On Boolean functions which are bent and negabent

Matthew G. Parker[1] and Alexander Pott[2]

[1] The Selmer Center, Department of Informatics, University of Bergen, N-5020 Bergen, Norway
[2] Institute for Algebra and Geometry, Faculty of Mathematics, Otto-von-Guericke-University Magdeburg, D-39016 Magdeburg, Germany

Abstract. Bent functions $f : \mathbb{F}_2^m \to \mathbb{F}_2$ achieve largest distance to all linear functions. Equivalently, their spectrum with respect to the Hadamard-Walsh transform is flat (i.e. all spectral values have the same absolute value). That is equivalent to saying that the function f has optimum periodic autocorrelation properties. Negaperiodic correlation properties of f are related to another unitary transform called the nega-Hadamard transform. A function is called *negabent* if the spectrum under the nega-Hadamard transform is flat. In this paper, we consider functions f which are simultaneously bent and negabent, i.e. which have optimum periodic and negaperiodic properties. Several constructions and classifications are presented.
Keywords. bent function, Boolean function, unitary transform, Hadamard-Walsh transform, correlation.

1 Introduction

Boolean functions $f : \mathbb{F}_2^m \to \mathbb{F}_2$ play an important role in cryptography. They should satisfy several properties, which are quite often impossible to be satisfied simultaneously. One property is the nonlinearity of a Boolean function, which means that the function is as far away from all linear functions as possible. Functions which achieve this goal are called *bent functions*. Equivalently, all Hadamard-Walsh coefficients of f are equal in absolute value.

There is another criteria which may be viewed as the negaperiodic analogue of the bent criteria. In spectral terms, it may be formulated as follows: Find functions whose nega-Hadamard spectrum is flat, i.e. all spectral values under the nega-Hadamard transform are equal in absolute value. Many bent functions are known, and also many negabent functions are known: It turns out that every linear function is negabent! In this paper, we are going to investigate the intersection of these two sets, i.e. we are searching for bent functions which are simultaneously negabent. At first view, it is not clear that such objects exist. An infinite series of bent-negabent functions has been found in [1, 2].

We give necessary and sufficient conditions for quadratic bent functions to be both bent and negabent, which is based on [2]. It turns out that such quadratic *bent-negabent* functions exist for all even m, which generalizes the series in [2].

More generally, we can describe all Maiorana-McFarland type bent functions which are simultaneously negabent. It seems to be difficult to exploit this condition in general.

The concept of a dual bent function is well known. If f is bent-negabent, then the dual has the same property. There is another interesting transformation which turns a bent-negabent function into a bent-negabent function. We call this *Schmidt complementation* since it is based on a construction in [3]. Therefore, we can construct orbits of bent-negabent functions starting from just one example. We may repeatedly apply dualization and Schmidt complementation. We will report some computational results.

This paper is organized as follows. In Section 2 we summarize some of the main results on bent and negabent functions which are needed throughout this paper.

In Section 3, we consider quadratic bent-negabent functions. In Section 4 we investigate Maiorana-McFarland bent functions. Transformations which preserve bent-negabentness are investigated in Section 5, in particular the Schmidt complementation. Finally, computational results are contained in the last Section 6.

2 Preliminaries

Let V_m denote the m-dimensional vector space $\mathbb{F}_2^m$. We consider functions $\tilde{f} : V_m \to \mathbb{C}$. In many cases, the image set is just $\{\pm 1\}$. Then we say that the function is *Boolean*. If $f : V_m \to \mathbb{F}_2$, we may easily turn it into a "complex-valued" Boolean function:

$$\tilde{f}(\mathbf{x}) := (-1)^{f(\mathbf{x})}.$$

Conversely, any function $\tilde{f} : V_m \to \{\pm 1\}$ determines a function $f : V_m \to \mathbb{F}_2$ by replacing -1 by 1 and 1 by 0. We also call f *Boolean*. The set of Boolean functions $\tilde{f} : V_m \to \mathbb{C}$ is embedded in a 2^m-dimensional unitary vector space $\mathcal{V}$ with an inner product

$$(\tilde{f}, \tilde{g}) = \sum_{\mathbf{x} \in V_m} \tilde{f}(\mathbf{x})\overline{\tilde{g}(\mathbf{x})}. \tag{1}$$

A function $\tilde{f} : V_m \to \mathbb{C}$ is determined by the values $\tilde{f}(\mathbf{x})$. It will be useful to interpret this vector of "function values" as a polynomial in $\mathbb{C}[\xi_1, \ldots, \xi_m]$: We define the multivariate polynomial

$$F = \sum_{\mathbf{x} \in V_m} a_{\mathbf{x}} \xi^{\mathbf{x}}, \tag{2}$$

where $\xi^{\mathbf{x}} := \xi_1^{x_1} \cdots \xi_m^{x_m}$, and $a_{\mathbf{x}} = \tilde{f}(\mathbf{x})$ for $\mathbf{x} \in V_m$. We call F the *indicator polynomial* of $\tilde{f}$. If $f : V_m \to \mathbb{F}_2$, we first have to turn f into a complex-valued function $(-1)^f$, as described above.

Note that $f : V_m \to \mathbb{F}_2$ itself may also be defined as a multivariate polynomial. Both polynomials, f and its indicator F, describe the same object of interest (the Boolean function f), but in a completely different way. Therefore, we will write $\mathbf{x}$ when we deal with $f : V_m \to \mathbb{F}_2$, and ξ when dealing with the indicator.

The set of polynomials $\sum_{\mathbf{x} \in V_m} a_{\mathbf{x}} \xi^{\mathbf{x}}$ forms a complex vector space $\mathcal{L}$ of dimension 2^m. On this vector space, we define the usual inner product:

$$(F, G) := \sum_{\mathbf{x} \in V_m} a_{\mathbf{x}} \overline{b_{\mathbf{x}}},$$

where $F = \sum a_{\mathbf{x}} \xi^{\mathbf{x}}$, $G = \sum b_{\mathbf{x}} \xi^{\mathbf{x}}$. If F and G are the indicator polynomials of two functions $\tilde{f}$ and $\tilde{g}$, then

$$(F, G) := \sum_{\mathbf{x} \in V_m} \tilde{f}(\mathbf{x})\overline{\tilde{g}(\mathbf{x})},$$

which is the same as (1). This shows that the indicator map $\mathcal{I} : \mathcal{V} \to \mathcal{L}$ which maps $\tilde{f}$ to F (as defined in (2)) is a unitary transform. Now we describe two important and interesting unitary transforms $\mathcal{L} \to \mathcal{L}$. Let $F := \sum_{\mathbf{x}} a_{\mathbf{x}} \xi^{\mathbf{x}}$ be a polynomial in $\mathcal{L}$. We define the *Hadamard transform*

$$\mathcal{H}_m(F) = \sum_{\mathbf{u} \in V_m} \hat{a}_{\mathbf{u}} \xi^{\mathbf{u}},$$

where

$$\hat{a}_{\mathbf{u}} = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in V_m} a_{\mathbf{x}} (-1)^{(\mathbf{x}, \mathbf{u})},$$

i.e. we evaluate the polynomial F (now considered as a mapping) at the vector $(\xi_1, \ldots, \xi_m)$ with $\xi_i = (-1)^{u_i}$, and divide by $2^{m/2}$. We will also denote $\hat{a}_{\mathbf{u}}$ by $\mathcal{H}_m(F)(\mathbf{u})$. By $(\cdot, \cdot)$, we denote the standard inner product on V_m.

It is well known and easy to see that the transform $\mathcal{H}_m$ is unitary, and it can be described (after fixing an appropriate basis of $\mathcal{L}$) by the following matrix:

$$\frac{1}{\sqrt{2^m}}(\mathbf{H} \otimes \cdots \otimes \mathbf{H})$$

where

$$\mathbf{H} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

We call this tensor product $\mathbf{H}_m$. If F is the indicator function of a Boolean function $f : V_m \to \mathbb{F}_2$, then

$$\mathcal{H}_m(F)(\mathbf{u}) = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in V_m} (-1)^{f(\mathbf{x})+(\mathbf{u},\mathbf{x})}.$$

This is the classical *Hadamard-Walsh transform* of f. The function f is called *bent* if $|\mathcal{H}_m(F)(\mathbf{u})| = 1$ for all $\mathbf{u} \in V_m$. Since $\sum_{\mathbf{x}}(-1)^{f(\mathbf{x})+(\mathbf{u},\mathbf{x})} \in \mathbb{Z}$, bent functions may exist only if $\sqrt{2^m}$ is an integer, hence if m is even. Actually, for all even m bent functions do exist, see [4], for instance. That article [4] includes an excellent survey on bent functions. Another good source for classical material on bent functions is [5] or [6], for instance.

The transform $\mathcal{H}_m$ is an involution, hence we have the following well known result:

Theorem 1. *If $f : V_m \to \mathbb{F}_2$ is a bent function, then $\mathcal{H}_m((-1)^f)$ is a Boolean function, which is again bent. We call this the dual of f, denoted by $f^\perp$.*

Example 1. The Boolean function $f : V_4 \to \mathbb{F}_2$ defined by $f(\mathbf{x}) = x_1x_2 + x_3x_4$ is bent: The indicator polynomial of $(-1)^f$ is

$$\begin{aligned} F = 1 &+ \xi_1\xi_2\xi_3\xi_4 + \xi_1\xi_3 + \xi_1\xi_4 + \xi_2\xi_3 + \xi_2\xi_4 + \xi_1 + \xi_2 + \xi_3 + \xi_4 \\ &-(\xi_1\xi_2 + \xi_3\xi_4 + \xi_1\xi_2\xi_3 + \xi_1\xi_2\xi_4 + \xi_1\xi_3\xi_4 + \xi_2\xi_3\xi_4). \end{aligned}$$

Using just the definition of $\mathcal{H}$, we obtain

$$\begin{aligned} \mathcal{H}_4(F) = 1 &+ \xi_1\xi_2\xi_3\xi_4 + \xi_1\xi_3 + \xi_1\xi_4 + \xi_2\xi_3 + \xi_2\xi_4 + \xi_1 + \xi_2 + \xi_3 + \xi_4 \\ &-(\xi_1\xi_2 + \xi_3\xi_4 + \xi_1\xi_2\xi_3 + \xi_1\xi_2\xi_4 + \xi_1\xi_3\xi_4 + \xi_2\xi_3\xi_4). \end{aligned}$$

This is the indicator function of the dual of f. In general, it is less straightforward to compute the function $f^\perp$ that corresponds to this indicator, but it turns out that

$$f^\perp = x_1x_2 + x_3x_4,$$

so, in this case, f is self-dual with respect to $\mathcal{H}$.

Let $I = \sqrt{-1}$ be the complex unit. Another unitary transform $\mathcal{N}_m$ is obtained if we evaluate F at all $\pm I$-vectors $(I \cdot (-1)^{u_1}, \ldots, I \cdot (-1)^{u_m})$ of length m. We define

$$\mathcal{N}_m(F) = \sum_{\mathbf{u} \in V_m} \tilde{a}_{\mathbf{u}} \xi^{\mathbf{u}},$$

where

$$\tilde{a}_{\mathbf{u}} = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in V_m} a_{\mathbf{x}} \prod_{i : x_i = 1} I^{2u_i+1},$$

where we compute $2u_i + 1$ modulo 4.

Again, we write $\mathcal{N}_m(F)(\mathbf{u})$ instead of $\tilde{a}_{\mathbf{u}}$.

We call this transform the *nega-Hadamard transform* $\mathcal{N}_m$. In matrix terms, it is described by the m-fold tensor product

$$\frac{1}{\sqrt{2^m}}(\mathbf{N}\otimes\cdots\otimes\mathbf{N})$$

where

$$\mathbf{N}=\begin{pmatrix}1 & I\\ 1 & -I\end{pmatrix}.$$

Another way to compute $\mathcal{N}_m(F)(\mathbf{u})$ is

$$\mathcal{N}_m(F)(\mathbf{u})=\frac{1}{\sqrt{2^m}}\sum_{\mathbf{x}\in V_m} a_{\mathbf{x}}\cdot(-1)^{(\mathbf{u},\mathbf{x})}\cdot I^{\mathrm{weight}(\mathbf{x})}. \tag{3}$$

where weight$(\mathbf{x})$ is the number of nonzero x_i in $\mathbf{x}$. If F is the indicator function of $(-1)^f$, this becomes

$$\mathcal{N}_m(F)(\mathbf{u})=\frac{1}{\sqrt{2^m}}\sum_{\mathbf{x}\in V_m}(-1)^{f(\mathbf{x})+(\mathbf{u},\mathbf{x})}\cdot I^{\mathrm{weight}(\mathbf{x})}. \tag{4}$$

A Boolean function f is called *negabent* if $|\mathcal{N}_m(F)(\mathbf{u})|=1$ for all $\mathbf{u}\in V_m$. In contrast to bent functions, negabent functions also exist if m is odd, see Proposition 1, for instance. The difference to the case of bent functions is that there are elements $1\pm I$ of absolute value $\sqrt{2}$ in $\mathbb{Z}[I]$, which is impossible in $\mathbb{Z}$.

The set of values $\mathcal{H}_m(F)(\mathbf{u})$ (resp. $\mathcal{N}_m(F)(\mathbf{u})$) is called the *spectrum* of F with respect to $\mathcal{H}_m$ (resp. $\mathcal{N}_m$).

Example 2. The function $f(\mathbf{x})=x_1x_2+x_2x_3+x_3x_4$ is bent and negabent, see Theorem 4.

Like $\mathcal{H}$, the nega-Hadamard transform is unitary: Since the polynomials $\xi^{\mathbf{x}}$, $\mathbf{x}\in V_m$, form an orthonormal basis of $\mathcal{L}$, it is sufficient to show that the polynomials $\mathcal{N}_m(\xi^{\mathbf{x}})$ are orthonormal in $\mathcal{L}$:

$$\begin{aligned}|(\mathcal{N}_m(\xi^{\mathbf{x}}),\mathcal{N}_m(\xi^{\mathbf{y}}))| &= \frac{1}{2^m}\left|\sum_{\mathbf{u}\in V_m}(-1)^{(\mathbf{u},\mathbf{x})}I^{\mathrm{weight}(\mathbf{x})}\cdot(-1)^{(\mathbf{u},\mathbf{y})}(-I)^{\mathrm{weight}(\mathbf{y})}\right|\\ &= \left|\frac{1}{2^m}\sum_{\mathbf{u}\in V_m}(-1)^{(\mathbf{u},\mathbf{x}+\mathbf{y})}I^{\mathrm{weight}(\mathbf{x})-\mathrm{weight}(\mathbf{y})}\right|\\ &= \begin{cases}1 \text{ if } \mathbf{x}=\mathbf{y}\\ 0 \text{ otherwise.}\end{cases}\end{aligned}$$

Surprisingly, affine functions are negabent:

Proposition 1. *All affine functions $f: V_m\to\mathbb{F}_2$ are negabent.*

Proof. If $f(\mathbf{x})=(\mathbf{a},\mathbf{x})$ is linear, then the nega-Hadamard transform of the indicator of $(-1)^f$ is

$$\mathcal{N}_m((-1)^f)(\mathbf{u})=\frac{1}{\sqrt{2^m}}\sum_{\mathbf{x}\in V_m}(-1)^{(\mathbf{u}+\mathbf{a},\mathbf{x})}\cdot I^{\mathrm{weight}(\mathbf{x})}.$$

We define

$$\alpha:=\frac{1}{\sqrt{2^{m-1}}}\sum_{\mathbf{x}\in V_m:x_1=0}(-1)^{(\mathbf{u}+\mathbf{a},\mathbf{x})}\cdot I^{\mathrm{weight}(\mathbf{x})}.$$

This is $\mathcal{N}_{m-1}((-1)^g)(\mathbf{u}')$, $\mathbf{u}' = (u_2, \ldots, u_m)$, for the linear function g on V_{m-1} which is the restriction of f to $\{\mathbf{x} \in V_m : x_1 = 0\}$. By induction, we may assume $|\alpha| = 1$. Depending on $u_1 + a_1$, we get

$$\mathcal{N}_m((-1)^f)(\mathbf{u}) = \frac{1}{\sqrt{2}}(\alpha + \alpha \cdot I) \qquad \text{or} \qquad \frac{1}{\sqrt{2}}(\alpha - \alpha \cdot I).$$

Both numbers have absolute value 1. Since the function $f(\mathbf{x}) = 1$ is also negabent, affine linear functions are negabent, too. □

The next proposition will also be of interest:

Proposition 2. $\mathbf{N}_m \mathbf{H}_m \mathbf{N}_m^{-1} = \mathbf{B}_m$, *where*

$$\mathbf{B}_m = \begin{pmatrix} 0 & \omega \\ \overline{\omega} & 0 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 0 & \omega \\ \overline{\omega} & 0 \end{pmatrix},$$

and $\omega = \frac{1}{\sqrt{2}}(1 + I)$ *is a primitive* 8*-th root of unity.*

Proof. Note

$$\begin{pmatrix} 1 & I \\ 1 & -I \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -I & I \end{pmatrix} = \begin{pmatrix} 0 & 2(1+I) \\ 2(1-I) & 0 \end{pmatrix} = 2\sqrt{2} \cdot \begin{pmatrix} 0 & \omega \\ \overline{\omega} & 0 \end{pmatrix}$$

and "tensoring". □

In this paper, we address the following problem:

Problem 1. Find Boolean functions f that are both bent and negabent.

The main results about these objects are the following:

- For all even m, there are examples of quadratic bent-negabent functions.
- Adding a certain polynomial, c, to a bent function gives a negabent function. Adding the same polynomial, c, to a negabent function if m is even gives a bent function.
- The dual of a bent-negabent function is again bent-negabent.
- We can characterize all Maiorana-McFarland bent functions which are bent-negabent.
- We give examples of bent-negabent functions which are not quadratic.

At the end of this section, we would like to explain the connection between the transforms $\mathcal{N}_m$ and $\mathcal{H}_m$ of F and correlation properties of f, where F is the indicator polynomial of $f : V_m \to \mathbb{F}_2$ in $\mathbb{C}[\xi_1, \ldots, \xi_m]$. Note that the polynomial ring $\mathbb{C}[\xi_1, \ldots, \xi_m]$ is an algebra by the usual multiplication $*$ of polynomials.

If $\mathbf{x} \in \mathbb{C}^m$, then obviously $F(\mathbf{x}) \cdot G(\mathbf{x}) = (F * G)(\mathbf{x})$. Note that both the Hadamard transform and the nega-Hadamard transform are nothing else than "evaluating F at certain vectors". Therefore, knowing the (nega-)Hadamard transform of F should give some information about $F*G$. We do not get full information about $F*G$, but only modulo some ideals, as we will explain now: Let I_- be the ideal in $\mathbb{C}[\xi_1, \ldots, \xi_n]$ generated by $\xi_1^2 - 1, \ldots, \xi_m^2 - 1$, and I_+ be the ideal generated by $\xi_1^2 + 1, \ldots, \xi_m^2 + 1$. Let H (resp. N) be the unique polynomial in $\mathcal{L}$ with $H \equiv (F * F) \bmod I_-$ (resp. $N \equiv (F * F') \bmod I_+$, where F' is the polynomial in $\mathcal{L}$ whose nega-Hadamard transform is the complex-conjugate of the nega-Hadamard transform of F).

Let $\mathbf{y} \in V_m$. The coefficient $c_{\mathbf{y}}$ of $\xi^{\mathbf{y}}$ in H is the *periodic autocorrelation coefficient*

$$c_{\mathbf{y}} = \sum_{\mathbf{x} \in V_m} (-1)^{f(\mathbf{x}) + f(\mathbf{x}+\mathbf{y})}.$$

If f is bent, then $H(\mathbf{x}) = (F * F)(\mathbf{x}) = F(\mathbf{x}) \cdot F(\mathbf{x}) = 2^m$ for all $\mathbf{x} \in V_m$. Therefore, H is a polynomial such that all values in its spectrum are $\sqrt{2^m}$ (note the normalization factor $\frac{1}{\sqrt{2^m}}$). The only such polynomial is $2^m \xi^{\mathbf{0}}$, hence $c_{\mathbf{y}} = 0$ if $\mathbf{y} \neq \mathbf{0}$, and $c_{\mathbf{0}} = 2^m$, where $\mathbf{0} = (0, 0, \ldots, 0)$.

Similarly, the coefficients $n_{\mathbf{y}}$ of $F * F'$ are all 0 (if $\mathbf{y} \neq \mathbf{0}$) provided f is negabent. They are called the *negaperiodic autocorrelation coefficients* of f. Note that $F' = \sum_{\mathbf{x} \in V_m} a_{\mathbf{x}} (-1)^{\mathrm{weight}(\mathbf{x})} \xi^{\mathbf{x}}$ if $F = \sum_{\mathbf{x} \in V_m} a_{\mathbf{x}} \xi^{\mathbf{x}}$. Therefore, one may compute these negaperiodic autocorrelation coefficients as follows:

$$n_{\mathbf{y}} = \sum_{\mathbf{x} \in V_m} (-1)^{f(\mathbf{x}) + f(\mathbf{x}+\mathbf{y})} \cdot (-1)^{\mathrm{weight}(\mathbf{x}+\mathbf{y})} \cdot (-1)^{(\mathbf{x},\mathbf{y})}.$$

We need the term $(-1)^{(\mathbf{x},\mathbf{y})}$ since our computations are modulo I_+: The inner product $(\mathbf{x}, \mathbf{y})$ counts the number of $i \in \{1, \ldots, m\}$ with $x_i = y_i = 1$, which is the number of "reductions" modulo $\xi_i^2 + 1$. Every such reduction yields a "-1" since $\xi_i^2 = -1$.

The coefficient of $\mathbf{0}$ in $F * F'$ (resp. $F * F$) is called the *trivial autocorrelation coefficient.*

The following Theorem summarizes this discussion:

Theorem 2. *A Boolean function is negabent if and only if all its nontrivial negaperiodic autocorrelation coefficients are* 0. *It is bent, if and only if all the nontrivial periodic autocorrelation coefficients are* 0.

3 Quadratic bent-negabent functions

We begin our investigation with the determination of quadratic bent-negabent functions. Let $\mathbf{M} = (a_{i,j})_{i,j=1,\ldots,m}$ be a symmetric matrix in $\mathbb{F}_2^{(m,m)}$ with zero diagonal. Then $\mathbf{M}$ defines a quadratic function

$$p(x_1, \ldots, x_n) = \sum_{i<j} a_{i,j} x_i x_j. \tag{5}$$

Conversely, any quadratic function (5) defines a symmetric matrix $\mathbf{M}$. Note that $\mathbf{M}$ may be viewed as the adjacency matrix of a graph with m vertices. If this graph is a path graph or complete (clique) graph, then we also call the corresponding quadratic function p a "path" or a "clique" function.

The following result is well known:

Theorem 3. *A quadratic function p is bent if and only if the corresponding matrix* $\mathbf{M}$ *has full rank.*

Similarly, one can characterize quadratic negabent functions. Actually, [2] contains a much more general result.

Theorem 4 ([2]). *A quadratic function p is negabent if and only if the matrix* $\mathbf{M} + \mathbf{I}$ *has full rank, where* $\mathbf{I}$ *is the identity matrix and* $\mathbf{M}$ *is the matrix corresponding to p.*

This theorem is the main ingredient to construct quadratic bent-negabent functions. Using a recursive formula for the determinants of matrices of the type

$$\mathbf{L}(v_1, \ldots, v_m) := \begin{pmatrix} v_1 & 1 & & & & \\ 1 & v_2 & 1 & & & \\ & 1 & v_3 & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & v_{m-1} & 1 \\ & & & & 1 & v_m \end{pmatrix} \in \mathbb{F}_2^{(m,m)} \tag{6}$$

(“empty” entries are 0) contained in [2], it can be shown that

$$\det(\mathbf{L}(1,\ldots,1)) = 1$$

if and only if $m \not\equiv 2 \bmod 3$, and

$$\det(\mathbf{L}(0,\ldots,0)) = 1$$

if and only if m is even. Hence the quadratic function

$$p(x_1,\ldots,x_m) = x_1x_2 + x_2x_3 + \ldots x_{m-1}x_m \tag{7}$$

is a bent-negabent pair if $m \not\equiv 2 \bmod 6$.

Theorem 5 shows that the case $m \not\equiv 2 \bmod 6$ is not really exceptional. For proof, we need the following recursive construction:

Lemma 1. *Let* $\mathbf{A}$ *be a symmetric matrix in* $\mathbb{F}_2^{(m,m)}$ *such that* $\mathbf{A}$ *and* $\mathbf{A}+\mathbf{I}$ *have rank* m*. Then the matrix*

$$\mathbf{A}' = \left(\begin{array}{c|c} \mathbf{A} & \\ & 1 \\ \hline 1 & \\ & \mathbf{B} \end{array}\right) \in \mathbb{F}_2^{(m+6,m+6)}$$

with

$$\mathbf{B} = \mathbf{L}(0,0,0,0,0,0) \in \mathbb{F}_2^{(6,6)}$$

(the matrix of the path graph, see (6)) has rank $m+6$*, and* $\mathbf{A}'+\mathbf{I}$ *has also rank* $m+6$*.*

Proof. Just do Gaussian elimination. $\square$

Theorem 5. *For all even* $m \geq 2$*, there exists a quadratic bent-negabent function* $f : V_m \to \mathbb{F}_2$*.*

Proof. For $m = 4, 6$ and 8, we take the quadratic functions corresponding to the matrices

$$\begin{pmatrix} 0&1&0&0\\ 1&0&1&0\\ 0&1&0&1\\ 0&0&1&0 \end{pmatrix}, \quad \begin{pmatrix} 0&1&0&0&0&0\\ 1&0&1&0&0&0\\ 0&1&0&1&0&0\\ 0&0&1&0&1&0\\ 0&0&0&1&0&1\\ 0&0&0&0&1&0 \end{pmatrix}$$

and

$$\begin{pmatrix} 0&1&0&1&0&0&0&1\\ 1&0&1&0&0&0&0&0\\ 0&1&0&1&0&0&0&0\\ 1&0&1&0&1&0&0&0\\ 0&0&0&1&0&1&0&0\\ 0&0&0&0&1&0&1&0\\ 0&0&0&0&0&1&0&1\\ 1&0&0&0&0&0&1&0 \end{pmatrix}$$

It is easy to check that these three quadratic forms are bent-negabent since the matrices as well as the matrices plus $\mathbf{I}$ have full rank, see Theorems 3 and 4. Lemma 1 finishes the proof. $\square$

The following Theorem may also serve as a basic ingredient to construct many bent-negabent functions. Here $\mathbf{J}$ denotes the matrix all of whose entries are 1, and $\mathbf{0}$ denotes the 0-matrix.

Theorem 6. *Let* $\mathbf{M} \in \mathbb{F}_2^{(n,n)}$ *be a symmetric matrix such that rank*$(\mathbf{M}) =$ *rank*$(\mathbf{M}+\mathbf{J}) = n$. *Then both*

$$\mathbf{M}' = \left(\begin{array}{c|c} \mathbf{0} & \mathbf{M} \\ \hline \mathbf{M} & \mathbf{J}+\mathbf{I} \end{array}\right)$$

and $\mathbf{M}' + \mathbf{I}$ *have rank* $2n$. *Therefore, the quadratic function* f *corresponding to* $\mathbf{M}'$ *is bent-negabent.*

Proof. The matrix $\mathbf{M}'$ has maximum rank since $\mathbf{M}$ has maximum rank. Therefore, f is bent, see Theorem 3. If we add the $(2n \times 2n)$ identity matrix to it, we obtain

$$\left(\begin{array}{c|c} \mathbf{I} & \mathbf{M} \\ \hline (\mathbf{M}+\mathbf{J}) & \mathbf{J} \end{array}\right).$$

This matrix has the same rank as

$$\mathbf{M}'' = \left(\begin{array}{c|c} \mathbf{J}+\mathbf{I} & \mathbf{M}+\mathbf{J} \\ \hline (\mathbf{M}+\mathbf{J}) & \mathbf{0} \end{array}\right).$$

But since we assume $\text{rank}(\mathbf{M}) = \text{rank}(\mathbf{M}+\mathbf{J}) = n$, the rank of $\mathbf{M}''$ is $2n$, which shows that f is also negabent (see Theorem 4). □

The following Theorem gives a huge family of matrices $\mathbf{M}$ of rank n such that $\mathbf{M}+\mathbf{I}$ has rank n, too. Unfortunately, n is even in this Theorem, hence we can only construct bent-negabent functions in V_m with $m \equiv 0 \bmod 4$:

Theorem 7. *Let* n *be even, and let* $\mathbf{M} \in \mathbb{F}_2^{(n,n)}$ *be a matrix where all rows and columns have odd weight (in other words,* $\mathbf{MJ} = \mathbf{JM} = \mathbf{J}$*). If* $\mathbf{M}$ *has maximum rank, then* $\mathbf{M}+\mathbf{J}$ *also has maximum rank.*

Proof. Observe that $(\mathbf{M}+\mathbf{J})^2 = \mathbf{M}^2$ and, more generally, $(\mathbf{M}+\mathbf{J})^{2s} = \mathbf{M}^{2s}$, $(\mathbf{M}+\mathbf{J})^{2s+1} = \mathbf{M}^{2s+1}+\mathbf{J}$. If $\mathbf{M}$ has even multiplicative order, then there exists s such that $\mathbf{M}^{2s} = (\mathbf{M}+\mathbf{J})^{2s} = \mathbf{I}$. Therefore, in this case $\mathbf{M}+\mathbf{J}$ has maximum rank. If $\mathbf{M}$ has odd multiplicative order, then there exists s such that $\mathbf{M}^{2s+1} = \mathbf{I}$, therefore $(\mathbf{M}+\mathbf{J})^{2s+1} = \mathbf{I}+\mathbf{J}$. But $(\mathbf{I}+\mathbf{J})^2 = \mathbf{I}$, since n is even. So, in this case, $\mathbf{M}+\mathbf{J}$ has maximum rank, too. □

We will show that "adding a clique" $c(\mathbf{x}) = \sum_{i<j} x_i x_j$ (see Theorem 12) turns a bent function into a negabent function and vice versa. For quadratic functions, this has the following interpretation:

Theorem 8. *Let* $\mathbf{M}$ *be a symmetric matrix in* $\mathbb{F}_2^{(m,m)}$*, where the diagonal of* $\mathbf{M}$ *is zero. Then the corresponding quadratic function is bent-negabent if and only if* $\mathbf{M}$ *and* $\mathbf{M}+\mathbf{I}+\mathbf{J}$ *have full rank.*

Proof If f is bent, then $\text{rank}(\mathbf{M}) = m$. If f is negabent, then $f+c$ is bent. The symmetric matrix that describes $f+c$ is $\mathbf{M}+\mathbf{I}+\mathbf{J}$, which must have full rank. □

This shows that the classification of all quadratic bent-negabent functions is equivalent to the determination of all simple graphs on m vertices such that the adjacency matrix of the graph and its complement both have $\mathbb{F}_2$-rank m.

Problem 2. Determine the number of quadratic bent-negabent functions with m variables.

4 Maiorana-McFarland bent-negabent functions

In this section, we briefly recall the Maiorana-McFarland construction of bent functions, and we characterize those functions which are both bent and negabent.

Let $\pi : V_n \to V_n$ be a permutation, and let $g : V_n \to \mathbb{F}_2$ be an arbitrary Boolean function. Then the function

$$\begin{aligned} f_{\pi,g} :\ & V_m \to \mathbb{F}_2 \\ & [\mathbf{x}, \mathbf{y}] \mapsto (\mathbf{x}, \pi(\mathbf{y})) + g(\mathbf{y}) \end{aligned},$$

where $m = 2n$, is bent. Here $[\cdot,\cdot]$ denotes the concatenation of vectors, and $(\cdot,\cdot)$ is the standard inner product.

Note that we are free to choose g. If we take $g(\mathbf{y}) = y_1 \cdots y_n$, bent functions of degree $m/2$ (if they are written as a multivariate polynomial) do exist. It is well known that this is the maximum degree. There exist bent-negabent functions of degree $m/2$ when $m = 6$ (for instance, $f(\mathbf{x}, \mathbf{y}) = x_1y_1y_2 + x_1y_2y_3 + x_2y_1y_2 + x_2y_2y_3 + x_1y_1 + x_1y_2 + x_2y_3 + x_3y_1 + x_3y_3$ is bent-negabent), but we do not know whether bent-negabent functions of degree $m/2$ exist for all even m.

Problem 3. Find the maximum degree of bent-negabent functions.

Note that all quadratic bent functions can be transformed by linear transformations to Maiorana-McFarland bent functions. This is a simple consequence of the fact that any quadratic function on V_m, $m = 2n$, of full rank can be transformed into $x'_1x'_{n+1} + x'_2x'_{n+2} + \ldots + x'_nx'_{2n}$ by a linear transformation

$$(x_1, \ldots, x_{2n}) \to \mathcal{L}(x_1, \ldots, x_{2n}) = (x'_1, \ldots, x'_{2n}).$$

However, such linear transformations do not preserve the bent-negabent property. For instance, $x_1x_2 + x_3x_4$ is bent, but not negabent, however $x_1x_2 + x_2x_3 + x_3x_4$ is bent-negabent, see Theorem 7. These two quadratic functions are equivalent via a linear coordinate transformation.

Therefore, we cannot say that all bent-negabent quadratic functions are "equivalent" to Maiorana-McFarland bent functions.

The next theorem gives a characterization of Maiorana-McFarland bent-negabent functions $f_{\pi,g}$ in terms of the permutation π and the function g:

Theorem 9. *Let $\{\mathbf{y}_1, \ldots, \mathbf{y}_{2^n}\} = V_n$, where the vectors are numbered such that*

$$\mathbf{H}_n = ((-1)^{(\mathbf{y}_i,\mathbf{y}_j)})_{i,j=1,\ldots,n}$$

is the matrix corresponding to the n-dimensional Hadamard-Walsh transform. Then $f_{\pi,g}$ is bent-negabent on V_m with $m = 2n$, if and only if all the entries in the matrix

$$\mathbf{N}_n\mathbf{P}\mathbf{D}\mathbf{N}_n^t$$

have absolute value 1, where $\mathbf{D}$ and $\mathbf{P}$ are defined as follows:

- $\mathbf{D}$ *is a diagonal matrix whose (i,i)-entry is $(-1)^{g(\mathbf{y}_i)}$.*
- $\mathbf{P}$ *is a permutation matrix such that the 1-entry in row i occurs in column j where $\pi(\mathbf{y}_i) = \mathbf{y}_j$.*

Proof. We have

$$\mathcal{N}_m((-1)^f)[\mathbf{u},\mathbf{v}] = \sum_{[\mathbf{x},\mathbf{y}]\in V_{2n}} (-1)^{(\mathbf{x},\pi(\mathbf{y}))+g(\mathbf{y})}(-1)^{([\mathbf{u},\mathbf{v}],[\mathbf{x},\mathbf{y}])} I^{\mathrm{weight}([\mathbf{x},\mathbf{y}])}$$
$$= \sum_{\mathbf{y}\in V_n} I^{\mathrm{weight}(\mathbf{y})}(-1)^{g(\mathbf{y})}(-1)^{(\mathbf{v},\mathbf{y})}\left(\sum_{\mathbf{x}\in V_n}(-1)^{(\mathbf{u},\mathbf{x})}(-1)^{(\mathbf{x},\pi(\mathbf{y}))}I^{\mathrm{weight}(\mathbf{x})}\right).$$

This is an entry of $\mathbf{N}_n\mathbf{H}_n\mathbf{PDN}_n^t$. We have $\mathbf{N}_n\mathbf{H}_n = \mathbf{B}_n\mathbf{N}_n$, where $\mathbf{B}_n$ is a diagonal matrix with all diagonal entries of absolute value 1 (see 2)), the matrix $\mathbf{N}_n\mathbf{H}_n\mathbf{PDN}_n^t$ has all entries of absolute value 1 iff $\mathbf{N}_n\mathbf{PDN}_n^t$ has this property.

□

It seems difficult to apply this Theorem in order to construct Maiorana-McFarland bent-negabent functions.

We say that a quadratic function p is Maiorana-McFarland if we can split the coordinates into two sets $x_1,\ldots,x_{m/2}$ and $x_{1+m/2},\ldots,x_m$, say, such that no term x_ix_j with $i\le m/2$ and $j>m/2$ is contained in p. The following construction shows that quadratic bent-negabent functions of Maiorana-McFarland type do exist:

Theorem 10. *Let $m=4n$, and let $\mathbf{P}$ and $\mathbf{Q}$ be permutation matrices of size n. Then the matrix*

$$\mathbf{M} = \left(\begin{array}{cc|cc} \mathbf{0} & \mathbf{0} & \mathbf{P} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{Q} & \mathbf{I} \\ \hline \mathbf{P}^t & \mathbf{Q}^t & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{0} \end{array}\right)$$

describes a quadratic function p of Maiorana-McFarland type which is bent and negabent.

Proof. Gaussian elimination both on $\mathbf{M}$ and $\mathbf{M}+\mathbf{I}$. □

Let $p(x_1,\ldots,x_{4n})$ be the quadratic function in Theorem 10. Numerical experiments indicate that we may always add a Boolean function $g(x_{2n+1},\ldots,x_{3n})$ to p to obtain another bent-negabent pair. More generally still, experiments indicate that $p(x_1,\ldots,x_{4n}) = (\mathbf{y},\phi(\mathbf{z})) + (\theta(\mathbf{z}),\mathbf{u}) + (\mathbf{u},\mathbf{v}) + g(\mathbf{z})$, where $\mathbf{y}=(x_1,\ldots,x_n)$, $\mathbf{z}=(x_{n+1},\ldots,x_{2n})$, $\mathbf{u}=(x_{2n+1},\ldots,x_{3n})$, $\mathbf{v}=(x_{3n+1},\ldots,x_{4n})$, and where $\phi,\theta: V_n\to V_n$ are both permutations, will always give examples of bent-negabent pairs on m variables from degree 2 up to degree $m/4$.

5 Transformations which preserve bent-negabentness

Theorem 11. *If f is a bent-negabent function, then its dual is again bent-negabent.*

Proof. This is an immediate consequence of Proposition 2. □

Ther are a few more transformations which produce new bent-negabent functions from a given bent-negabent function.

Lemma 2. *Let $f: V_m\to\mathbb{F}_2$ be a bent-negabent function. Then*

1. *The Boolean function $f'(\mathbf{x}) = f(\mathbf{x}) + (\sum_{i=1}^m a_ix_i) + b$, where $(a_1,\ldots,a_m)\in V_m$, $b\in\mathbb{F}_2$, is bent-negabent.*
2. *The Boolean function $f'(\mathbf{x}) = f(x_1+h_1, x_2+h_2,\ldots,x_m+h_m)$ is bent-negabent.*
3. *If π denotes a permutation on the set of indices $\{1,\ldots,m\}$, then $f(x_{\pi(1)},\ldots,x_{\pi(m)})$ is bent-negabent.*

Proof. We just look at (1). This is well known and also easy to see for bent functions f. The same reasoning shows that negabentness is preserved: Let $l(\mathbf{x}) = \sum_{i=1}^m a_i x_i + b$, and let $\mathbf{a} = (a_1, \ldots, a_m)$. Then

$$\mathcal{N}_m(f')(\mathbf{u}) = \sum_{\mathbf{x}\in V_m} (-1)^{f(\mathbf{x})+(\mathbf{a},\mathbf{x})+b} I^{\text{weight}(\mathbf{x})}(-1)^{(\mathbf{u},\mathbf{x})} = (-1)^b \mathcal{N}_m((-1)^f)(\mathbf{u}+\mathbf{a}).$$

□

The following construction is more interesting. It is implicitly contained in Theorem 4.6 of [3].

Theorem 12. *Let $f : V_m \to \mathbb{F}_2$ be a bent function. Then $f+c$ is negabent, where $c(x_1, \ldots, x_n) = \sum_{i<j} x_i x_j$. Conversely, if m is even and f is negabent, then $f + c$ is bent.*

Proof. Let $f : V_m \to \mathbb{F}_2$ be a bent function. Then

$$\begin{aligned}\mathcal{N}_m(f+c)(\mathbf{u}) &= \sum_{\mathbf{x}\in V_m} (-1)^{f(\mathbf{x})+\sum_{i<j} x_i x_j}(-1)^{(\mathbf{u},\mathbf{x})} I^{\text{weight}(\mathbf{x})} \\ &= \sum_{\mathbf{x}\in V_m} (-1)^{f(\mathbf{x})}(-1)^{(\mathbf{u},\mathbf{x})} I^{2c(\mathbf{x})+\text{weight}(\mathbf{x})},\end{aligned}$$

where we compute the exponents on the right-hand side modulo 4. We note

$$\sum_i x_i + 2\sum_{i<j} x_i x_j = (\sum_i x_i)^2 \quad \text{in integers } \mathbb{Z}$$

where $\sum x_i = \text{weight}(\mathbf{x})$. Moreover,

$$(\sum_i x_i)^2 \equiv \begin{cases} 0 \bmod 4 & \text{if weight}(\mathbf{x}) \text{ is even} \\ 1 \bmod 4 & \text{if weight}(\mathbf{x}) \text{ is odd.}\end{cases}$$

Let E_m denote the set of vectors of even weight, and let O_m be the set of vectors of odd weight. We define

$$\begin{aligned} x_e &= \sum_{\mathbf{x}\in E_m} (-1)^{f(\mathbf{x})}(-1)^{(\mathbf{u},\mathbf{x})} \\ x_o &= \sum_{\mathbf{x}\in O_m} (-1)^{f(\mathbf{x})}(-1)^{(\mathbf{u},\mathbf{x})}.\end{aligned}$$

Note that both these numbers are integers. We write $\mathcal{N}_m(f+c)(\mathbf{u})$ as follows:

$$\mathcal{N}_m(f+c)(\mathbf{u}) = x_e + I x_o$$

Now we use that f is bent, therefore

$$1 = |\mathcal{H}_m(f)(\mathbf{u})| = |x_e + x_o|$$

and

$$1 = |\mathcal{H}_m(f)(\mathbf{u}+\mathbf{j})| = |x_e - x_o|,$$

where $\mathbf{j} = (1, \ldots, 1)$ is the all-one-vector. This is only possible if $x_e = 0$ and $|x_o| = 1$, or vice versa. Therefore, $|\mathcal{N}_m(f+c)(\mathbf{u})| = 1$.

Now let us assume that a function g is negabent. We put $f = g + c$, hence, by assumption,

$$|\mathcal{N}_m(f+c)(\mathbf{u})| = 1 = x_e^2 + x_o^2.$$

Moreover, $x_e = n_e/\sqrt{2^m}$, and $x_o = n_o/\sqrt{2^m}$ for some integers n_e and n_o. Therefore, $n_e^2 + n_o^2 = 2^m$. If m is even, one easily shows that this is possible only if one of the two integers n_e, n_o is $\pm 2^{m/2}$, and the other is 0. Therefore, $|\mathcal{H}_m(f)(\mathbf{u})| = 1$, i.e. $f = g + c$ is bent.

□

Corollary 1. *If f is a bent-negabent function, then $f + c$ is also bent-negabent.*

Remark 1. Assume that g is negabent, and m is odd. Then the proof above shows that the Hadamard-Walsh coefficients of $g + c$ are in $\{0, \pm 2^{(m+1)/2}\}$, since in this case the possible solutions of $n_e^2 + n_o^2 = 2^m$ are $n_e, n_o = \pm 2^{(m-1)/2}$. Therefore, it is possible that $n_e^2 + n_o^2 = 0$.

6 Orbits of bent-negabent functions

One can view the operations that preserve the bent-negabent property, as discussed in the previous section, as generators of a group, where the action of any member of the group preserves the bent-negabent property. The two particularly interesting symmetry operations, described in Theorem 11 and Corollary 1, are involutary and, in combination with the symmetry operations of Lemma 2, generate a group of symmetries, $\mathcal{G}$, whose application on a single bent-negabent function generates an orbit of bent-negabent functions. We also consider the more trivial group, $\mathcal{E}$, generated just by the symmetries of Lemma 2. In table 1 we enumerate the number of orbits generated by the action of $\mathcal{E}$ and by $\mathcal{G}$ on the (homogeneous) quadratic Boolean functions for small numbers of variables. Note that, for quadratics, symmetry 2 of Lemma 2 is contained in symmetry 1 and does not contribute new functions to the orbit.

Table 1. Enumeration of bent-negabent quadratic coset leaders over n variables with respect to the bent-negabent symmetry groups, $\mathcal{E}$ and $\mathcal{G}$

n	number of orbits generated by $\mathcal{E}$	number of orbits generated by $\mathcal{G}$
2	0	0
4	1	1
6	10	2
8	1272	161
10	1727780	144861

In a future paper we shall investigate and characterise these orbits in more detail.

References

1. Parker, M.G.: The constabent properties of Golay-Davis-Jedwab sequences. IEEE Int. Symp. Inform. Theory, Sorrento, (2000) 302
2. Riera, C., Parker, M.G.: Generalized bent criteria for boolean functions (I). IEEE **52** (2006) 4142–4159
3. Schmidt, K.U.: Quaternary constant-amplitude codes for multicode cdma, submitted to IEEE Transactions on Information Theory, (2006)
4. Carlet, C.: Boolean functions for cryptography and error correcting codes. In Crama, Y., Hammer, P., eds.: Boolean Methods and Models. Cambridge University Press (to appear)
5. Assmus, Jr., E.F., Key, J.D.: Designs and their codes. Cambridge University Press, Cambridge (1992)
6. Golomb, S.W., Gong, G.: Signal design for good correlation. Cambridge University Press, Cambridge (2005)