigma(x_1, \ldots, x_m) &= (x_1, x_1 + x_2, \ldots, x_{k-1} + \psi(x_k), \phi(x_k) + x_{k+1}, \ldots, x_{m-1} + x_m) \\ g(x_1, \ldots, x_m) &= h(x_k), \end{aligned}$$

ψ, ϕ are permutations on V_n, and $h : V_n \to \mathbb{F}_2$ is an arbitrary Boolean function. (In other words, $\psi_1, \ldots, \psi_m, \phi_1, \ldots, \phi_{m-1}$ are identity maps except for $\psi := \psi_k$ and $\phi := \phi_k$, and $h_1, \ldots, h_m$ are zero except for $h := h_k$.) Then f is bent-negabent.

A lemma is required to prove the theorem.

Lemma 5. *Let s be a nonnegative integer. For any $u_1, \ldots, u_s, z_{s+1} \in V_n$ define*

$$E_s(z_{s+1}) := \prod_{j=1}^{s} \sum_{z_j \in V_n} (-1)^{(z_{j+1}+u_j) \cdot z_j} \imath^{\mathrm{wt}(z_j)},$$

where an empty product is defined to be equal to 1. Then we have

$$E_s(z_{s+1}) = \begin{cases} 2^{sn/2} \omega^c (-1)^{a \cdot z_{s+1}} & \text{if} \quad s \equiv 0 \pmod 3 \\ 2^{sn/2} \omega^c (-1)^{a \cdot z_{s+1}} \imath^{-\mathrm{wt}(z_{s+1})} & \text{if} \quad s \equiv 1 \pmod 3 \\ 2^{(s+1)n/2} \omega^c \delta_{z_{s+1}+a} & \text{if} \quad s \equiv 2 \pmod 3 \end{cases}$$

for some $c \in \mathbb{Z}_8$ and $a \in V_n$. Here δ_a denotes the Kronecker delta function, i.e., δ_a equals 1 if $a = 0$ and is zero otherwise.

Proof. The lemma is certainly true for $s = 0$. We proceed by induction on s, where we use the lemma as a hypothesis. Observe that for $s > 0$ we have

$$E_s(z_{s+1}) = \sum_{z_s \in V_n} (-1)^{(z_{s+1}+u_s)\cdot z_s} i^{\mathrm{wt}(z_s)} E_{s-1}(z_s).$$

Now assume that the lemma is true for $s \equiv 0 \pmod 3$. Using Lemma 1, we have for $s \equiv 1 \pmod 3$

$$\begin{aligned} E_s(z_{s+1}) &= 2^{(s-1)n/2}\omega^c \sum_{z_s \in V_n} (-1)^{(z_{s+1}+u_s+a)\cdot z_s} i^{\mathrm{wt}(z_s)} \\ &= 2^{sn/2}\omega^{c+n} i^{-\mathrm{wt}(z_{s+1}+u_s+a)} \\ &= 2^{sn/2}\omega^{c'}(-1)^{a'\cdot z_{s+1}} i^{-\mathrm{wt}(z_{s+1})}, \end{aligned}$$

where $c' = c + n - 2\,\mathrm{wt}(u_s + a)$ and $a' = a + u_s$. This proves the lemma for $s \equiv 1 \pmod 3$ provided that it holds for $s \equiv 0 \pmod 3$. Now assume that the lemma is true for $s \equiv 1 \pmod 3$. Then for $s \equiv 2 \pmod 3$ we obtain

$$\begin{aligned} E_s(z_{s+1}) &= 2^{(s-1)n/2}\omega^c \sum_{z_s \in V_n} (-1)^{(z_{s+1}+u_s+a)\cdot z_s} \\ &= 2^{(s+1)n/2}\omega^{c'}\delta_{z_{s+1}+a'}. \end{aligned}$$

where $c' = c$ and $a' = a + u_s$. Assuming that the lemma is true for $s \equiv 2 \pmod 3$, we have for $s \equiv 0 \pmod 3$

$$\begin{aligned} E_s(z_{s+1}) &= 2^{sn/2}\omega^c \sum_{z_s \in V_n} (-1)^{(z_{s+1}+u_s)\cdot z_s} i^{\mathrm{wt}(z_s)} \delta_{z_s+a} \\ &= 2^{sn/2}\omega^{c'}(-1)^{a'\cdot z_{s+1}}, \end{aligned}$$

where $c' = c + 2\,\mathrm{wt}(a) + 4a \cdot u_s$ and $a' = a$. This completes the induction. □

Proof (of Theorem 4). We define the relabeling $z_{2j} := x_j$ and $z_{2j-1} := y_j$ for $j = 1, 2, \ldots, m$, so that we have

$$\begin{aligned} &f(x_1, \ldots, x_m, y_1, \ldots, y_m) = \\ &\quad h(z_{2k}) + \sum_{j=1}^{2k-2} z_j \cdot z_{j+1} + z_{2k-1} \cdot \psi(z_{2k}) + \sum_{j=2k+2}^{2m} z_{j-1} \cdot z_j + z_{2k+1} \cdot \phi(z_{2k}). \end{aligned}$$

Write

$$\mathcal{N}(f)(u_1, \ldots, u_{2m}) = 2^{-mn} \sum_{z_{2k} \in V_n} (-1)^{h(z_{2k}) + z_{2k}\cdot u_{2k}} i^{\mathrm{wt}(z_{2k})} P(z_{2k}) Q(z_{2k}), \quad (2)$$

where

$$P(z_{2k}) = \prod_{j=1}^{2k-2} \sum_{z_j \in V_n} (-1)^{(z_{j+1}+u_j)\cdot z_j} i^{\mathrm{wt}(z_j)} \sum_{z_{2k-1} \in V_n} (-1)^{(\psi(z_{2k})+u_{2k-1})\cdot z_{2k-1}} i^{\mathrm{wt}(z_{2k-1})}$$

$$Q(z_{2k}) = \prod_{j=2k+2}^{2m} \sum_{z_j \in V_n} (-1)^{(z_{j-1}+u_j)\cdot z_j} i^{\mathrm{wt}(z_j)} \sum_{z_{2k+1} \in V_n} (-1)^{(\phi(z_{2k})+u_{2k+1})\cdot z_{2k+1}} i^{\mathrm{wt}(z_{2k+1})}.$$

In what follows, we treat the case $k \equiv 0 \pmod 3$, the case $(m-k) \equiv 1 \pmod 3$ can be proved similarly (essentially, the roles of $P(z_{2k})$ and $Q(z_{2k})$ are exchanged). If $k \equiv 0 \pmod 3$, we have $2k-1 \equiv 2 \pmod 3$ and from Lemma 5

$$P(z_{2k}) = 2^{kn}\omega^c \delta_{\psi(z_{2k})+a} \tag{3}$$

for some $c \in \mathbb{Z}_8$ and $a \in V_n$. Now $k \equiv 0 \pmod 3$ implies $m-k \equiv m \pmod 3$, so $2(m-k) \equiv 0 \pmod 3$ or $1 \pmod 3$. Hence by Lemma 5

$$Q(z_{2k}) = \begin{cases} 2^{(m-k)n}\omega^d(-1)^{b\cdot\phi(z_{2k})} & \text{if } m \equiv 0 \pmod 3 \\ 2^{(m-k)n}\omega^d(-1)^{b\cdot\phi(z_{2k})}i^{-\operatorname{wt}(\psi(z_{2k}))} & \text{if } m \equiv 2 \pmod 3 \end{cases} \tag{4}$$

for some $d \in \mathbb{Z}_8$ and $b \in V_n$. Combining (2), (3), and (4), we arrive at

$$\begin{aligned} &\mathcal{N}(f)(u_1,\dots,u_{2m}) \\ &= \begin{cases} \omega^{c+d} \displaystyle\sum_{z_{2k}\in V_n} (-1)^{h(z_{2k})+z_{2k}\cdot u_{2k}+b\cdot\phi(z_{2k})} i^{\operatorname{wt}(z_{2k})}\delta_{\psi(z_{2k})+a} & \text{if } m \equiv 0 \pmod 3 \\ \omega^{c+d} \displaystyle\sum_{z_{2k}\in V_n} (-1)^{h(z_{2k})+z_{2k}\cdot u_{2k}+b\cdot\phi(z_{2k})}\delta_{\psi(z_{2k})+a} & \text{if } m \equiv 2 \pmod 3. \end{cases} \end{aligned}$$

In either case the term inside the sum is zero unless $z_{2k} = \psi^{-1}(a)$. Therefore, $|\mathcal{N}(f)(u_1,\dots,u_{2m})| = 1$, as was claimed. □

Example 6. Take $m = 2$ and $k = 1$ in Theorem 4. Then f reads

$$f(x_1,x_2,y_1,y_2) = y_1\cdot\psi(x_1) + \phi(x_1)\cdot y_2 + y_2\cdot x_2 + h(x_1).$$

In this way we can construct bent-negabent functions in $4n$ variables of degree ranging from 2 to n.

In general, whenever $m \not\equiv 1 \pmod 3$, we can use Theorem 4 to construct bent-negabent functions in $2mn$ variables of degree ranging from 2 to n. This yields bent-negabent functions in $2t$ variables for every $t \geq 2$ and $t \not\equiv 1 \pmod 6$; if $t \not\equiv 1 \pmod 3$, we can take $n = 1$ and $m = t$, and if $t \equiv 1 \pmod 3$ and $t \not\equiv 1 \pmod 6$, we can take $n = 2$ and $m = t/2$.

In the remainder of this section we apply Theorem 3 to construct further bent-negabent functions by taking a partial dual of f given in (1). We therefore have to prove that the partial dual of f exists with respect to certain subspaces of V and to find an explicit expression for this function.

Write $V = U \oplus W$, where $\dim W = k$ and $k \leq mn$. Suppose that we have a function $\tau : V \to V$. We can separate τ on U and W by defining $|W|$ functions $\tau_z : U \to U$ and $|U|$ functions $\tau_x : W \to W$ such that

$$\tau(x,z) = (\tau_z(x), \tau_x(z)), \quad x \in U, z \in W.$$

Lemma 7. *With the notation as above, define $a : V \oplus V \to \mathbb{F}_2$ by*

$$a(x,z,y,w) = \tau(x,z)\cdot(y,w) + c(x,z), \quad x,y \in U,\ z,w \in W,$$

where $c : V \to \mathbb{F}_2$. Then a is bent with respect to $W \oplus W$ if for every $x \in U$ the map τ_x is a permutation on W. Moreover, in this case, the partial dual of a with respect to $W \oplus W$ is given by

$$\tilde{a}_{W\oplus W}(x,u,y,v) = \tau_z(x)\cdot y + u\cdot z + c(x,z), \quad \textit{where} \quad z = \tau_x^{-1}(v).$$

Proof. We have

$$\begin{aligned}\mathcal{H}_{W\oplus W}(a)(x,u,y,v) &= 2^{-k}\sum_{z,w\in W}(-1)^{\tau(x,z)\cdot(y,w)+c(x,z)+u\cdot z+v\cdot w}\\ &= 2^{-k}\sum_{z,w\in W}(-1)^{\tau_z(x)\cdot y+\tau_x(z)\cdot w+c(x,z)+u\cdot z+v\cdot w}\\ &= 2^{-k}\sum_{z\in W}(-1)^{\tau_z(x)\cdot y+c(x,z)+u\cdot z}\sum_{w\in W}(-1)^{(\tau_x(z)+v)\cdot w}.\end{aligned}$$

The inner sum is zero unless $z = \tau_x^{-1}(v)$, in which case the sum is equal to 2^k. Therefore

$$\mathcal{H}_{W\oplus W}(a)(x,u,y,v) = (-1)^{\tilde{a}_{W\oplus W}(x,u,y,v)},$$

where $\tilde{a}_{W\oplus W}$ is given in the lemma. □

Now partition the set $\{1,2,\ldots,m\}$ into the two subsets

$$S = \{s_1,\ldots,s_k\} \quad \text{and} \quad T = \{t_1,\ldots,t_{m-k}\}.$$

Given $x \in V$, we shall write $x_S = (x_{s_1},\ldots,x_{s_k})$ and $x_T = (x_{t_1},\ldots,x_{t_{m-k}})$. As before, let U and W be vector spaces over $\mathbb{F}_2$ such that $V = U \oplus W$ and, if $(x_1,\ldots,x_m) \in V$, we have $x_S \in W$ and $x_T \in U$.

Theorem 8. *With the notation as above, f, given in (1), is bent with respect to $U \oplus U$ and bent with respect to $W \oplus W$. Moreover, the partial dual of f with respect to $W \oplus W$ is given by*

$$\tilde{f}_{W\oplus W}(x_T,x_S,y_T,y_S) = w_T\cdot y_T + x_S\cdot z_S + g(x_T,z_S),$$

where

$$z_j = \begin{cases} x_j & \textit{if} \;\; j \notin S\\ \psi_j^{-1}(y_j+\phi_{j-1}(z_{j-1})) & \textit{if} \;\; j \in S,\end{cases}$$

and

$$w_j = \phi_{j-1}(z_{j-1}) + \psi_j(x_j) \qquad \textit{for} \quad j \in T.$$

By convention, x_0 is the all-zero vector and ϕ_0 is the identity map.

Proof. Observe that for every $x_S \in W$ the function $\sigma_{x_S}(x_T)$ is a permutation on U. Similarly, for every $x_T \in U$ the function $\sigma_{x_T}(x_S)$ is a permutation on W. Hence, by Lemma 7, f is bent with respect to $U \oplus U$ and bent with respect to $W \oplus W$. Using Lemma 7, the partial dual of f with respect to $W \oplus W$ can be written as

$$\tilde{f}_{W\oplus W}(x_T,x_S,y_T,y_S) = \sigma_{z_S}(x_T)\cdot y_T + x_S\cdot z_S + g(x_T,z_S), \quad z_S = \sigma_{x_T}^{-1}(y_S).$$

Now we first find z_S by solving the system of k equations implied by

$$\sigma_{x_T}(z_S) = y_S.$$

Then z_S can be used to find $\sigma_{z_S}(x_T)$. The solution is given in the theorem. □

Starting from Theorem 4, the preceding theorem together with Theorem 3 can be used to construct further bent-negabent functions of the form (1). If $m = 2$, it is easy to check that we do not obtain any new bent-negabent functions. But for larger m the function f and a partial dual of f generally have a different structure. However, explicit expressions for the partial dual of f can look rather cumbersome, so we illustrate the application of Theorem 8 by an example.

Example 9. Take $m = 3$ and $k = 2$ in Theorem 4. Then f reads

$$f(x_1, x_2, x_3, y_1, y_2, y_3) = \sigma(x_1, x_2, x_3) \cdot (y_1, y_2, y_3) + g(x_1, x_2, x_3),$$

where

$$\begin{aligned} \sigma(x_1, x_2, x_3) &= (x_1, x_1 + \psi(x_2), \phi(x_2) + x_3) \\ g(x_1, x_2, x_3) &= h(x_2). \end{aligned}$$

Now set $S = \{0, 1, 2\}$, so that $W = V$, and apply Theorem 8. Then $\tilde{f}_{W \oplus W}$ is the usual dual of f and given by

$$\tilde{f}(x_1, x_2, x_3, y_1, y_2, y_3) = \sigma'(y_1, y_2, y_3) \cdot (x_1, x_2, x_3) + g'(y_1, y_2, y_3),$$

where

$$\begin{aligned} \sigma'(y_1, y_2, y_3) &= (y_1, \psi^{-1}(y_1 + y_2), y_3 + \phi(\psi^{-1}(y_1 + y_2))) \\ g'(y_1, y_2, y_3) &= h(\psi^{-1}(y_1 + y_2)). \end{aligned}$$

The function $\tilde{f}$ is by Theorem 3 negabent.

5 A Bound on the Degree

It is well known that, if $n > 1$, bent Boolean functions in $2n$ variables have a maximum algebraic degree of n [1]. If $n \in \{2, 3\}$, the maximum degree of a bent-negabent function in $2n$ variables is also equal to n. For example, the cubic function $f : V_6 \to \mathbb{F}_2$

$$\begin{aligned} &f(x_1, x_2, x_3, y_1, y_2, y_3) = \\ &\qquad y_1(x_1x_2 + x_2x_3 + x_1 + x_2) + y_2(x_1x_2 + x_2x_3 + x_3) + y_3(x_1 + x_3) \end{aligned}$$

is bent-negabent. Note that f belongs to the Maiorana–McFarland class. In this section we prove that the degree of a Maiorana–McFarland-type bent-negabent function in $2n$ variables is at most $n - 1$ for $n > 3$.

Theorem 10. *Let σ be a permutation on V_n and let $g : V_n \to \mathbb{F}_2$ be an arbitrary Boolean function. Suppose that the function $f : V_n \oplus V_n \to \mathbb{F}_2$ given by*

$$f(x, y) = \sigma(x) \cdot y + g(x)$$

is negabent. Then, if $n > 3$, the degree of f is at most $n - 1$.

The proof of the theorem requires a lemma.

Lemma 11. *The nega-Hadamard transform of a negabent function on V_n contains only values of the form $\omega^n i^k$, where $\omega = (1 + i)/\sqrt{2}$ and $k \in \mathbb{Z}_4$.*

Proof. Let $2^{-\frac{n}{2}} S$ denote an arbitrary value of the nega-Hadamard transform of a negabent function on V_n. Then $\Re(S)$ or $\Im(S)$ must be integers and $|S|^2 = 2^n$ must be a sum of two squares (one of them may be zero). From Jacobi's two-square theorem we know that 2^n has a unique representation as a sum of two squares, namely $2^n = (2^{n/2})^2 + 0^2$ if n is even, and $2^n = (2^{(n-1)/2})^2 + (2^{(n-1)/2})^2$ if n is odd. Hence, if n is even, either $\Re(S)$ or $\Im(S)$ must be zero. If n is odd, we must have $|\Re(S)| = |\Im(S)|$, which proves the lemma. □

Proof (of Theorem 10). Using Lemma 1, we obtain

$$\begin{aligned}
\mathcal{N}(f)(u, v) &= 2^{-n} \sum_{x,y \in V_n} (-1)^{\sigma(x)\cdot y + g(x) + u\cdot x + v\cdot y} i^{\mathrm{wt}(x)+\mathrm{wt}(y)} \\
&= 2^{-n} \sum_{x \in V_n} (-1)^{g(x)+u\cdot x} i^{\mathrm{wt}(x)} \sum_{y \in V_n} (-1)^{(\sigma(x)+v)\cdot y} i^{\mathrm{wt}(y)} \\
&= 2^{-\frac{n}{2}} \omega^n \sum_{x \in V_n} (-1)^{g(x)+u\cdot x}\, i^{\mathrm{wt}(x)-\mathrm{wt}(\sigma(x)+v)} \\
&= 2^{-\frac{n}{2}} \omega^n i^{-\mathrm{wt}(v)} \sum_{x \in V_n} (-1)^{g(x)+u\cdot x+v\cdot\sigma(x)}\, i^{\mathrm{wt}(x)-\mathrm{wt}(\sigma(x))} \\
&= 2^{-\frac{n}{2}} \omega^n i^{-\mathrm{wt}(v)} \sum_{x \in V_n} (-1)^{g(x)+u\cdot x+v\cdot\sigma(x)}\, i^{w(x)},
\end{aligned}$$

where

$$w(x) = \sum_{j=1}^{n} (x_j + 3\sigma_j(x)) \pmod 4$$

and $\sigma_j(x)$ is the jth component of $\sigma(x)$, so that $\sigma(x) = (\sigma_1(x), \ldots, \sigma_n(x))$. Now write $w(x)$ in 2-adic expansion, viz $w(x) = l(x) + 2q(x)$ with

$$\begin{aligned}
l(x) &= \sum_{j=1}^{n} (x_j + \sigma_j(x)) \pmod 2 \\
q(x) &= \sum_{j=1}^{n} \sigma_j(x) + \sum_{1\le j<k\le n} [(x_j x_k + \sigma_j(x)\sigma_k(x)] + \sum_{1\le j,k\le n} x_j \sigma_k(x) \pmod 2.
\end{aligned}$$

Then we have

$$\begin{aligned}\Re(\omega^{-n} i^{\mathrm{wt}(v)} \mathcal{N}(f)(u,v)) &= 2^{-\frac{n}{2}-1} \sum_{x \in V_n} (-1)^{g(x)+q(x)+v\cdot\sigma(x)+u\cdot x}[1+(-1)^{l(x)}] \\ &= \frac{1}{2}[\mathcal{H}(h_v)(u) + \mathcal{H}(h_{\bar{v}})(\bar{u})], \qquad (5)\end{aligned}$$

where $h_v(x) = g(x) + q(x) + v \cdot \sigma(x)$ and $\bar{u}$ is the complement of u. Similarly we obtain

$$\Im(\omega^{-n} i^{\mathrm{wt}(v)} \mathcal{N}(f)(u,v)) = \frac{1}{2}[\mathcal{H}(h_v)(u) - \mathcal{H}(h_{\bar{v}})(\bar{u})]. \qquad (6)$$

By assumption, $|\mathcal{N}(f)(u,v)| = 1$, and by Lemma 11, either the real part or the imaginary part of $\mathcal{N}(f)(u,v)$ must be zero. First suppose that n is even. Then ω^{-n} is a 4th root of unity and either (5) or (6) must be zero. Hence h_v must be bent for every $v \in V_n$, which implies that for $n > 2$ the degree of h_v can be at most $n/2$ [1]. Now let n be odd. Then ω^{-n} is an 8th root of unity and the absolute values of (5) and (6) must be equal. This can only happen if the Hadamard spectrum of h_v contains only the values 0 and $\pm\sqrt{2}$ (such functions are called almost-bent functions [2]). It is known [2, Thm. 1] that the degree of such a function is at most $(n+1)/2$.

For either $n \geq 3$ we conclude that the degree of $h_v(x)$ is at most $\lceil n/2 \rceil$ for every $v \in V_n$. This implies that the degree of $v \cdot \sigma(x)$ is bounded by $\lceil n/2 \rceil$ for every $v \in V_n$ and $n \geq 3$. Note that, since σ is a permutation, $\sigma_j(x)\sigma_k(x) = 1$ has exactly 2^{n-2} solutions in V_n, so for $n \geq 3$ each of the terms $\sigma_j(x)\sigma_k(x)$ cannot have degree equal to n (see, e.g., [6, Ch. 13, Thm. 1]). Therefore, the degree of q is at most $\max\{n-1, \lceil n/2 \rceil + 1\}$. It follows that, if $n > 3$, the degree of q and, therefore, the degree of g is bounded by $n-1$, which proves the theorem. □

References

1. Rothaus, O.S.: On 'bent' functions. J. Comb. Theory (A) **20** (1976) 300–305
2. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes and Cryptography **15**(2) (Nov. 1998) 125–156
3. Parker, M.G., Pott, A.: On Boolean functions which are bent and negabent. In: Proc. of Sequences, Subsequences, and Consequences (Lecture Notes in Computer Science). Volume 4893., Berlin, Germany: Springer Verlag (Dec. 2007) 9–23
4. Parker, M.G.: The constabent properties of Golay-Davis-Jedwab sequences. In: Int. Symp. Information Theory, Sorrento, IEEE (June 2000) 302
5. Riera, C., Parker, M.G.: One and two-variable interlace polynomials: A spectral interpretation. In: International Workshop, Proceedings of WCC2005, Bergen, Norway, Revised Selected Papers, (Lecture Notes in Computer Science). Volume 3969., Berlin, Germany: Springer Verlag (March 2005) 397–411
6. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. Amsterdam, The Netherlands: North Holland (1977)