Dimensional doubly dual hyperovals and bent functions

Ulrich Dempwolff

Abstract

We show that dimensional doubly dual hyperovals over $\mathbb{F}_2$ define bent functions. We also discuss some known and a few new examples of dimensional doubly dual hyperovals and study the associated bent functions.

Keywords: dimensional dual hyperoval, bent function

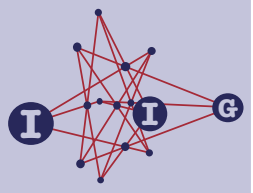
MSC 2000: 51A45, 05B25

1. Introduction

A set $\mathbf{D}$ of n-dimensional subspaces of a finite dimensional vector space V over a finite field (say $V = V(m, q)$) is called a *dual hyperoval of rank* n, we use the symbol DHO as an abbreviation, if $|\mathbf{D}| = (q^n - 1)/(q - 1) + 1$, $\dim X \cap Y = 1$ and $X \cap Y \cap Z = 0$ for three different $X, Y, Z \in \mathbf{D}$. The DHO *splits over the subspace* W if $V = X \oplus W$ for all $X \in \mathbf{D}$. In this paper we are interested in DHOs, which are also DHOs with respect to the dual space: We call $\mathbf{D}$ a *doubly dual hyperoval of rank* n, we abbreviate DDHO, if $m = 2n$ and $\mathbf{D}$ is also a DHO with respect to the dual space, i.e. if $\dim X + Y = 2n - 1$ and $X + Y + Z = V$ for three different $X, Y, Z \in \mathbf{D}$.

Remark 1.1. (i) A set of $(q^n - 1)/(q - 1) + 1$ subspaces of rank n such that any two generate a hyperplane and any three the whole space V is called a *dimensional hyperoval* in [3] and [8]. So our notion of a DDHO is compatible with the notation in the literature.

(ii) Usually DHOs of rank n are called $(n - 1)$*-dimensional dual hyperovals*. However in our context it seems more natural to use the notions of vector spaces than the language of projective geometry. DHOs are only known for



vector spaces of even characteristic and the majority of examples are DHOs over $\mathbb{F}_2$. In this paper *we look exclusively at DHOs over* $\mathbb{F}_2$, in particular $|\mathbf{D}| = 2^n$.

Seemingly unrelated to DHOs is the notion of a bent function. Let $V = V(2n, 2)$ be an $2n$-dimensional space over $\mathbb{F}_2$. A function $f : V \to \mathbb{F}_2$ is called a *bent function*, if its support is a difference set in V. Equivalently, a function f is bent, if the absolute value of the Fourier transform has the constant value 2^n, i.e. if

$$|\widehat{f}(v)| = \left| \sum_{x \in V} (-1)^{f(x)+x\cdot v} \right| = 2^n, \quad v \in V.$$

There is a vast literature on bent functions. DHOs have been studied intensively too. Yoshiara [23] is a survey article on DHOs. Investigations of DDHOs are contained in Taniguchi [16] and Yoshiara [22].

Starting point of our paper is a connection between DDHOs and bent functions, which is proved in the next section:

Theorem 1.2. *Let* $\mathbf{D}$ *be a dual hyperoval in* $V = V(2n, 2)$ *of rank* n.

(a) *Set*

$$B = (\bigcup_{S \in \mathbf{D}} S) - 0.$$

Then the characteristic function of B *is bent iff* $\mathbf{D}$ *is doubly dual.*

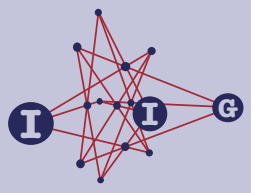
(b) *Assume that* $\mathbf{D}$ *splits with respect to the subspace* W. *Set*

$$B = W \cup \bigcup_{S \in \mathbf{D}} S.$$

Then the characteristic function of B *is bent iff* $\mathbf{D}$ *is doubly dual.*

This motivates a search for DDHOs. In the third section we define symplectic and orthogonal DHOs (called DHOs of polar type in [22]), discuss their representations and some of their properties. Such DHOs are automatically doubly dual (see Corollary 3.5). In Section 4 we present examples of DDHOs. Some of them are known but others appear to be new. The main emphasis will lie on the construction of symplectic DHOs, which are not orthogonal DHOs. In Section 5 we investigate the bent functions associated to these DDHOs (in the sense of Theorem 1.2). We also will discuss possible isomorphisms between the examples of Section 4.

This article is a predecessor of a forthcoming paper [6] by Kantor and the author. There it is shown that orthogonal DDHOs can be produced in large numbers by projections from orthogonal spreads. This is a variation of Kantor's technique, which uses projections of orthogonal spreads to produce symplectic spreads (see for instance [12, 13, 14]).



2. Bent functions and doubly dual hyperovals

Definitions. Set $V = V(m, 2)$. For $f \in \mathcal{F}_m = \mathbb{F}_2^V$ and $x \in V$ define the *Fourier coefficient* at v by

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

and call the function $\widehat{f} : V \to \mathbf{C}$ 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. if $v \in f^{-1}(1)$). For $v \in V$ define $v^\perp : V \to \mathbb{F}_2$ by $v^\perp(x) = v \cdot x$ (usual dot product). Finally we set $|f| = |f^{-1}(1)|$. Let $m = 2n$. The function $f \in \mathcal{F}_{2n}$ is a *bent function* if $\widehat{f}(x) \in \{\pm 2^n\}$ for all $x \in V$. The next two results with their proofs come from [1].

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

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

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

Proof. We observe

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

which implies (a). From (a) we get $\widehat{f}(v) = \sum_x (-1)^{f(x)+v\cdot x} = 2^m - 2|f + v^\perp|$, which is assertion (b). □

Proposition 2.2. *Let $f \in \mathcal{F}_{2n}$. Equivalent are:*

(a) *f is bent.*

(b) *$|f + v^\perp| = 2^{2n-1} \pm 2^{n-1}$ for all $v \in V$.*

(c) *There exists $\epsilon \in \{\pm 1\}$ such that $|f| = 2^{2n-1} + \epsilon 2^{n-1}$ and $|f \cap v^\perp| = 2^{2n-2} + \epsilon 2^{n-1}$ or $= 2^{2n-2}$ for all $0 \neq v \in V$.*

Proof. (a)⇒(b). We have, by Lemma 2.1, $\pm 2^n = \widehat{f}(v) = 2^{2n} - 2|f + v^\perp|$.

(b)⇒(c). From (b) we get $|f| = |f + 0^\perp| = 2^{2n-1} + \epsilon 2^{n-1}$ with some $\epsilon = \pm 1$. Moreover for $v \neq 0$ we use

$$|f \cap v^\perp| = \frac{1}{2}(|f| + |v^\perp| - |f + v^\perp|).$$

This implies assertion (c).

(c)⇒(a). Now we use

$$\widehat{f}(v) = 2^{2n} - 2|f + v^\perp| = 2^{2n} - 2(|f| + |v^\perp| - 2|f \cap v^\perp|).$$

Using (c) we get assertion (a). □

We use Proposition 2.2 to verify Theorem 1.2:

Proof of Theorem 1.2. First we note, that $|\mathbf{D}| = 2^n$ by the definition of a DHO, and that every nontrivial vector of V lies either in 2 or none elements from $\mathbf{D}$.

(a) An application of the sieve formula shows $|B| = 2^{2n-1} - 2^{n-1}$. Let $v \in V - 0$. Let $S_1, \ldots, S_k$ be the spaces of $\mathbf{D}$ which are in $v^\perp$; note that k can be 0. Set $B_0 = (S_1 \cup \cdots \cup S_k) - 0$. By the sieve formula

$$|B_0| = k(2^n - 1) - \binom{k}{2} = \frac{k}{2}(2^{n+1} - k - 1).$$

Set $\mathbf{D}' = \mathbf{D} - \{S_1, \ldots, S_k\}$. Then $|S' \cap B_0| = k$ for $S' \in \mathbf{D}'$. Set $B_1 = (B \cap v^\perp) - B_0$. Since $|S' \cap v^\perp| = 2^{n-1} - 1$ we see $|B_1 \cap S'| = 2^{n-1} - k - 1$. Consider the incidence structure $(B_1, \mathbf{D}')$. We deduce $2|B_1| = (2^n - k)(2^{n-1} - k - 1)$. This implies

$$|B \cap v^\perp| = |B_0| + |B_1| = 2^{2n-2} + 2^{n-2}(k - 2).$$

If $\mathbf{D}$ is doubly dual then always $k = 0$ or $= 2$, i.e. $|B \cap v^\perp| = 2^{2n-2}$ or $= 2^{2n-1} - 2^{n-1}$. Hence f_B is bent by Proposition 2.2. If $\mathbf{D}$ is not doubly dual, then we can choose v such that $0 \neq k \neq 2$. Then $|B \cap v^\perp| \neq 2^{2n-2}$ and $\neq 2^{2n-2} - 2^{n-1}$. So f_B is not bent in this case.

(b) Now B is partitioned into W and $(\bigcup_{S \in \mathbf{D}} S) - 0$. We deduce from (a) that $|B| = 2^{2n-1} + 2^{n-1}$.

Let $v \in V - 0$. Assume first $W \subseteq v^\perp$. Then $S \not\subseteq v^\perp$ for all $S \in \mathbf{D}$. As $B \cap v^\perp$ is partitioned into W and $((\bigcup_{S \in \mathbf{D}} S) - 0) \cap v^\perp$ we deduce from (a) $|B \cap v^\perp| = 2^n + 2^{2n-2} - 2^{n-1} = 2^{2n-2} + 2^{n-1}$.

Assume next $W \not\subseteq v^\perp$. Then $|W \cap v^\perp| = 2^{n-1}$. If $v^\perp$ contains precisely k spaces from $\mathbf{D}$, we deduce from (a)

$$|B \cap v^\perp| = 2^{2n-2} + 2^{n-2}(k - 2) + 2^{n-1}.$$

If $\mathbf{D}$ is doubly dual, we have $k = 0$ or 2 and $|B \cap v^\perp| = 2^{2n-2}$ or $= 2^{2n-2} + 2^{n-1}$. Again f_B is bent by Proposition 2.2. If however $\mathbf{D}$ is not doubly dual, we can choose v such that $0 \neq k \neq 2$. Thus $|B \cap v^\perp| \neq 2^{2n-2}$ nor $\neq 2^{2n-2} + 2^{n-1}$ and f_B is not bent in this case. □

Remark 2.3. (a) All known DHOs do split over some subspace of its ambient space. So the extra assumption of a splitting DHO in part (b) of Theorem 1.2 seems to be not very restrictive.

(b) The definition of bent functions of partial spread type (see [9], [10, Corollary 1]) agrees formally completely with the definition of bent functions associated with DDHOs.

3. Representations

We first review some basic facts about splitting DHOs and introduce some notation. We will see that representations of translation planes and splitting DHOs are closely related. We then discuss in particular symplectic and orthogonal DHOs. The following lemma is useful.

Lemma 3.1. *Let V be a $2n$-dimensional vector space over a field F, $\beta : V \times V \to F$ be a nondegenerate, symplectic bilinear form, and U_0, U_1 isotropic subspaces such that $V = U_0 \oplus U_1$.*

(a) *One can identify $V = U \times U$, $U_0 = U \times 0$, and $U_1 = 0 \times U$ with an n-dimensional F-space U. Moreover β can be written in the form*

$$\beta((x, y), (x', y')) = \sigma(x, y') - \sigma(y, x'),$$

where σ is a nondegenerate, symmetric bilinear form on U.

(b) *Let W be an isotropic subspace of V of the form $W = \{(x, xR) \mid x \in U\}$, $R \in \mathrm{End}(U)$ and let β be represented as in* (a).

(1) *Then R is a self-adjoint operator with respect to σ.*

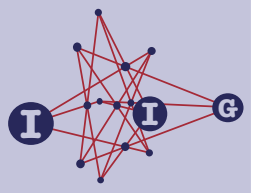
(2) *Let β' be a nondegenerate, symplectic bilinear form on V such that $U \times 0$, $0 \times U$, and W are isotropic. Then there exist $T, S \in \mathrm{GL}(U)$ such that*

$$\beta'((x, y), (x', y')) = \beta((xS, yT), (x'S, y'T)).$$

Moreover $(ST^\star)R^\star = R(ST^\star)^\star$. Here a symbol $Q^\star$ denotes the operator adjoint with respect to σ to $Q \in \mathrm{End}(U)$.

Proof. (a) This follows from basic properties of symplectic spaces (see for instance [20, p. 69]): As the Witt-index of V is n, one can choose bases $\{u_1, \ldots, u_n\}$ of U_0 and $\{w_1, \ldots, w_n\}$ of U_1 such that $\beta(u_i, w_j) = \delta_{ij}$, $1 \leq i, j \leq n$. Making the obvious identifications we obtain the assertion.

(b) Assertion (1) follows from the description of β. For the second assertion we use Witt's theorem, i.e. all nondegenerate, symplectic bilinear forms



are equivalent. So by Witt's theorem we find an equivalence mapping $P \in \mathrm{GL}(V)$, which fixes $0 \times U$ and $U \times 0$ which transforms β into β'. If we write $P = \mathrm{diag}(S, T)$, $S, T \in \mathrm{GL}(U)$, we get the first assertion of (2). Since W is isotropic with respect to β' too we have for all $x, x' \in U$

$$0 = \beta'((x, xR), (x', x'R)) = \sigma(x, x'RTS^\star) - \sigma(x, x'ST^\star R^\star)),$$

which leads to the second assertion of (2). □

Definition 3.2. Let $V = U \times U$, $U = V(n, 2)$, be a $2n$-dimensional $\mathbb{F}_2$-space and $\mathbf{D}$ a DHO of rank n on V.

(a) We call the DHO *symplectic*, if V admits a nondegenerate, symplectic from such that all spaces of $\mathbf{D}$ are isotropic with respect to this bilinear form. We call the DHO *orthogonal*, if V admits a nondegenerate, quadratic from such that all spaces of $\mathbf{D}$ are totally singular with respect to this quadratic form. In the case of a splitting DHO we also assume that this DHO splits over an isotropic subspace or a totally singular subspace respectively.

(b) Assume that $\mathbf{D}$ splits over $0 \times U$. Then the DHO can be represented in the form

$$\mathbf{D} = \mathbf{D}_B = \{S_a \mid a \in U\}, \quad S_a = \{(x, xB(a)) \mid x \in \mathbb{F}_2^n\},$$

with an injection

$$B : U \to \mathrm{End}(U), \quad B(0) = 0.$$

We will also call (simulating the language of translation planes) the set $\Psi_B = \{B(a) \mid a \in U\}$ of endomorphisms a *DHO-set*. If the mapping B is linear, one calls $\mathbf{D}$ a *bilinear dimensional dual hyperoval*.

On the other hand a set $0 \in \Psi = \{B(a) \mid a \in U\} \subseteq \mathrm{End}(U)$ is a DHO-set iff

(1) $\mathrm{rk}(B(a) + B(b)) = n - 1$ for all $a, b \in U$, $a \neq b$.

(2) Let $a \in U$. Then $\{\ker(B(a) + B(b)) \mid b \in U - \{a\}\}$ is the set of 1-spaces in U.

A bilinear DHO admits an elementary abelian group $\mathcal{T}$ group of automorphisms whose elements are the transformations T_a, $a \in U$, defined by

$$(x, y)T_a = (x, xB(a) + y).$$

This group is called the *translation group* of the DHO. Note that the DHO splits over the fixed point set $C_V(\mathcal{T})$ (which is $= 0 \times U$) of the translation group. In the case of a bilinear symplectic or orthogonal DHO we do assume by definition that this fixed point set is an isotropic or totally singular subspace respectively.

Remark 3.3. Assume that $\mathbf{D}$ is symplectic, that the DHO-set Ψ_B represents the DHO (as under (b)), and that $0 \times U$ is isotropic. We assume that the symplectic form has the shape

$$((x,y),(x',y')) = \sigma(x,y') + \sigma(y,x'),$$

where σ is a nondegenerate, symmetric bilinear form on U (see Lemma 3.1). Then all operators $B(a)$ are *symmetric (self-adjoint)* with respect to σ, i.e.

$$\sigma(x, yB(a)) = \sigma(xB(a), y)$$

$x, y \in U$. Assume now that the DHO is orthogonal and $0 \times U$ is totally singular with respect to a quadratic form Q where

$$Q(x,y) = \sigma(x,y),$$

i.e. Q polarizes to the above symplectic form. Then all $B(a)$'s are *skew symmetric* with respect to σ, i.e.

$$\sigma(x, xB(a)) = 0$$

for $x \in U$.

Lemma 3.4. *Let $\mathbf{D}$ be a DHO of rank n on $V = U \times U$, $U = V(n,2)$, which splits over $0 \times U$ and let σ be a symmetric, nondegenerate bilinear form on U. Let Ψ_B be a DHO-set associated with $\mathbf{D}$. Equivalent are:*

(a) *$\mathbf{D}$ is doubly dual.*

(b) *$\Psi_B^\star = \{B^\star(a) \mid a \in U\}$ is a DHO-set. Here $B^\star(a) = B(a)^\star$ is adjoint to $B(a)$ with respect to σ.*

Proof. Define on V a symplectic bilinear form by $((x,y),(x_1,y_1)) = \sigma(x,y_1) + \sigma(y,x_1)$. Then the symplectic form induces a duality on V and $\mathbf{D}$ is doubly dual iff $\mathbf{D}^\perp = \{X^\perp \mid X \in \mathbf{D}\}$ is a DHO. Now

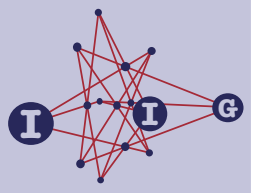
$$S_a^\perp = \{(x, xB(a)) \mid x \in U\}^\perp = \{(xB^\star(a), x) \mid x \in U\}.$$

So $\mathbf{D}^\perp$ is a DHO (which splits over $U \times 0$) iff $\Psi_B^\star$ is a DHO-set. □

This implies:

Corollary 3.5. *Symplectic DHOs are doubly dual.*

Remark 3.6. With the above notation define $\sigma(x,y) = x \cdot y$, $x, y \in U$, (usual dot product) and identify $\mathrm{End}(U)$ with the matrix space $\mathbb{F}_2^{n\times n}$. Then a DHO-set Ψ_B defines a symplectic DHO, if all operators $B(a)$ are symmetric, i.e. $B(a)^t =$



$B(a)$. The DHO will be even orthogonal, if in addition the diagonal elements of $B(a)$ are 0.

A variation: identify U with $F = \mathbb{F}_{2^n}$ and define on F a nondegenerate, symmetric bilinear form σ by taking the trace form

$$\sigma(x, y) = \mathrm{Tr}(xy),$$

where $\mathrm{Tr} : F \to \mathbb{F}_2$ is the absolute trace. Then a symplectic form $(\cdot, \cdot)$ is defined on $F \times F$ by

$$((x, y), (x_1, y_1)) = \sigma(x, y_1) + \sigma(x_1, y) = \mathrm{Tr}(xy_1) + \mathrm{Tr}(x_1 y).$$

A linear operator L on F has the form

$$L = \sum_{i=0}^{n-1} T_i(a_i),$$

where the operator $T_j(b)$ is defined by

$$xT_j(b) = bx^{2^j}.$$

The adjoint operators of $T_j(b)$ and L with respect σ have the form

$$T_j(b)^\star = T_{-j}(b^{2^{-j}}) \quad \text{and} \quad L^\star = \sum_{i=0}^{n-1} T_i(a_{-i}^{2^i})$$

(indices are read modulo n). In particular L is self-adjoint iff $a_i = a_{-i}^{2^i}$ for all i and L is skew symmetric iff in addition $a_0 = 0$ holds.

Example 3.7. Let $\Psi = \mathrm{Sk}(3, \mathbb{F}_2)$ be the set of skew symmetric 3×3-matrices over $\mathbb{F}_2$. We check immediately that Ψ is a DHO-set. Hence by Corollary 3.5 Ψ defines a DDHO on $V = \mathbb{F}_2^6$.

Bilinear DHOs and the Knuth operations. Let $\mathbf{D}$ be a splitting, bilinear DHO in $V = U \times U$, $U = V(n, 2)$, of rank n. In this case we may assume that there is an additive mapping $B : U \to \mathrm{End}(U)$, such that the DHO is described by the DHO-set $\Psi_B = \{B(y) \mid y \in U\}$. For $y \in F$ define the operator $B^o(y) \in \mathrm{End}(U)$ by

$$xB^o(y) = yB(x).$$

Then $\Psi_{B^o} = \{B^o(y) \mid y \in U\}$ is a DHO-set too and the bilinear DHO $\mathbf{D}^o$ defined by B^o is the *opposite DHO*. We know that the set $B^\star$ (see Lemma 3.4) only defines a DHO iff $\mathbf{D}$ is doubly dual. We call in this case the associated

DHO $\mathbf{D}^\star$ the *dual DHO*. In analogy to the terminology of semifields we call the operations $\mathbf{D} \mapsto \mathbf{D}^o$ and $\mathbf{D} \mapsto \mathbf{D}^\star$ the *Knuth operations*. It then follows that a bilinear DDHO produces six bilinear DDHOs $\mathbf{D}$, $\mathbf{D}^o$, $\mathbf{D}^\star$, $\mathbf{D}^{o\star}$, $\mathbf{D}^{\star o}$, $\mathbf{D}^{o\star o}$. All these facts follow from [11, Sec. 5]. In particular we record:

Lemma 3.8 (Y. Edel)**.** *Let $\mathbf{D}$ be a bilinear DDHO and assume the notation from above.*

(a) *Equivalent are:*

(1) *$\mathbf{D}$ is a symplectic DHO.*

(2) *$\mathbf{D}^{o\star}$ is a symmetric DDHO, i.e $xB^{o\star}(y) = yB^{o\star}(x)$ for all $x, y \in U$.*

(b) *Equivalent are:*

(1) *$\mathbf{D}$ is an orthogonal DHO.*

(2) *$\mathbf{D}^{o\star}$ is an alternating DDHO, i.e $xB^{o\star}(x) = 0$ for all $x \in U$.*

Remark 3.9. A main result in Taniguchi [16, Thm. 11] (with a somewhat technical proof) essentially states that alternating DHOs are doubly dual, iff their rank is odd. But skew symmetric operators have an even rank, i.e. orthogonal DHOs must have an odd rank. So Lemma 3.8 provides a simple explanation of Taniguchis result.

We end this section with two uniqueness properties of symplectic and orthogonal DHOs.

Lemma 3.10. *Let $U = V(n, 2)$, $V = U \times U$, and $\mathbf{D}$ a DHO which splits over $0 \times U$. Then there is at most one symplectic form on V such that $0 \times U$ and the spaces in $\mathbf{D}$ are isotropic.*

Proof. Write $\mathbf{D} = \{S_a \mid a \in U\}$, $S_a = \{(x, xB(a)) \mid x \in U\}$ as usual and assume that β and β' are nondegenerate, symplectic forms, which satisfy the assumptions of the lemma. We represent these symplectic forms as in (b) of Lemma 3.1. Then $B(a) = B^\star(a)$ (with respect to σ) for $a \in U$ and $B(a)X^\star = XB(a)$ where $X = ST^\star$. Thus

$$\ker B(a) = \ker B(a)X^\star = \ker XB(a).$$

Hence X fixes $\ker B(a)$ for all $a \in U$. We obtain $X = \mathbf{1}$ or $T = (S^\star)^{-1}$ where $P = \operatorname{diag}(S, T)$ as in the proof of Lemma 3.1. But a computation shows that then P is an isometry with respect to β, i.e. $\beta' = \beta$. □

Lemma 3.11. *Let $U = V(n, 2)$, $V = U \times U$, and $\mathbf{D}$ a DHO which splits over $0 \times U$. Let β be a symplectic form on V such that $0 \times U$ and the spaces in $\mathbf{D}$ are isotropic. Assume that β is represented by the symmetric bilinear form σ on U as*

in (a) *of Lemma 3.1. Suppose that Q is a quadratic form, which polarizes to β such that $0 \times U$ and the spaces in $\mathbf{D}$ are totally singular. Then $Q(x,y) = \sigma(x,y)$ for all $(x,y) \in V$.*

Proof. Clearly, the quadratic form given in the lemma polarizes to β. It is well known (and easily verified) that any other quadratic form which polarizes to β has the shape $Q + \lambda$ where λ is a linear form on V. But as Q vanishes on the spaces $0 \times U$ and $U \times 0 \in \mathbf{D}$, we see that λ vanishes on this spaces too, i.e. $\lambda = 0$. □

Remark 3.12. Assume that the DHO in Lemma 3.11 is represented as usual by $\mathbf{D} = \{S_a \mid a \in U\}$, $S_a = \{(x, xB(a)) \mid x \in U\}$. We already know that the $B(a)$'s are self-adjoint with respect to σ. If $\mathbf{D}$ is even orthogonal and $0 \times U$ is totally singular too, the operators $B(a)$ are even skew symmetric, i.e. $\sigma(x, xB(a)) = 0$ for all $x \in U$.

4. Examples

In this section we discuss some old and some new DDHOs. The main emphasis lies on symplectic examples. Throughout this section we fix the following notation:

$$\nu \in \mathbb{F}_4 - \mathbb{F}_2,\ n \text{ is an odd number} > 3,\ F = \mathbb{F}_{2^n},\ \text{and } V = F \times F.$$

By $\mathrm{Tr} : F \to \mathbb{F}_2$ we denote the absolute trace. When we say that an operator on F is self-adjoint, we always refer to the trace form.

Example 4.1 (Yoshiara, [21])**.** We consider the DHOs of [21] in a slightly different representation. Let $1 \leq r, t < n$. For $y \in F$ define a $\mathbb{F}_2$-linear operator $B(y)$ on F by

$$xB(y) = x(T_r(y) + T_{-r}(y^{2^t})) = x^{2^r} y + x^{2^{-r}} y^{2^t}.$$

Finally define $\mathbf{D} = \mathbf{D}_{r,t} = \{S_a \mid a \in F\}$, $S_a = \{(x, xB(a)) \mid x \in F\}$, as usual. It was shown in [16] that $\mathbf{D}$ defines a DDHO iff

$$(t, n) = (2r, n) = (t + 2r, n) = 1.$$

Note that $B(y)^\star = B(y)$ if $t = -r$. In that case $\mathbf{D}$ is symplectic, even orthogonal since $B(y)$ is even skew symmetric. Do other parameters lead to symplectic DHOs? The answer is provided by [22, Proposition 6]. We give an an alternative proof of this result.

Proposition 4.2 (S. Yoshiara)**.** *Let* $(t,n) = (2r,n) = (2r+t,n) = 1$. *Then the DHO* $\mathbf{D}_{r,t}$ *is symplectic iff* $t = -r$.

Proof. By Lemma 3.1 the DDHO $\mathbf{D}_{r,t}$ can only be symplectic if there exists a $A \in \mathrm{GL}_{\mathbb{F}_2}(F)$ such that

$$AB(y)^\star = B(y)A^\star \quad \text{for all} \quad y \in F.$$

Let $A = \sum_{i=0}^{n-1} T_i(a_i)$. Then $A^\star = \sum_{i=0}^{n-1} T_i(a_{-i}^{2^{-i}})$ and $B(y)^\star = T_r(y^{2^{t+r}}) + T_{-r}(y^{2^{-r}})$. Evaluating the condition $B(y)A^\star = AB(y)^\star$ leads to the equations

$$a_{i-r}^{2^r} y^{2^{r+t}} + a_{i+r}^{2^{-r}} y^{2^{-r}} = a_{r-i}^{2^{r-i}} y^{2^{i-r}} + a_{-i-r}^{2^{-i-r}} y^{2^{i+r+t}} \quad \text{for all} \quad y \in F$$

and $0 \le i < n$. The coefficients in such an equation can only be nontrivial if exponents of y on the LHS occur also on the RHS, i.e. one has $i = 0, \pm(r+t)$. Inspecting the equation for $i = 2r+t$ shows $a_{3r+t} = a_{-3r-t} = 0$. Then these three equations show that the only nontrivial coefficients can be $a_{\pm r}$ or $a_{\pm(r+t)}$. The equation for $i = 2r$ involves $a_{\pm r}$ and it follows $a_r = a_{-r} = 0$ as the respective exponents of y for these coefficient occur only once in this equation. So the only possible nontrivial coefficients are a_{r+t} and a_{-r-t}. The remaining equations which involve these coefficients occur for $i = \pm t$. An inspection of these two equations shows, that a_{r+t} or a_{-r-t} can only be nontrivial if $r = -t$ and $a_0^{2^t} = a_0$. But we observed already that for $r = -t$ the DHO $\mathbf{D}_{r,-r}$ is symplectic. The proof is complete. □

The next four examples describe bilinear DHOs, which are symplectic but not orthogonal (see Proposition 4.16). The symmetric Knuth image of the first example has been studied already by Taniguchi and Yoshiara [19].

Example 4.3. For $y \in F$ we define a $\mathbb{F}_2$-linear mapping $B(y)$ on F by

$$xB(y) = x(y + y^{2^{n-1}}) + x^4 y + (xy)^{2^{n-2}}.$$

Set

$$\mathbf{D} = \{S_y \mid y \in F\}, \quad S_y = \{(x, xB(y)) \mid x \in F\}.$$

That $\mathbf{D}$ is a symplectic DDHO follows from:

Lemma 4.4. *The set* $\mathbf{D}$ *is a symplectic, bilinear DHO on* V.

Proof. Clearly, the operators $B(y)$ are all self-adjoint with respect to the trace form. So we have only to show that $\mathbf{D}$ is a DHO, i.e. we have to show that each $B(y)$, $y \neq 0$ has rank $n-1$ and that $\ker B(y) \neq \ker B(z)$ for $0 \neq y \neq z \neq 0$. Now

$x \in \ker B(y)$ iff $x(y + y^{2^{n-1}}) + x^4 y + (xy)^{2^{n-2}} = 0$ or after taking the fourth power we see that (x, y) is a root of

$$f(X, Y) = (XY)^4 + X^4 Y^2 + X^{16} Y^4 + XY.$$

Or after dividing by XY and multiplying with Y^{-3} we see that (x, y^{-1}) is a root of

$$g(X, Y) = Y^3 + X^3 Y^2 + X^{15} + X^3,$$

which factorizes over $E = \mathbb{F}_{2^{2n}}$ as $g(X, Y) = g_0(X, Y) g_1(X, Y) g_{-1}(X, Y)$ with

$$g_0(X, Y) = Y + X^5 + X^3 + X$$

and

$$g_i(X, Y) = X^5 + \nu^i X^3 + \nu^{-i} X + \nu^i Y$$

for $i = \pm 1$. We show that $g_1(X, Y) g_{-1}(X, Y)$ has no root in $(F^\star)^2$ and that $x \mapsto x^5 + x^3 + x$ is bijective on F which in turn will prove our claim.

Suppose $(x, y) \in (F^\star)^2$ is a root of $g_1(X, Y) g_{-1}(X, Y)$, say of $g_1(X, Y)$. As (x, y) is fixed by the involutory automorphism of E and since this automorphism interchanges $g_1(X, Y)$ with $g_{-1}(X, X)$, we see that (x, y) is a root of both polynomials. Hence

$$0 = g_1(x, y) + g_{-1}(x, y) = x^3 + x + y \quad \text{or} \quad y = x^3 + x.$$

But then $0 = g(x, y) = x^{15} + x^7$ and $x = 1$ and $y = 0$, a contradiction.

Now we show that the polynomial $X^5 + X^3 + X$ is a permutation polynomial. Assume the converse. Then the polynomial $h(X, Y) = X^5 + X^3 + X + Y^5 + Y^3 + Y$ has a root (x, y), $x \neq y$. But $h(X, Y) = (X + Y) h_1(X, Y) h_{-1}(X, Y)$ with

$$h_i(X, Y) = X^2 + \nu^i XY + Y^2 + \nu^{-i}$$

for $i = \pm 1$. So if (x, y) is a root of $h_i(X, Y)$ then also of $h_{-i}(X, Y)$. This in turn shows

$$0 = h_1(x, y) + h_2(x, y) = xy + 1$$

or $y = x^{-1}$. But then $x^2 + x^{-2} + 1 = h_1(x, x^{-1}) = 0$, which implies $x \in \mathbb{F}_4 - \mathbb{F}_2$, a contradiction. □

Remark 4.5. Since the DHOs from Example 4.3 are bilinear DDHOs one can use the Knuth operations. By Lemma 3.8 the mapping B^{o*} defines a symmetric, bilinear DHO of the form

$$xB^{o*}(y) = xy + x^4 y + xy^4 + (xy)^2.$$

This shows that that the symmetric DHO is a DHO described by Taniguchi and Yoshiara in [19, Sec. 3]. The verification that the mapping B^{o*} defines a DHO in [19] is simpler than our verification of the DHO property. But the proof of Taniguchi and Yoshiara does not show that B^{o*} defines a *doubly* dual DHO. So our result needs a separate verification.

Example 4.6. For $y \in F$ we define a $\mathbb{F}_2$-linear mapping $B(y)$ on F by

$$xB(y) = x(y + \mathrm{Tr}(y)) + x^2y + (xy)^{2^{n-1}}.$$

Set

$$\mathbf{D} = \{S_y \mid y \in F\}, \quad S_y = \{(x, xB(y)) \mid x \in F\}.$$

Then $\mathbf{D}$ is a symplectic, bilinear DDHO. This follows from follows from:

Lemma 4.7. *The set* $\mathbf{D}$ *is a symplectic, bilinear DHO on* V.

Proof. Clearly, all operators $B(y)$ are self-adjoint with respect to the trace form. We have to show that each $B(y)$, $y \neq 0$ has rank $n-1$ and that $\ker B(y) \neq \ker B(z)$ for $0 \neq y \neq z \neq 0$. Now $x \in \ker B(y)$ iff $x(y+\mathrm{Tr}(y))+x^2y+(xy)^{2^{n-1}} = 0$ or after squaring we see that (x, y) is a root of

$$f(X, Y) = XY + (XY)^2 + X^2\mathrm{Tr}(Y) + X^4Y^2.$$

Clearly, for $y = 1$ we get $x = 1$ as the unique root of $f(X, 1)$. So we assume from now on $y \in F - \{0, 1\}$.

For the case $\mathrm{Tr}(y) = 0$ we substitute the variable Y by Y^2+Y in $f(X, Y)$ and obtain the polynomial $f_0(X, Y) = f(X, Y^2+Y)$, which factorizes as $f_0(X, Y) = XY(Y + 1)g(X, Y)$ with

$$g(X, Y) = X^3Y^2 + X^3Y + XY^2 + XY + 1 = Y^2(X^3 + X) + Y(X^3 + X) + 1.$$

Note that this polynomial has no roots of the form $(1, y)$. Multiply with X^{-3} and substitute X by $Z = X^{-1}$. Then

$$g(Z, Y) = Z^3 + (Y^2 + Y)Z^2 + Y^2 + Y.$$

So for a solution $(z, y) \in (F - \{0, 1\})^2$ we have $y^2 + y = \frac{z^3}{z^2+1}$. Substitute $u = \frac{1}{1+z}$. Then $y^2 + y = u^2(\frac{u+1}{u})^3 = u^2 + u + 1 + u^{-1}$. Hence $\mathrm{Tr}(u^{-1}) = 1$ or $\mathrm{Tr}(x^{-1}) = \mathrm{Tr}(z) = 0$ where $x = z^{-1}$. We set $F_0 = \{x \in F^\star \mid \mathrm{Tr}(x) = 0\}$. We have already seen that the mapping ϕ

$$F_0 \ni z \mapsto \phi(z) = \frac{z^3}{z^2 + 1}$$

sends F_0 into F_0.

CLAIM: This mapping is bijective.

If not, then the polynomial $X^3(Y^2+1)+Y^3(X^2+1)$ and hence the polynomial

$$k(X,Y) = (X^2+X)^3(Y^4+Y^2+1) + (Y^2+Y)^3(X^4+X^2+1)$$

has a nontrivial root in $F_0^2 - \{(x,x) \mid x \in F_0\}$. Here we use that the mapping $x \mapsto x^2 + x$ is bijective on F_0. This polynomial factorizes over $E = \mathbb{F}_{2^{2n}}$ as $k(X,Y) = (X+Y)(X+Y+1)k_1(X,Y)k_{-1}(X,Y)\ell_1(X,Y)\ell_{-1}(X,Y)$ with

$$k_i(X,Y) = XY + \nu^i X + \nu^i Y + \nu^i$$

and

$$\ell_i(X,Y) = XY + \nu^i X + \nu^{-i} Y$$

for $i = \pm 1$. Let $(x,y) \in F_0^2$, $x \neq y$, be a root of $k(X,Y)$. Then (x,y) is a root of one of the $k_i(X,Y)$'s or $\ell_i(X,Y)$'s. The involutory automorphism of E interchanges the polynomials $k_1(X,Y)$ and $k_{-1}(X,Y)$ as well as $\ell_1(X,Y)$ and $\ell_{-1}(X,Y)$ but fixes x and y. So if (x,y) is a root of $k_i(X,Y)$ ($\ell_i(X,X)$), it is also a root of $k_{-i}(X,Y)$ ($\ell_{-i}(X,Y)$). If (x,y) is a root of $k_i(X,Y)$, we get

$$0 = k_1(x,y) + k_{-1}(x,y) = x + y + 1, \quad \text{i.e.} \quad y = x+1$$

and $\mathrm{Tr}(x) \neq \mathrm{Tr}(y)$, a contradiction.

If (x,y) is a root of $\ell_i(X,Y)$, we get

$$0 = \ell_1(x,y) + \ell_{-1}(x,y) = x + y, \quad \text{i.e.} \quad y = x,$$

again a contradiction. So the claim holds. This shows that for each $y \in F_0$ we have a unique $x \in F$ with $f(x,y) = 0$. Moreover $\mathrm{Tr}(x^{-1}) = 0$.

For the case $\mathrm{Tr}(y) = 1$ we substitute the variable Y by Y^2+Y+1 in $f(X,Y)$ and obtain the polynomial $f_1(X,Y) = f(X, Y^2+Y+1)$, which factorizes over E as $f_1(X,Y) = Xh(X,Y)h_1(X,Y)h_{-1}(X,Y)$ with

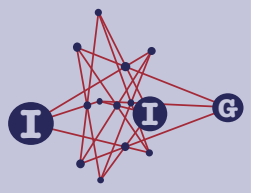
$$h(X,Y) = XY^2 + XY + X + 1$$

and

$$h_i(X,Y) = XY + \nu^i X + Y + \nu^{-i}$$

for $i = \pm 1$. As before: If (x,y) is a root of $h_i(X,Y)$ it is also a root of $h_{-i}(X,Y)$. In that case we have

$$0 = h_1(x,y) + h_{-1}(x,y) = x + 1, \quad \text{i.e.} \quad x = 1,$$



a contradiction. So a root (x, y) of $f_1(X, Y)$ is a root of $h(X, Y)$, i.e.

$$x = \frac{1}{y^2 + y + 1}.$$

In particular $\mathrm{Tr}(x^{-1}) = 1$.

So a root x for $\mathrm{Tr}(y) = 1$ is never a root for $\mathrm{Tr}(y) = 0$. Since the maps ϕ and $x \mapsto \frac{1}{x^2+x+1}$ are injective on the sets F_0 and $F_0 + 1$, the proof is complete. □

Remark 4.8. Again the DDHOs from Example 4.6 are bilinear. Using the Knuth operations we obtain symmetric, bilinear DHOs defined by the mapping B^{o*} of the form

$$xB^{o*}(y) = xy + x^2y + xy^2 + \mathrm{Tr}(xy).$$

Example 4.9. For $y \in F$ we define a $\mathbb{F}_2$-linear mapping $B(y)$ on F by

$$xB(y) = (x + x^2)(y + \mathrm{Tr}(y)) + (x^4 + x^{2^{n-2}})\mathrm{Tr}(y) + x^{2^{n-1}}(y^{2^{n-1}} + \mathrm{Tr}(y)).$$

Set

$$\mathbf{D} = \{S_y \mid y \in F\}, \quad S_y = \{(x, xB(y)) \mid x \in F\}.$$

Then $\mathbf{D}$ is a symplectic DDHO. This follows from follows from:

Lemma 4.10. *The set* $\mathbf{D}$ *is a symplectic, bilinear DHO on* V.

Proof. Clearly, all operators $B(y)$ are self-adjoint with respect to the trace form. We have to show that each $B(y)$, $y \neq 0$ has rank $n - 1$ and that $\ker B(y) \neq \ker B(z)$ for $0 \neq y \neq z \neq 0$. Now $x \in \ker B(y)$ iff

$$(x + x^2)(y + \mathrm{Tr}(y)) + (x^4 + x^{2^{n-2}})\mathrm{Tr}(y) + x^{2^{n-1}}(y^{2^{n-1}} + \mathrm{Tr}(y)) = 0. \qquad (*)$$

For $y = 1$ we get $x + x^{2^{n-2}} = 0$ or $x^{16} = x$ and hence $x = 1$ as n is odd. So we assume from now on $y \in F_0 = F - \{0, 1\}$ and that (x, y), $x \neq 0$, is a solution of equation $(*)$.

Case $\mathrm{Tr}(y) = 0$. After squaring the equation we see that (x, y) is a root of the polynomial $(X^2 + X^4)Y^2 + XY$. Since y has a trivial trace we can write $y = y_1 + y_1^2$. Substituting Y by $Y + Y^2$ we see that (x, y_1) is a root of the polynomial $f(X, Y) = X(Y + Y^2) + (X^2 + X^4)(Y^2 + Y^4) = XY(Y + 1)g(X, Y)$, where

$$g(X, Y) = Y^2(X^3 + X) + Y(X^3 + X) + 1$$

is the same polynomial which occurred in the case $\mathrm{Tr}(y) = 0$ in the proof of Lemma 4.7. We use this part: So if $\mathrm{Tr}(y) = 0$, $y \in F_0$, then there is a unique $x = x_y \in F_0$ such that $f(x, y) = 0$. Moreover the mapping $y \mapsto x_y$ is injective and $\mathrm{Tr}(x^{-1}) = 0$.

CASE $\mathrm{Tr}(y) = 1$. After taking the fourth power of (∗) we see that (x, y) is a root of $(X^4 + X^8)(Y^4 + 1) + X^2(Y^2 + 1) + X^{16} + X$. We can write $y = 1 + y_1 + y_1^2$. Substitute in the polynomial Y by $1 + Y + Y^2$. Then (x, y_1) is a root of the polynomial $f(X, Y) = (X^4 + X^8)(Y^4 + Y^8) + X^2(Y^2 + Y^4) + X^{16} + X$ which factorizes over $E = \mathbb{F}_{2^{2n}}$ as $f(X, Y) = Xf_0(X, Y)f_1(X, Y)f_{-1}(X, Y)$ with

$$f_0(X, Y) = X^5 + X^3 + XY^4 + XY^2 + X + 1$$

and

$$f_i(X, Y) = X^5 + X^3Y^2 + \nu^i X^3 + X^2 + XY^2 + \nu^i X + 1$$

for $i = \pm 1$. If (x, y_1) is a root of one of the last two factors, it is also a root of the other factor. But then

$$0 = f_1(x, y_1) + f_{-1}(x, y_1) = x^3 + x \quad \text{or} \quad x = 1.$$

But then $f_1(1, y_1) = 1$, a contradiction. Hence (x, y_1) is a root of $f_0(X, Y)$. Multiply $f_0(x, y_1) = 0$ with x^{-1}. We get $0 = x^4 + x^2 + y_1^4 + y_1^2 + x^{-1} + 1$ or $\mathrm{Tr}(x^{-1}) = 1$. Set $z = x^{-1}$. Then (z, y_1) is a root of $Z^5 + Z^4(Y^2 + Y + 1)^2 + Z^2 + 1$. We write $z = z_1^2 + z_1 + 1$ and observe that (z_1, y_1) is a root of

$$g(Z, Y) = (Z^2 + Z + 1)^5 + (Z^2 + Z + 1)^4(Y^2 + Y + 1)^2 + (Z^2 + Z + 1)^2 + 1,$$

which factorizes as $g(Z, Y) = g_1(Z, Y)g_2(Z, Y)$ with

$$g_1(Z, Y) = Z^5 + Z^4Y^2 + Z^3 + Z^2Y^2 + Z + Y^2 + 1$$

and

$$g_2(Z, Y) = Z^5 + Z^4Y^2 + Z^4 + Z^3 + Z^2Y^2 + Z^2 + Z + Y^2.$$

This implies

$$y_1^2 = \frac{z_1^5 + z_1^3 + z_1 + 1}{z_1^4 + z_1^2 + 1} \quad \text{or} \quad y_1^2 = \frac{z_1^5 + z_1^3 + z_1 + 1}{z_1^4 + z_1^2 + 1} + 1.$$

We claim:

(1) The mapping $\phi : z \mapsto \frac{z^5+z^3+z+1}{z^4+z^2+1}$ is a bijection on F_0.

(2) If $z_1, z_2 \in F_0$ and $\frac{z_1^5+z_1^3+z_1+1}{z_1^4+z_1^2+1} = \frac{z_2^5+z_2^3+z_2+1}{z_2^4+z_2^2+1} + 1$, then $z_2 = z_1 + 1$.

In case (2) we have $z_1 + z_1^2 = z_2 + z_2^2$. So if the claim is verified, we see that for $y \in F_0$, $\mathrm{Tr}(y) = 1$ there is a unique $0 \neq x = x_y \in F_0$ such that equation (∗) holds, $\mathrm{Tr}(x^{-1}) = 1$, and $y \mapsto x_y$ is a injection.

We first prove claim (1). The polynomial $h(X,Y) = (X^5+X^3+X+1)(Y^4+Y^2+1)+(Y^5+Y^3+Y+1)(X^4+X^2+1)$ factorizes over $E = \mathbb{F}_{2^{2n}}$ as $h(X,Y) = (X+Y)h_1(X,Y)h_{-1}(X,Y)$ with

$$h_i(X,Y) = X^2Y^2 + \nu^i X^2 + X + \nu^i Y^2 + Y + \nu^i$$

for $i = \pm 1$. If $\phi(z_1) = \phi(z_2)$, then (z_1, z_2) is a root of the polynomial $h(X,Y)$. Assume $z_1 \neq z_2$. Then (z_1, z_2) is a root of one of the $h_i(X,Y)$'s and so of both of them. We get

$$0 = h_1(z_1,z_2) + h_{-1}(z_1,z_2) = z_1^2 + z_2^2 + 1, \quad \text{or} \quad z_2 = z_1 + 1.$$

But $h_1(z_1, z_1+1) = z_1^4 + z_1^2 + 1 = 0$ which is impossible. So (1) holds.

We now prove claim (2). If (2) holds, then (z_1, z_2) is a root of the polynomial $\ell(X,Y) = h(X,Y) + (X^4+X^2+1)(Y^4+Y^2+1)$, which factorizes over E as $\ell(X,Y) = (X+Y+1)\ell_1(X,Y)\ell_{-1}(X,Y)$ with

$$\ell_i(X,Y) = X^2Y^2 + \nu^i X^2 + X + \nu^i Y^2 + Y + 1$$

for $i = \pm 1$. If (z_1, z_2) is a root of one $\ell_i(X,Y)$, then, as usual, it is a root of both factors. This implies

$$0 = \ell_1(z_1,z_2) + \ell_{-1}(z_1,z_2) = z_1^2 + z_2^2, \quad \text{or} \quad z_2 = z_1.$$

But $\ell_1(z_1,z_1) = z_1^4 + 1 = 0$, which is impossible. So (2) holds.

From case 1 and 2 we conclude that for $y \in F_0$ there is a unique $x = x_y \neq 0$ such that (x,y) is a solution of equation (*). Moreover $x_y \in F_0$ and $\mathrm{Tr}(x^{-1}) = 0$, if $\mathrm{Tr}(y) = 0$ and $\mathrm{Tr}(x^{-1}) = 1$, if $\mathrm{Tr}(y) = 1$. Then using (1) and (2) we conclude that the mapping $y \mapsto x_y$ is a bijection of $F^\star$. The proof is complete. □

Remark 4.11. Using the Knuth operations we obtain a symmetric, bilinear DHO defined by B^{o*}. It has the form

$$xB^{o*}(y) = xy + x^2y + xy^2 + \mathrm{Tr}(x^4y + x^2y + xy + xy^2 + xy^4).$$

Example 4.12. For $y \in F$ we define a $\mathbb{F}_2$-linear, self-adjoint mapping $B(y)$ on F by

$$xB(y) = x\mathrm{Tr}(y) + \mathrm{Tr}(x)y^{2^{n-2}} + \mathrm{Tr}(x^4y) + xy^{2^{n-1}} + x^2y^{2^{n-2}} + x^{2^{n-1}}y^{2^{n-3}}.$$

Set

$$\mathbf{D} = \{S_y \mid y \in F\}, \quad S_y = \{(x, xB(y)) \mid x \in F\}.$$

Then $\mathbf{D}$ is a symplectic, bilinear DDHO: Taking the 8-th power of the equation $0 = xB(y)$ and replacing (by abusing the notation) x^4 by x we obtain

$$0 = x^2\mathrm{Tr}(y) + \mathrm{Tr}(x)y^2 + \mathrm{Tr}(xy) + x^4y^2 + x^2y^4 + xy.$$

The assertion follows from two results of Peter Müller [15].

Proposition 4.13 (P. Müller). *Let $5 \leq n$ be an odd integer, $F = \mathbb{F}_{2^n}$, and $\mathrm{Tr} : F \to \mathbb{F}_2$ is the absolute trace. Set*

$$f(X,Y) = X^2\mathrm{Tr}(Y) + \mathrm{Tr}(X)Y^2 + \mathrm{Tr}(XY) + X^2Y^4 + X^4Y^2 + XY. \qquad (1)$$

Then for any $0 \neq x \in F$ there is a unique $0 \neq y = y(x) \in F$ with $f(x,y) = 0$. Furthermore, the map $x \mapsto y(x)$ is bijective on $F^\star$.

We also need:

Lemma 4.14 (P. Müller). *Let F be a finite extension of $\mathbb{F}_2$ of odd degree, and $\mathrm{Tr} : F \to \mathbb{F}_2$ the trace map. Then for each $0 \neq x \in F$ with $\mathrm{Tr}(x) = 0$, there is a unique t in F with $x = \frac{(t+1)^3}{t}$.*

We start with the proof of the lemma.

Proof. We have $x = u^2 + u$ where u is unique up to adding 1 and we assume for the moment that a t has been found as required and show the uniqueness. Since $x = \frac{(t+1)^3}{t} = t^2 + t + 1 + \frac{1}{t}$ we have $\mathrm{Tr}(\frac{1}{t}) = 1$. So we have a v in F (unique up to adding 1) with $t = \frac{1}{v^2+v+1}$. Replacing in the equation $0 = x + \frac{(t+1)^3}{t}$ the term x by $u^2 + u$ and t by the fraction in v we obtain the equation

$$0 = (uv^2 + v^3 + uv + u)(uv^2 + v^3 + uv + v^2 + u + v + 1).$$

So $u = \frac{v^3}{v^2+v+1}$ or $u = \frac{(v+1)^3}{v^2+v+1}$. Note that the latter expression arises from the former by replacing v by $v + 1$ and also by adding 1 to the former expression. But replacing v by $v + 1$ does not change t. This shows the uniqueness of t. Reverting the previous steps shows the existence of the desired t. □

We are now in the position to prove the proposition.

Proof of Proposition 4.13. The function $f(X,Y)$ is symmetric in X and Y. If we show the first assertion of Proposition 4.13, the second one does follow. We first claim that if $f(x,y) = 0$ one has:

$$\mathrm{Tr}(xy) = \mathrm{Tr}(x)\mathrm{Tr}(y) \qquad (2)$$
$$\mathrm{Tr}(x^2y) = \mathrm{Tr}(xy^2) \qquad (3)$$

Equation (3) follows if we apply the trace to the equation $f(x,y) = 0$. We write the equation $0 = x^2 f(x,y)$ as $x^4\mathrm{Tr}(y) = (xy)^2\mathrm{Tr}(x) + x^2\mathrm{Tr}(xy) + x^6y^2 + (xy)^4 + x^3y$ and apply again the trace. This shows

$$\mathrm{Tr}(x)\mathrm{Tr}(y) = \mathrm{Tr}(x^6y^2 + (xy)^4 + x^3y) = \mathrm{Tr}(xy) + \mathrm{Tr}((x^3y)^2 + x^3y) = \mathrm{Tr}(xy)$$

and equation (2) is true too. We now distinguish the cases $\mathrm{Tr}(x) = 1$ and $\mathrm{Tr}(x) = 0$.

CASE $\mathrm{Tr}(x) = 1$. In this case we have

$$\mathrm{Tr}(\frac{1}{x}) = \mathrm{Tr}(y). \tag{4}$$

Assume first $\mathrm{Tr}(y) = 1$. By (2) also $\mathrm{Tr}(xy) = 1$. Then

$$0 = f(x, y) = (xy + 1)(xy + x^2 + 1)(xy + y^2 + 1).$$

The trace of the last two factors is 1. So the first factor vanishes and $y = \frac{1}{x}$ which implies (4).

Assume now $\mathrm{Tr}(y) = 0$. So $\mathrm{Tr}(xy) = 0$ too. We get

$$0 = f(x, y) = (x^3y + x^2y^2 + 1)(x + y)y.$$

The latter two factors do not vanish, i.e. $0 = x^3y + x^2y^2 + 1$. We divide by x and take the trace. Using equation (3) we get $\mathrm{Tr}(\frac{1}{x}) = 0$ as required.

We also note that for $\mathrm{Tr}(\frac{1}{x}) = 1$ the unique solution of $f(x, Y) = 0$ is $y = \frac{1}{x}$.

It remains to show that for $\mathrm{Tr}(\frac{1}{x}) = 0$ the is a unique y such that $0 = x^3y + x^2y^2 + 1$ and $\mathrm{Tr}(y) = \mathrm{Tr}(xy) = 0$. First, it is clear that there is at most one such y, because if y_1 and y_2 are roots of $x^3Y + x^2Y^2 + 1$, then $x = y_1 + y_2$, contradicting $\mathrm{Tr}(x) = 1$ and $\mathrm{Tr}(y_i) = 0$. It remains to show that there is at least one solution. Since $\mathrm{Tr}(\frac{1}{x}) = 0$, there is a $t \in F^\star$ such that $\frac{1}{x} = t^2 + t$, so $x = \frac{1}{t} + \frac{1}{t+1}$. Since $\mathrm{Tr}(x) = 1$ we have $\mathrm{Tr}(\frac{1}{t}) \neq \mathrm{Tr}(\frac{1}{t+1})$. As the expression for x does not change upon replacing t with $t + 1$, we may assume $\mathrm{Tr}(\frac{1}{t+1}) = 1$. Set

$$y = \frac{t^3}{t + 1}.$$

A calculation shows that indeed $x^3y+x^2y^2+1 = 0$. Moreover $y = t^2+t+1+\frac{1}{t+1}$, hence $\mathrm{Tr}(y) = 0$. Also $\mathrm{Tr}(xy) = \mathrm{Tr}(\frac{1}{t^2+t} \cdot \frac{t^3}{t+1}) = \mathrm{Tr}(\frac{1}{t+1}) + 1 = 0$, as required.

CASE $\mathrm{Tr}(x) = 0$. From (2) we deduce $\mathrm{Tr}(xy) = 0$. We first show that for any such $x \in F^\star$, there is at least one $y \in F^\star$ with $f(x, y) = 0$. In the present case y is then a root of the polynomial

$$f(x, Y) = x\mathrm{Tr}(Y) + x^3Y^2 + xY^4 + Y.$$

If we look for roots with $\mathrm{Tr}(y) = 0$, then we need to solve $x^3Y + xY^3 + 1 = 0$. The curve $X^3Y + XY^3 + 1 = 0$ is parametrized by

$$x = \frac{(t + 1)^3}{t}, \quad y = \frac{t^3}{t + 1}.$$

Similarly, for $\mathrm{Tr}(y) = 1$ we have to consider the curve $X^3Y^2 + XY^4 + X + Y = 0$ which is parametrized by

$$x = \frac{(t+1)^3}{t}, \quad y = \frac{1}{t^2+t} = \frac{1}{t} + \frac{1}{t+1}.$$

By Lemma 4.14 (as $\mathrm{Tr}(x) = 0$) there is a $t \in F^\star$ with $x = \frac{(t+1)^3}{t} = t^2 + t + 1 + \frac{1}{t}$. Set

$$y_1 = \frac{t^3}{t+1} = t^2 + t + 1 + \frac{1}{t+1} \quad \text{and} \quad y_2 = \frac{1}{t^2+t} = \frac{1}{t} + \frac{1}{t+1}.$$

The condition $\mathrm{Tr}(x) = 0$ implies $\mathrm{Tr}(\frac{1}{t}) = 1$. Thus

$$\mathrm{Tr}(y_1) = 1 + \mathrm{Tr}(\frac{1}{t+1}) \quad \text{and} \quad \mathrm{Tr}(y_2) = 1 + \mathrm{Tr}(\frac{1}{t+1}) = \mathrm{Tr}(y_1).$$

So if $\mathrm{Tr}(\frac{1}{t+1}) = 0$, then $\mathrm{Tr}(y_2) = 1$ and we set $y = y_2$. If $\mathrm{Tr}(\frac{1}{t+1}) = 1$, then $\mathrm{Tr}(y_1) = 0$ and we set $y = y_1$. At any rate, we get a solution y of $f(x, Y) = 0$ in the case of $\mathrm{Tr}(x) = 0$.

We need to show the uniqueness of y. Suppose there is another y' with $f(x, y') = 0$. From the parametrizations, which give in both cases a bijection between the pairs (x, y) and the parameter t, it is clear that y and y' must correspond to different cases. So $\mathrm{Tr}(y) \neq \mathrm{Tr}(y')$. By Lemma 4.14 t is uniquely determined by x. So the parameter t is the same for y and y'. But then $\mathrm{Tr}(y) = \mathrm{Tr}(y')$ (as we have seen above), a contradiction. The proof is complete. □

Remark 4.15. Since our DHO is bilinear, one can use the Knuth operations and obtains a symmetric, bilinear DHO B^{o*} of the form

$$xB^{o*}(y) = x^4\mathrm{Tr}(y) + \mathrm{Tr}(x)y^4 + \mathrm{Tr}(xy) + x^2y^2 + x^8y^4 + x^4y^8.$$

Proposition 4.16. *The DHOs of Examples 4.3, 4.6, 4.9, and 4.12 are symplectic but not orthogonal.*

Proof. Apply Lemma 3.10, Lemma 3.11 and Remark 3.12. □

There is an alternative way to verify this fact: Use the associated symmetric DHOs obtained from the Knuth operations. If one of our DHOs would be orthogonal, its associated symmetric DHO would even be alternating. Assume that the additive map $B' : F \to \mathrm{End}(F)$ defines the additively closed DHO-set of this alternating DHO. Then define a mapping $\kappa : F \to F$ by setting $\kappa(0) = 0$ and defining $\kappa(a)$ as the nontrivial element in $\ker B'(a)$ for $a \neq 0$. Then by Taniguchis [17, Prop. 3] κ would be linear. So one needs to rule out the linearity of κ. However to verify this non-linearity seems to be somewhat unpleasant.

We close this section with a simple series of orthogonal, non-bilinear DHOs.

Example 4.17. For $y \in F$ define a $\mathbb{F}_2$-linear mapping $B(y)$ by

$$xB(y) = xy^2 + \mathrm{Tr}(xy)y$$

and set

$$\mathbf{D} = \{S_y \mid y \in F\}, \quad S_y = \{(x, xB(y)) \mid x \in F\}.$$

Then $\mathbf{D}$ is an orthogonal DDHO. Indeed, this follows immediately from the projection method in [6]. However an ad hoc verification is simple too:

Lemma 4.18. *The set $\mathbf{D}$ is an orthogonal DHO. The group $M = \{\mu_a : (x, y) \mapsto (a^{-1}x, ay) \mid a \in F^\star\}$ is a group of automorphisms of $\mathbf{D}$.*

Sketch of the proof. Clearly, the operators $B(y)$ are skew symmetric. Note that $(x, xB(y))\mu_a = (z, zB(ya))$ for $y = z^{-1}x$, i.e. $S_y\mu_a = S_{ya}$. So in order to show that $\mathbf{D}$ is a DHO it is enough to show

(1) $\{S_0 \cap S_y \mid y \neq 0\}$ is the set of 1-spaces of S_0 and

(2) $\{S_1 \cap S_y \mid y \neq 1\}$ is the set of 1-spaces of S_1.

But clearly $S_0 \cap S_y = \langle (y^{-1}, 0) \rangle$ for $y \neq 0$ and (1) follows.

We now prove (2). We already know $S_0 \cap S_1 = \langle (1, 0) \rangle$. Let $y \in F - \{0, 1\}$ and $(x, xB(1)) \in S_y$. Then

$$xy^2 + \mathrm{Tr}(xy)y = x + \mathrm{Tr}(x).$$

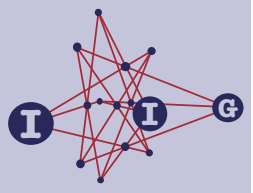
We determine the non-trivial solutions of this equation.

Note first that $\mathrm{Tr}(xy) \neq \mathrm{Tr}(x)$: If $\mathrm{Tr}(xy) = \mathrm{Tr}(x) = 0$, we get $y = 1$, a contradiction. If $\mathrm{Tr}(xy) = \mathrm{Tr}(x) = 1$, we get $x = y/(y^2 + 1)$ and then $\mathrm{Tr}(x) = 0$, a contradiction.

If $\mathrm{Tr}(1/(1 + y^2)) = 1$, we see that $x = 1/(1 + y^2)$ is a solution, whereas if $\mathrm{Tr}(1/(1 + y^2)) = 0$, then $x = y/(1 + y^2)$ is a solution. Since $1/(1 + y^2)$ and $y^2/(1 + y^2)$ have different traces we see that all solutions are different. Also from the fact $\mathrm{Tr}(xy) \neq \mathrm{Tr}(x)$ one deduces that for a fixed y there is at most one non-trivial solution. □

Lemma 4.19. *The DHOs from Example 4.17 are not bilinear.*

Proof. We take the notation from Example 4.17 and assume that $\mathbf{D}$ is a bilinear DHO of rank n. Then there exists a translation group $\mathcal{T}$ in the automorphism group with the following properties: The group is an elementary abelian 2-group of order 2^n which acts regularly on $\mathbf{D}$, the DHO splits over $W = C_V(\mathcal{T})$, and $\mathcal{T}$ acts trivially on V/W. By [5, Thm. 4.10] the translation group is normal in the automorphism group of the DHO. Therefore the cyclic group M of order



$2^n - 1$ from the proof of Lemma 4.18 fixes W. The only proper M-spaces in V are $S_0 = F \times 0$ and $S' = 0 \times F$: After tensoring with F we see that $\mu_a \in M$ has the eigenvalues $a^{-1}, a^{-2}, a^{-4}, \ldots$ on $F \otimes S$ and on $F \otimes S'$ the eigenvalues are $a, a^2, a^4, \ldots$. This shows $W = S'$. As $\mathcal{T}$ is elementary abelian there exists an isomorphism $\tau : (F, +) \to \mathcal{T}$ such that $S_0\tau_y = S_y$. From the properties of the translation group we deduce

$$(x_1, x_2)\tau_y = (x_1, x_1B(y) + x_2).$$

But then $\{B(y) \mid y \in F\}$ is an additive subgroup of $\mathrm{End}(F)$. It is easily checked that this is not true. So $\mathbf{D}$ is not bilinear. □

5. Associated bent functions, isomorphisms

We now determine the bent functions which are associated with the examples of the previous section (in the sense of Theorem 1.2).

Let $\mathbf{D}$ be a DDHO of rank n in the space $V = V(2n, 2)$, which splits over the subspace W of V. We call the characteristic function of the set $(\bigcup_{S\in\mathbf{D}} S) - 0$ the *small bent function* and the characteristic function of the set $W \cup \bigcup_{S\in\mathbf{D}} S$ the *big bent function associated with the DDHO*.

We recall from [4]: Let Q be a quadratic form of $(+)$-type on $V = V(2n, 2)$, $S(V)$ the set of singular vectors, and U a totally singular subspace of dimension m. Then the characteristic function of $(S(V) \cap U^\perp) \cup (V - U^\perp - S(V))$ is a bent function, which was called *standard parabolic of degree* m in [4]. Finally, we recall that two boolean functions f_1 and f_2 on V are called *equivalent* iff there exist $T \in \mathrm{GL}(V)$, $v \in V$, a linear functional λ on V, and $a \in \mathbb{F}_2$ such that $f_2(x) = f_1(xT + v) + \lambda(x) + a$.

The bent functions associated with the the orthogonal DHOs, in particular the DDHOs $\mathbf{D}_{r,-r}$ from Example 4.1 and the DDHOs from Example 4.17 are determined by the following result.

Proposition 5.1. *The big bent function of an orthogonal DHO of rank n is equivalent to a nondegenerate, quadratic form in $2n$-variables. The small bent function is equivalent to a standard parabolic bent function of degree n.*

Proof. Let Q be a nondegenerate, quadratic form of $(+)$-type on $V = V(2n, 2)$. Let $\mathbf{D}$ be an orthogonal DHO of rank n in V, which splits over the totally singular subspace W. Since $|S(V)| = |W \cup \bigcup_{S\in\mathbf{D}} S|$ we have that the big bent function is $Q + 1$. Now $W = W^\perp$. This shows that the characteristic function of the complement of $(\bigcup_{S\in\mathbf{D}} S) - 0$ consists of W and the non-singular vectors in

$V - W$ and is therefore standard parabolic of degree n. So the small bent function is equivalent to a standard parabolic bent function of degree n. □

Proposition 5.2. *Let f be a bent function associated with a DDHO $\mathbf{D} = \mathbf{D}_{r,t}$, $t \neq -r$, from Example 4.1. Then f is a small or big bent function of cyclic trace type (in the sense of [4, (3.2)]) according as to whether f is big or small respectively.*

Proof. We use the terminology of Example 4.1, i.e $\mathbf{D} = \{S_y \mid y \in F\}$ with $S_y = \{(x, x^{2^r}y + x^{2^{-r}}y^{2^t}) \mid x \in F\}$ is a DDHO of rank n. We set $B = \bigcup_{a \in F} S_a - 0$ and want to show that the characteristic function is a bent function of cyclic trace type in the sense of [4].

Let $0 < k < 2^n$ be the unique number such that

$$k(2^{r+t} - 2^r) \equiv 2^{2r+t} - 1 \pmod{2^n - 1}.$$

By the choice of k for any $x \in F^\star$ we have

$$x^{(2^r-k)2^t} = x^{2^{-r}-k},$$

which shows

$$\begin{aligned}\mathrm{Tr}(x^{-k}(x^{2^r}y + x^{2^{-r}}y^{2^t})) &= \mathrm{Tr}(x^{2^r-k}y + x^{2^{-r}-k}y^{2^t})) \\ &= \mathrm{Tr}(x^{2^r-k}y + (x^{2^r-k}y)^{2^t}) = 0.\end{aligned}$$

So

$$B = \{(a, a^k b) \mid a \in F^\star,\, b \in F_0\}, \quad \text{with} \quad F_0 = \{x \in F \mid \mathrm{Tr}(x) = 0\},$$

whose characteristic function is a small bent function of cyclic trace type in the terminology of [4, (3.2)]. Similarly, one sees that the characteristic function of $B \cup 0 \times F$ is a big bent function of cyclic trace type. □

In order to describe the bent functions associated with Examples 4.3, 4.6, and 4.9, we introduce a series of bent functions related to the bent functions of parabolic type from [4].

Proposition 5.3. *Let Q be a quadratic form of $(+)$-type on $V = V(2n, 2)$, $n > 3$. Let $S(V)$ be the set of singular vectors and W be a totally singular subspace of dimension n.*

(a) *Let W_0 be a n-dimensional subspace such that $(S(V) - W) \cap W_0 = \emptyset$. Then the characteristic function of $B = (S(V) - W) \cup W_0$ is a bent function. Furthermore, $W_0 = A \oplus (W \cap W_0)$ with an anisotropic space A of dimension ≤ 2.*

(b) *There exist subspaces W_0 and A satisfying the assertions of* (a)*, such that* $\dim A = 0, 1,$ *or* 2 *holds.*

(c) *Let W_0, A, and B be as in* (a)*. Let $T \in \mathrm{GL}(V)$ be a transformation which leaves B invariant. Then T is an isometry. More precisely, T is contained in $\mathrm{O}(V,Q)_{W\cap W_0,W_0}$, the common stabilizer in the orthogonal group of the subspaces $W \cap W_0$ and W_0.*

Proof. (a) Assume first $n \equiv 0 \pmod 2$. Then V has an orthogonal spread $\mathbf{S}$ which contains W (see for instance [12, Sec. 4]). Then $(\mathbf{S} - \{W\}) \cup \{W_0\}$ is a partial spread of size $2^{n-1}+1$. So the characteristic function of B is a bent function of partial spread type (see [9], [10, Corollary 1]).

Assume now $n \equiv 1 \pmod 2$. Then there exists an orthogonal DHO $\mathbf{D}$ which splits over W. For instance we can choose a DHO $\mathbf{D}_{r,-r}$ of Example 4.1 or the DHO of Example 4.17. But then we can apply Theorem 1.2 to B.

Write $W_0 = \mathrm{Rad}(W_0) \oplus A$ where $\mathrm{Rad}(W_0) = \{x \in W_0 \cap W_0^\perp \mid Q(x) = 0\}$ is the radical of W_0. Form the choice of W_0 we know that the singular vectors of this space lie in W. If A is not anisotropic, then A contains a hyperbolic pair $\{v, w\}$ of singular vectors, i.e. v and w are not perpendicular to each other. This follows from the well known classification of quadratic forms over finite fields. But then v and w cannot both lie in W, a contradiction. Thus A is anisotropic, $W_0 \cap W = \mathrm{Rad}(W_0)$, and again by the classification of quadratic forms over finite fields we have $\dim A \leq 2$.

(b) We need to find W_0 such that the anisotropic part has dimension 1 or 2. Let $\{v_1, \ldots, v_n, w_1, \ldots, w_n\}$ be a basis of singular vectors, such that $\beta(v_i, w_j) = \delta_{ij}$, and $\beta(v_i, v_j) = \beta(w_i, w_j) = 0$ for all $0 \leq i, j \leq n$, where β is obtained by polarization from Q. Set $W_0 = \langle v_1 + w_1, v_2, \ldots, v_n\rangle$ and $W_0' = \langle v_1 + w_1, v_1 + v_2 + w_2, v_3, \ldots, v_n\rangle$. Then $\dim \mathrm{Rad}(W_0) = n - 1$ and $\dim \mathrm{Rad}(W_0') = n - 2$.

(c) We claim that ST is totally singular for $S \in \mathbf{D}$: Assume ST is not totally singular. From the classification of quadratic forms over finite fields we deduce that ST contains at least $2^{n-1} - 2^{n-2} = 2^{n-2}$ nonsingular vectors. Since $ST \subseteq B$ these vectors must lie in $W_0 - (W_0 \cap W)$. Assume $\dim(ST \cap W_0) = m$. As $W_0 \cap W$ has codimension $\dim A$ in W_0 we see that ST contains at most 2^{m-1} nonsingular vectors, if $\dim A = 1$ and at most $3 \cdot 2^{m-2}$ nonsingular vectors, if $\dim A = 2$. In any case we deduce $m \geq n - 1$. Let $S \neq S' \in \mathbf{D}$. If $S'T$ is not singular, we get $n - 2 \leq \dim(ST \cap S'T \cap W_0) \leq 1$, a contradiction. Hence $S'T$ is singular and the nontrivial vector in $ST \cap S'T$ is singular too. But for any $0 \neq uT \in ST$ we can find $S' \in \mathbf{D}$ such that $S \cap S' = \langle u\rangle$, which shows that all elements of ST are singular, contradicting the assumption. So the claim holds. In particular, singular vectors which are covered by the DHO,

are still singular after the application of T.

For $0 \neq w \in W$ and $S \in \mathbf{D}$ the space $S_w = S \cap \langle w \rangle^\perp$ is a hyperplane and thus $U = \langle w \rangle \oplus S_w$ is a totally singular n-space such that $U - \langle w \rangle$ lies in $B - W_0$. So UT contains at least $2^n - 2$ singular vectors, i.e. UT is totally singular too. This shows that T leaves the set of singular vectors invariant, i.e. T is an isometry. Also T preserves $W_0 - (W_0 \cap W)$, the set of nonsingular vectors in B. Thus T fixes $W_0 = \langle W_0 - (W_0 \cap W) \rangle$ and $\mathrm{Rad}(W_0) = W_0 \cap W$ too. The proof is complete. □

Definition 5.4. Let f be a bent function defined as in Proposition 5.3 and let $d = \dim A$. We call f a *bent function of standard type with defect* d.

Here we recall that the nondegenerate, quadratic forms were called bent functions of standard type in [4]. I.e. "standard type with defect 0" means that the bent function is a nondegenerate, quadratic form. Bent functions of standard type with defect 1 (or 2) resemble closely standard parabolic bent functions of degree $n-1$ (or $n-2$): It follows from (c) of Proposition 5.3 that the automorphism groups are non-isomorphic but that the lowest term of the derived series of the automorphism groups are isomorphic.

Proposition 5.5. *Let f be a bent function associated with a DHO from Example 4.3, 4.6, or 4.9 and let n be its rank. The bent function is equivalent to a standard parabolic bent function of degree n, if f is small, and it is of standard type with defect 1, if f is big.*

Proof. As in the examples we identify $V = F \times F$, $F = \mathbb{F}_{2^n}$, and we define two quadratic forms Q and Q_1 on V by

$$Q(x,y) = \mathrm{Tr}(xy), \quad Q_1(x,y) = Q(x,y) + \mathrm{Tr}(y).$$

So both quadratic forms polarize to the same symplectic form β, which is described in Remark 3.6. We claim that Q_1 vanishes on the supports of the small bent functions. First we consider Example 4.3 and apply Q_1 to a typical vector of the support:

$$\begin{aligned} Q_1(x, xB(y)) &= Q(x, xB(y)) + \mathrm{Tr}(xB(y)) \\ &= \mathrm{Tr}(x^2y + x^2y^{2^{n-1}} + x^5y + x^{2^{n-2}+1}y^{2^{n-2}}) \\ &\qquad + \mathrm{Tr}(xy + xy^{2^{n-1}} + x^4y + (xy)^{2^{n-2}}) \\ &= \mathrm{Tr}(x^2y) + \mathrm{Tr}(x^2y^{2^{n-1}}) + \mathrm{Tr}(x^4y) + \mathrm{Tr}(xy^{2^{n-1}}) \\ &= 0. \end{aligned}$$

In the case of Example 4.6 we get

$$\begin{aligned} Q_1(x, xB(y)) &= Q(x, xB(y)) + \mathrm{Tr}(xB(y)) \\ &= \mathrm{Tr}(x^2y + x^2\mathrm{Tr}(y) + x^3y + x^{2^{n-1}+1}y^{2^{n-1}}) \\ &\qquad + \mathrm{Tr}(xy + x\mathrm{Tr}(y) + x^2y + (xy)^{2^{n-1}}) \\ &= 0. \end{aligned}$$

In the case of Example 4.9 we have

$$\begin{aligned} Q_1(x, xB(y)) &= Q(x, xB(y)) + \mathrm{Tr}(xB(y)) \\ &= \mathrm{Tr}(x(xy + x\mathrm{Tr}(y)) + \mathrm{Tr}(xy + x^2y + (xy)^{2^{n-1}} + x^{2^{n-1}}\mathrm{Tr}(y)) \\ &= 0. \end{aligned}$$

The first assertion follows.

The fixed point set of the translation group is $W = 0 \times F$ and the subspace $\{(0, y) \mid \mathrm{Tr}(y) = 0\}$ is the radical of W with respect to Q_1. The second assertion follows from Proposition 5.3. □

Lemma 5.6. *Let f be a small bent function associated with a DHO from Example 4.12. Let n be the rank of the DHO. Then f is not standard parabolic of degree n.*

Proof. As usual we identify $V = F \times F$, $F = \mathbb{F}_{2^n}$, and define a quadratic form Q by

$$Q(x, y) = \mathrm{Tr}(xy).$$

Assume that f is standard parabolic of degree n. Then there exists a nondegenerate, quadratic form Q_1 such that the spaces of our DHO $\mathbf{D}$ are totally singular with respect to Q_1. By Lemma 3.10 both quadratic form must polarize to the same bilinear form, i.e. $Q_1 = Q + \lambda$ with a linear functional λ. Since $F \times 0 = S_0 \in \mathbf{D}$ we have $0 = Q_1(x, 0) = \lambda(x, 0)$. This shows $Q_1(x, y) = Q(x, y) + \lambda(0, y)$. So we can identify λ with a linear functional on F. Such a linear functional can be written uniquely as $y \mapsto \mathrm{Tr}(ay)$. Hence there is a uniquely determined $a \in F$ such that

$$Q_1(x, y) = Q(x, y) + \mathrm{Tr}(ay).$$

Elements in $S_1 \in \mathbf{D}$ have the form $(x, x + \mathrm{Tr}(x) + \mathrm{Tr}(x) + x + x^2 + x^{2^{n-1}}) = (x, x^2 + x^{2^{n-1}})$. Thus $\mathrm{Tr}(a(x^2 + x^{2^{n-1}})) = 0$ for all $x \in F$. This implies $a = 1$. So for all $x, y \in F$ we have

$$0 = Q_1(x, xB(y)) = \mathrm{Tr}(x \cdot xB(y)) + \mathrm{Tr}(xB(y)).$$

Firstly,

$$\begin{aligned}\mathrm{Tr}(x\cdot xB(y)) &= \mathrm{Tr}\big(x^2\mathrm{Tr}(y)+xy^{2^{n-2}}\mathrm{Tr}(x)+x\mathrm{Tr}(x^4y)\\ &\qquad +x^2y^{2^{n-1}}+x^3y^{2^{n-2}}+x^{2^{n-1}+1}y^{2^{n-3}}\big)\\ &= \mathrm{Tr}(x)\mathrm{Tr}(y)+\mathrm{Tr}(x^2y^{2^{n-1}})\\ &= \mathrm{Tr}\big(x(\mathrm{Tr}(y)+y^{2^{n-2}})\big)\end{aligned}$$

and secondly

$$\begin{aligned}\mathrm{Tr}(xB(y)) &= \mathrm{Tr}\big(x\mathrm{Tr}(y)+y^{2^{n-2}}\mathrm{Tr}(x)+\mathrm{Tr}(x^4y)\\ &\qquad +xy^{2^{n-1}}+x^2y^{2^{n-2}}+x^{2^{n-1}}y^{2^{n-3}}\big)\\ &= \mathrm{Tr}\big(x(y^{2^{n-1}}+y^{2^{n-3}})\big).\end{aligned}$$

Clearly, the mapping $y\mapsto \mathrm{Tr}(y)+y^{2^{n-2}}+y^{2^{n-1}}+y^{2^{n-3}}$ has non-zero values (consider the degree of this polynomial). So for such a y we can choose x such that

$$1=\mathrm{Tr}\big(x(\mathrm{Tr}(y)+y^{2^{n-2}}+y^{2^{n-1}}+y^{2^{n-3}})\big)=Q_1(x,xB(y)).$$

But this contradicts the assumption, the proof is complete. □

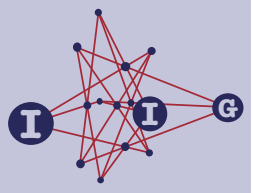
Isomorphisms. We now show that the examples of Section 4 produce essentially nonisomorphic DHOs.

First of all, the DHOs $\mathbf{D}_{r,t}$, $r\neq -t$, form Example 4.1 cannot be isomorphic to DHOs $\mathbf{D}_{r,-r}$ or to DHOs from Examples 4.3, 4.6, 4.9, 4.12, or 4.17 by Lemma 4.2. The orthogonal DHOs from Example 4.17 cannot be isommorphic to the examples from 4.1, 4.3, 4.6, 4.9, or 4.12 by Lemma 4.19. Also the isomorphism problem for two DHOs from Example 4.1 has been solved in [21] and [18].

Since the DHOs from Examples 4.3, 4.6, 4.9, 4.12 are symplectic but not orthogonal (Proposition 4.16) we only have to exclude isomorphisms between these examples. A possible isomorphism between DDHOs maps the support of one small bent function to the support of the small bent function of the other DDHO. So by Proposition 5.5 and Lemma 5.6 the DHOs from Examples 4.3, 4.6, and 4.9 cannot be isomorphic to DHOs from Example 4.12.

Finally, to a DHO $\mathbf{D}$ on V one can associate a semi-biplane $(V,\mathbf{L})$, $\mathbf{L}=\{S+v\mid S\in\mathbf{D},\,v\in V\}$. For the Examples 4.3, 4.6, and 4.9 and dimensions $n=5$ and 7 we calculated with the help of a computer the 2-rank of the incidence matrix:

n	Example 4.3	Example 4.6	Example 4.9
5	326	327	326
7	3766	3818	3828



This shows that the DHOs from these examples are pairwise not isomorphic for dimension 7. Another computer calculation showed that in dimension 5 the DHO from Example 4.3 *is isomorphic* to the DHO from Example 4.9. We *conjecture, that for dimension* ≥ 7 *the DHOs from Examples 4.3, 4.6, and 4.9 are pairwise not isomorphic.*

Final remarks.

(a) The selection of the examples of Section 4 was influenced by the author's search for bilinear symplectic DHOs of rank 5, which are defined over $\mathbb{F}_2$, i.e. it was assumed that the expression $xB(y)$ is a polynomial in x and y with coefficients in $\mathbb{F}_2$. Some of the examples found by this search lead to the series in Examples 4.3, 4.6, 4.9, and 4.12.

(b) Since the examples of Section 4 are defined over $\mathbb{F}_2$, one observes that the mapping $\phi : F \times F \ni (x, y) \mapsto (x^2, y^2) \in F \times F$ ($F = \mathbb{F}_{2^n}$ as usual) induces an automorphism of order n the DHO. The automorphism groups of the DHOs of Example 4.1 are determined in [21] and [18]. Using the methods of [7] it is not hard to show that a DHO of rank n from Example 4.17 has an automorphism group of the form

$$M \cdot \langle \phi \rangle \simeq \mathbb{F}_{2^n}^\star \cdot \mathrm{Gal}(\mathbb{F}_{2^n} : \mathbb{F}_2)$$

(M has the same meaning as in the proof of Lemma 4.18). The computation of the automorphism groups of DHOs from from Examples 4.3, 4.6, 4.9, and 4.12 appears to be rather difficult. Computer calculations indicate that the automorphism group should have the form $\mathcal{T} \cdot \langle \phi \rangle$ ($\mathcal{T}$ is the translation group of the DHO). However the DHO $\mathbf{D}$ from Example 4.12 for $n = 5$ seems to play an exceptional role. In this case the automorphism group has the form (computer calculation) $\mathrm{Aut}(\mathbf{D}) \simeq \mathcal{T} \cdot \mathrm{Alt}(5)$.

(c) The MAGMA software package [2] was very useful for the computation of small examples (for instance computations of isomorphisms and automorphisms of semi-biplanes) and the investigation of specific polynomials in two variables over finite fields (for instance finding factorizations).

(d) A computer search of the author for DDHOs of rank 4 was not successful. We conjecture that DDHOs only exist for odd ranks.

(e) In [6] it will be shown that orthogonal DHOs exist in large numbers. Orthogonal DHOs are in particular symplectic. Computer experiments for rank 5 indicate that the number of symplectic but not orthogonal DHOs of rank n should be larger than the number of orthogonal DHOs of this rank. Unfortunately the constructions of [6] are restricted to orthogonal DHOs only.

Acknowledgments. We thank Peter Müller for pointing out Proposition 4.13 and Lemma 4.14 to us and for his permission to use these results in this article. We also thank him for background information concerning curves over finite fields. We thank Yves Edel for his assistance in MAGMA programming and the computation of some large examples.

References

[1] **T. Bending**, *Bent functions, SDP designs and their automorphism groups*, Ph. D. Thesis, Queen Mary and Westfield College, Univ. London, 1993.

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

[3] **B. Cooperstein** and **J. Thas**, On generalized k-arcs in$PG(2n, q)$, *Ann. Combin.* **5** (2001), 141–152.

[4] **U. Dempwolff**, Automorphisms and equivalence of bent functions and difference sets in elementary abelian 2-groups, *Comm. Algebra* **34** (2006), 1077–1131.

[5] **U. Dempwolff** and **Y. Edel**, Dimensional dual hyperovals and APN functions with translation groups, *J. Algebraic Combin.* **39** (2014), 457–496.

[6] **U. Dempwolff** and **W. Kantor**, Dimensional dual hyperovals, symplectic and orthogonal spreads, *J. Algebraic Combin.*, to appear.
arXiv: 1303.4073.

[7] **U. Dempwolff** and **P. Müller**, Permutation polynomials and translation planes of even order, *Adv. Geom.*, to appear.
DOI: 10.1525/advgeom.2011.050.

[8] **A. Del Fra**, On d-dimensional dual hyperovals, *Geom. Dedicata* **79** (2000), 157–178.

[9] **J. Dillon**, *Elementary Hadamard difference sets*, Ph. D. Thesis, University of Maryland, 1974.

[10] _____, Elementary Hadamard difference sets, in *Graph Theory and Computing*, Proc. 6th S.E. Conf. Comb., Utilitas Math. Boca Raton, 237–249, 1975.

[11] **Y. Edel**, On some representations of quadratic APN functions and dimensional dual hyperovals, *RIMS Kokyuroku* **1687** (2010), 118–130.

[12] **W. Kantor**, Spreads, translation planes and Kerdock set I, *SIAM J. Alg. Disc. Math.* **3** (1981), 151–165.

[13] _____, Commutative semifields and symplectic spreads, *J. Algebra* **270** (2003), 98–114.

[14] **W. Kantor** and **M. Williams**, Nearly flag-transitive affine planes, *Adv. Geom.* **10** (2010), 161–183.

[15] **P. Müller**, personal communication.

[16] **H. Taniguchi**, On the duals of certain d-dimensional dual hyperovals in $PG(2d+1,2)$, *Finite Fields Appl.* **15** (2009), 673–681.

[17] _____, On the dual of the dual hyperoval from APN function $f(x) = x^3 + tr(x^9)$, *Finite Fields Appl.* **18** (2012), 210–221.

[18] **H. Taniguchi** and **S. Yoshiara**, On dimensional dual hyperovals $\mathcal{S}^{d+1}_{\sigma,\phi}$, *Innov. Incidence Geom.* **1** (2005), 197–219.

[19] _____, A new construction of the d-dimensional Buratti-Fra dual hyperoval, *Europ. J. Combin* **33** (2012), 1030–1042.

[20] **D. Taylor**, *The Geometry of the Classical Groups*, Heldermann Verlag, 1992.

[21] **S. Yoshiara**, A family of d-dimensional dual hyperovals in $\mathrm{PG}(2d+1,2)$, *European J. Combin* **20** (1999), 589–603.

[22] _____, Some remarks dimensional dual hyperovals of polar type, *Bull. Belg. Math. Soc. Simon Stevin* **12** (2006), 925–936.

[23] _____, Dimensional dual arcs, in *Finite Geometries, Groups and Computation*, Proc. of Conf. Pingree Park 2004, Col. USA, 247–266, 2006.

Ulrich Dempwolff

DEPARTMENT OF MATHEMATICS, TECHNICAL UNIVERSITY, 67653 KAISERSLAUTERN, GERMANY

e-mail: dempwolff@mathematik.uni-kl.de