

Geometric and Design-theoretic Aspects of Semibent Functions I

Ulrich Dempwolff, Timo Neumann

Abstract

The two parts of this paper consider combinatorial and geometric aspects of semibent functions. In the first part of this note we obtain 2-designs from semibent functions and we characterize their automorphism groups. In the second part semibent functions of partial spread type with a linear structure are investigated.

1 Introduction

Before we consider semibent functions we recall geometric properties of bent functions which motivate this note. Set $V = V(2n, 2)$ and let $f : V \rightarrow \text{GF}(2)$ be a bent function. It is well known that this implies that the support of f is a difference set in V . Vice versa it can be shown that the characteristic function of a difference set in V is a bent function (see for instance [2], [7], [8]). One can also associate a second symmetric design to a bent function: One takes V as the point set. The blocks are formed by symmetric differences of the support of f with suitable hyperplanes of V , one from each parallel class. The second class of designs was studied in particular by Kantor [10], [11] and by Bending [2] (who calls this design the addition design of f).

Assume now that $V = V(2n + 1, 2)$ has odd dimension. A function $f : V \rightarrow \text{GF}(2)$ is called a *semibent function* if for all $x \in V$ we have

$$\sum_{v \in V} (-1)^{f(v) + v \cdot x} = 0, \pm 2^{n+1}.$$

In this first part of the paper we look for designs associated with semibent functions. The space V cannot contain a difference set by a result of Mann [12] which even excludes the existence of symmetric designs of size 2^{2n+1} . In particular the translates of the support of f cannot form a design. However we will show (Theorem 3.4) that again symmetric differences of the support of f with suitable hyperplanes of V form a design. We also characterize the automorphism group of this design by the automorphism group of the semibent function (Corollary 3.10).

In part II of this paper we consider semibent functions of partial spread type with a linear structure, i.e. a vector $0 \neq v \in V$ such that $x \mapsto f(x) + f(x + v)$ is constant.

2 Preliminary results

Definitions. Set $V = V(m, 2)$. For $f \in \mathcal{F} = \mathcal{F}_m = V^{\text{GF}(2)}$ and $x \in V$ define the *Fourier coefficient* at x by

$$\widehat{f}(x) = \sum_{v \in V} (-1)^{f(v)+v \cdot x}$$

and call the function $\widehat{f} : V \rightarrow \mathbf{C}$ the *Fourier transform* of f . We sometimes identify f with its support $\{x \in V \mid f(x) = 1\}$ and write $v \in f$ if $f(v) = 1$ (i.e. $v \in f^{-1}(1)$). For $x \in V$ define $x^\perp : V \rightarrow \text{GF}(2)$ by $x^\perp(v) = x \cdot v$ and $x^\top : V \rightarrow \text{GF}(2)$ by $x^\top(v) = x \cdot v + 1$. Also by x^\flat we denote one of these functions without specifying it. Finally we set $|f| = |f^{-1}(1)|$. A vector $0 \neq v \in V$ is called a *linear structure* of f if $x \mapsto f(x) + f(x+v)$ is a constant function V . The function $f \in \mathcal{F}_m$ is a *bent function* if m is even and $\widehat{f}(x) \in \{\pm 2^{m/2}\}$ for all $x \in V$ and f is a *semibent function* (see [4], [5]) if m is odd and $\widehat{f}(x) \in \{0, \pm 2^{(m+1)/2}\}$ for all $x \in V$.

Remarks. (a) Bent functions and semibent functions are closely related: the restriction of a bent function to any hyperplane is a semibent function. Conversely, with two complementary semibent functions $f_1, f_2 \in \mathcal{F}_m$ (see [13] or [14]) one can produce a bent function in \mathcal{F}_{m+1} .

(b) In contrast to bent functions semibent functions may have a linear structure. If such a linear structure exists it is unique (see [13] or [14]).

We record for convenience some basic facts about Boolean functions. The proofs can be found for instance in [2], [7], [8], or [13].

Lemma 2.1. For $f \in \mathcal{F}_m$:

(a) $\sum_{x \in V} (-1)^{f(x)} = 2^m - 2|f|$

(b) $\widehat{f}(x) = 2^m - 2|f + x^\perp|$

(c) For $v \in V$ define the character $\chi_v : V \rightarrow \{\pm 1\}$ by $\chi_v(x) = (-1)^{v \cdot x}$.

(i) Let $0 \neq v \in V$. Then

$$\sum_{x \in f^{-1}(1)} \chi_v(x) = - \sum_{x \in f^{-1}(0)} \chi_v(x).$$

(ii) Let $0 \neq v \in V$. Then

$$\widehat{f}(v) = -2 \sum_{x \in f^{-1}(1)} \chi_v(x).$$

Lemma 2.2. *Let $m = 2n + 1$ be odd and f be semibent. Then $|f| = 2^{2n} - 2^n$ if $\widehat{f}(0) = 2^{n+1}$, $|f| = 2^{2n} + 2^n$ if $\widehat{f}(0) = -2^{n+1}$, and $|f| = 2^{2n}$ if $\widehat{f}(0) = 0$.*

Lemma 2.3. *Let $m = 2n + 1$ be odd. Equivalent are:*

- (a) *f is semibent.*
- (b) *$|f + x^\perp| \in \{2^{2n}, 2^{2n} \pm 2^n\}$ for all $x \in V$.*

3 Semibent functions and designs

In this section we set

$$V = V(2n + 1, 2).$$

The following proposition determines intersections of supports of semibent functions of the form $f + b^?$, $b \in V$.

Proposition 3.1. *Let f be semibent and $|B_1| = |B_2|$ for $B_1 = f + x^?$, $B_2 = f + y^?$, and $x \neq y$. Then:*

$$|B_1 \cap B_2| = \begin{cases} 2^{2n-1}, & |B_1| = 2^{2n}, \\ 2^{2n-1} + 2^n, & |B_1| = 2^{2n} + 2^n, \\ 2^{2n-1} - 2^n, & |B_1| = 2^{2n} - 2^n. \end{cases}$$

Proof. As $x^? + y^?$ is of the form $(x + y)^?$:

$$\begin{aligned} 2|B_1 \cap B_2| &= |B_1| + |B_2| - |B_1 \triangle B_2| = 2|B_1| - |f + x^? + f + y^?| \\ &= 2|B_1| - |(x + y)^?| = 2|B_1| - 2^{2n} \\ &= \begin{cases} 2^{2n}, & |B_1| = 2^{2n}, \\ 2^{2n} + 2^{n+1}, & |B_1| = 2^{2n} + 2^n, \\ 2^{2n} - 2^{n+1}, & |B_1| = 2^{2n} - 2^n. \end{cases} \end{aligned}$$

□

The next lemma follows from [4], Prop. 4 but we also indicate it's easy proof.

Lemma 3.2. *Let $f \in \mathcal{F}$ be semibent.*

- (a) *There are precisely 2^{2n} vectors x with $|f + x^\perp| = 2^{2n}$.*
- (b) *Let $|f| = 2^{2n} - 2^n$ and $f(0) = 1$. Then there are precisely $2^{2n-1} - 2^{n-1}$ vectors x with $|f + x^\perp| = 2^{2n} - 2^n$ and precisely $2^{2n-1} + 2^{n-1}$ vectors y with $|f + y^\perp| = 2^{2n} + 2^n$.*

Sketch of proof. Part (a) is a consequence of the well known Parseval equation. To prove part (b) we denote by a_\pm the number of x with $|f + x^\perp| = 2^{2n} \pm 2^n$. By (a) $a_+ + a_- = 2^{2n}$. Moreover using Lemma 2.2 we compute

$$-a_+ + a_- = \frac{1}{2^{n+1}} \sum_{x,v} (-1)^{f(v)+x \cdot v} = -2^n.$$

Hence $2a_- = 2^{2n} - 2^n$. □

Remark. We observe that $|f + x^\perp| = 2^{2n} + \epsilon 2^n$, $\epsilon \in \{\pm 1\}$, implies $|f + x^\top| = 2^{2n} - \epsilon 2^n$.

NOTATION. Let $f \in \mathcal{F}_{2n+1}$ be semibent and $x \in V$. We call $\overline{f}(x) = \widehat{f}(x)/2^{n+1} \in \{0, \pm 1\}$ the *normalized Fourier coefficient* at x .

Assertion (b) of the next lemma characterizes the functions $f + b^?$ whose supports have size $2^{2n} - 2^n$. It will be needed to determine block sizes of the incidence structures defined after this lemma.

Lemma 3.3. *Let $f \in \mathcal{F}$ be semibent, $|f| = 2^{2n} - 2^n$, and $p, b \in V$.*

(a) *Set $A_{p,b} = \overline{f(0)\overline{f + b^\perp}(0)} - (-1)^{f(p)+p \cdot b}$. Then*

$$A_{p,b} = \begin{cases} 2, & p \in f + b^\perp, |f| = |f + b^\perp|, \\ -2, & p \notin f + b^\perp, |f + b^\perp| = 2^{2n} + 2^n, \\ 0, & p \in f + b^\perp, |f + b^\perp| = 2^{2n} + 2^n, \\ & \text{or } p \notin f + b^\perp, |f| = |f + b^\perp|, \\ 1, & p \in f + b^\perp, |f + b^\perp| = 2^{2n}, \\ -1, & p \notin f + b^\perp, |f + b^\perp| = 2^{2n}. \end{cases}$$

(b) *Set $B_{p,b} = \frac{\overline{f + b^\perp}(0)}{2} A_{p,b}$. Then*

$$B_{p,b} = \begin{cases} 1, & p \in f + b^\perp, |f| = |f + b^\perp|, \text{ or } p \in f + b^\top, |f| = |f + b^\top|, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. (a)

$$\overline{f + b^\perp}(0) = \begin{cases} 1, & |f + b^\perp| = |f|, \\ -1, & |f + b^\perp| = 2^{2n} + 2^n, \\ 0, & |f + b^\perp| = 2^{2n}, \end{cases}$$

and

$$(-1)^{f(p)+p \cdot b} = \begin{cases} -1, & p \in f + b^\perp, \\ 1, & p \notin f + b^\perp. \end{cases}$$

The assertion follows.

(b) If $|f + b^\perp| = 2^{2n}$ then $\overline{f + b^\perp}(0) = 0$ and hence $B_{p,b} = 0$.

Assume $|f + b^\perp| = 2^{2n} - 2^n$. Then $\overline{f + b^\perp}(0) = 1$ and by (a)

$$B_{p,b} = \begin{cases} 1, & p \in f + b^\perp, \\ 0, & p \notin f + b^\perp. \end{cases}$$

Assume $|f + b^\perp| = 2^{2n} + 2^n$. Then $\overline{f + b^\perp}(0) = -1$ and by (a)

$$B_{p,b} = \begin{cases} 0, & p \in f + b^\perp, \\ (-1)^2 = 1, & p \notin f + b^\perp. \end{cases}$$

□

Definition. Let f be semibent. By Lemma 3.2 we know that there are precisely 2^{2n} vectors b such that $|f + b^\perp| \neq 2^{2n}$ and for such a b there is precisely one $\epsilon \in \{\perp, \top\}$ such that $|f + b^\epsilon| = 2^{2n} - 2^n$ by the remark following Lemma 3.2. Then we denote by $[b]$ its support $\{x \in V \mid (f + b^\epsilon)(x) = 1\}$. We denote by \mathbf{P} the set of these $[b]$'s. We say $[b]$ is incident (and write $b * p$) with $p \in V$ if $(f + b^\epsilon)(p) = 1$. Set $\mathbf{A}^-(f) = (\mathbf{P}, V, *)$. We call in this context \mathbf{P} the set of *points* and V the set of *blocks*.

Theorem 3.4. $\mathbf{A}^-(f)$ is a $2 - (2^{2n}, 2^{2n-1} - 2^{n-1}, 2^{2n-1} - 2^n)$ design.

Proof. The incidence structure has 2^{2n} points, 2^{2n+1} blocks, and by definition $r = 2^{2n} - 2^n$ blocks at each point. By Proposition 3.1 each pair of points is incident with $2^{2n-1} - 2^n$ blocks. It remains to show that each block contains a constant number k of points which in turn implies that this number is (using the basic equation $v \cdot r = b \cdot k$) $k = \frac{r}{2} = 2^{2n-1} - 2^{n-1}$. By Lemma 3.3 (b) the number of points incident with the block p is

$$k_p = \sum_{b \in V} B_{b,p} = \sum_{b \in V} \frac{\overline{f + b^\perp}(0)}{2} (\overline{f(0)f + b^\perp}(0) - (-1)^{f(p)+p \cdot b}).$$

It is sufficient to show that the number

$$\sum_{b \in V} \overline{f + b^\perp}(0) (-1)^{f(p)+p \cdot b}$$

is independent of p . We compute:

$$\begin{aligned} \sum_{b \in V} \overline{f + b^\perp}(0) (-1)^{f(p)+p \cdot b} &= \frac{1}{2^{n+1}} \sum_{b,v} (-1)^{f(v)+v \cdot b + f(p)+p \cdot b} \\ &= \frac{1}{2^{n+1}} \sum_v (-1)^{f(v)+f(p)} \sum_b (-1)^{(v+p) \cdot b} \\ &= \frac{1}{2^{n+1}} \sum_v (-1)^{f(v)+f(p)} 2^{2n+1} \delta_{0,v+p} \\ &= \frac{1}{2^{n+1}} (-1)^{2f(p)} 2^{2n+1} = 2^n \end{aligned}$$

□

Definition. Let f be semibent. Then f defines in a completely analogous fashion a $2 - (2^{2n}, 2^{2n-1} + 2^{n-1}, 2^{2n-1} + 2^n)$ design $\mathbf{A}^+(f)$ if we take the $f + b^\epsilon$

with $|f + b^\epsilon| = 2^{2n} + 2^n$. Following Bending we call the designs $\mathbf{A}^-(f)$ and $\mathbf{A}^+(f)$ the *addition designs of f* .

Designs with repeated blocks are exactly those which are induced by semibent functions with a linear structure:

Theorem 3.5. *Let $f \in \mathcal{F}$ be semibent. Equivalent are:*

- (a) *f has a linear structure.*
- (b) *Every block in $\mathbf{A}^-(f)$ and $\mathbf{A}^+(f)$ has multiplicity 2.*
- (c) *One block in $\mathbf{A}^-(f)$ or $\mathbf{A}^+(f)$ has multiplicity > 1 .*

Proof. The implication (b) \Rightarrow (c) is trivial.

Set $\mathcal{B} = \{b \in V \mid \widehat{f}(b) \neq 0\}$.

(c) \Rightarrow (a). Assume that the two vectors v, w induce the same block in $\mathbf{A}^-(f)$. For $b \in \mathcal{B}$ we have an $\epsilon \in \{\perp, \top\}$ such that $f + b^\epsilon$ represents a point and

$$f(v) + b^\epsilon(v) = f(w) + b^\epsilon(w), \text{ i.e. } f(v) + v \cdot b = f(w) + w \cdot b.$$

The last equation holds for all $b \in \mathcal{B}$. This shows that $v + w$ is perpendicular to all vectors in $\mathcal{B}_0 = \mathcal{B} + b_0$, $b_0 \in \mathcal{B}$. As $|\mathcal{B}_0| = 2^{2n}$ we see that \mathcal{B}_0 is a subspace of dimension $2n$. Then $V - \mathcal{B}$ is either a hyperplane or the complement of a hyperplane. By [13], (2.29) **(Lemma.** *Let f be semibent. Set $V_=(f) = \{x \in V \mid \widehat{f}(x) = 0\}$. Then exactly one of the following holds: (1) f admits a linear structure $v \in V$, $\dim\langle V_=(f) \rangle = 2n$, and $f(x + v) = f(x) + 1$ for $x \in V$. (2) f admits a linear structure $v \in V$, $\dim\langle V_=(f) + v \rangle = 2n$, and $f(x + v) = f(x)$ for $x \in V$. (3) $\dim\langle V_=(f) \rangle = \dim\langle V_=(f) + v \rangle = 2n + 1$ and f does not have a linear structure.)* f has a linear structure.

(a) \Rightarrow (b). Suppose that f has a linear structure v and set $H = \langle v \rangle^\perp$. By [13], (2.29) $\{\mathcal{B}, V - \mathcal{B}\} = \{H, V - H\}$.

Assume $H = V - \mathcal{B}$. By [13], (2.29) $f(x + v) = f(x) + 1$ for all $x \in V$. Then for $b \in \mathcal{B}$

$$f(x + v) + (x + v) \cdot b = f(x) + 1 + x \cdot b + 1 = f(x) + x \cdot b$$

which implies that the point represented by $f + b^\top$ is incident with x and $x + v$, i.e. these two vectors induce the same block.

Assume $H = \mathcal{B}$. By [13], (2.29) $f(x + v) = f(x)$ for all $x \in V$ and a similar computation shows that x and $x + v$ induce the same block. \square

Remark. If f has a linear structure v one can identify multiple blocks. In this way the design $\mathbf{A}^-(f)$ ($\mathbf{A}^+(f)$) is converted into a symmetric $2 - (2^{2n}, 2^{2n-1} - 2^{n-1}, 2^{2n-2} - 2^{n-1})$ design $\mathbf{A}^-(f)'$ (symmetric $2 - (2^{2n}, 2^{2n-1} + 2^{n-1}, 2^{2n-2} + 2^{n-1})$ design $\mathbf{A}^+(f)'$). We may assume $v \cdot v = 1$ (as any automorphism of V preserves the semibent property of a function and the existence

of a linear structure as well). Set $W = \langle v \rangle^\perp$. Then it is easy to see that $\mathbf{A}^-(f)' \simeq \mathbf{A}^-(f_W)$ ($\mathbf{A}^+(f)' \simeq \mathbf{A}^+(f_W)$) where $\mathbf{A}^-(f_W)$ and $\mathbf{A}^+(f_W)$ are the addition designs of the bent function f_W (see [2], [11]).

For the remainder of this section we consider the automorphism groups of the addition designs. We follow the work of Bending [2], sec. 10 and generalize slightly his arguments. Since his thesis was not published in a journal we take the liberty to present all proofs in detail. As Bending characterized the automorphism groups of addition designs of bent functions and in view of the remark above, it suffices to consider only semibent functions which do not have a linear structure.

THE GROUP $\text{GB}(V)$. The following group defines equivalence of semibent functions in the most general way (see [2], [9]). For $[A, p, b, \epsilon] \in \text{GB}(V) = \text{GL}(V) \times V \times V^t \times \text{GF}(2)$ and $f \in \mathcal{F}$ define the function $[A, p, b, \epsilon]f \in \mathcal{F}$ by

$$[A, p, b, \epsilon]f(x) = f(xA + p) + x \cdot b + \epsilon.$$

By a straightforward computation we obtain

$$[A, p, b, \epsilon] \circ [B, q, c, \nu] = [AB, pB + q, b + Ac, p \cdot c + \epsilon + \nu].$$

This shows that these mappings form a subgroup of $\text{Sym}(\mathcal{F})$ which is isomorphic to the matrix group

$$\left\{ \left(\begin{array}{ccc} 1 & 0 & 0 \\ b & A & 0 \\ \epsilon & p & 1 \end{array} \right) \mid [A, p, b, \epsilon] \in \text{GB}(V) \right\} \leq \text{GL}(2n + 2, 2).$$

We note that a semibent function is mapped by $[A, p, b, \epsilon]$ onto a semibent function again. The stabilizer $\text{GB}(V)_f = \{[A, p, c, \epsilon] \in \text{GB}(V) \mid [A, p, c, \epsilon]f = f\}$ is the *automorphism group* of f . Our aim is to show that this group coincides with the automorphism group of the associated addition designs (see Corollary 3.10).

Lemma 3.6. *Let π be a permutation of $W = V(m, 2)$, $m \geq 3$, and \mathcal{A} a set of (affine) hyperplanes which is invariant under π . Assume further that v_1, \dots, v_m is a basis of W and $v_1^?, \dots, v_m^? \in \mathcal{A}$. Then $\pi \in \text{AGL}(W)$.*

Proof. Set $\mathcal{A}^* = \mathcal{A} \cup \{W - X \mid X \in \mathcal{A}\}$. Then \mathcal{A}^* is π -invariant too. Therefore we may assume from now on $\mathcal{A}^* = \mathcal{A}$. In particular $v_1^\perp, \dots, v_m^\perp \in \mathcal{A}$. Denote by $\langle \mathcal{A} \rangle$ the abelian group generated by \mathcal{A} with respect to the symmetric difference of sets. Since $(X \Delta Y)\pi = X\pi \Delta Y\pi$ we may even assume $\langle \mathcal{A} \rangle = \mathcal{A}$. Moreover $u^\perp \Delta w^\perp = (u + w)^\perp$ for $u, v \in W$. Hence, by assumption we can assume that \mathcal{A} is the set of all hyperplanes. In particular $\text{AGL}(W)$ leaves \mathcal{A} invariant. Choose $\tau \in \text{AGL}(W)$ such that $\pi\tau$ fixes the vector 0. Then $\pi\tau$ leaves the set of all linear hyperplanes invariant, i.e. $\pi\tau$ is an automorphism of the point-hyperplane design associated with W . A theorem of Dembowski-Wagner [6] shows that $\pi\tau$

is a collineation of $\text{PG}(W)$. Therefore by the fundamental theorem of projective geometry $\pi\tau \in \text{PGL}(W) = \text{GL}(W)$ which implies $\pi \in \text{AGL}(W)$. \square

Lemma 3.7. *Let $\beta : x \mapsto xA + v$ be an invertible, affine transformation on V and $g \in \mathcal{F}$. Denote by $g\beta$ the function whose support is the image of the support of g under β . Then $g\beta = [A^{-1}, vA^{-1}, 0, 0]g$, i.e. $g\beta(x) = g(\beta^{-1}(x)) = g(xA^{-1} + vA^{-1})$.*

Proof. $y = xA + p \in g\beta$ iff $x = yA^{-1} + pA^{-1} \in g$. Hence $g\beta(y) = 1 \Leftrightarrow g(yA^{-1} + pA^{-1}) = 1$. \square

NOTATION. Let f be semibent. We define $f_* : V \rightarrow \text{GF}(2)$ by $f_*(b) = 1$ if $|f + b^\perp| = 2^{2n} - 2^n$ and $f_*(b) = 0$ otherwise. Then the point $[b]$ in $\mathbf{A}^-(f)$ is represented by $f + b^\perp + f_*(b) + 1$.

Proposition 3.8. *Let $f, g \in \mathcal{F}$ be semibent functions which have no linear structure. Let $|f| = |g| = 2^{2n} - 2^n$ and let $\alpha : \mathbf{A}^-(f) \rightarrow \mathbf{A}^-(g)$ be an isomorphism of designs. Then there exists an element $[A, p, c, \epsilon] \in \text{GB}(V)$ with $g = [A, p, c, \epsilon]f$, $\epsilon = f_*(A^{-1}c) + p \cdot A^{-1}c + 1$ such that $x\alpha = xA^{-1} + pA^{-1}$, $x \in V$, and $[b]\alpha = [Ab + c]$, $[b] \in \mathbf{P}$.*

Proof. Let \mathcal{A}_f be the set of symmetric differences of elements from \mathbf{P} (of $\mathbf{A}^-(f)$). As f has no linear structure \mathcal{A}_f satisfies the assumptions of Lemma 3.6. The same holds for \mathcal{A}_g (defined analogously as \mathcal{A}_f), and by the proof of this lemma we can even assume $\mathcal{A}_g = \mathcal{A}_f$. Therefore α induces on V an affine transformation. Choose $A \in \text{GL}(V)$ and $p \in V$ such that $x\alpha = xA^{-1} + pA^{-1}$. Also $f\alpha = g + c^\perp + \epsilon$ with $|f| = |g + c^\perp + \epsilon|$. Lemma 3.7 implies

$$f(xA + p) = g(x) + x \cdot c + \epsilon, \quad x \in V.$$

Therefore $g = [A, p, c, \epsilon]f$. Set $y = xA + p$. Then

$$[A, p, c, \epsilon]f(x) = f(xA + p) + x \cdot c + \epsilon = f(y) + y \cdot (A^{-1}c) + p \cdot (A^{-1}c) + \epsilon.$$

Now $|f| = |g|$ implies $f_*(A^{-1}c) + 1 = p \cdot A^{-1}c + \epsilon$. I.e. $\epsilon = f_*(A^{-1}c) + p \cdot A^{-1}c + 1$.

As $f + b^\perp + f_*(b) + 1$ represents $[b] \in \mathbf{P}$ we get by Lemma 3.7

$$\begin{aligned} (f + b^\perp + f_*(b) + 1)\alpha(x) &= f(xA + p) + (xA + p) \cdot b + f_*(b) + 1 \\ &= g(x) + x \cdot c + \epsilon + (xA + p) \cdot b + f_*(b) + 1 \\ &= g(x) + x \cdot (Ab + c) + p \cdot (b + A^{-1}c) + f_*(b) + f_*(A^{-1}c). \end{aligned}$$

This implies $[b]\alpha = [Ab + c]$. \square

Corollary 3.9. *Let f be semibent, $|f| = 2^{2n} - 2^n$ and $[A, p, c, \epsilon] \in \text{GB}(V)$ such that $[A, p, c, \epsilon]f = f$. Then this map induces $\alpha \in \text{Aut}(\mathbf{A}^-(f))$ such that $x\alpha = xA^{-1} + pA^{-1}$, $x \in V$, and $[b]\alpha = [Ab + c]$, $[b] \in \mathbf{P}$.*

Proof. Define $x\alpha = xA^{-1} + pA^{-1}$ and let $[b]\alpha$ be represented by

$$\begin{aligned} (f + b^\perp + f_*(b) + 1)\alpha(x) &= f(xA + p) + (xA + p) \cdot b + f_*(b) + 1 \\ &= f(x) + x \cdot (Ab + c) + p \cdot (b + A^{-1}c) + f_*(b) + f_*(A^{-1}c) \end{aligned}$$

By Lemma 3.7 this function has size $2^{2n} - 2^n$ and represents therefore $[Ab + c]$. Moreover $q \in [b]$ (i.e. $f(q) + q \cdot b + f_*(b) + 1 = 1$) is equivalent to $q\alpha \in [Ab + c]$ (again by Lemma 3.7). Hence $[A, p, c, \epsilon]$ defines an automorphism α of $\mathbf{A}^-(f)$ with $x\alpha = xA^{-1} + pA^{-1}$ and $[b]\alpha = [Ab + c]$. \square

Proposition 3.8 and Corollary 3.9 imply:

Corollary 3.10. *Let f be semibent, $|f| = 2^{2n} - 2^n$. Then*

$$\text{Aut}(\mathbf{A}^-(f)) = \text{Aut}(\mathbf{A}^+(f)) \simeq \text{GB}(V)_f.$$

4 Properties shared by semibent and plateaued functions

Let $m \geq 4$ be an arbitrary integer. A function $f \in \mathcal{F}_m$ is called *plateaued* if there exist a number $r \geq m/2$ such that $\widehat{f}(x) \in \{0, \pm 2^r\}$ for all $x \in V = V(m, 2)$ (see [4] or [14]). Bent functions ($r = m/2$) and semibent functions ($r = (m + 1)/2$) are special cases of plateaued functions. We describe combinatorial and geometric properties which all plateaued functions share. Under (a) we observe that addition designs are always present. There are also connections to perfect ternary arrays (b) and regular graphs (c).

(a) There are precisely 2^{2m-2r} vectors such that $\widehat{f}(x) \neq 0$ and $|f| = 2^{m-1} - \epsilon 2^{r-1}$ where ϵ is the sign of $\widehat{f}(0)$ (see [4], Prop. 4). For $\epsilon = \pm 1$ there are precisely 2^{2m-2r} functions $f + b^?$ such that its support $[b]$ has size $2^{m-1} - \epsilon 2^{r-1}$. Taking again these $[b]$'s as the point set of an incidence structure and V as the set of blocks we obtain a $2 - (2^{2m-2r}, 2^{2m-2r} - \epsilon 2^{m-r-1}, 2^{m-2} - \epsilon 2^{r-1})$ design. The verification is literally the same as the proof of Theorem 3.4. However as r increases these designs become gradually less interesting.

(b) Define for the plateaued function f the matrix

$$A = (2^{-r} \widehat{f}(x + y))_{x, y \in V} \in \{0, \pm 1\}^{2^m \times 2^m}.$$

Then $A^2 = 2^{3n-2r} \mathbf{1}_{2^m \times 2^m}$ which shows that A is a perfect ternary array of strength 2^{3n-2r} over V (see [1]). Thus plateaued functions can be viewed as perfect ternary arrays over elementary abelian 2-groups.

(c) Define for the plateaued function f a graph Γ on V by joining x with y iff $f(x + y) = 1$. Then Γ is a regular graph and V acts as a vertex-transitive group. Let $x \in V$. We call $W_f(x) = \sum_{y \in V} (-1)^{x \cdot y} f(y)$ the *Walsh coefficient* at

x . Note that $W_f(x) = -\widehat{f}(x)/2$ if $x \neq 0$ and $W_f(0) = |f|$. The eigenvalues of the adjacency matrix are the Walsh coefficients (see Bernasconi, Codenotti [3]). In particular Γ has 3 eigenvalues if f is bent and Γ is then a strongly regular graph. If f is plateaued but not bent the graph has 4 eigenvalues. It seems that not much is known about these graphs.

References

- [1] K.T. Arasu, J.F. Dillon, Perfect ternary arrays, in Difference sets, sequences and their correlation properties (Bad Windsheim 1998), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 542, Kluver, 1999.
- [2] T. Bending, Bent functions, SDP designs and their automorphism groups, Thesis, Queen Mary and Westfield College, Univ. London, 1993.
- [3] A. Bernasconi, C. Codenotti, Spectral analysis of boolean functions as a graph eigenvalue problem, IEEE Trans. Computers, 50(2001), 984-985.
- [4] A. Canteaut, P. Charpin: Decomposing bent functions, IEEE Trans. Inf. Theory, 49(2003), 2004-2019.
- [5] S. Chee, S. Lee, K. Kim, Semi-bent functions, LNCS 917, *Advances in cryptology* (ASIACRYPT-94), Springer, 1994, pp. 107-118.
- [6] P. Dembowski, A. Wagner, Some characterizations of finite projective spaces, Arch. Math. 11(1960), 465-469.
- [7] J. Dillon, A survey of bent functions, NSA Tech. Jour., Special Issue, 1972, 191-215.
- [8] J. Dillon, Elementary Hadamard difference sets, in Proc. 6-th. S.E. Conf. Comb., Graph Theory and Computing, Utilitas Math. Boca Raton, 1975, 237-249.
- [9] X. Hou, Cubic bent functions, Discrete Math., 189(1998), 149-161.
- [10] W. Kantor, Symplectic groups, symmetric designs and line ovals, Jor. Alg. 33(1975), 43-58.
- [11] W. Kantor, Exponential numbers of two weight codes, difference sets and symmetric designs, Discrete Math. 46(1983), 95-98.
- [12] B. Mann, Difference sets in elementary abelian groups, Ill. Jour. Math. 9(1965), 212-219.
- [13] T. Neumann, "Bent functions", Diploma Thesis, Universität Kaiserslautern, 2006.
<http://www.mathematik.uni-kl.de/~dempw/Thesis.html>

- [14] Y. Zheng, X.-M. Zhang, Relationships between bent functions and complementary plateaued functions, LNCS 1787, ICISC 99, Springer 1999, pp. 60-75.