Equivalence for negabent functions and their relative difference sets

Nurdagül Anbar[1,2], Wilfried Meidl[1,3], Alexander Pott[1]

[1]Otto-von-Guericke University Magdeburg,
Universitätsplatz 2, 39106 Magdeburg, Germany
[2]Johannes Kepler Universität Linz,
Altenbergerstrasse 69, 4040-Linz, Austria
[3]Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria

August 2, 2018

Abstract

A bent function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, n even, can be transformed into a negabent function, or slightly more general into a bent$_4$, also called shifted bent function, by adding a certain quadratic term. If n is odd, then negabent functions similarly correspond to semibent functions with some additional property. Whereas bent functions induce relative difference sets in $\mathbb{F}_2^n \times \mathbb{F}_2$, negabent functions induce relative difference sets in $\mathbb{F}_2^{n-1} \times \mathbb{Z}_4$. We analyse equivalence of negabent functions respectively of their relative difference sets. We show that equivalent bent functions can correspond to inequivalent negabent functions, hence one can obtain inequivalent relative difference sets in $\mathbb{F}_2^{n-1} \times \mathbb{Z}_4$ with EA-equivalence. We also show that this is not the case when n is odd. Finally we analyse the class of semibent functions that corresponds to negabent functions and show that though partially bent semibent functions always can be shifted to negabent or bent$_4$ functions, there are many semibent functions which do not correspond to negabent and bent$_4$ functions.

1 Introduction

Let f be a function from an n-dimensional vector space V_n over $\mathbb{F}_2$ to $\mathbb{F}_2$. The *Walsh transform* of f is the function

$$\mathcal{W}_f(u) = \sum_{x \in V_n} (-1)^{f(x)+\langle u,x \rangle},$$

where $\langle u, x\rangle$ is a (nondegenerate) inner product in V_n. If $V_n = \mathbb{F}_2^n$, we will always use the conventional dot product, if $V_n = \mathbb{F}_{2^n}$, we take $\langle u, x\rangle = \mathrm{Tr_n}(ux)$ as an inner product, where $\mathrm{Tr_n}(z)$ denotes the absolute trace of $z \in \mathbb{F}_{2^n}$.

The function f is called a *bent function* if $|\mathcal{W}_f(u)| = 2^{n/2}$ for all $u \in V_n$. Equivalently, f is bent if $f(x) + f(x + a)$ is balanced for all nonzero $a \in V_n$. Clearly, bent functions only can exist when n is even. For n odd, a function $V_n \to \mathbb{F}_2$ is called *semibent* if $\mathcal{W}_f(u) \in \{0, \pm 2^{(n+1)/2}\}$ for all $u \in V_n$.

In a combinatorial interpretation, a bent function is a relative difference set in the elementary abelian group. Recall that a k-elementary subset R of a group G of order mn with a normal subgroup N of order n is called an (m, n, k, λ)-*relative difference set* relative to N, if every element in $G \setminus N$ can be written as a difference of two elements of R in λ ways and there is no such representation for nonzero elements of N. The subgroup N is then also called the forbidden subgroup. Let now f be a Boolean function from V_n to $\mathbb{F}_2$, then f is bent if and only if the graph $\{(x, f(x)) : x \in V_n\}$ of f is a $(2^n, 2, 2^n, 2^{n-1})$-relative difference in the elementary abelian group $V_n \times \mathbb{F}_2$ with forbidden subgroup $\{0\} \times \mathbb{F}_2$ (this is both easy to see and well known).

Closely related to bent functions, and when n is odd to semibent functions, are negabent functions, or, slightly more general, bent$_4$ functions. Negabent and bent$_4$ functions induce relative difference sets, but in the group $\mathbb{F}_2^{n-1} \times \mathbb{Z}_4$, as follows:
Let B be a nonalternating bilinear form from $V_n \times V_n$ to $\mathbb{F}_2$. Consider $G := (V_n \times \mathbb{F}_2, *)$, where "$*$" is defined by $(x_1, y_1) * (x_2, y_2) := (x_1 + x_2, y_1 + y_2 + B(x_1, x_2))$ for any $(x_1, y_1), (x_2, y_2) \in V_n \times \mathbb{F}_2$. Then G is a group, which is isomorphic to $\mathbb{F}_2^{n-1} \times \mathbb{Z}_4$, see [12]. For instance one may obtain B from a nonalternating bilinear form $\mathcal{B}$ from $V_n \times V_n$ to V_n with an inner product $\langle , \rangle$ in V_n as $B(x_1, x_2) = \langle c, \mathcal{B}(x_1, x_2)\rangle$ for every nonzero $c \in V_n$. A natural solution is to choose $\mathcal{B}(x_1, x_2) = x_1 x_2$ if $V_n = \mathbb{F}_{2^n}$ and $\mathcal{B}(x_1, x_2) = x_1 \odot x_2$ if $V_n = \mathbb{F}_2^n$, where $u \odot v = (u_1 v_1, \ldots, u_n v_n)$ for $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$, see [22]. Hence we may represent the group $\mathbb{F}_2^{n-1} \times \mathbb{Z}_4$ as $G_c := (\mathbb{F}_{2^n} \times \mathbb{F}_2, *_c)$, respectively $G_c := (\mathbb{F}_2^n \times \mathbb{F}_2, *_c)$, where "$*_c$" is defined by

$$(x_1, y_1) *_c (x_2, y_2) := (x_1 + x_2, y_1 + y_2 + \langle c^2, x_1 x_2\rangle) \tag{1.1}$$

for any $(x_1, y_1), (x_2, y_2) \in \mathbb{F}_{2^n} \times \mathbb{F}_2$, respectively by

$$(x_1, y_1) *_c (x_2, y_2) := (x_1 + x_2, y_1 + y_2 + \langle c, x_1 \odot x_2\rangle) \tag{1.2}$$

for any $(x_1, y_1), (x_2, y_2) \in \mathbb{F}_2^n \times \mathbb{F}_2$. For technical reasons, in the univariate case we use c^2 instead of c in accordance with [1]. The graph of a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, respectively $f : \mathbb{F}_2^n \to \mathbb{F}_2$, is then a $(2^n, 2, 2^n, 2^{n-1})$-relative difference set in G_c with forbidden subgroup $\{0\} \times \mathbb{F}_2$ if

$$f(x) + f(x + a) + \langle c^2, ax\rangle, \quad \text{respectively} \quad f(x) + f(x + a) + \langle c, a \odot x\rangle, \tag{1.3}$$

is balanced for all nonzero a. Again, this is not difficult to see using

$$(x, y)^{-1} = (x, y + \langle c^2, x^2 \rangle), \quad \text{respectively} (x, y)^{-1} = (x, y + \langle c, x \odot x \rangle).$$

If we choose the conventional dot product for $\mathbb{F}_2^n$, and for $\mathbb{F}_{2^n}$ the standard inner product $\langle u, v \rangle = \mathrm{Tr_n}(uv)$, then the Boolean functions satisfying (1.3) are the multivariate bent$_4$ functions defined as in [8], respectively the univariate bent$_4$ functions defined as in [1]. Specifying c we also use the notation c-bent$_4$. Recall that then c-bent$_4$ functions are called *negabent* when $c = \mathbf{1} = (1, 1, \ldots, 1) \in \mathbb{F}_2^n$, respectively $c = 1 \in \mathbb{F}_{2^n}$.

We remark that the component functions of modified planar functions defined in multivariate and in univariate form as in [22], are exactly bent$_4$ functions defined as above. Recall that modified planar functions were introduced for the purpose of representing $(2^n, 2^n, 2^n, 1)$-relative difference sets in the group $(\mathbb{Z}_4^n, +)$. This group can be represented on the set $\mathcal{G} = V_n \times V_n$, as $(\mathcal{G}, *)$ where "$*$" is defined by

$$(x_1, y_1) * (x_2, y_2) := (x_1 + x_2, y_1 + y_2 + \mathcal{B}(x_1, x_2)) \tag{1.4}$$

for a nonalternating bilinear form $\mathcal{B}$ from $V_n \times V_n$ to V_n. In [22], modified planar functions are defined to describe $(2^n, 2^n, 2^n, 1)$ relative difference sets in the group $\mathcal{G}$ with the natural choice $\mathcal{B}(x_1, x_2) = x_1 x_2$, respectively $\mathcal{B}(x_1, x_2) = x_1 \odot x_2$.

Note that whereas all bilinear forms $B(x_1, x_2) = \mathrm{Tr_n}(c^2 x_1 x_2)$, $c \in \mathbb{F}_{2^n}^*$, are nondegenerate, for the bilinear forms $B(x_1, x_2) = c \cdot (x_1 \odot x_2)$, nonzero $c \in \mathbb{F}_2^n$, this only applies for $c = \mathbf{1}$. Hence, under some aspects, multivariate bent$_4$ functions behave different than univariate bent$_4$ functions. For instance, every univariate affine function is c-bent$_4$ for every nonzero c, whereas a multivariate affine function is not c-bent$_4$ for any c different from $\mathbf{1}$, see [1] for the details. Solely the negabent functions in multivariate form can be obtained from those in univariate form choosing a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

Both, univariate and multivariate bent$_4$ functions are closely related to bent, respectively semibent functions. If n is even, then a bent$_4$ function is a bent function shifted by a quadratic term. If n is odd, then bent$_4$ functions are shifted to a subclass of semibent functions, see Lemma 2.2 and 2.3 in Section 2.

In this article we investigate equivalence of negabent, or more general of bent$_4$ functions, in two different aspects. In the first interpretation we regard two negabent functions as equivalent if the corresponding relative difference sets are equivalent in the conventional sense. The second concept uses the correspondence between negabent functions and bent, respectively semibent functions. We may call two negabent functions *shifted equivalent* if their corresponding bent functions (semibent functions) are EA-equivalent. After recalling some preliminaries in Section 2, we analyse equivalence for negabent functions in Section 3. Section 4 deals with the case

that n is even. We show that equivalence of negabent functions implies shifted equivalence, i.e. EA-equivalence of the corresponding bent functions, but conversely, two EA-equivalent bent functions can induce inequivalent relative difference sets in $\mathbb{F}_2^{n-1} \times \mathbb{Z}_4$. In Section 5 we show that the situation is different for odd n, where, in general, equivalence of negabent functions and EA-equivalence of the corresponding semibent functions is the same. In Section 6 we analyse semibent functions with respect to negabentness. In particular we show that semibent functions which are partially bent always correspond to bent$_4$ functions, which is not true for arbitrary semibent functions. However, we show that some semibent functions that are not partially bent can be used to construct negabent functions.

2 Preliminaries

Recall that a c-bent$_4$ function f from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is a function for which $f(x+a)+f(x)+\mathrm{Tr_n}(c^2ax)$ is balanced for every nonzero $a \in \mathbb{F}_{2^n}$. In multivariate form a c-bent$_4$ function is defined as a function for which $f(x+a)+f(x)+c\cdot(a\odot x)$ is balanced for every nonzero $a \in \mathbb{F}_2^n$. We described already in the introduction that c-bent functions give rise to relative difference sets in G_c, see (1.1). The graph $\mathcal{G}_f = \{(x, f(x)) : x \in \mathbb{F}_{2^n})\}$ of a c-bent$_4$ function f is a $(2^n, 2, 2^n, 2^{n-1})$ relative difference set in G_c whose forbidden subgroup is $\{0\} \times \mathbb{F}_2$.

Alternatively, in multivariate framework the groups we consider are the groups $G_c := (\mathbb{F}_2^n \times \mathbb{F}_2, *_c)$, with multiplication given as in (1.2), which are again isomorphic to $\mathbb{F}_{2^{n-1}} \times \mathbb{Z}_4$, and for which the graphs of multivariate c-bent$_4$ functions are $(2^n, 2, 2^n, 2^{n-1})$ relative difference sets.

For a nonzero $c \in \mathbb{F}_{2^n}$ we define the function $\sigma(c, x)$ on $\mathbb{F}_{2^n}$ by

$$\sigma(c, x) = \sum_{0 \le i < j < n} (cx)^{2^i} (cx)^{2^j} \ . \tag{2.1}$$

Some properties of σ are summarized in the following lemma.

Lemma 2.1. *(i) σ is Boolean.*

(ii) For every $x_1, x_2 \in \mathbb{F}_{2^n}$ we have

$$\sigma(c, x_1 + x_2) = \sigma(c, x_1) + \sigma(c, x_2) + \mathrm{Tr}_n(c^2 x_1 x_2) + \mathrm{Tr}_n(cx_1)\mathrm{Tr}_n(cx_2) \ , \tag{2.2}$$

where Tr_n is the absolute trace from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, cf. [1, Lemma 5].

(iii) $\sigma(x) := \sigma(1, x)$ can be represented as

$$\sigma(x) = \begin{cases} \sum_{i=1}^{m-1} \mathrm{Tr}_n(x^{2^i+1}) + \sum_{i=1}^{m-1} x^{2^{m+i}+1} & \text{if } n = 2m, \\ \sum_{i=1}^{m} \mathrm{Tr}_n(x^{2^i+1}) & \text{if } n = 2m+1. \end{cases}$$

Lemma 2.2. *[1] If n is even, then a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is c-bent$_4$ if and only if $f(x)+\sigma(c,x)$ is bent. If n is odd, then a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is c-bent$_4$ if and only if $g(x) = f(x) + \sigma(c,x)$ is semibent such that $|\mathcal{W}_g(u)| \neq 0$ if and only if $|\mathcal{W}_g(u+c)| = 0$ for all $u \in \mathbb{F}_{2^n}$.*

In multivariate case the function $s_2^c(x)$, defined as (see [8])

$$s_2^c(x) := \sum_{1 \leq i < j \leq n} (c_i x_i)(c_j x_j)$$

for $c = (c_1, \ldots, c_n)$, $x = (x_1, \ldots, x_n)$ in $\mathbb{F}_2^n$, plays a similar role as $\sigma(c,x)$ for univariate functions. Note that $s_2^c(x) = s_2(c \odot x)$, where $s_2(x)$ is the homogeneous symmetric Boolean function with algebraic degree 2. The version of Lemma 2.2 for multivariate functions is as follows, see [8, 11, 19, 23]:

Lemma 2.3. *If n is even, then a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is c-bent$_4$ if and only if $f(x) + s_2^c(x)$ is bent. If n is odd, then a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is c-bent$_4$ if and only if $g(x) = f(x) + s_2^c(x)$ is semibent such that $|\mathcal{W}_g(u)| \neq 0$ if and only if $|\mathcal{W}_g(u+c)| = 0$ for all $u \in \mathbb{F}_2^n$.*

We remark that one can also analyse shifts of plateaued functions other than semibent functions. The resulting functions are plateaued, see [2], but do not correspond to relative difference sets.

We intentionally use both representations of Boolean functions, univariate and multivariate, to emphasize that the results we present here are independent from these (or other) representations.

For the proofs of some results we may without loss of generality switch from univariate to multivariate representation.

3 Equivalence for $bent_4$ functions

Recall that two relative difference sets R_1 and R_2 of a group $(G,+)$ are called equivalent if $R_2 = \varphi(R_1) + b$ for an automorphism φ of G and an element $b \in G$. For relative difference sets in the elementary abelian group, equivalence precisely corresponds to extended affine equivalence (EA-equivalence) for Boolean functions. Recall that two functions f_1, f_2 from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, respectively from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, are EA-equivalent if

$$f_2(x) = f_1(\mathcal{L}(x) + \alpha) + \mathrm{Tr_n}(\beta x) + b$$

for some $\alpha, \beta \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_2$ and a linearized permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}$, respectively, if

$$f_2(x) = f_1(Ax + a) + b \cdot x + c$$

for some $a, b \in \mathbb{F}_2^n$, $c \in \mathbb{F}_2$ and an invertible $n \times n$-matrix A over $\mathbb{F}_2$.

In order to develop a concept of equivalence for c-bent$_4$ functions, $c \in \mathbb{F}_{2^n}^*$, which describes equivalence of their relative difference sets, we are interested in the automorphism group of $G_c = (\mathbb{F}_{2^n} \times \mathbb{F}_2, *_c)$, with $(x_1, y_1) *_c (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + \mathrm{Tr}_n(c^2 x_1 x_2))$. Observing that $\theta : G_1 \to G_c$ given by $\theta(x, y) = (x/c, y)$ is an isomorphism, it is sufficient to determine the automorphism group of G_c for $c = 1$. A similar argument applies for the multivariate case.

The most obvious automorphisms of G_1 are $(x, y) \to (\mathcal{L}(x), y)$ for which $\mathcal{L}$ is an *isometry*, i.e. $\mathcal{L}$ is a linear transformation satisfying $\mathrm{Tr_n}(\mathcal{L}(x)\mathcal{L}(y)) = \mathrm{Tr_n}(xy)$ for all $x, y \in \mathbb{F}_{2^n}$. This can easily be confirmed by direct calculations. Hence the group of isometries on $\mathbb{F}_{2^n}$ is a subgroup of $\mathrm{Aut}(G_1)$. Before representing the whole automorphism group, which requires the function σ given by Equation (2.1), we remark that in [10] these automorphisms are called orthogonal.

Lemma 3.1. *Let $\mathcal{L}$ be a permutation of $\mathbb{F}_{2^n}$ and $\beta \in \mathbb{F}_{2^n}$. Then the function $\psi_{\mathcal{L},\beta} : \mathbb{F}_{2^n} \times \mathbb{F}_2 \mapsto \mathbb{F}_{2^n} \times \mathbb{F}_2$ defined by*

$$\psi_{\mathcal{L},\beta}(x, y) = (\mathcal{L}(x), y + \sigma(x) + \sigma(\mathcal{L}(x)) + \mathrm{Tr}_n(\beta x))$$

is an automorphism of G_1 if and only if $\mathcal{L}$ is linearized such that $\mathrm{Tr}_n(x) = \mathrm{Tr}_n(\mathcal{L}(x))$ for all $x \in \mathbb{F}_{2^n}$.

Proof. The map $\psi_{\mathcal{L},\beta}$ is an automorphism of G_1 if and only if for any $(x_1, y_1), (x_2, y_2) \in \mathbb{F}_{2^n} \times \mathbb{F}_2$ we have

$$\psi_{\mathcal{L},\beta}(x_1, y_1) * \psi_{\mathcal{L},\beta}(x_2, y_2) = \psi_{\mathcal{L},\beta}(x_1 + x_2, y_1 + y_2 + \mathrm{Tr}_n(x_1 x_2)) \ .$$

By the definition of $*$ and $\psi_{\mathcal{L},\beta}$, this holds if and only if the following equality holds:

$$\begin{aligned}&(\mathcal{L}(x_1), y_1 + \sigma(x_1) + \sigma(\mathcal{L}(x_1)) + \mathrm{Tr}_n(\beta x_1)) * (\mathcal{L}(x_2), y_2 + \sigma(x_2) + \sigma(\mathcal{L}(x_2)) + \mathrm{Tr}_n(\beta x_2)) \\ &= (\mathcal{L}(x_1 + x_2), y_1 + y_2 + \mathrm{Tr}_n(x_1 x_2) + \sigma(x_1 + x_2) + \sigma(\mathcal{L}(x_1 + x_2)) + \mathrm{Tr}_n(\beta(x_1 + x_2))).\end{aligned}$$

This implies that

$$\mathcal{L}(x_1) + \mathcal{L}(x_2) = \mathcal{L}(x_1 + x_2) \ , \text{ i.e. } \mathcal{L} \text{ is linear, and} \tag{3.1}$$

$$\begin{aligned}&\sigma(x_1) + \sigma(\mathcal{L}(x_1)) + \mathrm{Tr}_n(\beta x_1) + \sigma(x_2) + \sigma(\mathcal{L}(x_2)) + \mathrm{Tr}_n(\beta x_2) + \mathrm{Tr}_n(\mathcal{L}(x_1)\mathcal{L}(x_2)) \\ &= \mathrm{Tr}_n(x_1 x_2) + \sigma(x_1 + x_2) + \sigma(\mathcal{L}(x_1 + x_2)) + \mathrm{Tr}_n(\beta(x_1 + x_2)) \ .\end{aligned} \tag{3.2}$$

Applying the identity in Equation (2.2), we then see that Equation (3.2) is equivalent to

$$\mathrm{Tr}_n(x_1)\mathrm{Tr}_n(x_2) = \mathrm{Tr}_n(\mathcal{L}(x_1))\mathrm{Tr}_n(\mathcal{L}(x_2)) \tag{3.3}$$

for any $x_1, x_2 \in \mathbb{F}_{2^n}$. Setting $x_1 = x_2 = x$ in Equation (3.3), we see that $\mathrm{Tr}_n(x) = \mathrm{Tr}_n(\mathcal{L}(x))$ for any $x \in \mathbb{F}_{2^n}$. Conversely, the property $\mathrm{Tr}_n(x) = \mathrm{Tr}_n(\mathcal{L}(x))$ implies Equation (3.3). Hence Equation (3.3) is equivalent to $\mathrm{Tr}_n(x) = \mathrm{Tr}_n(\mathcal{L}(x))$ for all $x \in \mathbb{F}_{2^n}$. □

By Theorem 4.1 in [9], the cardinality of the automorphism group of $G_1 \equiv \mathbb{F}_{2^{n-1}} \times \mathbb{Z}_4$ is equal to

$$|\mathrm{Aut}(G_1)| = 2^{\frac{n(n+1)}{2}} \prod_{k=1}^{n-1} (2^k - 1) \ . \tag{3.4}$$

To show that every automorphism of G_1 is of the form given in Lemma 3.1, we need the following definition.

Definition 3.2. Let $\alpha \in \mathbb{F}_{2^n}^*$ and

$$\Omega_\alpha := \{\mathcal{L} \mid \mathcal{L} : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n} \text{ linearized pemutation with } \mathrm{Tr}_n(\alpha x) = \mathrm{Tr}_n(\alpha \mathcal{L}(x)) \text{ for all } x \in \mathbb{F}_{2^n}\} \ .$$

We note that for any $\alpha \in \mathbb{F}_{2^n}^*$, the set Ω_α forms a group and the group of isometries is a subgroup of Ω_1.

Proposition 3.3. *The cardinality of Ω_α is the same for every nonzero $\alpha \in \mathbb{F}_{2^n}$.*

Proof. Let α be a nonzero element in $\mathbb{F}_{2^n}$. By definition, a linearized permutation $\mathcal{L}$ is in Ω_1 if and only if $\mathrm{Tr}_n(x) = \mathrm{Tr}_n(\mathcal{L}(x))$ for all $x \in \mathbb{F}_{2^n}$. This holds if and only if for all $x \in \mathbb{F}_{2^n}$

$$\mathrm{Tr}_n(\alpha x) = \mathrm{Tr}_n(\mathcal{L}(\alpha x)) \ . \tag{3.5}$$

Set $\tilde{\mathcal{L}}(x) := (1/\alpha)\mathcal{L}(\alpha x)$. Then we have $\mathrm{Tr}_n(\mathcal{L}(\alpha x)) = \mathrm{Tr}_n(\alpha \tilde{\mathcal{L}}(x))$, i.e. by Equation (3.5) we have $\mathrm{Tr}_n(\alpha x) = \mathrm{Tr}_n(\alpha \tilde{\mathcal{L}}(x))$ for all $x \in \mathbb{F}_{2^n}$. Hence there exists a one to one correspondence between the sets Ω_1 and Ω_α, which proves our claim. □

Proposition 3.4. *Let $G := (\mathbb{F}_{2^n} \times \mathbb{F}_2, *)$ be the group defined by Equation (1.1) for $c = 1$. Then the automorphism group $\mathrm{Aut}(G)$ is given by*

$$\mathrm{Aut}(G) = \{\psi_{\mathcal{L},\beta} \mid \psi_{\mathcal{L},\beta}(x, y) = (\mathcal{L}(x), y + \sigma(x) + \sigma(\mathcal{L}(x)) + \mathrm{Tr}_n(\beta x)) \ , \mathcal{L} \in \Omega_1, \beta \in \mathbb{F}_{2^n}\} \ .$$

Proof. Note that every linear permutation $\mathcal{L}$, satisfying $\mathrm{Tr}_n(x) = \mathrm{Tr}_n(\mathcal{L}(x))$ for all $x \in \mathbb{F}_{2^n}$, gives rise to 2^n distinct automorphisms of G (arising from 2^n choices for $\beta \in \mathbb{F}_{2^n}$). Hence, by Equation (3.4), it is enough to show that there exist $2^{n(n-1)/2} \prod_{k=1}^{n-1}(2^k - 1)$ such linear permutations. Fixing a basis $\mathcal{B}$ for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, we identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$, and thereby $\mathrm{Tr_n}(\alpha x)$ with $\langle v, x\rangle$ for some nonzero vector $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ (where $\langle v, x\rangle$ denotes the standard dot product). By Proposition 3.3, we are looking for the number of linear permutations $P : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ such that

$$\langle v, x\rangle = \langle v, P(x)\rangle \text{ for all } x \in \mathbb{F}_2^n \ .$$

This is equal to the number of $n \times n$ invertible matrices $M = (m_{ij})$ with

$$x \cdot v^t = Mx \cdot v^t \text{ for all } x \in \mathbb{F}_2^n \ , \tag{3.6}$$

where v^t is the transpose of the row matrix v. By Proposition 3.3, without loss of generality, we fix $v = (1, 0, \ldots, 0)$. Then by Equation (3.6) we conclude that the number of desired linear permutations is equal to the number of invertible $n \times n$ invertible matrices $M = (m_{ij})$ whose first row is $(1, 0, \ldots, 0)$. This is equal to

$$(2^n - 2)(2^n - 2^2) \cdots (2^n - 2^{n-1}) = 2^{\frac{n(n-1)}{2}} \prod_{k=1}^{n-1} (2^k - 1) \ ,$$

which gives the desired result. □

Remark 3.5. It can be seen from the definition of $\psi_{\mathcal{L},\beta}$ that the group operation "$\circ$" in $\mathrm{Aut}(G_1)$ $\psi_{\mathcal{L}_1,\beta_1} \circ \psi_{\mathcal{L}_2,\beta_2} = \psi_{\mathcal{L}_1 \circ \mathcal{L}_2, \alpha(\beta_1,\beta_2)}$, where $\alpha(\beta_1, \beta_2) \in \mathbb{F}_{2^n}$ such that $\mathrm{Tr}_n(\alpha(\beta_1, \beta_2)x) = \mathrm{Tr}_n(\beta_2 x + \beta_1 \mathcal{L}_2(x))$.

Remark 3.6. The automorphism group $\mathrm{Aut}(G_c)$ of $G_c = (\mathbb{F}_{2^n} \times \mathbb{F}_2, *_c)$ consists of $\psi_{\mathcal{L},\beta}$ defined by

$$\psi_{\mathcal{L},\beta}(x, y) = (c\mathcal{L}(x), y + \sigma(c, x) + \sigma(c, \mathcal{L}(x)) + \mathrm{Tr}_n(\beta x)) \ ,$$

where $\mathcal{L}$ is a linearized permutation such that $\mathrm{Tr}_n(cx) = \mathrm{Tr}_n(c\mathcal{L}(x))$ for all $x \in \mathbb{F}_{2^n}$.

The following corollary confirms the initial observation on isometries.

Corollary 3.7. *The group* $\{\varphi_{\mathcal{L},\beta} \mid \mathcal{L}$ *is an isometry,* $\beta \in \mathbb{F}_{2^n}\}$ *with* $\varphi_{\mathcal{L},\beta}(x, y) = (\mathcal{L}(x), y + \mathrm{Tr_n}(\beta x))$ *is a subgroup of* $Aut(G_1)$.

Proof. First note that $\mathrm{Tr_n}(\mathcal{L}(x)\mathcal{L}(y)) = \mathrm{Tr_n}(xy)$ for all $x, y \in \mathbb{F}_{2^n}$ implies $\mathrm{Tr_n}(\mathcal{L}(x)) = \mathrm{Tr_n}(x)$ for all $x \in \mathbb{F}_{2^n}$. For $\mathcal{L} \in \Omega_1$, we claim that $\sigma(x) + \sigma(\mathcal{L}(x))$ is a linear mapping if and only if $\mathcal{L}$ is an isometry. As a consequence for an isometry $\mathcal{L}$ we have $\psi_{\mathcal{L},\beta}(x, y) = (\mathcal{L}(x), y + \mathrm{Tr_n}(\beta' x))$ for some $\beta' \in \mathbb{F}_{2^n}$. In particular, $\psi_{\mathcal{L},\beta}(x, y) = (\mathcal{L}(x), y)$ if $\sigma(x) + \sigma(\mathcal{L}(x)) = \mathrm{Tr_n}(\beta x)$. It remains to show our claim. Let $\mathcal{L} \in \Omega_1$, i.e. $\mathrm{Tr}_n(x) = \mathrm{Tr}_n(\mathcal{L}(x))$ for all $x \in \mathbb{F}_{2^n}$. Then by Equation (2.2), for $x, y \in \mathbb{F}_{2^n}$, we have the following equalities.

$$\begin{aligned}
&\sigma(x + y) + \sigma(\mathcal{L}(x + y)) \\
&= \sigma(x) + \sigma(y) + \mathrm{Tr}_n(xy) + \mathrm{Tr}_n(x)\mathrm{Tr}_n(y) \\
&\qquad + \sigma(\mathcal{L}(x)) + \sigma(\mathcal{L}(y)) + \mathrm{Tr}_n(\mathcal{L}(x)\mathcal{L}(y)) + \mathrm{Tr}_n(\mathcal{L}(x))\mathrm{Tr}_n(\mathcal{L}(y)) \\
&= \sigma(x) + \sigma(y) + \sigma(\mathcal{L}(x)) + \sigma(\mathcal{L}(y)) + \mathrm{Tr}_n(xy) + \mathrm{Tr}_n(\mathcal{L}(x)\mathcal{L}(y)) \qquad (3.7)
\end{aligned}$$

By Equation (3.7) we then conclude that $\sigma(x) + \sigma(\mathcal{L}(x))$ is linear if and only if $\mathrm{Tr}_n(xy) = \mathrm{Tr}_n(\mathcal{L}(x)\mathcal{L}(y))$, i.e. $\mathcal{L}$ is an isometry. □

By Proposition 3.4 we obtain the following theorem on equivalence of negabent functions.

Theorem 3.8. *Let f_1, f_2 be negabent functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Then the corresponding difference sets $\{(x, f_1(x)) : x \in \mathbb{F}_{2^n}\}$ and $\{(x, f_2(x)) : x \in \mathbb{F}_{2^n}\}$ of G_1 are equivalent if and only if*

$$f_2(x) = f_1(\mathcal{L}(x) + \alpha) + \sigma(\mathcal{L}(x)) + \sigma(x) + \mathrm{Tr_n}(\beta x) + b$$

for some $\alpha, \beta \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_2$ and a linearized permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}$ for which $\mathrm{Tr_n}(\mathcal{L}(x)) = \mathrm{Tr_n}(x)$ for all $x \in \mathbb{F}_{2^n}$. Note that if f_1 is quadratic, we may assume $\alpha = 0$.

Remark 3.9. As for the difference sets in the elementary abelian 2-group, the shifts of a difference set in G_1 are obtained by using affine instead of linear transformations and by the addition of the constant $b \in \mathbb{F}_2$.

4 Equivalence and shifted equivalence: The case n even

If n is even, then by Lemma 2.2 a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is c-bent$_4$ if and only if $f(x) + \sigma(c, x)$ is bent. Therefore, we can shift a c-bent$_4$ function to the corresponding bent function, perform an EA-equivalence transformation on the bent function and shift the result back to a c-bent$_4$ function, see Figure 1. Here we concentrate, without loss of generality, to the case $c = 1$, which means the negabent case. Accordingly we call negabent$_4$ functions f_1 and f_2 shifted equivalent, if the corresponding bent functions are EA-equivalent, i.e.

$$f_2(x) = (f_1 + \sigma)(\mathcal{L}(x) + \alpha) + \sigma(x) + \mathrm{Tr}_n(\beta x) + b$$

for some $\alpha, \beta \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_2$ and a linearized permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}$. Using that $\sigma(\mathcal{L}(x) + \alpha) = \sigma(\mathcal{L}(x))+$ affine function, we may simplify this expression and now call two negabent functions f_1 and f_2 *shifted equivalent* if there is a linearized permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}$, elements $\alpha, \beta \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_2$ such that

$$f_2(x) = f_1(\mathcal{L}(x) + \alpha) + \sigma(\mathcal{L}(x)) + \sigma(x) + \mathrm{Tr}_n(\beta x) + b.$$

By Theorem 3.8, equivalent negabent functions are always shifted equivalent. We now show that the latter concept is more general. Since the proof uses the theory of quadratic functions, we recall some basic facts about quadratic functions in n variables.

By a (much more general) result of McEliece [7], which uses a technical result of Dickson [5] we have the following lemma.

Lemma 4.1. *Every homogeneous quadratic bent function g_1 (quadratic bent function without linear and constant term) from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is equivalent to*

$$g(x_1, \ldots, x_n) = x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n \ , \tag{4.1}$$

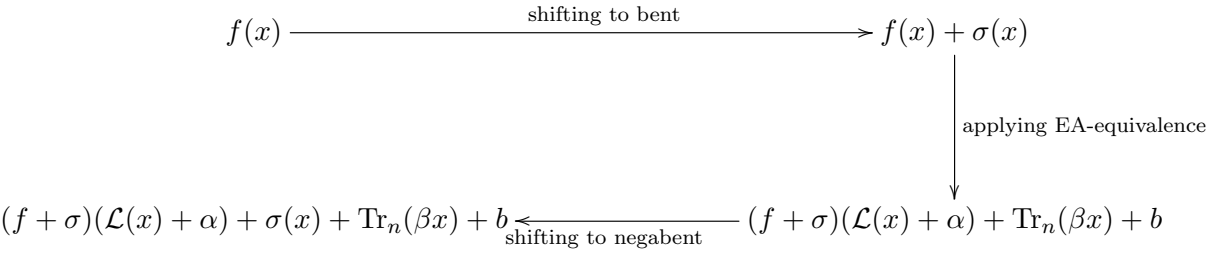

Figure 1: Shifted eqivalence

by a linear coordinate transformation, i.e.

$$g_1(x_1,\ldots,x_n) = g((x_1,\ldots,x_n)A)$$

for a non-singular $n \times n$ matrix A over $\mathbb{F}_2$. The number N_g of homogeneous quadratic bent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ (all equivalent to g) is given as

$$N_g = 2^{m^2-1}(2^m+1)\frac{\prod_{i=1}^{n}(2^i-1)}{\prod_{i=1}^{m}(2^{2i}-1)} \ . \tag{4.2}$$

For a (homogeneous) quadratic function $g : \mathbb{F}_2^n \mapsto \mathbb{F}_2$, we denote by $O(g)$ the group of linear transformations fixing g and it is called the *orthogonal group* associated to g. Note that $2^{n+1} \cdot |\mathrm{GL}(n,2)| = N_g \cdot |O(g)|$, where the factor 2^{n+1} counts the number of affine shifts of quadratic bent functions. We obtain (see [5])

$$|O(g)| = 2(2^m-1)2^{m(m-1)}\prod_{i=1}^{m-1}(2^{2i}-1) \ . \tag{4.3}$$

Theorem 4.2. *Two EA-equivalent bent functions can induce inequivalent difference sets in G_1. In other words: There are shifted equivalent negabent functions which are not equivalent.*

Proof. We first note that $\mathrm{Aut}(G_1)$ acts on the set of negabent functions. The action "$\cdot$" is given by

$$\psi_{\mathcal{L},\beta} \cdot f(x) := f(\mathcal{L}(x)) + \sigma(\mathcal{L}(x)) + \sigma(x) + \mathrm{Tr_n}(\beta x) \ .$$

We denote by H_f the stabilizer subgroup of f, i.e.

$$H_f := \{\psi_{\mathcal{L},\beta} \mid \psi_{\mathcal{L},\beta} \in \mathrm{Aut}(G_1) \ \text{ with } \ \psi_{\mathcal{L},\beta} \cdot f = f\} \ .$$

Now let f be a quadratic negabent function and $g = f + \sigma$ be the corresponding bent function, which is fixed by the transformations $O(g)$ (for the univariate case we can obtain g from (4.1)

choosing a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, the orthogonal group is determined accordingly). Then for any transformation $\mathcal{L} \in O(g) \cap \Omega_1$ (see Definition 3.2 for Ω_1) the automorphism $\psi_{\mathcal{L},0}$ fixes f as

$$\psi_{\mathcal{L},0} \cdot f(x) = (f + \sigma)(\mathcal{L}(x)) + \sigma(x) = g(\mathcal{L}(x)) + \sigma(x) = g(x) + \sigma(x) = f(x) \ .$$

Hence $\{\psi_{\mathcal{L},0} \mid \mathcal{L} \in O(g) \cap \Omega_1\}$ is a subgroup of H_f. In particular, for some positive integer k, we have $|H_f| = k|O(g) \cap \Omega_1|$. By Theorem 3.8 and using that f is quadratic, we know that $\tilde{f}$ and f are equivalent if and only if $\tilde{f}(x) = f(\mathcal{L}(x)) + \sigma(\mathcal{L}(x) + \alpha) + \sigma(x) + \mathrm{Tr_n}(\beta x) + b$ for some $\mathcal{L} \in \Omega_1$, $\alpha, \beta \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_2$. Since σ is a quadratic function, this is equivalent to $\tilde{f}(x) = f(\mathcal{L}(x)) + \sigma(\mathcal{L}(x)) + \sigma(x) + \mathrm{Tr_n}(\tilde{\beta} x) + \tilde{b}$ for some $\tilde{\beta} \in \mathbb{F}_{2^n}$ and $\tilde{b} \in \mathbb{F}_2$. Hence by the orbit-stabilizer theorem, the number of distinct negabent quadratic functions which are equivalent to f under the action of G_1 is

$$L_n := \frac{2|\mathrm{Aut}(G)|}{k|O(g) \cap \Omega_1|} \ .$$

Since equivalence implies shifted equivalence, we have $L_n \leq 2^{n+1} N_n$, where $2^{n+1} N_n$ is the total number of quadratic bent functions (including affine terms), respectively, the number of distinct negabent functions of algebraic degree at most 2. Then it is sufficient to observe that the equality $L_n = 2^{n+1} N_n$ can not hold. Note that the equality holds if and only if

$$\frac{2|\mathrm{Aut}(G)|}{k|O(g) \cap \Omega_1|} = \frac{2^{n+1}|\mathrm{GL}(n,2)|}{|O(g)|} \ , \tag{4.4}$$

Since $|\mathrm{Aut}(G)| = 2^n|\Omega_1| = 2^n|\mathrm{GL}(n,2)|/(2^n - 1)$, Equation(4.4) implies that $|O(g)| = (2^n - 1)k|O(g) \cap \Omega_1|$, and hence $2^n - 1$ has to divide $|O(g)|$. Using n even, say $n = 2m$, by Equation (4.3) we conclude that $2^m + 1$ has to divide $(2^m - 1)\prod_{i=1}^{m-1}(2^{2i} - 1)$. This does in general not hold (e.g. for m for which $2^m + 1$ is prime), hence in general in $L_n \leq 2^{n+1} N_n$ we have strict inequality. □

Remark 4.3. In fact among $m \leq 12$ only for $m = 3$ the term $(2^m - 1)\prod_{i=1}^{m-1}(2^{2i} - 1)$ is divisible by $2^m + 1$ (calculations by conventional calculator).

Remark 4.4. The existence of a relative difference set R with parameters $(2^n, 2, 2^n, 2^{n-1})$ implies the existence of an incidence structure: the points are the group elements, and the blocks are the translates $R + g := \{r + g \ : \ r \in R\}$, see [12], for instance. These incidence structures are divisible designs (see [14] for background from design theory). There is an obvious concept of isomorphism of incidence structures. Two incidence structures are isomorphic if there is a bijection between the point sets which induce a bijection between the block sets (which are just subsets of the point set). It is easy to see that equivalent difference sets give rise to isomorphic incidence structures, but not vice versa: there are, for instance, four inequivalent bent functions

(whose supports are inequivalent difference sets) on 6 variables, see [13]. These give rise to three different symmetric designs with parameters $(64, 28, 12)$, see [13], again. In the context of our investigation we may ask whether the designs that we obtain via inequivalent but shifted equivalent negabent functions are isomorphic. It turns out that shifted equivalent negabent functions can give rise to nonisomorphic designs. For instance, the bent function f given by $f(x_1, x_2, x_3x_4x_5x_6) = x_1x_2 + x_3x_4 + x_5x_6 + x_1x_3x_5$ and the equivalent one given by $g(x) = f(Ax)$ with

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

give rise to inequivalent negabent functions (by adding $\sum_{i<j} x_ix_j$) whose corresponding designs are not isomorphic (computations using MAGMA [6]).

We also checked all the bent functions equivalent to $x_1x_2 + x_3x_4$ and their corresponding negabent functions. All the divisible designs that we obtained are equivalent, and they are equivalent to the divisible design corresponding to the elementary abelian relative difference set

$$\{(x_1, x_2, x_3, x_4, x_1x_2 + x_3x_4 \ : \ x_1, x_2, x_3, x_4 \in \mathbb{F}_2\} \subset \mathbb{F}_2^5.$$

It is well known that a relative difference set can be obtained form a divisible design if the design has a point and block regular automorphism group. The full automorphism group of the design described by a quadratic function is huge, therefore it is not a surprise that the full full automorphism group contains other groups (isomorphic to $\mathbb{Z}_2^n \times \mathbb{Z}_4$) which act regularly on points and blocks. That would explain why all the designs that we found via shifted equivalent negabent functions are isomorphic if we start with a quadratic bent function.

5 Equivalence and shifted equivalence: The case n odd

In the case of n even, we have seen that two shifted equivalent negabent functions can correspond to two inequivalent difference sets. In this section we investigate negabent functions for n odd. Recall that when n is odd, then for a c-bent$_4$ function f, the function $g(x) = f(x) + \sigma(c, x)$ is a semibent function satisfying the property

$$|\mathcal{W}_g(u)| \neq 0 \quad \text{if and only if} \quad |\mathcal{W}_g(u + c)| = 0 \quad \text{for all } u \in \mathbb{F}_{2^n}. \tag{5.1}$$

This condition shows that for 2^{n-1} of the u's we have $\mathcal{W}_g(u)| \neq 0$ provided f is semibent. Hence for semibent functions, the condition (5.1) is equivalent to $\mathcal{W}_g(u)\mathcal{W}_g(c + u) = 0$. A

fundamental difference to the case of n even is that an EA-equivalence transformation on the semibent function g may destroy the Property (5.1), so that the resulting semibent function does not correspond to a negabent respectively a c-bent$_4$ function. Hence we first scan the set of EA-equivalence transformations with respect to Property (5.1). Let f be a negabent function or more general a c-bent$_4$ function, and let $g = f + \sigma$ be the corresponding semibent function. By definition of EA-equivalence, we have to consider the following cases:

(i) For $b \in \mathbb{F}_2$, let $\tilde{g}(x) = g(x) + b$. Since for any $u \in \mathbb{F}_{2^n}$ we have $\mathcal{W}_{\tilde{g}}(u) = (-1)^b \mathcal{W}_g(u)$, with g, the EA-equivalent function $\tilde{g}$ has Property (5.1) as well.

(ii) For $\beta \in \mathbb{F}_{2^n}$, let $\tilde{g}(x) = g(x) + \mathrm{Tr}_n(\beta x)$. Since for any $u \in \mathbb{F}_{2^n}$ we have $\mathcal{W}_{\tilde{g}}(u) = \mathcal{W}_g(u+\beta)$, the equality $\mathcal{W}_{\tilde{g}}(u) = 0$ holds if and only if $\mathcal{W}_g(u+\beta) = 0$, which holds if and only if $\mathcal{W}_g(u+\beta+c) \neq 0$. This implies that $\tilde{g}$ has Property (5.1).

(iii) For $\alpha \in \mathbb{F}_{2^n}$, let $\tilde{g}(x) = g(x+\alpha)$. Since for any $u \in \mathbb{F}_{2^n}$ we have $\mathcal{W}_{\tilde{g}}(u) = (-1)^{\mathrm{Tr_n}(\alpha u)} \mathcal{W}_g(u)$, with g, also $\tilde{g}$ has Property (5.1).

(iv) Finally we consider $\tilde{g} = g(\mathcal{L}(x))$ for a linearized permutation $\mathcal{L} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. We will next show that Property (5.1) is preserved if and only if $\mathcal{L}$ satisfies the identity $\mathrm{Tr}_n(c\mathcal{L}(x)) = \mathrm{Tr}_n(cx)$, i.e. $\mathcal{L} \in \Omega_c$.

More generally, we have the following lemma:

Lemma 5.1. *Let g be a semibent function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ such that for all $u \in \mathbb{F}_{2^n}$ we have $\mathcal{W}_g(u)\mathcal{W}_g(u+c) = 0$ for some nonzero $c \in \mathbb{F}_{2^n}$, and let $\mathcal{L}$ be a linearized permutation of $\mathbb{F}_{2^n}$. Suppose that $\mathrm{Tr}_n(c\mathcal{L}(x)) = \mathrm{Tr}_n(dx)$, then $\tilde{g}(x) = g(\mathcal{L}(x))$ satisfies $\mathcal{W}_{\tilde{g}}(u)\mathcal{W}_{\tilde{g}}(u+d) = 0$ for all $u \in \mathbb{F}_{2^n}$.*
Suppose conversely that $\mathrm{Tr}_n(c\mathcal{L}(x)) = \mathrm{Tr}_n(dx)$ and $\tilde{g}(x) = g(\mathcal{L}(x))$ satisfies $\mathcal{W}_{\tilde{g}}(u)\mathcal{W}_{\tilde{g}}(u+d) = 0$ for all $u \in \mathbb{F}_{2^n}$. Then $\mathcal{W}_g(u)\mathcal{W}_g(u+c) = 0$ for all $u \in \mathbb{F}_{2^n}$.

Proof. For g given as in the lemma and a linearized permutation $\mathcal{L}$ we have the following equalities.

$$\begin{aligned}
0 &= \mathcal{W}_g(u)\mathcal{W}_g(u+c) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{g(x)+\mathrm{Tr_n}(ux)} \sum_{y\in\mathbb{F}_{2^n}} (-1)^{g(y)+\mathrm{Tr_n}(cy)+\mathrm{Tr_n}(uy)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{g(\mathcal{L}(x))+\mathrm{Tr_n}(u\mathcal{L}(x))} \sum_{y\in\mathbb{F}_{2^n}} (-1)^{g(\mathcal{L}(y))+\mathrm{Tr_n}(c\mathcal{L}(y))+\mathrm{Tr_n}(u\mathcal{L}(y))} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{g(\mathcal{L}(x))+\mathrm{Tr_n}(\tilde{u}x)} \sum_{y\in\mathbb{F}_{2^n}} (-1)^{g(\mathcal{L}(y))+\mathrm{Tr_n}(c\mathcal{L}(y))+\mathrm{Tr_n}(\tilde{u}y)}
\end{aligned}$$

If $\mathrm{Tr}_n(c\mathcal{L}(x)) = \mathrm{Tr}_n(dx)$, then

$$0 \;=\; \sum_{x\in\mathbb{F}_{2^n}} (-1)^{g(\mathcal{L}(x))+\mathrm{Tr_n}(\tilde{u}x)} \sum_{y\in\mathbb{F}_{2^n}} (-1)^{g(\mathcal{L}(y))+\mathrm{Tr_n}(dy)+\mathrm{Tr_n}(\tilde{u}y)} = \mathcal{W}_{\tilde{g}}(\tilde{u})\mathcal{W}_{\tilde{g}}(\tilde{u}+d)$$

for all $\tilde{u} \in \mathbb{F}_{2^n}$. For the converse statement, observe that $g(x) = \tilde{g}(\mathcal{L}^{-1}(x))$. Since $\mathrm{Tr}_n(c\mathcal{L}(x)) = \mathrm{Tr}_n(dx)$ implies that $\mathrm{Tr}_n(d\mathcal{L}^{-1}(x)) = \mathrm{Tr}_n(cx)$, the converse follows. □

From Lemma 5.1 we obtain the following corollary.

Corollary 5.2. *(i) Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, n odd, be a c-bent$_4$ function, and let $\mathcal{L}$ be a linearized permutation. Then the function $\tilde{f}(x) = f(\mathcal{L}(x)) + \sigma(c, \mathcal{L}(x)) + \sigma(d, x)$ is d-bent$_4$ where d is the unique element that satisfies $\mathrm{Tr}_n(c\mathcal{L}(x)) = \mathrm{Tr}_n(dx)$.*

(ii) Let $\mathcal{L}$ be a linearized permutation of $\mathbb{F}_{2^n}$, n odd, and suppose that $\mathrm{Tr}_n(\mathcal{L}^{-1}(x)) = \mathrm{Tr}_n(cx)$. Then f and $\tilde{f} = f(\mathcal{L}(x)) + \sigma(c, \mathcal{L}(x)) + \sigma(x)$ are both negabent functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ if and only if f is negabent and c-bent$_4$.

Proof. (i) For a c-bent$_4$ function f, the function $g(x) = f(x) + \sigma(c, x)$ is semibent satisfying the Property (5.1). Let $d \in \mathbb{F}_{2^n}^*$ be the (unique) element for which $\mathrm{Tr_n}(c\mathcal{L}(x)) = \mathrm{Tr_n}(dx)$. By Lemma 5.1, the semibent function $\tilde{g}(x) = f(\mathcal{L}(x))+\sigma(c, \mathcal{L}(x))$ then satisfies $\mathcal{W}_{\tilde{g}}(u)\mathcal{W}_{\tilde{g}}(u+d) = 0$. By Lemma 2.2, the function $\tilde{f}$ is d-bent$_4$.
(ii) By Lemma 5.1 for a linearized permutation $\mathcal{L}$ with $\mathrm{Tr}_n(\mathcal{L}^{-1}(x)) = \mathrm{Tr}_n(cx)$, the function $\tilde{g}(x) = g(\mathcal{L}(x)) = f(\mathcal{L}(x)) + \sigma(c, \mathcal{L}(x))$ is semibent with $\mathcal{W}_{\tilde{g}}(u)\mathcal{W}_{\tilde{g}}(u+1) = 0$ for all $u \in \mathbb{F}_{2^n}$ if and only if $\mathcal{W}_g(u)\mathcal{W}_g(u+c) = 0$ for all $u \in \mathbb{F}_{2^n}$. Hence (ii) follows. □

Note that for a negabent function f, the transformation $f \to f \circ \mathcal{L} + \sigma \circ \mathcal{L} + \sigma$ always preserves negabentness if $\mathrm{Tr}_n(\mathcal{L}(x)) = \mathrm{Tr}_n(x)$. Whether such transformations with other linearized permutations $\mathcal{L}$ preserve the negabentness of f depends on special properties of f, respectively of the semibent function $g = f + \sigma$ corresponding to f. Differently to the case of n even, for n odd we have the following corollary.

Corollary 5.3. *Let $\mathcal{L}$ be a linearized permutation of $\mathbb{F}_{2^n}$, $\alpha, \beta \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_2$. The transformation $f \to f(\mathcal{L}(x)+\alpha)+\sigma(\mathcal{L}(x))+\sigma(x)+\mathrm{Tr_n}(\beta x)+b$ preserves negabentness for any negabent function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ if and only if $\mathrm{Tr}_n(\mathcal{L}(x)) = \mathrm{Tr}_n(x)$. These transformations exactly represent the automorphisms of the group G plus a shift by a constant.*

Proof. By Theorem 3.8 the indicated transformations exactly represent the automorphisms of the group G plus a shift by a constant, and hence preserve negabentness. We still have to show that there are no other transformations that preserve negabentness. In order to show this, we have to find two semibent functions g_1, g_2 for which $\mathcal{W}_{g_i}(u)\mathcal{W}_{g_i}(u+1) = 0$, $i = 1, 2$, hence they are negabent, and for which there exists no $c \neq 1$ such that $\mathcal{W}_{g_i}(u)\mathcal{W}_{g_i}(u+c) = 0$ for

both $i = 1$ and $i = 2$. That means, none of the transformations in Corollary 5.2(ii) with $c \neq 1$ can transform both g_1 and g_2 to a negabent function. The existence of such semibent functions g_1, g_2 will be shown in the following section. □

Remark 5.4. We particularly emphasize that when n is odd, in general one can not generate inequivalent relative difference sets in $\mathbb{Z}_4 \times \mathbb{F}_2^{n-1}$ by performing EA-equivalence transformations on the semibent function corresponding to the negabent function which represents the relative difference set. This is different to the situation when n is even.

We also remark that the following procedure does not yield new relative difference sets: let f be a negabent function and $g(x) = f(x) + \sigma(x)$ the corresponding semibent function. Let $\mathcal{L}$ be a linearized permutation, then $\mathrm{Tr_n}(\mathcal{L}(x)) = \mathrm{Tr_n}(dx)$ for some nonzero $d \in \mathbb{F}_{2^n}$, and hence by Lemma 5.1 the function $\tilde{f}(x) = f(\mathcal{L}(x)) + \sigma(\mathcal{L}(x)) + \sigma(d, x)$ is d-bent$_4$. We can now apply the group isomorphism from G_d to G_1 given by $(x, y) = (x/d, y)$ to obtain a negabent function given as $\bar{f}(x) = f(\mathcal{L}(x/d)) + \sigma(\mathcal{L}(x/d)) + \sigma(d, x/d)$. However, this gives $\bar{f}(x) = f(\mathcal{L}'(x)) + \sigma(\mathcal{L}'(x)) + \sigma(x)$, where $\mathcal{L}'(x) = \mathcal{L}(x/d)$ satisfies $\mathrm{Tr_n}(\mathcal{L}'(x)) = \mathrm{Tr_n}(x)$.

6 Semibent functions and bent$_4$ functions

Recall that by Lemma 2.2 when n is odd, a function f from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is c-bent$_4$ if and only if $g(x) = f(x) + \sigma(c, x)$ is semibent and $\mathcal{W}_g(u)\mathcal{W}_g(u + c) = 0$ for all $u \in \mathbb{F}_{2^n}$. Similarly, in the multivariate case, $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is c-bent$_4$ if and only if $g(x) = f(x) + s_2^c(x)$ is semibent and $\mathcal{W}_g(u)\mathcal{W}_g(u + c) = 0$ for all $u \in \mathbb{F}_{2^n}$. Hence only semibent functions with special properties can be shifted to bent$_4$ functions. A natural question is whether this property is quite exclusive or if there are many semibent functions satisfying this property at least for some c.

We first investigate a subclass of the class of semibent functions, the class of partially bent functions which are simultaneously semibent, for short partially semibent functions. This class contains all quadratic semibent functions. Recall that g is called partially bent if for all $a \in \mathbb{F}_{2^n}$ ($a \in \mathbb{F}_2^n$) the derivative $D_a g(x) = g(x + a) + g(x)$ is either balanced or constant. The set of elements a for which $D_a g$ is constant forms a vector space called the linear space Λ_g of g. As easily observed, a partially bent function g is s-plateaued where s is the dimension of Λ_g. More precisely we have the following lemma (see e.g. [4]).

Lemma 6.1. *Let g be a partially bent function with a one-dimensional linear space $\Lambda_g = \{0, \gamma\}$. Then g is semibent and the support of the Walsh transform $\mathcal{W}_g$ is a coset of the orthogonal complement of Λ_g.*

With Lemma 6.1 we can show that a semibent function which is partially bent satisfies the Condition (5.1) for half of the elements c in $\mathbb{F}_{2^n}$ ($\mathbb{F}_2^n$).

Corollary 6.2. *Let n be odd and let g be a semibent function from $\mathbb{F}_{2^n}$ ($\mathbb{F}_2^n$) to $\mathbb{F}_2$ which is partially bent. Let Λ_g be the linear space of g, and let $\Lambda_g^\perp$ be its orthogonal complement. Then $\mathcal{W}_g(u)\mathcal{W}_g(u+c) = 0$ if and only if $c \notin \Lambda_g^\perp$.*

Proof. Since Λ_g has dimension 1, the dimension of $\Lambda_g^\perp$ is $n-1$, and $\mathbb{F}_{2^n}$ ($\mathbb{F}_2^n$) is partitioned into $\Lambda_g^\perp$ and its coset, one of which is the support of $\mathcal{W}_g$. The condition $\mathcal{W}_g(u)\mathcal{W}_g(u+c) = 0$ holds for an element c in $\mathbb{F}_{2^n}$ ($\mathbb{F}_2^n$) if and only if for all u, exactly one of u and $u+c$ is in $\Lambda_g^\perp$. This applies if and only if $c \notin \Lambda_g^\perp$. □

Partially semibent functions are easy to obtain. For instance a bent function in n variables, seen as a function in $n+1$ variables is a partially bent semibent function. However they are still a special class of semibent functions. A construction of semibent functions (and more general of plateaued functions), which are not partially bent has been presented in [21]. We employ this construction to show that there exist semibent functions which do not satisfy Property (5.1) for any c, i.e. they can not be shifted to a c-bent$_4$ function for any c. We first recall the construction in [21], which is a version of the Maiorana-McFarland construction:
Let $\pi : \mathbb{F}_2^m \mapsto \mathbb{F}_2^{m+1}$ be an injective map and let $g : \mathbb{F}_2^m \times \mathbb{F}_2^{m+1} \mapsto \mathbb{F}_2$ be the function defined by $g(x,y) = \pi(x) \cdot y$, where "$\cdot$" is the standard inner product on $\mathbb{F}_2^{m+1}$. Then the Walsh coefficient of g at $(\beta,\gamma) \in \mathbb{F}_2^m \times \mathbb{F}_2^{m+1}$ is given as follows:

$$\begin{aligned}\mathcal{W}_g(\beta,\gamma) &= \sum_{(x,y)\in\mathbb{F}_2^m\times\mathbb{F}_2^{m+1}} (-1)^{\pi(x)\cdot y+\beta\cdot x+\gamma\cdot y} = \sum_{x\in\mathbb{F}_2^m} (-1)^{\beta\cdot x} \sum_{y\in\mathbb{F}_2^{m+1}} (-1)^{(\pi(x)+\gamma)\cdot y} \\ &= \begin{cases} \pm 2^{m+1} & \text{if } \gamma \in \mathrm{Im}(\pi)\ , \\ 0 & \text{if } \gamma \notin \mathrm{Im}(\pi)\ , \end{cases} \end{aligned} \tag{6.1}$$

where $\mathrm{Im}(\pi)$ is the image of π. Hence g is semibent and the support of $\mathcal{W}_g$ is determined by the image of π.

We now show that Property (5.1) is not a universal property of semibent functions.

Proposition 6.3. *If $n \geq 7$, there exists a semibent function g such that for all $c \in \mathbb{F}_{2^n}$ there is an element u such that $\mathcal{W}_g(u)\mathcal{W}_g(u+c) \neq 0$.*

Proof. We use the above recalled construction and determine the injective map π so that g does not satisfy Property (5.1) for any $c = (c_1, c_2) \in \mathbb{F}_2^m \times \mathbb{F}_2^{m+1}$. Therefore we have to construct π such that for any choice of $c = (c_1, c_2)$ the resulting function $g(x,y)$ satisfies

$$W_g(\beta,\gamma) = 0 \quad \text{and} \quad W_g(\beta+c_1,\gamma+c_2) = 0 \quad \text{or}$$

$$W_g(\beta,\gamma) \neq 0 \quad \text{and} \quad W_g(\beta+c_1,\gamma+c_2) \neq 0$$

for some $(\beta, \gamma) \in \mathbb{F}_2^m \times \mathbb{F}_2^{m+1}$. Note that $|W_g(\beta, \gamma)|$ is independent of β. Hence by (6.1) our aim is to construct π such that for every $c_2 \in \mathbb{F}_2^{m+1}$ there exists γ for which

$$\gamma \notin \mathrm{Im}(\pi) \ \text{ and } \ \gamma + c_2 \notin \mathrm{Im}(\pi) \ , \quad \text{or} \quad \gamma \in \mathrm{Im}(\pi) \ \text{ and } \ \gamma + c_2 \in \mathrm{Im}(\pi) \ . \tag{6.2}$$

Let $m \geq 3$ and let W be an m-dimensional subspace of $\mathbb{F}_2^{m+1}$, hence $\mathbb{F}_2^{m+1} = W \cup (v + W)$ for some vector $v \in \mathbb{F}_2^{m+1} \setminus W$. For an element $w \in W$ we choose an injection $\pi : \mathbb{F}_2^m \mapsto \mathbb{F}_2^{m+1}$ such that

$$\mathrm{Im}(\pi) = (W \setminus \{0, w\}) \cup \{v, v + \tilde{w}\} \quad \text{for some } \tilde{w} \in W \text{ with } \tilde{w} \neq w.$$

We show that π has Property (6.2) distinguishing three cases:

- If $c_2 \notin \mathrm{Im}(\pi)$, then with $\gamma = 0$ we have $\gamma \notin \mathrm{Im}(\pi)$ and $\gamma + c_2 \notin \mathrm{Im}(\pi)$.
- If $c_2 = v$ or $c_2 = v + \tilde{w}$, then with $\gamma = \tilde{w}$ we have $\gamma \in \mathrm{Im}(\pi)$ and $\gamma + c_2 \in \mathrm{Im}(\pi)$.
- If $c_2 \in W \setminus \{0, w\}$, then there exists $w_1 \in W \setminus \{0, w\}$ such that $c_2 + w_1 \in W \setminus \{0, w\}$ (here we use $m \geq 3$). With $\gamma = w_1$, we then have $\gamma \in \mathrm{Im}(\pi)$ and $\gamma + c_2 \in \mathrm{Im}(\pi)$.

□

Similarly as in the proof of Proposition 6.3, we can construct semibent functions $g(x, y)$ satisfying $\mathcal{W}_g(u)\mathcal{W}_g(u + c) = 0$, $c = (c_1, c_2) \in \mathbb{F}_2^m \times \mathbb{F}_2^{m+1} = \mathbb{F}_2^{2m+1}$, for a unique nonzero $c_2 \in \mathbb{F}_2^{m+1}$ (and every $c_1 \in \mathbb{F}_2^m$):
For a nonzero element $c_2 \in \mathbb{F}_2^{m+1}$, $m \geq 2$, let W be an m-dimensional subspace of $\mathbb{F}_2^{m+1}$ which does not contain c_2, and hence $\mathbb{F}_2^{m+1} = W \cup (c_2 + W)$. Choose an injection $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^{m+1}$ such

$$\mathrm{Im}(\pi) = (W \setminus \{0\}) \cup \{c_2\} \ .$$

Then we have

$$\gamma \in \mathrm{Im}(\pi) \ \text{ if and only if } \ \gamma + c_2 \notin \mathrm{Im}(\pi) \ ,$$

and consequently g satisfies $\mathcal{W}_g(u)\mathcal{W}_g(u + c) = 0$, for $c = (c_1, c_2)$, $c_1 \in \mathbb{F}_2^m$ arbitrary. For $d = (d_1, d_2) \in \mathbb{F}_2^m \times \mathbb{F}_2^{m+1}$ with $d_2 \neq c_2$, we distinguish two cases:

- If $d_2 \notin \mathrm{Im}(\pi)$, with $\gamma = 0$ we have $\gamma \notin \mathrm{Im}(\pi)$ and $\gamma + d_2 \notin \mathrm{Im}(\pi)$.
- If $d_2 \in \mathrm{Im}(\pi)$, $d_2 \neq c_2$, then for any $\gamma \in W$, $\gamma \neq d_2$ (here we use $m \geq 2$) we have $d_2 + \gamma \in \mathrm{Im}(\pi)$.

Hence for $d = (d_1, d_2)$ with $d_2 \neq c_2$, Property (5.1) does not hold. We conclude the following lemma.

Lemma 6.4. *There exist semibent functions g_1, g_2 which both satisfy (5.1) for $c = 1$ and for which there is no $c \neq 1$ such that both, g_1 and g_2, satisfy (5.1).*

Proof. With the above described procedure we can construct a semibent function $g_1 : \mathbb{F}_2^{2m+1} \to \mathbb{F}_2$ satisfying (5.1) if and only if $c = (j_1, \ldots, j_m, 1, 1 \ldots, 1)$, $j_i \in \mathbb{F}_2$. Switching variables we can construct a semibent function g_2 satisfying (5.1) if and only if $c = (1, 1 \ldots, 1, j_{m+2}, \ldots, j_{2m+1})$, $j_i \in \mathbb{F}_2$. The semibent functions g_1, g_2 satisfy then the required properties. □

Remark 6.5. Lemma 6.4 also finishes the proof of Corollary 5.3.

As we observed above, many linear coordinate transformations preserve the property $\mathcal{W}_g(u)\mathcal{W}_g(u+1) = 0$ of a partially bent (semibent) function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. However as we will point out in the following, EA-equivalence transformations on quadratic semibent functions still do not provide new relative difference sets in $\mathbb{F}_2^{n-1} \times \mathbb{Z}_4$.

We recall that Ω_1 is the group of linearized permutations $\mathcal{L}$ on $\mathbb{F}_{2^n}$ satisfying $\mathrm{Tr}_n(\mathcal{L}(x)) = \mathrm{Tr}_n(x)$.

Proposition 6.6. *Two linearized permutations H_1 and H_2 of $\mathbb{F}_{2^n}$ are in the same left coset of Ω_1 if and only if $\mathrm{Tr}_n(H_1^{-1}(x)) = \mathrm{Tr}_n(H_2^{-1}(x)) = \mathrm{Tr}_n(cx)$ for some nonzero $c \in \mathbb{F}_{2^n}$.*

Proof. Note that the identity $\mathrm{Tr}_n(H_1^{-1}(x)) = \mathrm{Tr}_n(H_2^{-1}(x))$ holds if and only if $\mathrm{Tr}_n(H_1^{-1} \circ H_2(x)) = \mathrm{Tr}_n(x)$ holds. By definition of Ω_1, this holds if and only if $H_1^{-1} \circ H_2(x) \in \Omega_1$, and our claim follows. □

Accordingly, we denote the left coset containing the linear transformations H satisfying $\mathrm{Tr}_n(H^{-1}(x)) = \mathrm{Tr}_n(cx)$ for a nonzero $c \in \mathbb{F}_{2^n}$ by S_c. Note that then $\Omega_1 = S_1$. Let g be a semibent function such that $g + \sigma$ is negabent. If $H \in S_c$, the function $g \circ H + \sigma$ is also negabent if and only if $\mathcal{W}_g(u)\mathcal{W}_g(u+c) = 0$ for all $u \in \mathbb{F}_{2^n}$, using Lemma 5.1. Furthermore, for a partially semibent function g and $H \in O(g)$, i.e. $g \circ H = g$, we have

$$\mathcal{W}_{g\circ H}(u)\mathcal{W}_{g\circ H}(u+1) = \mathcal{W}_g(u)\mathcal{W}_g(u+1) = 0 \ ,$$

and hence $H \in S_c$ for some $c \notin \Lambda_g^{\perp}$ by Corollary 6.2. In particular, we have $O(g) \subset \cup_{c \notin \Lambda_g^{\perp}} S_c$. We will use the following lemma.

Lemma 6.7. *Let $g : \mathbb{F}_{2^n} \to \mathbb{F}_2$, n odd, be a semibent function such that for all $u \in \mathbb{F}_{2^n}$ we have $\mathcal{W}_g(u)\mathcal{W}_g(u+1) = 0$ and $\mathcal{W}_g(u)\mathcal{W}_g(u+c) = 0$ for some nonzero $c \in \mathbb{F}_{2^n}$, and let $H \in S_c$. Then $g \circ H + \sigma$ and $g + \sigma$ are equivalent negabent functions if and only if*

$$g \circ \tilde{H}(x) = g(x + \alpha) + \mathrm{Tr}_n(\beta x) + c$$

for some $\tilde{H} \in S_c$, $\alpha, \beta \in \mathbb{F}_{2^n}$ and $c \in \mathbb{F}_2$.

Proof. By Lemma 5.1 the assumptions $\mathcal{W}_g(u)\mathcal{W}_g(u+c) = 0$ for all $u \in \mathbb{F}_{2^n}$ and $H \in S_c$ imply that $\tilde{g} = g \circ H$ satisfies $\mathcal{W}_{\tilde{g}}(u)\mathcal{W}_{\tilde{g}}(u+1) = 0$ for all $u \in \mathbb{F}_{2^n}$, hence $g \circ H + \sigma$ is a negabent function. By definition, $g \circ H + \sigma$ and $g + \sigma$ are equivalent if and only there exists $\tilde{\mathcal{L}} \in \Omega_1$ such that

$$g \circ H(x) + \sigma(x) = (g+\sigma)(\tilde{\mathcal{L}}(x) + \alpha) + \sigma(\tilde{\mathcal{L}}(x)) + \sigma(x) + \mathrm{Tr}_n(ax) + b \tag{6.3}$$

for some $\alpha, a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_2$. By the additive property of σ in Equation (2.2), we conclude that Equation (6.3) holds if and only if

$$g \circ H(x) = g(\tilde{\mathcal{L}}(x) + \alpha) + \mathrm{Tr}_n(\tilde{b}x) + c \tag{6.4}$$

for some $\alpha, \tilde{b} \in \mathbb{F}_{2^n}$ and $c \in \mathbb{F}_2$. With $\tilde{H} = H \circ \tilde{\mathcal{L}}^{-1}$ the claim follows. □

In particular, by Lemma 6.7, the functions $g \circ H + \sigma$ and $g + \sigma$ are equivalent for any $H \in S_c$, if $g \circ \tilde{H}(x) = g(x)$ for some $\tilde{H} \in S_c$, i.e. if $S_c \cap O(g)$ is not empty. We will use this observation to show the following result.

Corollary 6.8. *For a linear coordinate transformation H let g and $\tilde{g} = g \circ H$ be quadratic semibent functions such that both $g + \sigma$ and $\tilde{g} + \sigma$ are negabent. Then the difference sets in G induced by $g + \sigma$ and $\tilde{g} + \sigma$ are equivalent.*

Proof. We first recall that $H \in S_c$ for some $c \notin \Lambda_g^\perp$. With the above observations it is sufficient to show that for all $c \notin \Lambda_g^\perp$ we have $S_c \cap O(g) \neq \emptyset$. For the proof we switch to multivariate notation, in which case the set S_c consists of the invertible matrices A for which $1 \cdot x = c \cdot Ax$. First we show that $S_c \cap O(g)$ is not empty for all $c \notin \Lambda_g^\perp$ for the standard quadratic semibent function $g : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ given by

$$g(x_1, \ldots, x_n) = x_1x_2 + \cdots + x_{n-2}x_{n-1} \ .$$

Observe that then the linear space Λ_g of g is $\{(0, \ldots, 0), (0, \ldots, 0, 1)\}$. That is, $c = (c_1, \ldots, c_n) \notin \Lambda_g^\perp$ if and only if $c_n = 1$. Let $A = (a_{i,j})$ be an $n \times n$ matrix such that $a_{i,i} = 1$ for $i = 1, \ldots, n$ and $a_{i,j} = 0$ for all $i \neq j$ and $i \neq n$. It can be easily seen that $g(Ax) = g(x)$, i.e. $A \in O(g)$, independently from the choice of the last row (except that $a_{n,n}$ has to be 1). This will enable us to construct a matrix $A \in S_c \cap O(g)$ for any given $c = (c_1, \ldots, c_n) \notin \Lambda_g^\perp$: we require for A being in S_c that $1 \cdot x = c \cdot Ax$, which applies if and only if

$$x_1 + \cdots + x_n = c_1x_1 + \ldots + c_{n-1}x_{n-1} + c_n(a_{n,1}x_1 + \ldots + a_{n,n-1}x_{n-1} + x_n). \tag{6.5}$$

Recalling that $c_n = 1$ if $c \notin \Lambda_g^\perp$, this is satisfied for every $x = (x_1, \ldots, x_n)$ with the (unique) choice $a_{n,i} = 1 + c_i$ for $i = 1, \ldots, n-1$.

For an element $c = (c_1, \ldots, c_{n-1}, 1)$ we denote the above constructed matrix by A_c. Let now $\tilde{g}$ be any quadratic semibent function for which $\tilde{g}+\sigma$ is negabent, and consequently $\tilde{g}(x) = g(Bx)$, where $B \in S_d$ for an element $d \notin \Lambda_g^{\perp}$. Recall that then $1 \cdot x = d \cdot Bx$ for all $x \in \mathbb{F}_2^n$. Observe that $O(\tilde{g})$ is then obtained as $O(\tilde{g}) = B^{-1}O(g)B$ since for any $A \in O(g)$

$$\tilde{g}(B^{-1}ABx) = g(BB^{-1}ABx) = g(ABx) = g(Bx) = \tilde{g}(x) \ .$$

As easily seen, the linear space $\Lambda_{\tilde{g}}$ of $\tilde{g}$ is obtained as $\Lambda_{\tilde{g}} = B^{-1}\Lambda_g$. Hence the elements of $\Lambda_{\tilde{g}}$ are of the form $B^t\gamma$ for an element $\gamma \in \Lambda_g^{\perp}$. Therefore $\tilde{c}$ is not in $\Lambda_{\tilde{g}}^{\perp}$ if and only if $\tilde{c} = B^t c$ for some $c \notin \Lambda_g^{\perp}$. To show that $S_{\tilde{c}} \cap O(\tilde{g}) \neq \emptyset$ for any given $\tilde{c} \notin \Lambda_{\tilde{g}}^{\perp}$, we will determine $e = (e_1, \ldots, e_{n-1}, 1)$ such that for the corresponding matrix $A_e \in O(g)$ we have $B^{-1}A_eB \in S_{\tilde{c}}$. Recall that $B^{-1}A_eB \in O(\tilde{g})$.

Let now $\tilde{c} = B^t c$ for some $c \notin \Lambda_{\tilde{g}}^{\perp}$. Then by definition, $B^{-1}A_eB$ is in $S_{\tilde{c}}$ if and only if $1 \cdot x = \tilde{c} \cdot (B^{-1}A_eBx)$ for all x. Together with the fact that $1 \cdot x = d \cdot Bx = x^t B^T d$ for all x, this holds if and only if

$$x^t B^t d = \tilde{c} \cdot (B^{-1}A_eBx) = (x^t B^t A_e^t B^{-t})\tilde{c} = x^t B^t A_e^t B^{-t} B^t c = x^t B^t A_e^t c$$

for all $x \in \mathbb{F}_2^n$. Consequently, $B^{-1}A_eB \in S_{\tilde{c}}$ if and only if $x^t B^t(d + A_e^t c) = 0$ for all $x \in \mathbb{F}_2^n$. Note that by the definition of A_e we have $A_e^t c = (c_1 + e_1 + 1, \ldots, c_{n-1} + e_{n-1} + 1, 1)$, and hence $d + A_e^t c = (d_1 + c_1 + e_1, \ldots, d_{n-1} + c_{n-1} + e_{n-1} + 1, 0)$. Therefore we (uniquely) obtain $e = (c_1 + d_1 + 1, \ldots, c_{n-1} + d_{n-1} + 1, 1)$.

□

7 Conclusion

Negabent functions in $2m$ variables can be obtained from bent functions by adding a certain quadratic polynomial. In this paper we have shown that equivalent bent functions may yield inequivalent negabent functions. We call such functions shifted equivalent. It is also possible that the corresponding designs of shifted equivalent but inequivalent negabent functions are not isomorphic. It would be interesting to understand shifted equivalence better. In particular, it would be nice to find invariants which are invariant under shifted equivalence. Since we found examples of inequivalent but shifted equivalent negabent functions whose corresponding designs are not isomorphic, parameters which are invariant under isomorphism of designs like the rank of an incidence matrix are not good candidates for such invariants.

The situation is different for functions in $2m+1$ variables. One may obtain negabent functions from semibent functions, but in this case equivalent semibent functions give rise to equivalent negabent functions.

In the case of quadratic negabent functions in 4 variables give rise to isomorphic design. Due to the large automorphism group of this design, it may be true that there is only one isomorphism class of designs that can be described by all the negabent functions associated with quadratic bent functions.

It would be also interesting to find infinite classes of shifted equivalent negabent functions which are provable non isomorphic.

Acknowledgement

Nurdagül Anbar is supported by the Austrian Science Fund (FWF): Project F5505–N26 and Project F5511–N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

References

[1] N. Anbar, W. Meidl, Modified planar functions and their components. Cryptogr. Commun. 10 (2018), 235–249.

[2] N. Anbar, C. Kaşıkcı, W. Meidl, A. Topuzoğlu, Shifted plateaued functions, preprint 2018.

[3] C. J. Colbourn, J.H. Dinitz, The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, 2006.

[4] A. Çeşmelioğlu, G. McGuire, W. Meidl, A construction of weakly and non-weakly regular bent functions, J. Comb. Theory, Series A, 119 (2012), 420–429.

[5] L. E. Dickson, Linear groups, Dover publications, Inc., New York, N.Y., 1958.

[6] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997), 235–265.

[7] R. J. McEliece, Quadratic forms over finite fields and second-order Reed-Muller codes, JPL Space Programs Summary, III, (1969), 37–58.

[8] S. Gangopadhyay, E. Pasalic, P. Stănică, A note on generalized bent criteria for Boolean functions. IEEE Trans. Inform. Theory 59 (2013), no. 5, 3233–3236.

[9] C.J. Hillar, D.L. Rhea, Automorphisms of finite abelian groups. Amer. Math. Monthly 114 (2007), 917–923.

[10] X.D. Hou, Classification of self dual quadratic bent functions. Des. Codes Cryptogr. 63 (2012), 183–198.

[11] M.G. Parker, A. Pott, On Boolean functions which are bent and negabent. Sequences, subsequences, and consequences, 9–23, Lecture Notes in Comput. Sci., 4893, Springer, Berlin, 2007.

[12] A. Pott, K.U. Schmidt, Y. Zhou, Semifields, relative difference sets, and bent functions. Algebraic curves and finite fields, 161–178, Radon Ser. Comput. Appl. Math., 16, De Gruyter, Berlin, 2014.

[13] A. Kholoha, A. Pott, Bent and related functions, 262–272. Handbook of Finite Fields, CRC Press, Boca Raton, 2013.

[14] T. Beth, D. Jungnickel, H. Lenz, Design theory, Cambridge University Press, Cambridge 1999.

[15] C. Riera, M.G. Parker, Generalized bent criteria for Boolean functions. I. IEEE Trans. Inform. Theory 52 (2006), no. 9, 4142–4159.

[16] S. Sarkar, Characterizing negabent Boolean functions over finite fields. Sequences and their applications – SETA 2012, 77–88, Lecture Notes in Comput. Sci., 7280, Springer, Heidelberg, 2012.

[17] K.U. Schmidt, M.G. Parker, A. Pott, Negabent functions in the Maiorana-McFarland class. Sequences and their applications – SETA 2008, 390–402, Lecture Notes in Comput. Sci., 5203, Springer, Berlin, 2008.

[18] K.U. Schmidt, Y. Zhou, Planar functions over fields of characteristic two. J. Algebraic Combin. 40 (2014), no. 2, 503–526.

[19] W. Su, A. Pott, X. Tang, Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree. IEEE Trans. Inform. Theory 59 (2013), 3387–3395.

[20] F. Zhang, Y. Wei, E. Pasalic, Constructions of bent-negabent functions and their relation to the completed Maiorana-McFarland class. IEEE Trans. Inform. Theory 61 (2015), 1496–1506.

[21] Y.L. Zheng, X.M. Zhang, On plateaued functions, IEEE Trans. Inform. Theory 47 (2001), no. 9, 1215–1223.

[22] Y. Zhou, $(2n, 2n, 2n, 1)$-relative difference sets and their representations. J. Combin. Des. 21 (2013), no. 12, 563–584.

[23] Y. Zhou, Difference Sets from Projective Planes. PhD-Thesis, OvGU Magdeburg (2013)

[24] Y. Zhou, L. Qu, Constructions of negabent functions over finite fields, Cryprography and Communications 9 (2017), 165–180.