# A New Class of Bent–Negabent Boolean Functions

Sugata Gangopadhyay and Ankita Chaturvedi

Department of Mathematics, Indian Institute of Technology Roorkee
Roorkee 247667 INDIA,
{gsugata, ankitac17}@gmail.com

**Abstract.** In this paper we develop a technique of constructing bent–negabent Boolean functions by using complete mapping polynomials. Using this technique we demonstrate that for each $\ell \geq 2$ there exits bent–negabent functions on $n = 12\ell$ variables with algebraic degree $\frac{n}{4} + 1 = 3\ell + 1$. It is also demonstrated that there exist bent–negabent functions on 8 variables with algebraic degrees 2, 3 and 4.

**Keywords:** Boolean functions, nega–Hadamard transforms, bent and negabent functions.

## 1 Introduction

Let $\mathbb{F}_2$ be the prime field of characteristic 2 and let $\mathbb{F}_2^n$ is the $n$-dimensional vector space over $\mathbb{F}_2$. A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called a Boolean function on $n$ variables. The reader is referred to Section 1.1 for all the basic notations and definitions related to Boolean functions.

Walsh, Hadamard, or Walsh–Hadamard transform has been exploited extensively for analyzing Boolean functions used in coding theory and cryptology [6]. For even $n$, the functions which attain the largest distance from the set of affine functions, that is the functions which have the largest nonlinearity are called bent functions. From the perspective of coding theory these functions attain the covering radius of the first order Reed–Muller code. A Boolean function on even number of variables is bent if and only if the magnitude of all the values in its Walsh–Hadamard spectrum are same, that is to say that a Boolean function is bent if and only if its Walsh–Hadamard spectrum is flat. Walsh–Hadamard transform is an example of a unitary transformation on the space of Boolean functions. Riera and Parker [18] considered some generalized bent criteria for Boolean functions by analyzing Boolean functions which have flat spectrum with respect of one or more transforms chosen from a set of unitatry transforms. The transforms chosen by Riera and Parker [18] are $n$-fold tensor product of the identity mapping $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the Walsh–Hadamard transformation and the nega–Hadamard transformation. Riera and Parker [18] mention that the choice of these transforms is motivated by a choice of local unitary transforms

that play an important role in the structural analysis of pure $n$-qubit stabilizer quantum states. A Boolean functions whose nega–Hadamard spectrum is flat is said to be a negabent function. The research initiated in [18] leads to a natural question of constructing Boolean function which are both bent and negabent. These functions are referred to as bent–negabent functions. This motivated several works in the area of Boolean functions [15, 23, 24] in the last few years. In Theorem 10 [23] it is proved that if $f$ is a Maiorana–McFarland type bent function on $n$ variables ($n$ even) which is also negabent then the algebraic degree of $f$ is atmost $n/2-1$. In Example 6 [23] a technique to construct bent–negabent functions on $4n$ variables of algebraic degree ranging from 2 to $n$ is described. Another technique to construct bent–negabent functions on $4n$ variables of algebraic degree ranging from 2 to $n-1$ is described in Theorem 7 [24]. Thus, although it is known that there may exist bent–negabent functions on $n$ variables ($n$ even) of algebraic degree up to $n/2-1$ there is no general construction of bent–negabent functions of algebraic degree greater that $\frac{n}{4}$, for all $n \equiv 0 \mod 4$. In this paper we describe a technique of constructing bent–negabent functions by using complete mapping polynomials of finite fields which are a special class of permutation polynomials [11, 14]. First we demonstrate the connection between existence of complete mapping polynomial over a finite field and the existence of a class of bent–negabent functions. Then we demonstrate that for each $\ell \geq 2$ there exit bent–negabent functions on $n = 12\ell$ variables with algebraic degree $\frac{n}{4}+1 = 3\ell+1$.

### 1.1 Definitions and Notations

The set of all Boolean functions on $n$ variables is denoted by $\mathcal{B}_n$. Any element $\mathbf{x} \in \mathbb{F}_2^n$ can be written as an $n$-tuple $(x_1, \ldots, x_n)$, where $x_i \in \mathbb{F}_2$ for all $i = 1, \ldots, n$. The set of integers, real numbers and complex numbers are denoted by $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ respectively. The addition over $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ is denoted by '+'. The addition over $\mathbb{F}_2^n$ for all $n \geq 1$, is denoted by $\oplus$. If $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ are two elements of $\mathbb{F}_2^n$, we define the scalar (or inner) product, respectively, the intersection by

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n, \mathbf{x} * \mathbf{y} = (x_1y_1, x_2y_2, \ldots, x_ny_n).$$

The cardinality of the set $S$ is denoted by $|S|$. If $z = a + b\imath \in \mathbb{C}$, then $|z| = \sqrt{a^2+b^2}$ denotes the absolute value of $z$, and $\overline{z} = a - b\imath$ denotes the complex conjugate of $z$, where $\imath^2 = -1$, and $a, b \in \mathbb{R}$. Any $f \in \mathcal{B}_n$ can be expressed in *algebraic normal form* (ANF) as

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{\mathbf{a}=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_{\mathbf{a}} \left( \prod_{i=1}^{n} x_i^{a_i} \right), \ \mu_{\mathbf{a}} \in \mathbb{F}_2.$$

The (*Hamming*) *weight* of $\mathbf{x} \in \mathbb{F}_2^n$ is $wt(\mathbf{x}) := \sum_{i=1}^{n} x_i$. The algebraic degree of $f$, $\deg(f) := \max_{\mathbf{a}\in\mathbb{F}_2^n}\{wt(\mathbf{a}) : \mu_{\mathbf{a}} \neq 0\}$. Boolean functions having algebraic

degree at most 1 are said to be *affine functions*. For any two functions $f, g \in \mathcal{B}_n$, we define the (*Hamming*) *distance* $d(f,g) = |\{\mathbf{x} : f(\mathbf{x}) \neq g(\mathbf{x}), \mathbf{x} \in \mathbb{F}_{2^n}\}|$.

The *Walsh–Hadamard transform* of $f \in \mathcal{B}_n$ at any point $\mathbf{u} \in \mathbb{F}_2^n$ is defined by

$$\mathcal{H}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}}.$$

The multiset $[\mathcal{H}_f(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_2^n]$ is said to be the Walsh–Hadamard spectrum of the function $f$. A function $f \in \mathcal{B}_n$ is a *bent function* if $|\mathcal{H}_f(\mathbf{u})| = 1$ for all $\lambda \in \mathbb{F}_2^n$. Bent functions (defined by Rothaus [19] more than thirty years ago) hold an interest among researchers in this area since they have maximum Hamming distance from the set of all affine Boolean functions. Several classes of bent functions were constructed by Rothaus [19], Dillon [8], Dobbertin [9], and later by Carlet [2].

The sum $\mathcal{C}_{f,g}(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x} \oplus \mathbf{z})}$ is the *crosscorrelation* of $f$ and $g$ at $z$. The *autocorrelation* of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{F}_2^n$ is $\mathcal{C}_{f,f}(\mathbf{u})$ above, which we denote by $\mathcal{C}_f(\mathbf{u})$. The multiset $[\mathcal{C}_f(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_2^n]$ is said to be the autocorrelation spectrum of the function $f$. It is known [6] that a function $f \in \mathcal{B}_n$ is bent if and only if $\mathcal{C}_f(\mathbf{u}) = 0$ for all $\mathbf{u} \neq 0$.

For a detailed study of Boolean functions we refer to Carlet [3, 4], and Cusick and Stănică [6].

The *nega–Hadamard transform* of $f \in \mathbb{F}_2^n$ at any vector $\mathbf{u} \in \mathbb{F}_2^n$ is the complex valued function:

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

The multiset $[\mathcal{N}_f(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_2^n]$ is said to be the nega–Hadamard spectrum of the function $f$. A function is said to be *negabent* if the nega–Hadamard transform is flat in absolute value, namely $|\mathcal{N}_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{F}_2^n$. The sum

$$C_{f,g}(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x} \oplus \mathbf{z})} (-1)^{\mathbf{x} \cdot \mathbf{z}}$$

is the *nega–crosscorrelation* of $f$ and $g$ at $z$. We define the *nega–autocorrelation* of $f$ at $\mathbf{u} \in \mathbb{F}_2^n$ by

$$C_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{u})} (-1)^{\mathbf{x} \cdot \mathbf{u}}.$$

The multiset $[C_f(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_2^n]$ is said to be the nega–autocorrelation spectrum of the function $f$.

The negaperiodic autocorrelation defined by Parker and Pott [15, 16] is as follows

$$n_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{u})} (-1)^{wt(\mathbf{u})} (-1)^{\mathbf{x} \cdot \mathbf{u}}.$$

It is to be noted that the difference between the above two definitions is not critical and both the defintions can be used.

The group of all invertible $n \times n$ matrices over $\mathbb{F}_2^n$ is denonted by $GL(n, \mathbb{F}_2)$. Two Boolean functions $f, g \in \mathcal{B}_n$ are said to be equivalent if there exist $A \in GL(n, \mathbb{F}_2)$, $\mathbf{b}, \mathbf{u} \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$ such that $g(\mathbf{x}) = f(\mathbf{x}A + \mathbf{b}) + \mathbf{u} \cdot \mathbf{x} + \epsilon$ for all $\mathbf{x} \in \mathbb{F}_2^n$. If $\mathbf{u} = 0$ and $\epsilon = 0$, then $f$ and $g$ are said to be affine equivalent.

### 1.2 Quadratic Boolean functions

The properties of quadratic Boolean functions, that is Boolean functions having algebraic degree 2, can be found in ([12], chapter 15). Suppose $f$ is a Boolean function of degree 2 on $n$ variables. The associated symplectic form of $f$ is a map $\Psi : \mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ defined by

$$\Psi(\mathbf{u}, \mathbf{v}) = f(0) + f(\mathbf{u}) + f(\mathbf{v}) + f(\mathbf{u} + \mathbf{v}).$$

The kernel $\mathcal{E}_f$ of $\Psi$ is defined as

$$\mathcal{E}_f = \{\mathbf{u} \in \mathbb{F}_2^n : \text{ for all } \mathbf{v} \in \mathbb{F}_2^n \text{ such that } \Psi(\mathbf{u}, \mathbf{v}) = 0\}.$$

The set $\mathcal{E}_f$ is a subspace of $\mathbb{F}_2^n$ with dimension $n - 2h$ where $2h$ is the rank of $\Psi$. It is known that two quadratic functions $f$ and $g$ are equivalent if and only in $dim(\mathcal{E}_f) = dim(\mathcal{E}_g)$ ([12], chapter 15, Theorem 4). We recall the following result (proposition A1 [1])

**Proposition 1.** *An element $a \in \mathcal{E}_f$ if and only if the function $D_a f$ is constant. The subspace $\mathcal{E}_f$ is the linear space of $f$.*

Since the autocorrelation spectrum of any bent function is zero at all points except at $\mathbf{u} = 0$ the linear space of any quadratic bent function is of dimension 0. Therefore by ([12], chapter 15, Theorem 4) and Proposition 1 all quadratic bent function are equivalent to each other.

Suppose $n = 2p$, $\pi : \mathbb{F}_2^p \longrightarrow \mathbb{F}_2^p$ is a permutation and $g : \mathbb{F}_2^p \longrightarrow \mathbb{F}_2$ is any Boolean function. Rothaus proved that a Boolean function $f : \mathbb{F}_2^p \times \mathbb{F}_2^p \longrightarrow \mathbb{F}_2$ defined by

$$f(\mathbf{x}, \mathbf{y}) = \pi(\mathbf{x}) \cdot \mathbf{y} + g(\mathbf{x}) \text{ for all } (\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^p \times \mathbb{F}_2^p$$

is a bent function. The collection of bent functions of this type is called the Maiorana-McFarland class, denoted by $\mathcal{M}$. If $\pi$ is an identity permutation and $g(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{F}_2^p$, then the function $h(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{p} x_i y_i$ for all $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^p \times \mathbb{F}_2^p$ is a quadratic bent function. Thus any quadratic bent function of $n$ variables is equivalent to $h$. Let $y_i = x_{p+i}$ for all $i = 1, \ldots, p$. For all $\mathbf{x} \in \mathbb{F}_2^n$ the function $h$ can be written as $h(\mathbf{x}) = \sum_{i=1}^{p} x_i x_{p+i}$. Throughout this paper $h$ will represent this particular function. From the above discussions it is clear that if $f \in \mathcal{B}_n$ is any quadratic bent then there exist $A \in GL(n, \mathbb{F}_2)$, $\mathbf{b}, \mathbf{u} \in \mathbb{F}_2^n$, and $\epsilon \in \mathbb{F}_2$ such that $h(\mathbf{x}) = f(\mathbf{x}A + \mathbf{b}) + \mathbf{u} \cdot \mathbf{x} + \epsilon$.

## 2 Construction of bent–negabent Boolean functions

Throughout this section $n = 2p$. A Boolean function is said to be symmetric if inputs of the same weight produce the same output, that is, $f(\mathbf{x}) = f(\sigma(\mathbf{x}))$, for any permutation $\sigma$. The function $s_2 \in \mathcal{B}_n$ defined by

$$s_2(\mathbf{x}) = \sum_{i<j} x_i x_j \text{ for all } (x_1, \ldots, x_n) \in \mathbb{F}_2^n$$

is a quadratic symmetric Boolean function. It is known that this function is a bent function. Therefore by the results of Section 1.2, $s_2$ is equivalent to the quadratic bent $h$ as defined in Section 1.2. The following theorem is due to Parker and Pott

**Theorem 1 (Theorem 24, [15]).** *Suppose $f \in \mathcal{B}_n$. If $f$ is a bent function then $f + s_2$ is negabent, and if $f$ is a negabent function then $f + s_2$ is bent.*

Using Theorem 1 we obtain:

**Lemma 1.** *A Boolean function $f \in \mathcal{B}_n$ is bent–negabent if and only if, $f$ and $f + s_2$ both are bent functions.*

*Proof.* Let $f \in \mathcal{B}_{2p}$ is a bent–negabent function. Since $f$ is a negabent function, $f + s_2$ is a bent function. Thus $f$ and $f + s_2$ both are bent functions.

Conversely let us suppose that $f$ and $f + s_2$ both are bent function. Since $f + s_2$ is a bent function $f + s_2 + s_2 = f$ is a negabent function. Therefore, $f$ is a bent–negabent function. □

The following theorem provides a strategy to construct bent–negabent functions.

**Theorem 2.** *Let $s_2(\mathbf{x}) = h(\mathbf{x}A + \mathbf{b}) + \mathbf{u} \cdot \mathbf{x} + \epsilon$ for all $\mathbf{x} \in \mathbb{F}_2^n$, where $A \in GL(n, \mathbb{F}_2)$, $\mathbf{b}, \mathbf{u} \in \mathbb{F}_2^p$ and $\epsilon \in \mathbb{F}_2$. Suppose $f \in \mathcal{B}_n$ is a bent function such that $f + h$ is also a bent function. Then $g \in \mathcal{B}_n$ define by*

$$g(\mathbf{x}) = f(\mathbf{x}A + \mathbf{b}) + h(\mathbf{x}A + \mathbf{b}) + \mathbf{u} \cdot \mathbf{x} + \epsilon = f(\mathbf{x}A + \mathbf{b}) + s_2(\mathbf{x}) \text{ for all } x \in \mathbb{F}_2^n$$

*is a bent–negabent function.*

*Proof.* The function $g$ is equivalent to $f + h$. Therefore $g$ is bent. The function $g + s_2$ is affine equivalent to $f$. Since $f$ is a bent function, $g + s_2$ is also a bent function. Therefore by Lemma 1 $g$ is a bent–negabent function. □

*Remark 1.* For definiteness we define $h$ as $h(x) = \sum_{i=1}^{n} x_i x_{p+i}$ for all $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$. However it should be noted that the Theorem 2 holds even if we replace $h$ by any quadratic bent Boolean function on $n$ variables.

Theorem 2 reduced the problem of constructing bent–negabent functions to characterizing bent functions $f$ such that $f + h$ is also a bent function. We observe that such functions can be constructed by using *complete mapping polynomials*.

### 2.1 Complete mapping polynomials

The field extension of $\mathbb{F}_2$ of degree $p$ denoted by $\mathbb{F}_{2^p}$. The finite field $\mathbb{F}_{2^p}$ is isomorphic to $\mathbb{F}_2^p$ as a vector space over $\mathbb{F}_2$. Any permutation of $\mathbb{F}_{2^p}$ can be identified with a permutation on $\mathbb{F}_2^p$. Any permutation on $\mathbb{F}_{2^p}$ can be represented by a polynomial in $\mathbb{F}_{2^p}[X]$ of degree atmost $2^p-2$. A polynomial $F(x) \in \mathbb{F}_{2^p}[X]$ is said to be a *complete mapping polynomial* if $F(X)$ and $F(X)+X$ both correspond to permutations on $\mathbb{F}_{2^p}$. For details on complete mapping polynomials we refer to [11, 14]. The following provides us a strategy to construct bent–negabent functions by using complete mapping polynomials.

**Proposition 2.** *Let $n = 2p$. Suppose $\pi_F$ denote the permutation on $\mathbb{F}_2^p$ induced by a complete mapping polynomial $F(X) \in \mathbb{F}_{2^p}[X]$. Let $f_F \in \mathcal{B}_n$ be defined by $f_F(\mathbf{x}) = \pi_F(x_1, \ldots, x_p)\cdot(x_{p+1}, \ldots, x_n)$ for all $\mathbf{x} \in \mathbb{F}_2^n$. Then the Boolean function $f_F + h$ is a Maiorana-McFarland type bent and*

$$g(\mathbf{x}) = f_F(\mathbf{x}A + \mathbf{b}) + h(\mathbf{x}A + \mathbf{b}) + \mathbf{u}\cdot\mathbf{x} + \epsilon = f_F(\mathbf{x}A + \mathbf{b}) + s_2(\mathbf{x}) \text{ for all } \mathbf{x} \in \mathbb{F}_2^n$$

*is a bent–negabent function. The algebraic degrees of $g$ and $f_F$ are equal.*

*Proof.* The proof is direct from the properties of complete mapping polynomials and Theorem 2.

### 2.2 Bent–negabent function on $n$ variables with algebraic degree greater than $\frac{n}{4}$

We consider a particular complete mapping polynomial constructed by Laigle-Chapuy [11].

**Theorem 3 (Theorem 4.3, [11]).** *Let $p$ be a prime and $(m, \ell) \in \mathbb{N}^2$. Let $k$ be the order of $p$ in $\mathbb{Z}/m\mathbb{Z}$. Take $q = p^{k\ell m}$ and $r$ a positive integer coprime with $q-1$. Assume $a \in \mathbb{F}_{p^{k\ell}}$ is such that $(-a)^m \neq 1$. Then the polynomials*

$$P(X) = X(X^{\frac{q-1}{m}} + a)$$

*and*

$$Q(X) = aX^{\frac{q-1}{m}+1}$$

*are complete mapping polynomials.*

First we construct a bent–negabent function on 24 variables having algebraic degree 7.

*Example 1.* Following the notations of Theorem 3 let $p = 2$ and $m = 3$. The order of $p$ in $\mathbb{Z}/3\mathbb{Z}$ is 2, that is $k = 2$. Choose $\ell = 2$. Thus, $k\ell m = (2)(2)(3) = 12$; $q = p^{k\ell m} = 2^{12}$. The polynomial $P(X) = X(X^{\frac{q-1}{m}} + a) = X(X^{1365} + a)$ where $a \in \mathbb{F}_{2^4} \setminus \mathbb{F}_{2^2}$. The last condition guarantees $(-a)^m = (-a)^3 \neq 1$. By using this polynomial $P(X)$ in Proposition 2 we obtain a bent–negabent function on 24 variables and algebraic degree 7. The algebraic degrees of the bent–netabent functions constructed in [23, 24] are bounded above by $\frac{n}{4}$. Thus the bent–negabent function constructed above does not belong to these classes.

In general we observe the following.

**Lemma 2.** *Suppose the prime $p = 2$, $m = 3$. The order of $p$ in $\mathbb{Z}/m\mathbb{Z}$, $k = 2$. Then for any $\ell \geq 2$ the polynomials*

$$P(X) = X(X^{\frac{2^{6\ell}-1}{3}} + a) \text{ and } Q(X) = aX^{\frac{2^{6\ell}-1}{3}+1}$$

*have algebraic degree $3\ell$.*

*Proof.* Let $t = \frac{2^{6\ell}-1}{3} + 1$.

$$\begin{aligned} t &= \frac{2^{6\ell}-1}{3} + 1 \\ &= \frac{2^{6\ell}-4+3}{3} + 1 \\ &= \frac{2^{6\ell}-4}{3} + 2 \\ &= \frac{2^2((2^2)^{3\ell-1}-1)}{2^2-1} + 2 \\ &= \underbrace{((2^2)^{3\ell-1} + (2^2)^{3\ell-2} + (2^2)^{3\ell-3} + \ldots + (2^2)^2 + 2^2)}_{3\ell-1 \text{ terms}} + 2 \\ &= \underbrace{2^{6\ell-2} + 2^{6\ell-4} + 2^{6\ell-6} + \ldots + 2^4 + 2^2 + 2}_{3\ell \text{ terms}}. \end{aligned} \tag{1}$$

This proves that both $P(X)$ and $Q(X)$ have degree $3\ell$. □

**Theorem 4.** *For each $\ell \geq 2$ there exit bent–negabent functions on $n = 12\ell$ variables with algebraic degree $\frac{n}{4} + 1 = 3\ell + 1$.*

*Proof.* For each $\ell \geq 2$ it is possible to construct $P(X)$ and $Q(X)$ as in Lemma 2 with $p = 2$ and $m = 3$. It is proved in Lemma 2 that $P(X)$ and $Q(X)$ both have algebraic degree $3\ell$. It is also to be noted that if $\ell \geq 2$ we can choose $a \in \mathbb{F}_{2^\ell} \setminus \mathbb{F}_2$ so that $(-a)^m \neq 1$. Therefore $P(X)$ and $Q(X)$ constructed in this way are complete mapping polynomials. If we use the Proposition 2 by inducing the permutation $\pi_F$ where $F(X) \in \{P(X), Q(X)\}$, then we obtain bent–negabent functions on $n = (2)(6\ell) = 12\ell$ variables with algebraic degree $3\ell + 1$. It is also to be noted that these functions may not be of Maiorana–McFarland type but belongs to the complete class of Maiorana–McFarland type functions. □

### 2.3 Existence of bent-negabent functions of degree 2, 3 and 4 on 8 variables Boolean functions

Y.Yuan et al.[25] obtained the degree distribution of complete mapping polynomial over $\mathbb{F}_{2^4} (= \mathbb{F}_{16})$. The results on complete mapping polynomial over $\mathbb{F}_{2^4}$ are given below.

**Theorem 5 ([25], Theorem 3).** *The complete mapping trinomial of the form* $ax^i + bx^j + cx$, $abc \neq 0$, *and* $15 > i > j > 1$ *must be one of the following*

1. $ax^4 + bx^2 + cx$
2. $ax^8 + bx^2 + cx$
3. $ax^8 + bx^4 + cx$
4. $ax^{11} + bx^7 + cx$

**Table 1.** Complete mapping polynomials of reduced degree 4,8,10,12 and 13 (algebraic degree 1,1,2,2,3 respectively).

| (reduced degree, algebraic degree ) | complete mapping polynomials |
|---|---|
| $(4, 1)$ | $a(x^4 + bx), ab \neq 0; b, b + a^{-1} \neq \alpha^3, \alpha^6, \alpha^9, \alpha^{12}$ |
| $(8, 1)$ | $a(x^8 + bx^2), ab \neq 0; b \neq \alpha^3, \alpha^6, \alpha^9, \alpha^{12}$; and $x^7 + bx + a^{-1}$has no root in $\mathbb{F}_{16}$ |
| $(10, 2)$ | $\alpha^4 x^{10} + \alpha^{13} x^9 + \alpha^2 x^8 + \alpha^7 x^{13} + \alpha^4 x$ |
| $(12, 2)$ | $\alpha^8 x^{12} + \alpha^{14} x^9 + \alpha^5 x^6 + \alpha^{11} x^3 + \alpha^5 x$ |
| $(13, 3)$ | $\alpha^{14} x^{13} + \alpha^8 x^{10} + \alpha^7 x^7 + \alpha^8 x$ |

Here $\alpha$ is a primitive element in $\mathbb{F}_{16}$.

In 2007, by searching with computer Y.Yuan et.al [25] obtained the degree distribution of complete mapping polynomial over $\mathbb{F}_{16}$ is given in Tabel 2.

**Table 2.** The degree distribution of complete mapping polynomial over $\mathbb{F}_{16}$ [25].

| reduced degree | algebraic degree | number of complete mapping polynomials |
|---|---|---|
| 1 | 1 | 224 |
| 4 | 1 | 6560 |
| 8 | 1 | 132480 |
| 10 | 2 | 798720 |
| 11 | 3 | 933888 |
| 12 | 2 | 22179840 |
| 13 | 3 | 220692480 |

**Theorem 6.** *There exists bent-negabent functions of degree* 2, 3 *and* 4 *on* 8 *variables.*

*Proof.* By Proposition 2 and Table 1, 2 and Theorem 5, we obtain bent-negabent functions of degree 2, 3 and 4 on 8 variables.

From Table 2, it is clear that there exists a large number of bent-negabent function of degree 2, 3 and 4.

**Acknowledgements** Part of this work is done during Sugata Gangopadhyay's visit to INRIA–Rocquencourt during June–July 2010. The authors thank Pascale Charpin and Matthew G. Parker for several helpful suggestions and discussions.

## References


1. A. Canteaut, C. Carlet, P. Charpin and C. Fontaine On cryptographic properties of the cosets of $R(1, m)$. *IEEE Transactions on Information Theory*, Vol. 47, no. 4, (2001) 1494-1513.
2. C. Carlet, *Two new classes of bent functions*, Adv. in Crypt. – Eurocrypt'93, LNCS 765 (1994), Springer–Verlag, 77–101.
3. C. Carlet, Boolean functions for cryptography and error correcting codes. In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.
4. C. Carlet, Vectorial Boolean functions for cryptography. In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.
5. P. Charpin and G. Kyureghyan. On a class of permutation polynomials over $\mathbf{F}_{2^n}$. In *SETA 2008*, LNCS 5203, pp. 368-376, Springer-Verlag, 2008.
6. T. W. Cusick, P. Stănică, Cryptographic Boolean functions and Applications, Elsevier–Academic Press, 2009.
7. L. E. Danielsen, T. A. Gulliver and M. G. Parker, *Aperiodic Propagation Criteria for Boolean Functions*, Inform. Comput. 204:5 (2006), 741–770.
8. J. F. Dillon, *Elementary Hadamard difference sets*, Proceedings of Sixth S. E. Conference of Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, 1975, 237–249.
9. H. Dobbertin, *Construction of bent functions and balanced Boolean functions with high nonlinearity*, In Fast Software Encryption (Workshop on Cryptographic Algorithms), Leuven 1994 (1995), LNCS 1008, Springer-Verlag, 61–74.
10. H. Dobbertin, G. Leander, *Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions*, Des. Codes Cryptography 49 (2008), 3–22.
11. Y. Laigle–Chapuy, *Permutation polynomials and applications to coding theory* Finite Fields and Their Applications 13 (2007) 58–70.
12. F. J. MacWilliams and N. J. A. Sloane. *The theory of error correcting codes* North-Holland, Amsterdam, 1977.
13. R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1983.
14. H. Niederreiter, K. H. Robinson, *Complete mappins of finite fields*, J. Austral. Math. Soc. (Series A) 33 (1982), 197–212.
15. M. G. Parker, A. Pott, *On Boolean functions which are bent and negabent.* In: S.W. Golomb, G. Gong, T. Helleseth, H.-Y. Song (eds.), SSC 2007, LNCS 4893 (2007), Springer, Heidelberg, 9–23.
16. M. G. Parker, A. Pott, personal communications.
17. C. Riera, M. G. Parker, *One and two-variable interlace polynomials: A spectral interpretation*, Proc. of WCC 2005, LNCS 3969 (2006), Springer, Heidelberg, 397–411.
18. C. Riera, M. G. Parker, *Generalized bent criteria for Boolean functions*, IEEE Trans. Inform. Theory 52:9 (2006), 4142–4159.
19. O. S. Rothaus, *On bent functions*, Journal of Combinatorial Theory Series A 20 (1976), 300–305.
20. P. Sarkar, S. Maitra, *Cross–Correlation Analysis of Cryptographically Useful Boolean Functions and S-Boxes*, Theory Comput. Systems 35 (2002), 39–57.
21. S. Sarkar, *On the symmetric negabent Boolean functions*, Indocrypt 2009, LNCS 5922 (2009), 136–143.

22. P. Savicky, *On the bent Boolean functions that are symmetric*, European J. Comb. 15 (1994), 407–410.
23. K. U. Schmidt, M. G. Parker, A. Pott, *Negabent functions in the Maiorana–McFarland class*. In: S.W. Golomb, M.G. Parker, A. Pott, A. Winterhof (eds.), SETA 2008, LNCS 5203 (2008), Springer, Heidelberg, 390–402.
24. P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. Kar Gangopadhyay, S. Maitra, *Nega–Hadamard transform, bent and negabent functions*, *SETA 2010, Lecture notes in Computer Science, LNCS,* vol. 6338, pp. 359-372, 2010.
25. Y. Yuan, Y. Tong, and H. Zhan, *Complete Mapping Polynomials over Finite Field* $\mathbb{F}_{16}$, C. Carlet and B. Sunar (Eds.): WAIFI 2007, LNCS 4547, pp. 147158, 2007 2007.
26. Y. Zhao, H. Li, *On bent functions with some symmetric properties*, Discrete Appl. Math. 154 (2006), 2537–2543.