2019

The connection between quadratic bent-negabent functions and the Kerdock code

Stnic, Pantelimon; Mandal, Bimal; Maitra, Subhamoy

P. Stanica, B. Mandal, S. Maitra, The connection between quadratic bent-negabent functions and the Kerdock code, Applicable Algebra in Engineering, Communication and Computing 30:5 (2019), 387-401.
http://hdl.handle.net/10945/64439

AAECC
https://doi.org/10.1007/s00200-019-00380-4

ORIGINAL PAPER

The connection between quadratic bent–negabent functions and the Kerdock code

Pantelimon Stănică[1] · **Bimal Mandal**[2] · **Subhamoy Maitra**[3]

Received: 29 August 2018 / Revised: 13 December 2018 / Accepted: 8 January 2019

Abstract
In this paper we prove that all bent functions in the Kerdock code, except for the coset of the symmetric quadratic bent function, are bent–negabent. In this direction, we characterize the set of quadratic bent–negabent functions and show some results connecting quadratic bent–negabent functions and the Kerdock code. Further, we note that there are bent–negabent preserving nonsingular transformations outside the well known class of orthogonal ones that might provide additional functions in the bent–negabent set. This is the first time we could identify non-orthogonal (nonsingular) linear transformations that preserve bent–negabent property for a special subset.

Keywords Boolean function · Bent function · Negabent function · Kerdock code

1 Introduction

In 1976, Rothaus [13] introduced the class of bent functions, having the maximum possible distance from the affine functions. Bent functions exist only in even number of variables and the degree of an n-variable bent functions is at most $\frac{n}{2}$ (for $n > 2$). A bent function of degree 2 is called a quadratic bent function [3,5,17]. A Boolean function is said to be negabent if its nega–Hadamard spectrum (defined as in Sect. 1.1) is flat [10,12,14,15]. The problem of constructing Boolean functions which are bent and

✉ Pantelimon Stănică
pstanica@nps.edu

Bimal Mandal
bimalmandal90@gmail.com

Subhamoy Maitra
subho@isical.ac.in

1 Department of Applied Mathematics, Naval Postgraduate School, Monterey, USA

2 R. C. Bose Centre for Security and Cryptology, Indian Statistical Institute, Kolkata, India

3 Applied Statistics Unit, Indian Statistical Institute, Kolkata, India

Published online: 31 January 2019

negabent at the same time was initiated by Riera and Parker [12], and later investigated in [10,14–16,18]. Parker and Pott [10] proposed to determine the number of quadratic bent–negabent functions with n variables. This was consequently resolved by Pott et al. [11], using the necessary and sufficient description of quadratic bent–negabent Boolean functions, shown by Parker and Pott [10].

In 1972, Kerdock [6] constructed a new class of nonlinear binary codes, which is a supercode of $\mathcal{RM}(1, m)$ and is a subcode of $\mathcal{RM}(2, m)$, called the Kerdock code (in his honor), where $\mathcal{RM}(r, m)$ is the set of m-variable Boolean functions of degree at most r (Reed–Muller code of order r). For more details we refer to [2,7–9]. Now, one can raise the following questions related to the quadratic bent–negabent functions:

- Is there any relation between quadratic bent–negabent functions and the Kerdock code?
- Can we construct all quadratic bent–negabent functions from the Kerdock code?

In this paper, we get positive results on the above two problems. We first prove that all the bent functions in Kerdock code, except for the coset of the symmetric quadratic bent function, are bent–negabent, and then derive a method so that one can construct all the quadratic bent–negabent functions from the Kerdock code. The construction method of all m-variable quadratic bent–negabent functions from the Kerdock code can be summarized as below:

- We first construct the Kerdock code $\mathcal{K}_m$ as in (3).
- We identify $2^{m-1}-2$ quadratic homogeneous bent–negabent functions $\{f_i\}_{1\le i\le 2^{m-1}-2}$ in $\mathcal{K}_m$.
- From each quadratic homogeneous bent–negabent function f_i, $1 \le i \le 2^{m-1}-2$, we construct the set $\mathcal{A}_S$ [defined in (4) for all $\emptyset \neq S \subset [1, m-1]$] by applying a special class of bent–negabent preserving linear transformations, as in Theorem 13.
- We add all 2^{m+1} affine functions to each $f \in \mathcal{A}_S$, $\emptyset \neq S \subset [1, m-1]$: the collection of all these functions is the set of all quadratic bent–negabent functions in m variables.

The paper is organized as follows. In Sect. 1.1, some basic definitions and known results are described. In Sect. 2, we find the connection between quadratic bent–negabent functions and the Kerdock code. For each Kerdock codeword (affine free), except the symmetric quadratic bent function, we construct disjoint sets of quadratic bent–negabent functions (affine free), and we prove that the union of these sets is equal to the set of quadratic bent–negabent functions (affine free). In Sect. 3 we find that there are bent–negabent preserving nonsingular transformations outside the well known orthogonal transformations class.

1.1 Preliminaries

Let $\mathbb{F}_2$, $\mathbb{F}_{2^m}$ and $\mathbb{F}_2^m = \{\mathbf{x} = (x_1, x_2, \ldots, x_m) : x_i \in \mathbb{F}_2, 1 \le i \le m\}$ be the prime field of characteristic 2, the extension field of degree m over $\mathbb{F}_2$ and the vector space of dimension m over $\mathbb{F}_2$, respectively. Let $\oplus$ denote the addition over $\mathbb{F}_2$. For $\mathbf{x} = (x_1, \ldots, x_m), \mathbf{y} = (y_1, \ldots, y_m) \in \mathbb{F}_2^m$, we define the vector space addition as $\mathbf{x} \oplus \mathbf{y} = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_m \oplus y_m)$ and the inner product as $\mathbf{x} \cdot \mathbf{y} =$

$x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_my_m$. The *complement* of an element $\mathbf{a} \in \mathbb{F}_2^m$ is $\mathbf{a} \oplus \mathbf{1}$. If $B = \{b_1, b_2, \ldots, b_m\}$ is a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$, then any $x \in \mathbb{F}_{2^m}$ can be written as $x = x_1b_1 \oplus x_2b_2 \oplus \cdots \oplus x_mb_m$, where $x_i \in \mathbb{F}_2$, $i = 1, 2, \ldots, m$. The vector $(x_1, x_2, \ldots, x_m)$ is said to be the coordinates (or components) of $x \in \mathbb{F}_{2^m}$, with respect to the basis B. The *cardinality* of a set S is denoted by $|S|$. Any function $f : \mathbb{F}_2^m \to \mathbb{F}_2$ (or, equivalently, $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$) is said to be a *Boolean function* in m variables, whose set will be denoted by $\mathcal{B}_m$. Any function $f \in \mathcal{B}_m$ can be uniquely represented as a multivariate polynomial, called the *algebraic normal form* (ANF) of f, that is,

$$f(x_1, x_2, \ldots, x_m) = \bigoplus_{\mathbf{u}=(u_1,\ldots,u_m)\in\mathbb{F}_2^m} \mu_{\mathbf{u}} \left(\prod_{i=1}^{m} x_i^{u_i} \right), \ \mu_{\mathbf{u}} \in \mathbb{F}_2, x_1, \ldots, x_m \in \mathbb{F}_2. \tag{1}$$

The *Hamming weight* of $\mathbf{x} \in \mathbb{F}_2^m$, $wt(\mathbf{x})$, is defined as $wt(\mathbf{x}) = \sum_{i=1}^m x_i$, where the sum is over the ring of integers, $\mathbb{Z}$. The *algebraic degree* of $f \in \mathcal{B}_m$, $\deg(f)$, is defined as $\deg(f) = \max_{\mathbf{u}\in\mathbb{F}_2^m}\{wt(\mathbf{u}) : \mu_{\mathbf{u}} \neq 0\}$. A Boolean function f defined as in (1) is said to be *homogeneous* of degree r if $\mu_{\mathbf{u}} = 0$ for all $\mathbf{u} \in \mathbb{F}_2^m$ such that $wt(\mathbf{u}) \neq r$ (and, of course, there exists $\mathbf{u}$ of $wt(\mathbf{u}) = r$ with $\mu_{\mathbf{u}} \neq 0$). We also identify $\mathbb{F}_2^m$ with $\mathbb{F}_{2^m}$ and take the inner product $x \cdot y = \mathrm{Tr}_1^m(xy)$, where $\mathrm{Tr}_1^m(x) = x \oplus x^2 \oplus x^{2^2} \oplus \cdots \oplus x^{2^{m-1}}$, for all $x \in \mathbb{F}_{2^m}$, is the absolute trace on $\mathbb{F}_{2^m}$.

The *Walsh–Hadamard transform* of $f \in \mathcal{B}_m$ at $\mathbf{u} \in \mathbb{F}_2^m$, denoted by $\mathcal{W}_f(\mathbf{u})$, is defined by

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

The multiset $[\mathcal{W}_f(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_2^m]$ is the *Walsh–Hadamard spectrum* of f. A function $f \in \mathcal{B}_m$ (where m is an even positive integer) is *bent* if and only if $\mathcal{W}_f(\mathbf{u}) = \pm 2^{\frac{m}{2}}$, for all $\mathbf{u} \in \mathbb{F}_2^m$. The *nega–Hadamard transform* of $f \in \mathbb{F}_2^m$ at $\mathbf{u} \in \mathbb{F}_2^m$, denoted by $\mathcal{N}_f(\mathbf{u})$, is defined by

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

where $\imath^2 = -1$. The multiset $[\mathcal{N}_f(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_2^m]$ is the *nega–Hadamard spectrum* of f. An m-variable Boolean function f is *negabent* if the absolute value $|\mathcal{N}_f(\mathbf{u})| = 1$, for all $\mathbf{u} \in \mathbb{F}_2^m$. For an even number of variables, a bent function $f \in \mathcal{B}_m$ is called *bent–negabent* if f is also *negabent*.

A Boolean function $f \in \mathcal{B}_m$ is called *symmetric* if $f(\mathbf{x}) = f(\mathbf{y})$, for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^m$ with $wt(\mathbf{x}) = wt(\mathbf{y})$ (invariant under any permutation of the input variables). Let s_2

be the elementary quadratic symmetric Boolean function in m variables, defined as

$$s_2(\mathbf{x}) = \bigoplus_{1 \le i < j \le m} x_i x_j. \tag{2}$$

Parker and Pott [10, Theorem 12] proved that adding s_2 to a bent (negabent) function transforms it to a negabent (bent) function.

Lemma 1 [10, Theorem 12] *Let m be an even integer. An m-variable Boolean function f is bent (negabent) if and only if $f \oplus s_2$ is negabent (bent).*

Thus, an even variable Boolean function f is bent–negabent if and only if both f and $f \oplus s_2$ are bent. Further, $f \in \mathcal{B}_m$ is bent–negabent if and only if $f \oplus s_2$ is bent–negabent. Let $GL(m, \mathbb{F}_2)$ be the group of all binary nonsingular matrices of order m and $SL(m, \mathbb{F}_2)$ be the group of all binary orthogonal matrices of order m.

Definition 2 A linear transformation $A \in GL(m, \mathbb{F}_2)$ is said to be weight invariant if $wt(\mathbf{x}) = wt(\mathbf{x}A)$, for all $\mathbf{x} \in \mathbb{F}_2^m$.

Schmidt et al. [14, Theorem 2] identified a subgroup of the bent preserving transformations which also preserves the negabent property.

Theorem 3 [14, Theorem 2] *Let m be an even integer and $f, g \in \mathcal{B}_m$ such that $g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{a}) \oplus \mathbf{b} \cdot \mathbf{x} \oplus \varepsilon$, for all $\mathbf{x} \in \mathbb{F}_2^m$ where $A \in SL(m, \mathbb{F}_2)$, $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m$ and $\varepsilon \in \mathbb{F}_2$. Then, if f is bent–negabent, g is also bent–negabent.*

Let $f \in \mathcal{B}_m$ be a quadratic bent function. By Dickson's theorem [8, Chapter 15, Thm. 4], there exists $A \in GL(m, \mathbb{F}_2)$, $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m$ and $\varepsilon \in \mathbb{F}_2$ such that $f(\mathbf{x}A \oplus \mathbf{a}) \oplus \mathbf{b} \cdot \mathbf{x} \oplus \varepsilon = s_2(\mathbf{x})$, for all $\mathbf{x} \in \mathbb{F}_2^m$.

2 The Kerdock code and quadratic bent–negabent functions

Let $m \ge 4$ be an even integer and $\ell = m - 1 = 2t + 1$. The *Kerdock code* of length 2^m, denoted by $\mathcal{K}_m$, is the union of certain cosets of $\mathcal{RM}(1, m)$ in $\mathcal{RM}(2, m)$, described below. Let $f \in \mathcal{B}_m$ on $\mathbb{F}_{2^\ell} \times \mathbb{F}_2$ be defined as

$$f(x, x_m) = \mathrm{Tr}_1^\ell \left(\bigoplus_{j=1}^{t} x^{2^j+1} \right) \oplus x_m \mathrm{Tr}_1^\ell(x),$$

for all $(x, x_m) \in \mathbb{F}_{2^\ell} \times \mathbb{F}_2$. Let

$$f_u(x, x_m) := f(ux, x_m) = \mathrm{Tr}_1^\ell \left(\bigoplus_{j=1}^{t} (ux)^{2^j+1} \right) \oplus x_m \mathrm{Tr}_1^\ell(ux), \ u \in \mathbb{F}_{2^\ell}. \tag{3}$$

The Kerdock code $\mathcal{K}_m$ is defined as the union of the cosets $f_u \oplus \mathcal{RM}(1, m)$, where u varies over $\mathbb{F}_{2^\ell}$. We know [2, Subsection 8.6.10] that the sum of any two distinct

functions f_u and f_v is bent. Note that for $u = 1$, $f_1(x, x_m) = f(x, x_m)$ is the m-variable quadratic symmetric function s_2, defined as in (2).

Lemma 4 *Let f_u and f_v be defined as in (3). Then $f_u \oplus f_v$ does not belong to the Kerdock code $\mathcal{K}_m$ unless $uv(u \oplus v) = 0$ (that is, $u = v$, or $u = 0$, or $v = 0$).*

Proof Let $u, v \in \mathbb{F}_{2^\ell}$, and f_u and f_v be defined as in (3). Then

$$\begin{aligned}
(f_u \oplus f_v)(x, x_m) &= f_u(x, x_m) \oplus f_v(x, x_m) \\
&= \mathrm{Tr}_1^\ell\left(\bigoplus_{j=1}^{t}\left(u^{2^j+1} \oplus v^{2^j+1}\right)x^{2^j+1}\right) \oplus x_m \mathrm{Tr}_1^\ell\left((u \oplus v)x\right) \\
&= \mathrm{Tr}_1^\ell\left(\bigoplus_{j=1}^{t}((u \oplus v)x)^{2^j+1}\right) \oplus x_m \mathrm{Tr}_1^\ell\left((u \oplus v)x\right) \\
&\quad \oplus \mathrm{Tr}_1^\ell\left(\sum_{j=1}^{t}\left(uv^{2^j} \oplus u^{2^j}v\right)x^{2^j+1}\right) \\
&= f_{u\oplus v}(x, x_m) \oplus \mathrm{Tr}_1^\ell\left(\bigoplus_{j=1}^{t}(uv^{2^j} \oplus u^{2^j}v)x^{2^j+1}\right),
\end{aligned}$$

which belongs to $\mathcal{K}_m$ if and only if $\mathrm{Tr}_1^\ell\left(\bigoplus_{j=1}^{t}\left(uv^{2^j} \oplus u^{2^j}v\right)x^{2^j+1}\right) = 0$, for all $x \in \mathbb{F}_{2^\ell}$. Since $3 \cdot 2^i \not\equiv 2^j + 1 \pmod{2^\ell - 1}$, where $0 \le i \le \ell - 1$ and $2 \le j \le t$, the coefficient of x^3 is equal to 0, that is, $u^2v \oplus u^2v = 0$, or equivalently, $u = v$, or $u = 0$, or $v = 0$. □

Theorem 5 *Let $m \ge 4$ be an even positive integer and $\ell = m - 1$. Then, for all $u \in \mathbb{F}_{2^\ell}\backslash\{0, 1\}$, the functions f_u defined as in (3) are bent–negabent.*

Proof We know that a function $f \in \mathcal{B}_m$ is bent–negabent if and only if both f and $f \oplus s_2$ are bent. It is clear that $f_0 = 0$ and $f_1 = s_2$, which are not bent–negabent. Let $u \in \mathbb{F}_{2^\ell}\backslash\{0, 1\}$. Then from [2, Subsection 8.6.10], we get $f_u \oplus s_2$ is bent, and so, f_u is bent–negabent. □

We know that bent–negabent functions are invariant under addition of affine functions. So, the functions in $\mathcal{K}_m$ corresponding to $u = 0$ and 1, whose set is $\mathcal{RM}(1, m)$ and $s_2 \oplus \mathcal{RM}(1, m)$, are not bent–negabent, and the functions in $\mathcal{K}_m$ of the form $f_u \oplus \mathcal{RM}(1, m)$, $u \in \mathbb{F}_{2^\ell}\backslash\{0, 1\}$, are bent–negabent. Thus, $\mathcal{K}_m$ contains 2^{m+1} affine functions, 2^{m+1} quadratic bent functions which are not negabent and $2^{2m} - 2^{m+2}$ quadratic bent–negabent functions. Let us denote the set

$$\bar{\mathcal{K}}_m = \mathcal{K}_m \oplus s_2 = \{f \in \mathcal{B}_m : f = g \oplus s_2 \text{ where } g \in \mathcal{K}_m\}.$$

Then $\bar{\mathcal{K}}_m$ is also a Kerdock code, called the s_2-complement of $\mathcal{K}_m$. Note that $\mathcal{K}_m \cap \bar{\mathcal{K}}_m = \mathcal{RM}(1, m) \cup (s_2 \oplus \mathcal{RM}(1, m))$. Thus, the lower bound of the number of quadratic bent–negabent functions in $m \ge 4$ (even) variables is $2^{2m+1} - 2^{m+3}$.

Example 6 Let $m = 4$. The total number of 4-variable quadratic bent functions, respectively, quadratic bent–negabent functions is 896, respectively, $384 = 2^{2\cdot 4+1} - 2^{4+3}$. The Kerdock code on 4 variables is $\mathcal{K}_4 = \{\mathcal{RM}(1,4), s_2 \oplus \mathcal{RM}(1,4), f_1 \oplus \mathcal{RM}(1,4), \ldots, f_6 \oplus \mathcal{RM}(1,4)\}$, where

$$\begin{aligned} f_1(\mathbf{x}) &= x_1x_4 \oplus x_2x_3 \oplus x_3x_4, \quad f_2(\mathbf{x}) = x_1x_2 \oplus x_1x_3 \oplus x_3x_4,\\ f_3(\mathbf{x}) &= x_1x_2 \oplus x_1x_4 \oplus x_2x_3, \quad f_4(\mathbf{x}) = x_1x_3 \oplus x_2x_3 \oplus x_2x_4,\\ f_5(\mathbf{x}) &= x_1x_3 \oplus x_1x_4 \oplus x_2x_4, \quad f_6(\mathbf{x}) = x_1x_2 \oplus x_2x_4 \oplus x_3x_4,\\ s_2(\mathbf{x}) &= x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4, \end{aligned}$$

for all $\mathbf{x} \in \mathbb{F}_2^4$. The s_2-complement of $\mathcal{K}_4$ is $\overline{\mathcal{K}_4} = \{\mathcal{RM}(1,4), s_2 \oplus \mathcal{RM}(1,4), h_1 \oplus \mathcal{RM}(1,4), \ldots, h_6 \oplus \mathcal{RM}(1,4)\}$, where $h_i(\mathbf{x}) = f_i(\mathbf{x}) \oplus s_2(\mathbf{x})$, $1 \le i \le 6$, for all $\mathbf{x} \in \mathbb{F}_2^4$.

Theorem 7 *Let $f, g \in \mathcal{K}_m$ be any two quadratic bent–negabent functions and $A \in GL(m, \mathbb{F}_2)$, $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m$ and $\varepsilon \in \mathbb{F}_2$ such that $g(\mathbf{x}A \oplus \mathbf{a}) \oplus \mathbf{b}\cdot\mathbf{x} \oplus \varepsilon = s_2(\mathbf{x})$, for all $\mathbf{x} \in \mathbb{F}_2^m$. Then $f(\mathbf{x}A \oplus \mathbf{a})$ is bent–negabent.*

Proof It is clear that $f(\mathbf{x}A \oplus \mathbf{a})$ is a bent function, for all $A \in GL(m, \mathbb{F}_2)$ and $\mathbf{a} \in \mathbb{F}_2^m$. Now, we show that $f(\mathbf{x}A \oplus \mathbf{a})$ is negabent, that is, $f(\mathbf{x}A \oplus \mathbf{a}) \oplus s_2(\mathbf{x})$ is bent. For $A \in GL(m, \mathbb{F}_2)$, $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m$, $\varepsilon \in \mathbb{F}_2$, since $f, g \in \mathcal{K}_m$ are quadratic bent–negabent functions, then,

$$\begin{aligned} f(\mathbf{x}) \oplus g(\mathbf{x}) \text{ is bent}, &\Leftrightarrow f(\mathbf{x}A \oplus \mathbf{a}) \oplus g(\mathbf{x}A \oplus \mathbf{a}) \text{ is bent},\\ &\Leftrightarrow f(\mathbf{x}A \oplus \mathbf{a}) \oplus g(\mathbf{x}A \oplus \mathbf{a}) \oplus \mathbf{b}\cdot\mathbf{x} \oplus \varepsilon \text{ is bent},\\ &\Leftrightarrow f(\mathbf{x}A \oplus \mathbf{a}) \oplus s_2(\mathbf{x}) \text{ is a bent function}, \end{aligned}$$

and so, we get the result. □

Remark 8 From Theorem 7, it is clear that for any quadratic bent–negabent function $f \in \mathcal{K}_m$, $f(\mathbf{x}A \oplus \mathbf{a})$ is bent–negabent where $\mathbf{a} \in \mathbb{F}_2^m$ and $A \in GL(m, \mathbb{F}_2)$, such that there exists a quadratic bent–negabent function $g \in \mathcal{K}_m$, $g \neq f$, with $g(\mathbf{x}A \oplus \mathbf{a}) \oplus \mathbf{b}\cdot\mathbf{x} \oplus \varepsilon = s_2(\mathbf{x})$, for all $\mathbf{x} \in \mathbb{F}_2^m$ and for some $\mathbf{b} \in \mathbb{F}_2^m$, $\varepsilon \in \mathbb{F}_2$. Conversely, if for a bent–negabent function g in $\mathcal{K}_m$, there exist $A \in GL(m, \mathbb{F}_2)$, $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m$ and $\varepsilon \in \mathbb{F}_2$ such that $g(\mathbf{x}A \oplus \mathbf{a}) \oplus \mathbf{b}\cdot\mathbf{x} \oplus \varepsilon = s_2(\mathbf{x})$, for all $\mathbf{x} \in \mathbb{F}_2^m$, then A is preserving the bent–negabent property for all bent–negabent functions in $\mathcal{K}_m$.

Next, we are going to identify the quadratic bent–negabent functions which do not belong to $\mathcal{K}_m \cup \overline{\mathcal{K}_m}$. In the rest of the paper we mainly work on the quadratic homogenous bent–negabent functions, i.e., affine free quadratic bent–negabent functions as we know that the bent–negabent property is invariant under addition of affine functions.

A matrix is said to be alternating if it is skew-symmetric. So for alternating matrices, the entries on the principal diagonal are all zero. Let $M_f = (m_{ij})_{m\times m}$ be a binary alternating matrix corresponding to an m-variable homogeneous quadratic Boolean function

$$f(\mathbf{x}) = \bigoplus_{1\le i<j\le m} c_{ij}x_ix_j,$$

where $m_{ij} = m_{ji} = c_{ij}$, if $i < j$, and $m_{ii} = 0$ for all $i = 1, 2, \ldots, m$.

It is known [8, Chapter 15] that a quadratic function $f \in \mathcal{B}_m$ is bent if and only if the binary alternating matrix M_f corresponding to the quadratic part of f is nonsingular, and Riera and Parker [12] proved that a quadratic function $f \in \mathcal{B}_m$ is negabent if and only if $M_f \oplus I_m$ is nonsingular, where I_m is an identity matrix of order m. Parker and Pott [10] later derived a necessary and sufficient condition on the matrix M_f for which f is bent–negabent, showing that f is bent–negabent if and only if M_f and $M_f \oplus I_m \oplus J_m$ both are nonsingular, where J_m is the $m \times m$ matrix all of whose entries are 1 (M_f is the alternating matrix corresponding to a homogeneous quadratic function $f \in \mathcal{B}_m$). We see that the condition in Parker and Pott's result simply says that the eigenvalues of M_f are $\neq 0$, and the eigenvalues of $\overline{M}_f$ (each entry is complemented) must be $\neq -1$ (we can also certainly express that same condition in terms of the strong regularity of the Cayley graphs associated to f and $f \oplus s_2$).

Example 9 Let $m = 4$, and M_f and M_g be two alternating matrices corresponding to $f(\mathbf{x}) = x_1x_2 \oplus x_3x_4$ and $g(\mathbf{x}) = x_1x_2 \oplus x_2x_3 \oplus x_1x_4$, respectively. Here, M_f and M_g both are nonsingular, but $M_f \oplus I_4 \oplus J_4$ is singular and $M_g \oplus I_4 \oplus J_4$ is nonsingular. Thus, g is bent–negabent, while f is bent but not negabent.

The number of homogeneous quadratic bent–negabent functions in m variables is the same as the number of binary alternating matrices M of order m such that M and $M \oplus I_m \oplus J_m$ (or $M \oplus I_m$) are both nonsingular. The total number of alternating binary matrices M of order m such that M and $M \oplus I_m \oplus J_m$ (or $M \oplus I_m$) are nonsingular was calculated in [11], thus solving the open problem proposed by Parker and Pott [10, Problem 2]. In [11], Pott et al. first counts the matrices M_1 and M_2 of order $m \times m$ with rank r and s, respectively, such that $M_1 \oplus M_2$ has rank k, where $0 \leq r, s, k \leq m$, and then derived the number of quadratic homogenous bent–negabent functions in m-variables in [11, Corollary 3].

Below, we will identify (construct) all the quadratic bent–negabent functions which do not belong to Kerdock code, and observe that the problem is related to the homogeneous bent–negabent codewords in the Kerdock code and the number of some nonsingular transformations satisfying some technical conditions (we will be more precise below).

Let m be an even positive integer. Any homogeneous quadratic Boolean functions $f \in \mathcal{B}_m$ can be written as

$$f(x_1, x_2, \ldots, x_m) = \bigoplus_{1 \leq i < j \leq m} c_{ij}x_ix_j = x_m \left(\bigoplus_{i=1}^{m-1} c_{im}x_i \right) \oplus \left(\bigoplus_{1 \leq i < j \leq m-1} c_{ij}x_ix_j \right),$$

for all $\mathbf{x} \in \mathbb{F}_2^m$ where $c_{ij} \in \mathbb{F}_2$, $1 \leq i < j \leq m$, and $\bigoplus_{i=1}^{m-1} c_{im}x_i$ and $\bigoplus_{1 \leq i < j \leq m-1} c_{ij}x_ix_j$ are linear and homogeneous quadratic function in $m-1$ variables $x_1, x_2, \ldots, x_{m-1}$, respectively. Let us assume that f is bent–negabent and set $c_i := c_{im} \in \mathbb{F}_2$, for all $1 \leq i \leq m-1$. Then $(c_1, c_2, \ldots, c_{m-1}) \notin \{(0, 0, \ldots, 0), (1, 1, \ldots, 1)\}$.

For easy writing, we denote $[1, m-1] := \{1, 2, \ldots, m-1\}$. For any proper subset $\emptyset \neq S \subset [1, m-1]$, we let

$$\mathcal{A}_S := x_m \left(\bigoplus_{i \in S} x_i \right) \oplus \mathcal{B}_S, \tag{4}$$

where $\mathcal{B}_S$ is the collection of all quadratic homogenous functions in the variables $x_1, x_2, \ldots, x_{m-1}$, such that all functions in $\mathcal{A}_S$ are bent–negabent. It is clear that $\mathcal{B}_S \neq \emptyset$, for all $\emptyset \neq S \subset [1, m-1]$, as each $\mathcal{A}_S$ contains exactly one homogeneous quadratic bent–negabent codeword in the Kerdock code $\mathcal{K}_m$. Also if S, T are two nonempty proper distinct subsets of $[1, m-1]$, then $\mathcal{A}_S \bigcap \mathcal{A}_T = \emptyset$.

Let $\mathcal{QBN}(m)$ be the set of all homogeneous quadratic bent–negabent functions in m variables. Then

$$\mathcal{QBN}(m) = \bigcup_{S \subset [1,m-1], S \neq \emptyset} \mathcal{A}_S,$$

where $\mathcal{A}_S$ is defined as in (4). For example, let $m = 4$, and so,

$$\begin{aligned}
\mathcal{A}_{\{1\}} &= x_4 x_1 \oplus \{x_1x_2 \oplus x_2x_3, x_1x_3 \oplus x_2x_3\},\\
\mathcal{A}_{\{2\}} &= x_4 x_2 \oplus \{x_1x_3 \oplus x_2x_3, x_1x_2 \oplus x_1x_3\},\\
\mathcal{A}_{\{3\}} &= x_4 x_3 \oplus \{x_1x_2 \oplus x_1x_3, x_1x_2 \oplus x_2x_3\},\\
\mathcal{A}_{\{1,2\}} &= x_4(x_1 \oplus x_2) \oplus \{x_1x_3, x_2x_3\},\\
\mathcal{A}_{\{1,3\}} &= x_4(x_1 \oplus x_3) \oplus \{x_2x_3, x_1x_2\},\\
\mathcal{A}_{\{2,3\}} &= x_4(x_2 \oplus x_3) \oplus \{x_1x_2, x_1x_3\}.
\end{aligned}$$

Here, the cardinality of each set is 2 (= 12/6). Also, for $m = 6$, computationally, we checked that the cardinality of $\mathcal{A}_S$ is equal to 192 (= 5760/30) where $\emptyset \neq S \subset [1, 5]$.

We will generalize the next lemma later on, but we believe providing the proof of this particular case gives better understanding of our constructive technique.

Lemma 10 *Let S_1 and S_2 be two nonempty proper subsets of $[1, m-1]$ with $|S_1| = |S_2| = r$, $1 \leq r \leq m-2$. Then $|\mathcal{A}_{S_1}| = |\mathcal{A}_{S_2}|$, where $\mathcal{A}_{S_j}$ are defined as in (4), $j = 1, 2$.*

Proof Let $S_1 = \{i_1, i_2, \ldots, i_r\}$, $S_2 = \{j_1, j_2, \ldots, j_r\} \subset [1, m-1]$, with $1 \leq r \leq m-2$ and $f \in \mathcal{A}_{S_1}$. Then f can be written as

$$f(\mathbf{x}) \in x_m(x_{i_1} \oplus x_{i_2} \oplus \ldots \oplus x_{i_r}) \oplus \mathcal{B}_{S_1},$$

for all $\mathbf{x} \in \mathbb{F}_2^m$ and $\mathcal{B}_{S_1}$ is defined as in (4). Let $A \in SL(m, \mathbb{F}_2)$ be an orthogonal matrix that maps $x_{i_t} = x_{j_t}$, for all $t = 1, 2, \ldots, r$, and so, $f(\mathbf{x}A) \in \mathcal{A}_{S_2}$. Again, it is clear that if $f, g \in \mathcal{A}_{S_1}$ with $f \neq g$ then $f(\mathbf{x}A) \neq g(\mathbf{x}A)$, otherwise $f(\mathbf{x}A) = g(\mathbf{x}A)$, implying $f = g$, which is a contradiction. We apply the same linear transformation A over $\mathcal{A}_{S_1}$, and we get the set $\mathcal{A}_{S_2}$. □

Remark 11 Let $S = \{i_1, i_2, \ldots, i_r\} \subset [1, m-1]$ with $1 \leq r \leq m-2$ and $f \in \mathcal{A}_S$. Since f is bent–negabent, then $f \oplus s_2$ is also bent–negabent and

$$f(\mathbf{x}) \oplus s_2(\mathbf{x}) \in x_m \left(\bigoplus_{i \in [1,m-1] \setminus S} x_i \right) \oplus \mathcal{B}_{[1,m-1]\setminus S},$$

that is, $f \oplus s_2 \in \mathcal{A}_{[1,m-1]\setminus S}$. Consequently, if S is a proper nonempty subset of $[1, m-1]$, then the cardinalities of $\mathcal{A}_S$ and $\mathcal{A}_{[1,m-1]\setminus S}$ are equal.

Thus, for an even m, if we know all the elements of $\mathcal{A}_{\{1\}}, \mathcal{A}_{\{1,2\}}, \ldots, \mathcal{A}_{\{1,2,\ldots,\frac{m}{2}-1\}}$, then using Lemma 10 and Remark 11 we can construct all homogeneous quadratic bent–negabent functions in m variables.

Proposition 12 *If $m \geq 4$, then*

$$|\mathcal{QBN}(m)| = 2 \sum_{j=1}^{\frac{m}{2}-1} \binom{m-1}{j} \left| \mathcal{A}_{\{1,2,\ldots,j\}} \right|.$$

For example let $m = 4$, $|\mathcal{QBN}(4)| = 2 \times 3|\mathcal{A}_{\{1\}}| = 12$, and for $m = 6$, $|\mathcal{QBN}(6)| = 2(5|\mathcal{A}_{\{1\}}| + 10|\mathcal{A}_{\{1,2\}}|) = 5760$.

Now, we construct all functions in $\mathcal{A}_S$ from the known Kerdock codewords that belong to this set. Let $\emptyset \neq S \subset [1, m-1]$ and define a set of nonsingular binary matrices $\mathcal{N}_S$ in the following way: $A \in \mathcal{N}_S$ if and only if $A \in GL(m, \mathbb{F}_2)$ and the quadratic term involving x_m in $f(\mathbf{x}A)$ is $x_m \left(\bigoplus_{i \in S} x_i \right)$, where $f \in \mathcal{K}_m \bigcap \mathcal{A}_S$. Let m be an even positive integer and $\mathcal{A}_{\{i\}}$, $1 \leq i \leq m-1$, be the set of homogeneous quadratic bent–negabent functions defined as in (4). Thus, if $f \in \mathcal{A}_{\{i\}}$, also belongs to the Kerdock code $\mathcal{K}_m$, then $f(\mathbf{x}) \in x_m x_i \oplus \mathcal{B}_{\{i\}}$, for all $\mathbf{x} \in \mathbb{F}_2^m$. For $A \in \mathcal{N}_{\{i\}}$, if the quadratic part of $f(\mathbf{x}A)$, say $g(\mathbf{x})$, is bent–negabent, then $g \in \mathcal{A}_{\{i\}}$. Therefore,

$$\mathcal{A}_{\{i\}} = \{g \in \mathcal{B}_m : g(\mathbf{x}) \text{ is the bent–negabent quadratic part of } f(\mathbf{x}A), \\ A \in \mathcal{N}_{\{i\}}, \mathbf{x} \in \mathbb{F}_2^m\}.$$

For example, for $m = 4$ and $S = \{1\}$, the corresponding Kerdock codeword is $f(\mathbf{x}) = x_4x_1 \oplus x_1x_2 \oplus x_2x_3$, $\mathbf{x} \in \mathbb{F}_2^4$. We apply all nonsingular transformations A on f such that x_1 and x_4 are fixed and $f(\mathbf{x}A)$ is bent–negabent. Then $f(\mathbf{x}A)$ belongs to $\mathcal{A}_{\{1\}}$. We get two functions in $\mathcal{A}_{\{1\}}$ by applying two orthogonal transformations on f: one is the identity transformation I_4 and the other one is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

In the next theorem, we generalize this concept for any proper nonempty subset $S \subset [1, m-1]$.

Theorem 13 *Let m be an even positive integer and $f \in \mathcal{K}_m \cap \mathcal{A}_S$ where $\mathcal{A}_S$ is defined as in (4), $S = \{i_1, i_2, \ldots, i_r\} \subset [1, m-1]$ with $1 \le r \le m-2$. Then*

$$\mathcal{A}_S = \{g \in \mathcal{B}_m : g(\mathbf{x}) \text{ is the bent–negabent quadratic part of } f(\mathbf{x}A), \\ A \in \mathcal{N}_S, \mathbf{x} \in \mathbb{F}_2^m\}.$$

Thus, the cardinality of $\mathcal{A}_S$, $\emptyset \neq S \subset [1, m-1]$ is the same as the minimum number of distinct nonsingular linear transformations $A \in \mathcal{N}_S$ such that the quadratic part of $f(\mathbf{x}A)$ is bent–negabent and distinct for different A's, that is, if $A, B \in \mathcal{N}_S$ are any two such nonsingular linear transformations, then the quadratic part of $f(\mathbf{x}A)$ and $f(\mathbf{x}B)$ are distinct bent–negabent functions, where $f \in \mathcal{K}_m \cap \mathcal{A}_S$.

Next, we are going to find the cardinalities of $\mathcal{A}_S$ and $\mathcal{A}_T$, when S and T are nonempty proper subsets of $[1, m-1]$ such that $1 \le |S| \neq |T| \le \frac{m}{2} - 1$. Let S be a proper subset of $[1, m-1]$ and the set $\mathcal{BM}_S$ be defined in the following way: all $M \in \mathcal{BM}_S$ are alternating binary nonsingular matrices of order m with diagonal zero, where the mth column of $M \in \mathcal{BM}_S$ is $x_{im} = \begin{cases} 1, & \text{if } i \in S; \\ 0, & \text{if } i \in [1, m-1] \backslash S. \end{cases}$

Theorem 14 *Let $\mathcal{A}_S$ and $\mathcal{A}_T$ be defined as in (4), where S and T are nonempty proper subsets of $[1, m-1]$ such that $1 \le |S| \neq |T| \le \frac{m}{2} - 1$. Then $|\mathcal{A}_S| = |\mathcal{A}_T|$.*

Proof If $f \in \mathcal{A}_S$ (or $\mathcal{A}_T$), the corresponding alternating binary matrix $M_f \in \mathcal{BM}_S$ (or $\mathcal{BM}_T$) as well as $M_f \oplus I_m$ are also nonsingular (see [12]). Suppose P is a nonsingular matrix constructed by elementary row operations such that it maps x_m^s to x_m^t. Define a mapping $\phi : \mathcal{BM}_S \longrightarrow \mathcal{BM}_T$ such that $\phi(M) = PMP^T$, for all $M \in \mathcal{BM}_S$. It is clear that ϕ is well defined, $\det(PMP^T) \neq 0$ and bijective, so $|\mathcal{BM}_S| = |\mathcal{BM}_T|$. Then it is sufficient to prove that $P(M_f \oplus I_m)P^T = PM_fP^T \oplus I_m$ is also nonsingular. The eigenvalues of $M_f \oplus I_m$ and $PM_fP^T \oplus I_m$ are equal, since

$$\begin{aligned} det(PM_fP^T \oplus I_m - xI_m) &= det(P(M_f \oplus I_m - xI_m)P^T) \\ &= det(M_f \oplus I_m - xI_m), \end{aligned}$$

and the theorem is shown. □

From Proposition 12 and Theorem 14, we get the next corollary, which shows that the total number of quadratic bent–negabent functions is a multiple of $|\mathcal{A}_{\{1\}}|$, where $\mathcal{A}_{\{1\}}$ was constructed by using the Kerdock code $\mathcal{K}_m$ [see Eq. (4)].

Corollary 15 *The number of quadratic homogeneous bent–negabent functions in m variables is equal to $(2^{m-1} - 2)\left|\mathcal{A}_{\{1\}}\right|$, where $\mathcal{A}_{\{1\}}$ is defined as in (4).*

Proof By Proposition 12 , $|\mathcal{QBN}(m)| = 2\sum_{j=1}^{\frac{m}{2}-1} \binom{m-1}{j} \left|\mathcal{A}_{\{1,2,\ldots,j\}}\right|$, and since $\left|\mathcal{A}_{\{1,2,\ldots,j\}}\right| = \left|\mathcal{A}_{\{1,2,\ldots,i\}}\right|$, for all i, j, by Theorem 14, then $\left|\mathcal{A}_{\{1,2,\ldots,j\}}\right| = \mathcal{A}_{\{1\}}$, which implies the corollary, using the identity $\sum_{j=1}^{\frac{m}{2}-1} \binom{m-1}{j} = 2^{m-2} - 1$. □

The cardinality of the bent–negabent property preserving subset of $\mathcal{N}_{\{1\}}$ does not give us the cardinality of $\mathcal{A}_{\{1\}}$, as it may possible be the case that two distinct elements of

$\mathcal{N}_{\{1\}}$ give us bent–negabent functions with the same quadratic part. For example, let $m = 4$ and $f \in \mathcal{K}_4 \bigcap \mathcal{A}_{\{1\}}$ of the form $f(\mathbf{x}) = x_1x_4 \oplus x_1x_2 \oplus x_2x_3$. Suppose

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then $f(\mathbf{x}A) = x_1x_4 \oplus x_1x_2 \oplus x_2x_3 \oplus x_2$, so the quadratic parts of $f(\mathbf{x}I_4)$ and $f(\mathbf{x}A)$ are the same.

Let r and j be any real number and nonnegative integer, respectively. The 2^2-binomial coefficient is defined as

$$\begin{bmatrix} r \\ j \end{bmatrix} = \prod_{i=1}^{j} \frac{2^{2r-2i+2} - 1}{2^{2i} - 1} \tag{5}$$

with $\begin{bmatrix} r \\ 0 \end{bmatrix} = 1$. For more details on these coefficients, we refer to [1,4]. In [11, Corollary 3], Pott et al. proved (non-constructively) that the number of all homogeneous quadratic bent–negabent functions in $m = 2n$ variables is equal to

$$|\mathcal{QBN}(2n)| = \frac{1}{2^n}\left(\sum_{j=0}^{n-1}(-1)^j 2^{j(j-1)} \begin{bmatrix} n \\ j \end{bmatrix} \prod_{r=1}^{n-j}(2^{2r-1} - 1)^2 + (-1)^n 2^{n(n-1)}\right).$$

From [11, Corollary 3] and Corollary 15, we derive the cardinality of $\mathcal{A}_{\{1\}}$ (or equivalently $\mathcal{A}_S$ for any nonempty proper subset S of $[1, m-1]$), and we get the next result.

Corollary 16 *The cardinality of $\mathcal{A}_{\{1\}}$ is*

$$\frac{1}{2^n(2^{m-1} - 2)}\left(\sum_{j=0}^{n-1}(-1)^j 2^{j(j-1)} \begin{bmatrix} n \\ j \end{bmatrix} \prod_{r=1}^{n-j}(2^{2r-1} - 1)^2 + (-1)^n 2^{n(n-1)}\right),$$

where $\begin{bmatrix} n \\ j \end{bmatrix}$ is defined as in (5).

3 Bent–negabent preserving transformations

From [14, Theorem 2] we know that the bent–negabent property of a Boolean function $f \in \mathcal{B}_m$ is invariant under the action of the orthogonal group $SL(m, \mathbb{F}_2)$. Here, we extend this invariant space. Let A^T be the transpose of a matrix A.

Lemma 17 *A linear transformation $A \in GL(m, \mathbb{F}_2)$ is weight invariant if and only if $A \in SL(m, \mathbb{F}_2)$.*

Proof We know that $wt(\mathbf{x}) = \mathbf{x}I_m\mathbf{x}^T$, for all $\mathbf{x} \in \mathbb{F}_2^m$ where I_m is an identity matrix of order m. Let $A \in SL(m, \mathbb{F}_2)$. Then $wt(\mathbf{x}A) = (\mathbf{x}A)I_m(\mathbf{x}A)^T = \mathbf{x}(AA^T)\mathbf{x}^T = \mathbf{x}I_m\mathbf{x}^T = wt(\mathbf{x})$, for all $\mathbf{x} \in \mathbb{F}_2^m$. Suppose $A \in GL(m, \mathbb{F}_2)$ such that $wt(\mathbf{x}) = wt(\mathbf{x}A)$, for all $\mathbf{x} \in \mathbb{F}_2^m$. Then

$$\mathbf{x}I_m\mathbf{x}^T = (\mathbf{x}A)I_m(\mathbf{x}A)^T \quad \Leftrightarrow \quad \mathbf{x}I_m\mathbf{x}^T = \mathbf{x}(AA^T)\mathbf{x}^T \quad \Leftrightarrow \quad \mathbf{x}(I_m \oplus AA^T)\mathbf{x}^T = 0,$$

which holds for all $\mathbf{x} \in \mathbb{F}_2^m$ only when $I_m = AA^T$, that is, $A \in SL(m, \mathbb{F}_2)$. □

Note that if $A \in SL(m, \mathbb{F}_2)$ is weight invariant then $A^{-1} = A^T$ is also weight invariant.

Proposition 18 *Let $\lambda \geq 1$ be an arbitrary positive integer and $\mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda)$ be the set of all nonsingular linear transformation of $GL(m, \mathbb{F}_2)$ defined by*

$$\begin{aligned}\mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda) = \{&A \in GL(m, \mathbb{F}_2) : wt(\mathbf{x}) \\ &\equiv wt(\mathbf{x}A) \pmod{4\lambda}, \text{ for all } \mathbf{x} \in \mathbb{F}_2^m\}.\end{aligned}$$

Then $\mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda)$ forms a subgroup of $GL(m, \mathbb{F}_2)$.

Proof For all $\lambda \geq 1$, it is clear that $SL(m, \mathbb{F}_2) \subseteq \mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda)$, so $\mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda) \neq \emptyset$. To show that $\mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda)$ forms a subgroup of $GL(m, \mathbb{F}_2)$ it is enough to show closure under multiplication, as well as under taking inverses. If $A, B \in \mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda)$, then, for all $\mathbf{x}$, $wt(\mathbf{x}) \equiv wt(\mathbf{x}A) \equiv wt(\mathbf{x}AB) \pmod{4\lambda}$, and $wt(\mathbf{x}A^{-1}) \equiv wt(\mathbf{x}A^{-1}A) = wt(\mathbf{x}) \pmod{4\lambda}$, hence the claim is shown. □

We had mentioned that $SL(m, \mathbb{F}_2) \subseteq \mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda)$, $\lambda \geq 1$, but the converse is not true in general, for $m \geq 6$. For $m = 4$, $SL(4, \mathbb{F}_2) = \mathcal{NLT}_{inv}(4, \mathbb{F}_2, 1)$.

Proposition 19 *Let λ_1 and λ_2 be two positive integers such that $\lambda_1 \mid \lambda_2$. Then $\mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda_2) \subseteq \mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda_1)$.*

Proof Let $A \in \mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda_2)$. Then $wt(\mathbf{x}) \equiv wt(\mathbf{x}A) \pmod{4\lambda_2}$, for all $\mathbf{x} \in \mathbb{F}_2^m$, i.e., $wt(\mathbf{x}) - wt(\mathbf{x}A) = 4\lambda_2 t$, for all $\mathbf{x} \in \mathbb{F}_2^m$ and for some positive integer t, and so $wt(\mathbf{x}) - wt(\mathbf{x}A) \equiv 0 \pmod{4\lambda_1}$, for all $\mathbf{x} \in \mathbb{F}_2^m$. □

From Proposition 19, it is clear that for any positive integer $\lambda \geq 1$, $\mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda) \subseteq \mathcal{NLT}_{inv}(m, \mathbb{F}_2, 1)$. In the next result, we prove that all the sets $\mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda)$, defined as in Proposition 18, preserve the bent–negabent property.

Theorem 20 *Let m, λ be positive integers, where m is even. Suppose $f, g \in \mathcal{B}_m$ such that f is bent–negabent and $g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{a}) \oplus \mathbf{b} \cdot \mathbf{x} \oplus \varepsilon$, for all $\mathbf{x} \in \mathbb{F}_2^m$, where $A \in GL(m, \mathbb{F}_2)$, $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m$ and $\varepsilon \in \mathbb{F}_2$. If $A \in \mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda)$, then g is bent–negabent.*

Proof From [10, Lemma 2] and [15, Theorem 2], we know that $g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{a}) \oplus \mathbf{b} \cdot \mathbf{x} \oplus \varepsilon$ is bent–negabent if and only if $f(\mathbf{x}A)$ is bent–negabent. Since $f(\mathbf{x}A)$ is bent

for all $A \in GL(m, \mathbb{F}_2)$, it is therefore sufficient to prove that $f(\mathbf{x}A)$ is negabent when $A \in \mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda)$. Observe that if $A \in \mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda)$, then $B = A^{-1} \in \mathcal{NLT}_{inv}(m, \mathbb{F}_2, \lambda)$. Further, $\imath^{wt(\mathbf{x})} = \imath^{wt(\mathbf{x}B)}$, for all $\mathbf{x} \in \mathbb{F}_2^m$, and so,

$$\begin{aligned} 2^{-\frac{m}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^m} (-1)^{f(\mathbf{x}A)\oplus \mathbf{u}\cdot\mathbf{x}} \imath^{wt(\mathbf{x})} &= 2^{-\frac{m}{2}} \sum_{\mathbf{y}\in\mathbb{F}_2^m} (-1)^{f(\mathbf{y})\oplus \mathbf{u}\cdot\mathbf{y}B} \imath^{wt(\mathbf{y}B)} \\ &= 2^{-\frac{m}{2}} \sum_{\mathbf{y}\in\mathbb{F}_2^m} (-1)^{f(\mathbf{y})\oplus \mathbf{u}B^T\cdot\mathbf{y}} \imath^{wt(\mathbf{y})} = \mathcal{N}_f(\mathbf{u}B^T), \end{aligned}$$

therefore, $f(\mathbf{x}A)$ is bent–negabent. □

The converse of the claim in Theorem 20 is not true in general, and we provide such counterexample for any positive integer m (even) and $\lambda = 1$. We can construct a class of nonsingular and non-orthogonal linear transformations that preserve the bent–negabent property for a special subset of quadratic bent–negabent functions, by considering the partition of quadratic bent–negabent functions defined as in (4).

Theorem 21 *For $m \geq 2$ and $1 \leq k \leq m-1$ a positive integer, let $f \in x_k x_m \oplus \mathcal{B}_{\{k\}}$, where $\mathcal{B}_{\{k\}}$ is defined as in (4). Then there exist a matrix $A \in GL(m, \mathbb{F}_2)$, non-orthogonal, with $A \notin \mathcal{NLT}_{inv}(m, \mathbb{F}_2, 1)$, such that $f(\mathbf{x}A)$ is bent–negabent. Furthermore, let A such a matrix, and $B \in \mathcal{NLT}_{inv}(m, \mathbb{F}_2, 1)$. Then $AB \notin \mathcal{NLT}_{inv}(m, \mathbb{F}_2, 1)$ and $f(\mathbf{x}AB)$ is bent–negabent.*

Proof Let $f \in x_k x_m \oplus \mathcal{B}_{\{k\}}$, where $\mathcal{B}_{\{k\}}$ is defined as in (4). Suppose $A = (a_{ij})_{m\times m}$, where $a_{km} = 1$, $a_{ii} = 1$ for all $i = 1, 2, \ldots, m$, and $a_{ij} = 0$, otherwise. It is clear that A is nonsingular and also non-orthogonal since $AA^T \neq I_m$. Further, for any $\mathbf{x} \in \mathbb{F}_2^m$,

$$\mathbf{x}A = (x_1, x_2, \ldots, x_{m-1}, x_m)A = (x_1, x_2, \ldots, x_{m-1}, x_m \oplus x_k),$$

and so $f(\mathbf{x}A) = f(\mathbf{x}) \oplus x_k$ for all $\mathbf{x} \in \mathbb{F}_2^m$, which is a bent–negabent function. Let $\mathbf{e}_i \in \mathbb{F}_2^m$ such that ith position is 1 and the other positions are equal to 0, $1 \leq i \leq m$. Then $\mathbf{e}_k A = \mathbf{e}_k \oplus \mathbf{e}_m$, and so $A \notin \mathcal{NLT}_{inv}(m, \mathbb{F}_2, 1)$.

For the second claim, we use the fact that, by the first claim, $f(\mathbf{y})$ (with $\mathbf{y} = \mathbf{x}A$) is bent–negabent, and so, $f(\mathbf{y}B)$ is bent–negabent via the definition of $\mathcal{NLT}_{inv}(m, \mathbb{F}_2, 1)$. Also, $AB \notin \mathcal{NLT}_{inv}(m, \mathbb{F}_2, 1)$, since, $\mathcal{NLT}_{inv}(m, \mathbb{F}_2, 1)$ is a group by Proposition 18. □

As an example of Theorem 21, let $m = 6$ and $f \in x_2x_6 \oplus \mathcal{B}_{\{2\}}$ of the form $f(x_1, x_2, \ldots, x_6) = x_2x_6 \oplus x_1x_3 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_3 \oplus x_3x_4$. Suppose

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

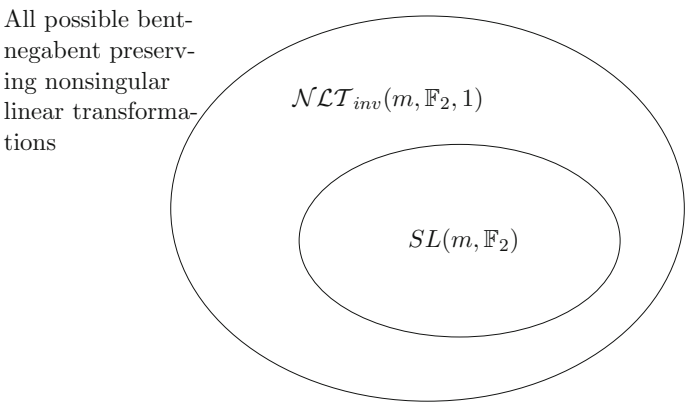

Fig. 1 Bent–negabent preserving nonsingular linear transformations

Then A is nonsingular (as $\det(B) \neq 0$), non-orthogonal (as $AA^T \neq I_6$), and $f((x_1, x_2, \ldots, x_6)A) = x_2x_6 \oplus x_1x_3 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_3 \oplus x_3x_4 \oplus x_2$, which is a bent–negabent function, but, $A \notin \mathcal{NLT}_{inv}(6, \mathbb{F}_2, 1)$ as $(0, 1, 0, 0, 0, 0)A = (0, 1, 0, 0, 0, 1)$.

4 Conclusion

In this paper, we first show that all quadratic Kerdock codewords in $\mathcal{K}_m$, except the coset of the symmetric quadratic bent function, are bent–negabent. Next, we construct $2^{m-1} - 2$ disjoint sets of quadratic bent–negabent functions (homogeneous) for each quadratic bent–negabent Kerdock codeword. We also show that the cardinalities of each of these disjoint sets are the same and that their union is the set of all quadratic bent–negabent functions (affine free) in m variables. Further, we find that there are nonsingular transformations which are non-orthogonal transformations preserving the bent–negabent property.

Acknowledgements The authors would like to thank the reviewers for extraordinarily useful criticisms and suggestions, and for providing us with a better code of Fig. 1. The paper was partly written while the first author visited the second and third authors at the Indian Statistical Institute, Kolkata. He would like to thank the hosts and the institute for hospitality and excellent working conditions.

References

1. Andrews, G.E.: The Theory of Partitions. Encyclopedia of Mathematics and its Applications, vol. 2. Cambridge University Press, Cambridge (1976)
2. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P. (eds.) Boolean Methods and Models, pp. 257–397. Cambridge University Press, Cambridge (2010)
3. Dillon, J.F.: A survey of bent functions. NSA Tech. J. (Special Issue) **191**, 215 (1972)
4. Delsarte, P., Goethals, J.M.: Alternating bilinear forms over $GF(q)$. J. Combin. Theory Ser. A **19**, 26–50 (1975)

5. Hu, H., Feng, D.: On quadratic bent functions in polynomial forms. IEEE Trans. Inf. Theory **53**(7), 2610–2615 (2007)
6. Kerdock, A.M.: A class of low-rate nonlinear binary codes. Inf. Control **20**(2), 182–187 (1972)
7. van Lint, J.H.: Kerdock codes and Preparata codes. Congressus Numerantium **39**, 25–41 (1983)
8. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
9. Mykkeltveit, J.: A note on Kerdock codes. JPL Technical Report 32-1526, pp. 82–83
10. Parker, M.G., Pott, A.: On Boolean functions which are bent and negabent. In: Golomb, S.W., Gong, G., Helleseth, T., Song, H.Y. (eds) Sequences, Subsequences, and Consequences, International Workshop, SSC 2007 LNCS, vol. 4893, pp. 9–23 (2007)
11. Pott, A., Schmidt, K.-U., Zhou, Y.: Pairs of quadratic forms over finite fields. Electron. J. Comb. **23**(2), P2.8 (2016)
12. Riera, C., Parker, M.G.: Generalized bent criteria for Boolean functions. IEEE Trans. Inf. Theory **52**(9), 4142–4159 (2006)
13. Rothaus, O.S.: On bent functions. J. Combin. Theory Ser. A **20**, 300–305 (1976)
14. Schmidt, K.-U., Parker, M.G., Pott, A.: Negabent functions in Maiorana–McFarland class. In: SETA 2008, LNCS, vol. 5203, pp. 390–402 (2008)
15. Stănică, P., Gangopadhyay, S., Chaturvedi, A., Gangopadhyay, A.K., Maitra, S.: Investigations on bent and negabent functions via the nega–Hadamard transform. IEEE Trans. Inf. Theory **58**(6), 4064–4072 (2012)
16. Su, W., Pott, A., Tang, X.: Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree. IEEE Trans. Inf. Theory **59**(6), 3387–3395 (2013)
17. Yu, N.Y., Gong, G.: Constructions of quadratic bent functions in polynomial forms. IEEE Trans. Inf. Theory **52**(7), 3291–3299 (2006)
18. Zhang, F., Wei, Y., Pasalic, E.: Constructions of bent–negabent functions and their relation to the completed Maiorana–McFarland class. IEEE Trans. Inf. Theory **61**(3), 1496–1506 (2015)