

Geometric and Design-theoretic Aspects of Semibent Functions II

Ulrich Dempwolff

Abstract

This paper is the successor of [8]. We now consider semibent functions with a linear structure. Semibent functions of partial spread type with a linear structure seem to be rare. We distinguish four classes of such semibent functions. For three classes we exhibit some examples.

1 Introduction

We continue the investigation of geometric properties of semibent functions which was begun in [8].

A semibent function $f : V = V(2n + 1, 2) \rightarrow \text{GF}(2)$ has a *linear structure* $0 \neq v \in V$, if $x \mapsto f(x) + f(x + v)$, $x \in V$, is constant. The two major constructions of bent functions, the Maiorana-McFarland type and the partial spread type, have analogues for semibent functions. We consider both classes of functions with the additional property of having a linear structure.

It can be easily seen that the Maiorana-McFarland type provides an abundant number of examples (see Example 3.1). On the other hand a computer search in dimension 7 for semibent functions of partial spread type with a linear structure rather surprisingly produced (up to equivalence) only six examples. Therefore the search for semibent functions of partial spread type with a linear structure appears to be an interesting task which motivated this note.

In section 3 we show that such semibent functions can be subdivided in four classes (Proposition 3.3). The major purpose of this note is to provide examples for each class and to find infinite series of semibent functions of the desired type: in fact we were able to find examples for three classes (Examples 3.4, 3.6 and Theorem 3.5) and we provide three infinite series (Example 3.4, Theorem 3.5). Note that some of these semibent functions are certainly known but the question of the simultaneous existence of a linear structure and a partial spread is more delicate.

The restriction of a bent function to a hyperplane is a semibent function [4]. In section 4 we investigate the question which of our examples is obtained as the restriction of a bent function of partial spread type to a hyperplane.

2 Notation and preliminary results

We introduce in this chapter some notation and list few preliminary results. The symbol $V(m, q)$ will always denote a m -dimensional vector space over $\text{GF}(q)$ and a symbol χ_B will denote the characteristic function of a set B .

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 . For $x \in V$ define $x^\perp : V \rightarrow \text{GF}(2)$ by $x^\perp(v) = x \cdot v$. 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* if m is odd and $\widehat{f}(x) \in \{0, \pm 2^{(m+1)/2}\}$ for all $x \in V$. The following, well-known result (see [8], 2.1 or [11]) will be needed later.

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 $\delta_v : V \rightarrow \{\pm 1\}$ by $\delta_v(x) = (-1)^{v \cdot x}$.

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

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

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

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

Remark. We recall the two major construction of bent-functions: Let $V = V(2n, 2)$. Write a vector in V as (x, y) with $x, y \in \text{GF}(2)^n$. Let π be an arbitrary permutation of $\text{GF}(2)^n$ and $g \in \mathcal{F}_n$. Then the function f defined by

$$f(x, y) = \pi(x) \cdot y + g(x)$$

is a bent function of *Maiorana-McFarland type*.

A *partial spread* in a vector space is a collection of pairwise disjoint subspaces. Let \mathcal{T} be a partial spread of n -dimensional subspaces of size 2^{n-1} or $2^{n-1} + 1$ in $V = V(2n, 2)$. Set

$$C = \begin{cases} \bigcup_{X \in \mathcal{T}} X^*, & |\mathcal{T}| = 2^{n-1} \\ \bigcup_{X \in \mathcal{T}} X, & |\mathcal{T}| = 2^{n-1} + 1. \end{cases}$$

Then $g = g_{\mathcal{T}} = \chi_C$ is a bent function of *partial spread type* (Dillon [11], [12]).

Orthogonal spaces over $\text{GF}(2)$. We recall some facts from geometric algebra (see [1], [10] or [14] for instance). Let V be a finite dimensional vector space over the field F and Q a quadratic form on V . We denote by b the symmetric bilinear form associated to Q which is defined by polarization: $b(v, w) = Q(v + w) - Q(v) - Q(w)$. From now on we assume that $F = \text{GF}(q)$ is finite and has characteristic 2. Then b is alternating (i.e. $b(v, v) = 0$ for all v).

Assume first that $\dim V = 2n$ is even. We recall that a subspace is totally singular if Q vanishes on this subspace. There are precisely two non-degenerate (i.e. (V, b) is a non-degenerate symplectic space) inequivalent forms which are distinguished by the Witt-Index. We say V is of *(+)-type* if V has Witt-index n (there exist totally singular subspaces of dimension n) and V has *(-)-type* if V has Witt-index $n - 1$ (i.e. there exist no totally singular subspaces of dimension n). If $q = 2$ then it is well known that a quadratic form is bent iff it is non-degenerate.

Assume now that $\dim V = 2n + 1$ is odd. Then the alternating form b must have a nontrivial radical. We are interested in the case that the radical V_0 is 1-dimensional. Let W be any complement of V_0 in V . Then W is non-degenerate with respect to Q . If Q vanishes on the radical we obtain two isometry classes according to the type of W . If Q does not vanish on the radical then we obtain only one isometry class since there exists another complement U of the radical which has the opposite type of W . We call this last class non-degenerate. Note that these quadratic forms are obtained by restricting a non-degenerate form in dimension $2n + 2$ to a hyperplane. If $q = 2$ it is easy to see that a quadratic form Q is semibent iff its associated alternating form has a radical of dimension 1. Finally we note that the alternating form b can be lifted to V/V_0 by

$$\bar{b}(u + V_0, v + V_0) = b(u, v)$$

turning this factor space into a symplectic space (i.e. \bar{b} is non-degenerate). The following lemma will be needed in the next section.

Lemma 2.2. *Let V be a non-degenerate symplectic space of dimension $2n$ over $\text{GF}(2)$ and let $G \simeq \text{AGL}(1, 2^n)$ be a subgroup of the symplectic group on V . Let Z be a cyclic subgroup of order $2^n - 1$ in G which acts semiregularly on V (i.e. $C_V(z) = \{v \in V \mid vz = v\} = 0$ for $1 \neq z \in Z$). Then a generator of Z has on V the eigenvalues $\omega, \omega^2, \dots, \omega^{2^{n-1}}$ and $\omega^{-1}, \omega^{-2}, \dots, \omega^{-2^{n-1}}$ where ω is suitably chosen generator of $\text{GF}(2^n)^*$.*

Proof. Let P be the normal Sylow 2-subgroup of G . Then we have a series

$$0 = V_0 \subset V_1 \subset \dots \subset V_m = V, \quad m \geq 2,$$

where V_j is the counter image of $C_{V/V_{j-1}}(P)$ in V (see [2], (5.15)). Clearly, all these spaces are Z -invariant. As Z acts semiregularly on V it also acts semiregularly on each factor V_j/V_{j-1} (see [15], I.18.6). Hence $\dim V_j/V_{j-1} \geq n$

which implies $m = 2$ and $\dim V_1 = \dim V/V_1 = n$. The space V_1^\perp and hence $V_1 \cap V_1^\perp$ is Z -invariant too. As the nontrivial vectors of V_1 form a Z -orbit we either have $V_1 = V_1^\perp$ (V_1 is totally singular) or $V_1 \cap V_1^\perp = 0$ (i.e. V_1 is non-degenerate).

Assume that V_1 is non-degenerate. Then $V = V_1 \oplus V_1^\perp$. Hence $u - uy \in V_1^\perp$ for $u \in V_1^\perp$ and $y \in P$. By the definition of $V_2 = V$ we have $u - uy \in V_1$. Hence $u \in C_V(P) = V_1$, i.e. $V = V_1$, a contradiction.

Therefore V_1 is totally singular. Let z be a generator of Z . Then z has the eigenvalues $\omega, \omega^2, \dots, \omega^{2^n-1}$ on V_1 for a suitably chosen generator ω of $\text{GF}(2^n)^*$. As $V_1 = V_1^\perp$ we can identify V/V_1 with the dual space of V_1 (identify $u + V_1 \in V/V_1$ with the linear functional $x \mapsto (x, u)$ where (\cdot, \cdot) is the symplectic form). This shows that the representation of Z on V/V_1 is contragredient (transpose-inverse) to the representation on V_1 . Hence z has the eigenvalues $\omega^{-1}, \omega^{-2}, \dots, \omega^{-2^n-1}$ on V/V_1 . \square

3 Semibent functions possessing a linear structure

In this section we set

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

We will define semibent functions of Maiorana-McFarland type and of partial spread type. We ask which of these constructions produces semibent functions with a linear structure.

Definition. We write a vector in V as $v = (x, y)$, where $x \in U = V(n+1, 2)$ and $y \in W = V(n, 2)$. Let $\phi : W \rightarrow U$ be an injection and $h \in \mathcal{F}_n$. Then $f \in \mathcal{F}_{2n+1}$ defined by

$$f(x, y) = x \cdot \phi(y) + h(y)$$

is semibent (Carlet [6]). We call f of *Maiorana-McFarland type*.

Example 3.1. Denote by $\{e_0, \dots, e_n\}$ the standard basis of U . Assume first that f has a form as above and that the first component of $\phi(y)$ is 0 for all $y \in W$. Then clearly e_0 is a linear structure for f .

This shows that semibent functions of Maiorana-McFarland type with a linear structure are abundant.

The restriction of a bent function to a hyperplane is semibent (see [4]). So the restriction of a bent function of partial spread type to a hyperplane should produce a semibent function of partial spread type. This motivates the definitions below.

Definition. A partial spread \mathcal{S} of subspaces of V is called a *partial spread of type I* if $\dim X = n$ for $X \in \mathcal{S}$, and if $Z \not\subseteq X + Y$ for every 3-set $\{X, Y, Z\} \subseteq \mathcal{S}$.

A partial spread \mathcal{S} of subspaces of V is called a *partial spread of type II* if $\mathcal{S} = \{X_0\} \cup \mathcal{S}_0$ such that $\dim X_0 = n + 1$, $\dim X = n$ for $X \in \mathcal{S}_0$, and if $Z \not\subseteq X + Y$ for every 3-set $\{X, Y, Z\} \subseteq \mathcal{S}$ with $X, Y \in \mathcal{S}_0$.

Remark. The rather technical condition " $Z \not\subseteq X + Y$ etc." will be needed below where we define semibent functions via partial spreads of type I or II. It is easy to see that the proof of the next lemma fails if this condition is violated.

Lemma 3.2. *Let \mathcal{S} be a partial spread in V of type I or II. The following holds:*

- (a) *Let $|\mathcal{S}| = 2^n + 1$. Set $f = f_{\mathcal{S}} = \chi_B$ for $B = \bigcup_{X \in \mathcal{S}} X$. Then f is semibent.*
- (b) *Let $|\mathcal{S}| = 2^n$. Set $f = f_{\mathcal{S}} = \chi_B$ for $B = \bigcup_{X \in \mathcal{S}} X^*$ and $X^* = X - \{0\}$. Then f is semibent.*

Proof. We only prove (a) in the case that the partial spread has type II. The verification of all other cases is similar. We have $|B| = 2^{n+1} + 2^n(2^n - 1) = 2^{2n} + 2^n$ which implies $\widehat{f}(0) = -2^{n+1}$ by Lemma 2.1. Let $0 \neq v \in V$. Assume first $X \not\subseteq \langle v \rangle^\perp$ for all $X \in \mathcal{S}$. Then $\sum_{x \in X^*} \delta_v(x) = -1$. This implies using again Lemma 2.1

$$\widehat{f}(v) = -2(\delta_v(X_0) + \sum_{X \in \mathcal{S}_0} \delta_v(X^*)) = -2 \cdot 2^n(-1) = 2^{n+1}.$$

Assume now that precisely one $X \in \mathcal{S}$ lies in $\langle v \rangle^\perp$. Then $\widehat{f}(v) = -2(2^{n+1} + 2^n(-1)) = -2^{n+1}$ if $X = X_0$, and if $X \neq X_0$ we obtain $\widehat{f}(v) = -2(2^n + 2^n(-1)) = 0$.

If $\langle v \rangle^\perp$ contains two $X, Y \in \mathcal{S}$ then by the definition above $\langle v \rangle^\perp \cap \mathcal{S} = \{X, Y\}$ and $\dim X = \dim Y = n$. Hence $\widehat{f}(v) = -2(2^{n+1} - 1 + (2^n - 1)(-1)) = -2^{n+1}$. \square

This lemma motivates the next definition.

Definition. Semibent functions defined as in Lemma 3.2 are of *partial spread type*. According to this lemma we make a subdivision: Let B be the support of the semibent function $f = f_{\mathcal{S}}$ of partial type. Assume first $0 \in B$. We call f (or B) of *type I.a* or *II.a* if \mathcal{S} has type I or II respectively. Assume now $0 \notin B$. We call f (or B) of *type I.b* or *II.b* if \mathcal{S} has type I or II respectively. Note that $|B| = 2^{2n}$ for type I.a and II.b, $= 2^{2n} + 2^n$ for type II.a and $= 2^{2n} - 2^n$ for type I.b.

The next result explains how a linear structure can occur in a semibent function of partial spread type.

Proposition 3.3. *Let $f = f_{\mathcal{S}} = \chi_B$ be semibent of partial spread type, i.e. $B = \bigcup_{X \in \mathcal{S}} X$ or $B = \bigcup_{X \in \mathcal{S}} X^*$ for some partial spread \mathcal{S} . Let $0 \neq v \in V$ be a linear structure on f . Then one of the following assertions holds:*

- (a) f has type II.a, $v \in X \in \mathcal{S}$, $\dim X = n + 1$, and $f(x) = f(x + v)$ for $x \in V$.
- (b) f has type I.a, $v \notin B$, and $f(x) = f(x + v) + 1$ for $x \in V$.
- (c) f has type I.a, $v \in B$, and $f(x) = f(x + v)$ for $x \in V$.
- (d) f has type I.b, $v \notin B$, and $f(x) = f(x + v)$ for $x \in V$.

Remark. The proposition shows that semibent functions of type II.b do not have a linear structure.

Proof. (1) Let v be in B . Then $f(x) = f(x + v)$ for $x \in V$ and $0 \in B$:

Let $v \in X^*$. Pick $y \in X^* - \{v\}$. Then $v + y \in X^*$ and therefore $f(y) = f(y + v)$. But then $f(x) = f(x + v)$ for all $x \in V$. In particular $f(0) = f(v + v) = f(v)$ which shows $0 \in B$.

(2) Assume $X \in \mathcal{S}$, $\dim X = n + 1$, and $X^* \subseteq B$. Then case (a) holds:

If $v \in B$ then $0 \in B$ (by (1)) and hence $|f| = 2^{2n} + 2^n$ and (a) holds. So assume $v \notin B$. If $0 \in B$ then $f(x) + 1 = f(x + v)$ and V is partitioned into B and $B + v$. But this contradicts $|B| = 2^{2n} + 2^n$. So $0 \notin B$ and with $X = X_0$

$$B = X_0^* \cup \bigcup_{i=1}^{2^n-1} X_i^*.$$

Suppose $f(x) = f(x + v) + 1$ for $x \in V$. Then $f(0) = f(v + v) = f(v) + 1$ and hence $0 \in B$, a contradiction.

Therefore $f(x) = f(x + v)$ for $x \in V$. This shows $X_0^* + v \subseteq B$. We claim

$$|(X_0^* + v) \cap X_i| \leq 1, \text{ for } i \geq 1.$$

If $v + x_0 = x_i$, $v + y_0 = y_i$ with $x_j, y_j \in X_j^*$, $j = 0, i$, then $x_0 + y_0 = x_i + y_i \in X_0 \cap X_i$ which implies $x_0 = y_0$, $x_i = y_i$ and the claim follows. This shows (as $X_0 \cap (X_0^* + v) = \emptyset$)

$$2^{n+1} - 1 = |X_0^*| = \sum_{i=1}^{2^n-1} |(X_0^* + v) \cap X_i^*| \leq 2^n - 1,$$

a contradiction. Note that this argument also shows $v \in X$, $\dim X = n + 1$ in case (a).

We assume from now on $\dim X = n$ for $X \in \mathcal{S}$. Hence either $B = \bigcup_{i=0}^{2^n} X_i$, $|B| = 2^{2n}$ or $B = \bigcup_{i=1}^{2^n} X_i^*$, $|B| = 2^{2n} - 2^n$.

(3) If $|B| = 2^{2n} - 2^n$ assertion (d) holds:

By (1) $v \notin B$. Hence $f(v) = f(0) = f(v + v)$. Therefore $f(x) = f(x + v)$ for $x \in V$ and (d) holds.

(4) If $|B| = 2^{2n}$ assertions (b) or (c) hold:

Assume $v \notin B$. Then $f(0) = f(v+v) \neq f(v)$. Therefore $f(x) = f(x+v) + 1$ for $x \in V$ and assertion (b) is true. Assume now $v \in B$. Then $f(x) = f(x+v)$ for $x \in V$ by the same argument and assertion (c) is true. \square

Remark. Although semibent functions of partial spread type with a non-trivial linear structure seem to be rare there are "obvious" examples which we treat in Example 3.4. They are quadratic forms over $\text{GF}(2)$ and one uses the existence of known, orthogonal or symplectic spreads. As expected the the generator of the radical is in these cases a linear structure. One may conjecture that semibent functions of partial spread type with a linear structure are always quadratic. However Theorem 3.5 and Examples 3.6 show that this conjecture is false. Theorem 3.5 provides a series of the desired semibent functions while Example 3.6 displays some sporadic functions. Note that our examples belong to cases (a), (b), and (d) of Proposition 3.3, i.e. we have no example for case (c).

Examples 3.4. (a) Let $W = V(4m, 2)$ and Q a non-degenerate quadratic form of (+)-type. It is well known that W possesses a partial spread \mathcal{T} of $2m$ -dimensional, totally singular subspaces (see [13], [16]).

Let $0 \neq v \in W$ be singular and set $V = \langle v \rangle^\perp$. Then $\mathcal{S} = \{X \cap V \mid X \in \mathcal{T}\}$ is a partial spread of type II such that $X = X \cap V$ for $v \in X$ while $\dim(X \cap V) = 2m - 1$ if $v \notin X$. Then the restriction Q_V of Q to V is of partial spread type II.a and v is a linear structure. Q_V belongs to case (a) of Proposition 3.3.

Let $w \in W$ be non-singular and set $V = \langle w \rangle^\perp$ and $\mathcal{S} = \{X \cap V \mid X \in \mathcal{T}\}$ then \mathcal{S} is a partial spread of type I.a such that $\dim(X \cap V) = 2m - 1$ for all $X \in \mathcal{T}$. Let $\langle v_0 \rangle$ be the radical with respect to the bilinear form induced by Q_V . Then Q_V is of partial spread type I.a and v_0 is a linear structure. Q_V belongs to case (b) of Proposition 3.3.

(b) Let $V = V(2n + 1, 2)$ and Q a non-degenerate quadratic form on V . Let b be the quadratic form associated to Q . Then the radical (with respect to b) $V_0 = \langle v_0 \rangle$ is one-dimensional and (see sec. 2) b induces on V/V_0 a non-degenerate symplectic form. It is well known (see [13], [16]) that V/V_0 contains symplectic spreads. For a member X/V_0 in such a spread there exists a unique totally singular space X_0 in V such that $X = X_0 \oplus V_0$. Hence V possesses a partial spread \mathcal{S} of n -dimensional, totally singular spaces which covers the set of singular vectors. Let B be the set of singular vectors. Then $B + v_0$ is the set of non-singular vectors. Therefore Q is a semibent function of partial spread type I.a with the linear structure v_0 . In fact Q belongs to case (b) of Proposition 3.3. We observe that this construction covers the second kind of examples in (a) in the case that n is odd.

The following concrete description of these partial spreads will be useful in section 4. Set $F = \text{GF}(2^n)$, $K = \text{GF}(2)$, $V = F \times F \times K$, and define a non-degenerate quadratic form $Q : V \rightarrow K$ by $Q(x, y, z) = \text{tr}(xy) + z$, where

$tr : F \rightarrow K$ is the trace map. Define subspaces ($\alpha \in F$):

$$V(\infty) = \{(x, 0, 0) \mid x \in F\}, \quad V(\alpha) = \{(\alpha x, x, tr(\alpha x^2)) \mid x \in F\}$$

Then $\mathcal{S} = \{V(\infty)\} \cup \{V(\alpha) \mid \alpha \in F\}$ is a partial spread which covers B . Moreover $v = (0, 0, 1)$ is a linear structure since $V - B = B + v$.

Theorem 3.5. *Set $F = \text{GF}(2^n)$ and $K = \text{GF}(2)$, $n \geq 3$, and consider $V = F \times F \times K$ as a K -space. Define $U(\infty) = \{(x, 0, 0) \mid x \in F\}$ and for $\beta \in F$ set*

$$U(\beta) = \{(\beta x^2, x, tr(\beta x)) \mid x \in F\},$$

where $tr : F \rightarrow K$ is the trace map. Then $\mathcal{S} = \{U(\infty)\} \cup \{U(\beta) \mid \beta \in F\}$ is a spread of type I.a. The associated semibent function is not a quadratic form.

Proof. Obviously \mathcal{S} is a partial spread. Define for $\gamma \in F$ the map $t_\gamma \in \text{GL}(V)$ by $(x, y, z)t_\gamma = (x + \gamma y^2, y, z + tr(\gamma y))$. Then $P = \{t_\gamma \mid \gamma \in F\}$ is a group which fixes $U(\infty)$ and acts regularly on $\mathcal{S} - \{U(\infty)\}$. Suppose $U(\alpha) \subseteq U(\beta) + U(\gamma)$. Clearly, for $\alpha \neq 0$, $\beta = 0$, and $\gamma = \infty$ the inclusion is false.

Therefore with respect to the action of P we may assume $\beta \neq \infty \neq \gamma$. Let α be ∞ . For every $x \in F$ there exists $y = y_x, z = z_x \in F$ with $(x, 0, 0) = (\beta y^2, y, tr(\beta y)) + (\gamma z^2, z, tr(\gamma z))$. This implies $z = y$ and $x = \beta y^2 + \gamma z^2 = (\beta + \gamma)y^2$. Thus $x \mapsto y_x$ is injective. Finally, $tr((\beta + \gamma)y) = 0$. Hence $\beta = \gamma$, a contradiction. So we may assume $\alpha \neq \infty$.

With regard to the action of P we may finally assume $\alpha = 0$ and $0 \neq \beta, \gamma \in F$, $\beta \neq \gamma$. In this case for every $x \in F$ there exists $y = y_x, z = z_x \in F$ such that $(0, x, 0) = (\beta y^2, y, tr(\beta y)) + (\gamma z^2, z, tr(\gamma z))$. This implies $x = y + z$ and $z = \frac{\beta}{\gamma}y$, where $u \mapsto \bar{u} = u^{2^{n-1}}$ denotes the inverse of the Frobenius automorphism. We conclude that the maps $x \mapsto y_x$ and $x \mapsto z_x$ are injective. Then $tr(\gamma z) = tr(\beta y)$ implies $tr((\gamma \frac{\beta}{\gamma} + \beta)y) = 0$. We obtain

$$\beta^{2^{n-1}-1} = \gamma^{2^{n-1}-1}$$

and thus $\beta = \gamma$, a contradiction and the claim follows.

Set $B = \bigcup_{X \in \mathcal{S}} X$ and $v = (0, 0, 1)$. Then $B \cap (B + v) = \emptyset$. Thus v is a linear structure for $f = \chi_B$. We note that f belongs to case (b) of Proposition 3.3.

We claim that f is not a quadratic form: For $0 \neq \gamma \in F$ define $z_\gamma \in \text{GL}(V)$ by $(x, y, z)z_\gamma = (\gamma x, \gamma y, z)$. These maps form a cyclic group Z isomorphic to F^* . Moreover $U(\infty)z_\gamma = U(\infty)$ and $U(\beta)z_\gamma = U(\beta/\gamma)$. As Z normalizes P we get $ZP \simeq \text{AGL}(1, F)$. Let z be a generator of Z . Then there exists a generator ω of F^* such that z has the eigenvalue 1 with multiplicity 1 and the eigenvalues $\omega, \omega^2, \dots, \omega^{2^{n-1}}$ each with multiplicity 2. Assume f is a quadratic form. Then the associated bilinear form would have a radical V_0 of dimension 1 (as f is semibent). But then we can apply Lemma 2.2 to the symplectic space V/V_0 and the group PZ . Thus as $n \geq 3$ we deduce that every eigenvalue has multiplicity 1, a contradiction. Therefore f is not a quadratic form. \square

Examples 3.6. (a) Let $V = V(7, 2)$ and let T be the elementary abelian group of order 8 generated by the matrices

$$t_i = \begin{pmatrix} 1_{3 \times 3} & A_i \\ 0_{4 \times 3} & 1_{4 \times 4} \end{pmatrix}, \quad 1 \leq i \leq 3,$$

where

$$A_1 = \begin{pmatrix} \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 1 & \cdot & 1 \\ 1 & \cdot & 1 & 1 \\ \cdot & 1 & 1 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 1 & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & 1 & \cdot & 1 \end{pmatrix}.$$

Set $U = \langle e_1, e_2, e_3 \rangle$ and $W = \langle e_4, e_5, e_6, e_7 \rangle$. Then $\mathcal{S} = \{W\} \cup \{Ut \mid t \in T\}$ is a partial spread of type II.a. Set $B = \bigcup_{X \in \mathcal{S}} X$. Then $B = B + e_7$, i.e. e_7 is a linear structure of $f = \chi_B$ and f belongs to case (a) of Proposition 3.3. The explicit form of f is:

$$f = 1 + x_1(x_4 + x_5) + x_2(x_4 + x_6) + x_3x_4 + x_1x_2x_4.$$

(b) Set $V = V(7, 2)$ and let f, B, \mathcal{S}, T, U have the same meaning as in (a). Set $B_1 = V - B$. Then $f_1 = f + 1 = \chi_{B_1}$ is also semibent and e_7 is again a linear structure. Set

$$C = \begin{pmatrix} \cdot & 1 & \cdot & 1 \\ \cdot & 1 & 1 & 1 \\ 1 & \cdot & \cdot & \cdot \end{pmatrix}, \quad U_1 = \{(u, uC) \mid u \in U\}.$$

and $\mathcal{S}_1 = \{U_1t \mid t \in T\}$. Then $B_1 = \bigcup_{X \in \mathcal{S}_1} X^*$, \mathcal{S}_1 is a partial spread of type I.b, and f_1 belongs to case (d) of Proposition 3.3.

(c) Let $V = V(7, 2)$ and let T be the elementary abelian group of order 8 generated by the matrices (by E_{ij} we denote a typical member of the standard basis of a matrix space)

$$t_1 = \begin{pmatrix} A & 0_{3 \times 1} & A \\ 0_{1 \times 3} & 1 & 0_{1 \times 3} \\ 0_{3 \times 3} & 0_{3 \times 1} & A \end{pmatrix}, \quad A = 1_{3 \times 3} + E_{12},$$

$$t_2 = \begin{pmatrix} B_1 & B_2 \\ 0_{4 \times 3} & B_3 \end{pmatrix}, \quad B_1 = 1_{3 \times 3} + E_{32}, \quad B_3 = 1_{4 \times 4} + E_{24}, \quad B_2 = \begin{pmatrix} 1 & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

$$t_3 = \begin{pmatrix} B_1 & C_2 \\ 0_{4 \times 3} & C_3 \end{pmatrix}, \quad C_3 = 1_{4 \times 4} + E_{21} + E_{24}, \quad C_2 = \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & 1 \end{pmatrix}.$$

Define U, W, \mathcal{S} , and B similar as in (a). Then \mathcal{S} is of type II.a and $B = B + e_7$, i.e. e_7 is a linear structure of $f = \chi_B$. The explicit form of f is:

$$f = 1 + x_1x_6 + x_2x_5 + x_3(x_4 + x_5 + x_6) + x_1x_3(x_5 + x_6) + x_2x_3x_6 + x_3x_5x_6.$$

(d) Set $V = V(11, 2)$ and let T be the elementary abelian group of order 32 generated by the matrices

$$t_i = \begin{pmatrix} 1_{5 \times 5} & A_i \\ 0_{6 \times 5} & 1_{6 \times 6} \end{pmatrix}, \quad 1 \leq i \leq 5,$$

where

$$A_1 = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & 1 & 1 & 1 \\ 1 & \cdot & 1 & \cdot & \cdot & \cdot \end{pmatrix}, \quad A_2 = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & 1 \\ \cdot & \cdot & \cdot & 1 & 1 & 1 \\ \cdot & \cdot & 1 & \cdot & 1 & \cdot \\ 1 & 1 & 1 & 1 & \cdot & \cdot \end{pmatrix},$$

$$A_3 = \begin{pmatrix} \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & 1 & 1 & \cdot & \cdot \\ 1 & \cdot & 1 & \cdot & \cdot & 1 \\ 1 & 1 & \cdot & 1 & 1 & 1 \\ \cdot & \cdot & 1 & \cdot & \cdot & 1 \end{pmatrix}, \quad A_4 = \begin{pmatrix} \cdot & 1 & \cdot & 1 & \cdot & \cdot \\ 1 & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & 1 & 1 \\ 1 & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & 1 & \cdot & \cdot \end{pmatrix},$$

$$A_5 = \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix}.$$

Set $U = \langle e_1, \dots, e_5 \rangle$ and $W = \langle e_6, \dots, e_{11} \rangle$. Then $\mathcal{S} = \{W\} \cup \{Ut \mid t \in T\}$ is a partial spread of type II.a. Set $B = \bigcup_{X \in \mathcal{S}} X$. We have $B = B + e_{11}$, i.e. e_{11} is a linear structure for $f = \chi_B$. The explicit form of f is:

$$f = 1 + x_5x_{10} + x_4x_{10} + x_4x_8 + x_4x_6 + x_4x_5x_{10} + x_4x_5x_8 + x_3x_{10} + x_3x_9 + x_3x_7 + x_3x_5x_{10} + x_3x_5x_9 + x_3x_4x_{10} + x_3x_4x_5x_{10} + x_2x_8 + x_2x_6 + x_2x_5x_6 + x_2x_4x_{10} + x_2x_4x_6 + x_2x_3x_9 + x_2x_3x_5x_{10} + x_2x_3x_4x_{10} + x_2x_3x_4x_8 + x_2x_3x_4x_6 + x_1x_9 + x_1x_7 + x_1x_5x_7 + x_1x_4x_8 + x_1x_4x_5x_{10} + x_1x_3x_{10} + x_1x_3x_7 + x_1x_3x_4x_{10} + x_1x_3x_4x_9 + x_1x_3x_4x_7 + x_1x_2x_4x_{10} + x_1x_2x_4x_6 + x_1x_2x_3x_{10} + x_1x_2x_3x_7 + x_1x_2x_3x_4x_{10}.$$

(e) Set $V = V(11, 2)$ and let f, B, \mathcal{S}, T, U have the same meaning as in (d). Set $B_1 = V - B$. Then $f_1 = f + 1 = \chi_{B_1}$ is also semibent and e_{11} is again a linear structure. Set

$$C = \begin{pmatrix} \cdot & \cdot & \cdot & 1 & 1 & \cdot \\ \cdot & 1 & 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & 1 & 1 & 1 & 1 \\ 1 & \cdot & 1 & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & 1 & 1 & 1 \end{pmatrix}, \quad U_1 = \{(u, uC) \mid u \in U\}.$$

and $\mathcal{S}_1 = \{U_1t \mid t \in T\}$. Then $B_1 = \bigcup_{X \in \mathcal{S}_1} X^*$, \mathcal{S}_1 is a partial spread of type I.b, and f_1 belongs to case (d) of Proposition 3.3.

4 Partial spread extensions of semibent functions

In this section we ask the question whether a semibent function of partial spread type with a linear structure is obtained as the restriction to a hyperplane of a bent function of partial spread type.

Definition. Let \mathcal{T} be a partial spread of $(n + 1)$ -dimensional spaces in $W = V(2n + 2, 2)$ such that $g = g_{\mathcal{T}}$ is a bent function of partial spread type (sec. 2) and let V be a hyperplane of W .

- (a) Define the partial spread $\mathcal{S} = \mathcal{T}_V = \{X \cap V \mid X \in \mathcal{T}\}$ in V . Then we call \mathcal{T} an *extension* of \mathcal{S} . Note that \mathcal{S} is a partial spread of type I or II. We also call the bent function $g_{\mathcal{T}}$ an *extension* of the semibent function $f_{\mathcal{S}}$.
- (b) Suppose, $\mathcal{T} \subseteq \widehat{\mathcal{T}}$ where $\widehat{\mathcal{T}}$ is a *spread* on W , i.e. $\widehat{\mathcal{T}}$ consists of $(n + 1)$ -dimensional, pairwise disjoint subspaces which cover W (we recall that a spread defines a translation plane of order 2^{n+1} (see [9])). Then

$$\mathcal{S}' = (\widehat{\mathcal{T}} - \mathcal{T})_V = \{X \cap V \mid X \in \widehat{\mathcal{T}} - \mathcal{T}\}$$

is a partial spread of type I or II on V too. In this case we say that $\widehat{\mathcal{T}}$ is a *full extension* of \mathcal{S} and \mathcal{S}' . Similarly we say that the semibent functions $f = f_{\mathcal{S}}$ and $f + 1 = f_{\mathcal{S}'}$ have a *full extension*.

We note:

Lemma 4.1. *Let f be a semibent function of partial spread type with a linear structure which has a full extension. Then f has type I.b or II.a.*

Proof. Let $W, V, \mathcal{T}, \widehat{\mathcal{T}} \dots$ etc. all have the same meaning as above. Without loss of generality we may assume $|\mathcal{T}| = 2^n + 1$ so that $|\widehat{\mathcal{T}} - \mathcal{T}| = 2^n$. Then f has type I.a or II.a and $f + 1$ has type I.b or II.b. Note that a semibent function has a linear structure iff the complementary function has the same linear structure. So assume that f and $f + 1$ have a linear structure. By Proposition 3.3 $f + 1$ must have type I.b. This implies that f has type II.a. \square

We turn now to extensions and full extensions of the semibent spreads (semibent functions) of our examples.

Example 4.2. (Extensions) (a) In the case of dimension $2n + 1 = 7$ we computed all possible extensions of the semibent spreads. It turns out that always extensions exist, usually more than one. The table displays the result of our computer calculations where the last line shows the number of equivalence classes of extensions.

Example	3.4.a	3.4.b	3.5	3.6.a	3.6.b	3.6.c
$ B $	72	64	64	72	56	72
Extensions	5	2	1	9	6	11

(b) It is clear that for every dimension of the form $2n+1$, n odd, the semibent functions of Example 3.4.a have extensions which are non-degenerate quadratic forms in $V(2n+2, 2)$.

(c) The semibent functions of Example 3.4.b have also extensions: As we have seen under (b) this is true for dimension $2n+1$, n odd. We will give however a general construction of extensions which cover the dimensions $2n+1$, n even, too. For this purpose let V, F, K, \mathcal{S} etc. be defined as in 3.4.b. Set $W = K \times V = K \times F \times F \times K$ and choose $a \in F$ such that $tr(a) = 1$. Define subspaces ($\alpha \in F$)

$$\begin{aligned} W(\infty) &= 0 \times V(\infty) \cup (0 \times V(\infty) + (1, 0, 0, 0)), \\ W(\alpha) &= 0 \times V(\alpha) \cup (0 \times V(\alpha) + (1, a\sqrt{\alpha}, 0, 1)), \end{aligned}$$

and set $\mathcal{S}_a = \{W(\infty)\} \cup \{W(\alpha) \mid \alpha \in F\}$. Once we have shown that \mathcal{S}_a is a partial spread we see immediately

$$\{Y \cap \langle (1, 0, 0, 0) \rangle^\perp \mid Y \in \mathcal{S}_a\} = \{0 \times X \mid X \in \mathcal{S}\}$$

and therefore \mathcal{S}_a is an extension of \mathcal{S} .

Verification of the spread property: It is obvious that $W(\infty) \cap W(\alpha) = 0$ for $\alpha \in F$.

Assume $0 \neq \alpha$ and $0 \neq v \in W(\alpha) \cap W(0)$. Then $v = (1, 0, x, 1) = (1, a\sqrt{\alpha} + \alpha x, x, tr(\alpha x^2) + 1)$. This implies $x = (\sqrt{\alpha})^{-1}a$ and $tr(\alpha x^2) = 0$. But $tr(\alpha x^2) = tr(a) = 1$, a contradiction.

Assume finally $0 \neq v \in W(\alpha) \cap W(\beta)$, $0 \neq \alpha \neq \beta \neq 0$. Then $v = (1, a\sqrt{\alpha} + \alpha x, x, tr(\alpha x^2) + 1) = (1, a\sqrt{\beta} + \beta x, x, tr(\beta x^2) + 1)$, which implies $x(\alpha + \beta) = a(\sqrt{\alpha} + \sqrt{\beta})$ and $tr((\alpha + \beta)x^2) = 0$. Hence $x = a/(\sqrt{\alpha} + \sqrt{\beta})$ and $tr((\alpha + \beta)x^2) = tr(a^2) = tr(a)^2 = 1$, a contradiction.

We note that the spread \mathcal{S}_1 - in this case n is odd - defines the quadratic form $Q(u, x, y, z) = tr(xy) + uz + z$. For $a \neq 1$ it can be shown that \mathcal{S}_a defines a bent function of twisted parabolic type in the sense of [7].

(d) A semibent function with a linear structure in $2n+1$ variables has degree $\leq n$. Hence in dimension 5 a function from Theorem 3.5 is quadratic and thus has an extension and by part (a) it has an extension in dimension 7 too. A computer search showed that the semibent function of Theorem 3.5 has for dimension 9 no extension. For dimension $2n+1 \geq 11$ the extension problem is open.

Remark. Example 4.2.d in dimension 9 shows that it is *false* to conjecture that each semibent function of partial spread type with a linear structure has

an extension.

Example 4.3. (Full extensions) We only have to consider types II.a and I.b. Obviously the semibent functions of Example 3.4.a of type II.a have no full extension: In a quadratic space of dimension $2n + 2$, $n \geq 2$, there are no $(n + 1)$ -dimensional subspaces containing only non-singular vectors.

The pair of semibent functions in Example 3.6.a and 3.6.b have extensions to four inequivalent full spreads in $V(8, 2)$. The spreads are associated to the following planes of order 16 (see [9]): Lorimer-Rahilly plane, the Johnson-Walker plane, the semifield plane with kernel $\text{GF}(2)$, and the semifield plane with kernel $\text{GF}(4)$. The pair of semibent functions in Example 3.6.d and 3.6.e has a full extension to a spread defining a translation plane of order 64 associated with a two-sided non-primitive semifield (see class XII of [17]).

Remarks. (a) The semifields of order 32 (Walker [18]) and of order 64 (Rua, Combarro, Ranilla [17]) have been classified. The representing spread sets form $\text{GF}(2)$ -spaces. The hyperplanes of these spaces induce partial spreads of size 16 or 32 on $W = V(10, 2)$ or $V(12, 2)$ respectively. We then investigated if for such a partial spread there exists some hyperplane V of W such that the intersection of V with the partial spread is the support of a semibent function with a linear structure. It turns out that this method does not produce a semibent function with a linear structure in the case of semifields of order 32. Among the 80 classes of semifields of order 64 there is just one class which produced examples (d) and (e) of 3.6.

(b) There are obvious problems and questions on semibent functions of partial spread type with a linear structure left:

- Are there more series of such functions?
- Find more examples which have full extensions.
- Are there examples which belong to case (c) of Proposition 3.3 or can this case be eliminated?
- Decide in dimension ≥ 11 the extension problem for the spreads from Theorem 3.5.

(c) Properties of semibent functions (and more general of plateaued functions) with linear structures are studied for instance in [3], [4], [5] and [19].

References

- [1] E. Artin, *Geometric Algebra*, Interscience, 1964.
- [2] M. Aschbacher, *Finite Group Theory*, Cambridge Univ. Press, 2000.
- [3] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, On cryptographic properties of the cosets of $R(1, m)$, *IEEE Trans. Inf. Theory*, 47(2001), 1494-1513.

- [4] A. Canteaut, P. Charpin: Decomposing bent functions, *IEEE Trans. Inf. Theory*, 49(2003), 2004-2019.
- [5] C. Carlet, Partially-bent functions, *Designs, Codes and Cryptography* 3(1993), 135-145.
- [6] C. Carlet, A larger class of cryptographic boolean functions via a study of the Maiorana-McFarland construction, LNCS 2442, *CRYPTO 2002*, Springer, 2002, pp. 459-564.
- [7] U. Dempwolff, Automorphisms and equivalence of bent functions and of difference sets in elementary abelian 2-groups, *Comm. Algebra* 34(2006), 1077-1131.
- [8] U. Dempwolff, T. Neumann, Geometric and Design-theoretic Aspects of Semibent Functions I, to appear in *Designs, Codes and Cryptography*.
- [9] U. Dempwolff, A. Reifart, The classification of translation planes of order 16 I, *Geom. Ded.*, 15(1983), 137-153.
- [10] J. Dieudonné, *La géométrie des groupes classiques*, Springer, 1955.
- [11] J. Dillon, A survey of bent functions, *NSA Tech. Jour.*, Special Issue, 1972, 191-215.
- [12] 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.
- [13] P. Dye, Partitions and their stabilizers of line complexes and quadrics, *Annali di mat.* 114(1977), 173-194.
- [14] L. Grove, *Classical Groups and Geometric Algebra*, AMS Graduate Studies, 2002.
- [15] B. Huppert, *Endliche Gruppen I*, Sptinger, 1967.
- [16] W. Kantor, Spreads, translation planes and Kerdock sets I, *SIAM J. Alg. Disc. Math.* 3(1982), 151-165.
- [17] I.F. Rúa, E.F. Combarro, J. Ranilla, Classification of semifields of order 64, *J. Algebra*, 322(2009), 4011-4029.
- [18] R.J. Walker, Determination of division algebras with 32 elements, *Proc. Symp. Appl. Math.*, 75(1962), 83-85.
- [19] Y. Zheng, X.-M. Zhang, On plateaued functions, *IEEE Trans. Inf. Theory*, 47(2001), 1215-1223.