J Algebr Comb (2015) 41:83–108
DOI 10.1007/s10801-014-0528-3

Orthogonal dual hyperovals, symplectic spreads, and orthogonal spreads

Ulrich Dempwolff · William M. Kantor

Received: 17 March 2013 / Accepted: 22 April 2014 / Published online: 28 May 2014

Abstract Orthogonal spreads in orthogonal spaces of type $V^+(2n+2, 2)$ produce large numbers of rank n dual hyperovals in orthogonal spaces of type $V^+(2n, 2)$. The construction resembles the method for obtaining symplectic spreads in $V(2n, q)$ from orthogonal spreads in $V^+(2n+2, q)$ when q is even.

Keywords Orthogonal dual hyperoval · Symplectic spread · Orthogonal spread

1 Introduction

A set $\mathbf{D}$ of n-dimensional subspaces spanning a finite $\mathbb{F}_q$-vector space V is called a *dual hyperoval* (DHO) *of rank* $n > 2$, if $|\mathbf{D}| = (q^n - 1)/(q - 1) + 1$, $\dim X_1 \cap X_2 = 1$ and $X_1 \cap X_2 \cap X_3 = 0$ for every three different $X_1, X_2, X_3 \in \mathbf{D}$. Usually DHOs are viewed projectively and called "dimensional dual hyperovals," but the vector space point of view seems better for our purposes. See the survey article [31] for many of the known DHOs, all of which occur in vector spaces of characteristic 2 and mostly are over $\mathbb{F}_2$, in which case $|\mathbf{D}| = 2^n$.

Our purpose is to show that the number of rank n *orthogonal* DHOs is not bounded above by any polynomial in 2^n; these DHOs occur in orthogonal spaces $V^+(2n, 2)$

U. Dempwolff
Department of Mathematics, Universität Kaiserslautern, 67653 Kaiserslautern, Germany
e-mail: dempwolff@mathematik.uni-kl.de

W. M. Kantor (✉)
Department of Mathematics, University of Oregon, Eugene, OR 97403, USA
e-mail: kantor@uoregon.edu

W. M. Kantor
College of Computer and Information Science, Northeastern University, Boston, MA 02115, USA

and all members are totally singular. Our DHOs will have a further property: they *split over a totally singular space* Y, meaning that $V = X \oplus Y$ for each DHO member X. For more concerning the number of inequivalent DHOs of rank n, see Sect. 8b.

Our source for such orthogonal DHOs in $V^+(2n, 2)$ is *orthogonal spreads* in $V^+(2n + 2, 2)$: sets $\mathbf{O}$ of totally singular $(n + 1)$-spaces such that each nonzero singular vector is in exactly one of them. Such orthogonal spreads exist if and only if n is odd. We use these for the following elementary result that is the basis for this paper:

Theorem 1.1 *Let* $\mathbf{O}$ *be an orthogonal spread in* $V^+(2n + 2, 2)$*. Let* P *be a point of* $Y \in \mathbf{O}$*, so that* $V := P^\perp/P \simeq V^+(2n, 2)$*. Then*

$$\mathbf{O}/P := \left\{\langle X \cap P^\perp, P\rangle/P \mid X \in \mathbf{O} - \{Y\}\right\}$$

is an orthogonal DHO *in* V *that splits over* Y/P*.*

Although we will show that many orthogonal DHOs can be obtained from orthogonal spreads with the help of Theorem 1.1, there are orthogonal DHOs that cannot be obtained by this method (see Sect. 8a).

Except in Sect. 7, q will always denote a power of 2 and almost always n will be odd. Our construction involves the close connection between orthogonal spreads in $V^+(2n+2, q)$ and symplectic spreads in $V(2n, q)$. Recall that a spread of n-spaces in $V = V(2n, q)$ is a set of $q^n + 1$ subspaces such that each nonzero vector is in exactly one of them; this determines an affine plane [7, p. 133]. A spread is called *symplectic* if there is a nondegenerate alternating bilinear form on V such that all members of the spread are totally isotropic. Any symplectic spread in $V(2n, q)$ can be lifted to an essentially unique orthogonal spread in $V^+(2n + 2, q)$; conversely, any orthogonal spread in $V^+(2n + 2, q)$ can be projected (in many ways, corresponding to arbitrary nonsingular points) in order to obtain symplectic spreads [13, Sec. 3], [19, Thm. 2.13] (cf. Definition 2.3 below). Theorem 1.1 produces many DHOs. There is at present no determination of the number of inequivalent orthogonal spreads, and the same is true for DHOs.

There is a simplified (and restricted) version of this process that does not take a detour using orthogonal spreads of higher-dimensional spaces. Given a symplectic spread $\mathbf{S}$ and distinct $X, Y \in \mathbf{S}$ it is standard to introduce "coordinates": a *spread-set* Σ for $\mathbf{S}$ (this is a set of self-adjoint linear operators). These coordinates can be distorted in a unique way to a set Δ_Σ of coordinates of an orthogonal DHO (this is a set of skew-symmetric operators; see Theorem 3.12), which we call a *shadow* of $\mathbf{S}$. In some situations, there are natural choices for X or Y. For example, if $\mathbf{S}$ defines a semifield plane, then we let Y be the shears axis; the semifield spreads in [19] produce the following

Theorem 1.2 *For odd composite* n *there are more than* $2^{n(\rho(n)-2)}/n^2$ *pairwise inequivalent orthogonal* DHO*s in* $V^+(2n, 2)$ *that are shadows of symplectic semifield spreads.*

Here $\rho(n)$ denotes the number of (not necessarily distinct) prime factors of the integer n. *The number in the theorem is not bounded above by any polynomial in*

2^n. The proof uses a somewhat general isomorphism result (Theorem 4.5) for DHOs arising from Theorem 1.1.

We also consider the symplectic spreads $\mathbf{S}$ of the nearly flag-transitive planes in [20]. Here, the automorphism group of $\mathbf{S}$ contains a normal cyclic group fixing precisely two members of $\mathbf{S}$ and acting regularly on the remaining ones, which leads to the following

Theorem 1.3 *For odd composite $n > 27$ there are more than $2^{3^{\rho(n)-1}}$ pairwise inequivalent orthogonal* DHO*s in $V^+(2n, 2)$ admitting a cyclic group of order $2^n - 1$ that fixes one member of the* DHO *and acts regularly on the remaining ones.*

This time, the number of DHOs is less than 2^n. We emphasize that there are many DHOs constructed using Theorem 1.1 not considered in the preceding two theorems (see Example 8.1).

In Sect. 7, we discuss a generalization of all of these results to the more general context of qDHOs.

The authors of this paper view spreads and DHOs in somewhat different manners: the first author prefers to think in terms of sets of operators [8,10], while the second prefers sets of subspaces and (often) quasifields [13,16,17,19,20]. We have mostly used the first approach (Theorem 1.1 being the main exception), and have tried to provide translations between the two points of view (Remarks 3.7, 3.10 and 3.13, Example 3.11 and Theorem 3.16).

2 Orthogonal DHOs and Theorem 1.1

All fields will have characteristic 2 except in Sect. 7. Theorem 1.1 is sufficiently elementary that almost no background is needed:

Proof of Theorem 1.1 It is standard that $V = P^\perp/P$ is an orthogonal space of type $V^+(2n, 2)$ and that each totally singular subspace X of $P^\perp$ has a totally singular image $\overline{X}$ in V. In particular, all members of $\mathbf{O}/P$ are totally singular of dimension n. Since $|\mathbf{O}/P| = 2^n$ it suffices to show that any two members of $\mathbf{O}/P$ intersect in a point and any three intersect trivially.

Let $X_1, X_2, X_3 \in \mathbf{O} - \{Y\}$ be distinct. Then $\overline{X}_i = \langle X_i \cap P^\perp, P\rangle/P$ and $\overline{Y} = Y/P$. Let $P = \langle w\rangle$.

Since $(X_1 \cap P^\perp) \cap (X_2 \cap P^\perp) = 0$ we have $\dim \overline{X}_1 \cap \overline{X}_2 \le 1$. On the other hand, $w = x_1 + x_2$ for some $0 \ne x_i \in X_i$. All vectors in the 2-space $\{0, w, x_1, x_2\}$ are singular, so this is a totally singular 2-space. Hence $x_i \in X_i \cap P^\perp$ and $\overline{X}_1 \cap \overline{X}_2 = \langle x_1, w\rangle/P = \langle x_2, w\rangle/P$ have dimension 1, as required.

Similarly, $\overline{X}_1 \cap \overline{X}_3 = \langle x_3, w\rangle/P$ with $w = x_1' + x_3$, $0 \ne x_1' \in X_1$, $0 \ne x_3 \in X_3$.

If $\overline{X}_1 \cap \overline{X}_2 \cap \overline{X}_3 \ne 0$ then $\overline{X}_1 \cap \overline{X}_2 = \overline{X}_1 \cap \overline{X}_3$, so that $\{0, w, x_1, x_2\} = \langle x_1, w\rangle = \langle x_1', w\rangle = \{0, w, x_1', x_3\}$ (our field is $\mathbb{F}_2$!). This is impossible, since $0 \ne x_2 \in X_2$, whereas X_2 intersects Y, X_1 and X_3 only in 0. Thus, $\mathbf{O}/P$ is a DHO.

Finally, if $x + P = y + P$ lies in $\overline{X_1} \cap \overline{Y}$ ($x \in X_1, y \in Y$), then $x \in X_1 \cap (y + P) \subseteq X_1 \cap Y = 0$, so that $\mathbf{O}/P$ splits over $\overline{Y}$. □

Definition 2.1 The DHO $\mathbf{O}/P$ in Theorem 1.1 is the *projection of* $\mathbf{O}$ *with respect to* P. Note that $Y \in \mathbf{O}$ is determined by P.

The notions of equivalence and automorphisms of symplectic or orthogonal spreads, and of DHOs, are crucial for our results:

Definition 2.2 $T \in \Gamma\mathrm{L}(V)$ is an *equivalence* $\mathbf{E} \to \mathbf{E}'$ between sets $\mathbf{E}$ and $\mathbf{E}'$ of subspaces of a vector space V if T sends $\mathbf{E}$ onto $\mathbf{E}'$. The *automorphism group* $\mathrm{Aut}(\mathbf{E})$ *of* $\mathbf{E}$ is the group of equivalences from $\mathbf{E}$ to itself.

Clearly, in Theorem 1.1 points P in the same $\mathrm{Aut}(\mathbf{O})$-orbit produce isomorphic DHOs $\mathbf{O}/P$ and the stabilizer $\mathrm{Aut}(\mathbf{O})_P$ of P induces an automorphism group of $\mathbf{O}/P$.

Our goal is the construction of large numbers of inequivalent DHOs. For this purpose, we need to compare the construction in Theorem 1.1 to ones in [13, Sect. 3] and [19, Thm. 2.13] (cf. Sect. 3.2). First we recall another standard property of orthogonal spaces $V^+(2m, q)$ [28, Thm. 11.61]: the set of totally singular m-spaces is partitioned into two equivalence classes where totally singular m-spaces X, Y are equivalent if and only if $\dim X \cap Y \equiv m \pmod 2$.

Definition 2.3 *(Lifts and projections of symplectic and orthogonal spreads)* Assume that n is odd. Let N be a nonsingular point of $\overline{V} = V^+(2n+2, q)$, so that $V := N^\perp/N \simeq V(2n, q)$ is a symplectic space. If $\mathbf{S}$ is a symplectic spread in V and $\mathcal{M}$ is one of the two classes of totally singular $(n+1)$-spaces in $\overline{V}$, then (since $n+1$ is even)

$$\{X \in \mathcal{M} \mid \langle X \cap N^\perp, N\rangle/N \in \mathbf{S}\}$$

is an orthogonal spread in $\overline{V}$, the *lift* of $\mathbf{S}$. (Changing $\mathcal{M}$ produces an equivalent orthogonal spread.)

This reverses: if $\mathbf{O}$ is an orthogonal spread in $V^+(2n+2, q)$, then

$$\mathbf{O}/N := \left\{\langle X \cap N^\perp, N\rangle/N \mid X \in \mathbf{O}\right\}$$

is a symplectic spread in V, the *projection* of $\mathbf{S}$ with respect to N. This strongly resembles Definition 2.1. As before, points N in the same $\mathrm{Aut}(\mathbf{O})$-orbit produce isomorphic spreads $\mathbf{O}/N$.

Proposition 2.4 *Let* $\mathbf{D}$ *be an orthogonal* DHO *of* $V = V^+(2n, 2)$. *Then*

(a) *n is odd, and*
(b) *If* $\mathbf{D}$ *splits over a totally singular subspace* Y, *then* $\bigcup_{X\in\mathbf{D}} X \cup Y$ *is the set of singular vectors in* V. *In particular,* Y *is the only totally singular subspace over which* $\mathbf{D}$ *splits.*

Proof (a) If X_1, X_2, X_3 are distinct members of $\mathbf{D}$, then any two have intersection of dimension 1. If n is even, then any two lie in different classes of totally singular n-spaces, whereas there are only two such classes.

(b) The set S_V of singular vectors of V has size $2^{2n-1}+2^n$. By Inclusion–Exclusion, $|\bigcup_{X\in\mathbf{D}} X| = 2^{2n-1}+1$. Thus, if $\mathbf{D}$ splits over the totally singular subspace Y then $Y-0=S_V-\bigcup_{X\in\mathbf{D}} X$. □

Remark 2.5 We will exclusively deal with orthogonal DHO*s that split over totally singular subspaces.* However, there are orthogonal DHOs (see [8, Prop. 5.4]) that split over subspaces that are not totally singular, but do not split over any totally singular subspace.

Any linear operator preserving an orthogonal DHO lies in the orthogonal group:

Proposition 2.6 *Let* $\mathbf{D}$ *and* $\mathbf{D}'$ *be orthogonal* DHO*s of* $V=V^+(2n,2)$ *that split over the totally singular subspace* Y*. If* $\Phi\in\mathrm{GL}(V)$ *sends* $\mathbf{D}$ *to* $\mathbf{D}'$*, then* Φ *lies in the stabilizer of* Y *in the orthogonal group* $\mathrm{O}(V)$.

Proof By Proposition 2.4b, $S_V=\bigcup_{X\in\mathbf{D}} X\cup Y$ is the set of all singular vectors in V. Every 3-dimensional subspace that has exactly six points in S_V not in Y is totally singular and hence has a seventh point in Y. Since every point of Y arises this way, Φ leaves S_V and Y invariant. □

Corollary 2.7 *Let* $\mathbf{D}$ *be an orthogonal* DHO *of* $V=V^+(2n,2)$ *that splits over the totally singular subspace* Y*. Then,* Y *is invariant under* $G=\mathrm{Aut}(\mathbf{D})$*, and the representation of* G *induced on* V/Y *is contragredient to the representation of* G *induced on* Y.

Proof The preceding proposition implies the first assertion. Since $Y=Y^\perp$, the bilinear form associated with the quadratic form induces a G-invariant duality from Y onto V/Y, which implies the second assertion. □

3 Coordinates and symplectic spread-sets

In this section, we use coordinates of orthogonal and symplectic spreads in order to describe operations that do not require projections from higher-dimensional orthogonal spreads. Throughout the remainder of this paper we will always have

$$U=V(n,q)\ \text{ and }\ V\cong U\oplus U,$$

where q is even except in Sect. 7. If U is equipped with a nondegenerate symmetric bilinear form $\mathsf{b}(\cdot,\cdot)$ we denote by $T^\star$ the operator adjoint to $T\in\mathrm{End}(U)$.

3.1 Coordinates for symplectic spreads, orthogonal spreads and orthogonal DHOs

Assume that V is a symplectic space, and denote by $\mathbf{E}$ either a symplectic spread, an orthogonal spread, or an orthogonal DHO in V that splits over a totally singular subspace. The symplectic form $(\cdot,\cdot)$ on V vanishes on all members of $\mathbf{E}$. For an orthogonal spread or DHO, all members of $\mathbf{E}$ are totally singular with respect to a quadratic form Q polarizing to $(\cdot,\cdot)$. For a DHO we always assume that $q=2$.

In order to coordinatize $\mathbf{E}$ we choose any distinct $X, Y \in \mathbf{E}$ if $\mathbf{E}$ is a symplectic or orthogonal spread. If $\mathbf{E}$ is a DHO that splits over a totally singular subspace Y then choose $X \in \mathbf{E}$.

We identify V with $U \oplus U$. We may assume that

$$X = U \oplus 0 \text{ and } Y = 0 \oplus U,$$

the symplectic form on $U \oplus U$ is

$$\big((x, y), (x', y')\big) = \mathsf{b}(x, y') + \mathsf{b}(y, x'), \tag{3.1}$$

and the quadratic form is

$$Q\big((x, y)\big) = \mathsf{b}(x, y). \tag{3.2}$$

For $Z \in \mathbf{E} - \{Y\}$ there is a unique $L \in \mathrm{End}(U)$ such that $Z = V(L)$, where

$$V(L) := \{(x, xL) \mid x \in U\}. \tag{3.3}$$

Each L is self-adjoint with respect to b if $\mathbf{E}$ is a symplectic spread (as Z is totally isotropic), and L is even skew-symmetric (i.e., $\mathsf{b}(x, xL) = 0$ for all x) if $\mathbf{E}$ is an orthogonal spread or a DHO (as Z is totally singular). The subspace $Z = X$ corresponds to $L = 0$. If $Z \neq X$ then L is invertible if $\mathbf{E}$ is a symplectic or orthogonal spread, while L has rank $n - 1$ in the DHO case. Hence, there is a set $\Xi \subseteq \mathrm{End}(U)$ containing 0 such that

$$\mathbf{E} = \{V(L) \mid L \in \Xi\} \cup \{Y\}$$

if $\mathbf{E}$ is a symplectic or orthogonal spread and

$$\mathbf{E} = \{V(L) \mid L \in \Xi\}$$

if $\mathbf{E}$ is an orthogonal DHO that splits over the totally singular subspace $Y = 0 \oplus U$.

Definition 3.1 Let $V = U \oplus U$, $\mathbf{E}$, X and Y be as above.

- If $\mathbf{E}$ is a symplectic spread, then Ξ is a (symplectic) *spread-set of* $\mathbf{E}$ *with respect to the ordered pair* (X, Y).
- If $\mathbf{E}$ is an orthogonal spread, then Ξ is a *Kerdock set of* $\mathbf{E}$ *with respect to the ordered pair* (X, Y) (cf. [13]).
- If $\mathbf{E}$ is an orthogonal DHO then Ξ is a DHO-*set of* $\mathbf{E}$ *with respect to* X. (Note that there is no choice for Y, the space over which $\mathbf{E}$ splits.)

Conversely, it is routine to check the following:

Lemma 3.2 *Assume that* $\Xi \subseteq \mathrm{End}(U)$ *is a set of self-adjoint operators containing* 0. *Define symplectic and quadratic forms on* $V = U \oplus U$ *using* (3.1) *and* (3.2).

(a) If $|\Xi| = q^n$ *and* $\det(L + L') \neq 0$ *for all distinct* $L, L' \in \Xi$, *then* $\mathbf{E} = \{V(L) \mid L \in \Xi\} \cup \{0 \oplus U\}$ *is a symplectic spread of* V.

(b) *If* $|\Xi| = q^{n-1}$, $\det(L + L') \neq 0$ *for all distinct* $L, L' \in \Xi$, *and all members of* Ξ *are skew-symmetric, then* $\mathbf{E} = \{V(L) \mid L \in \Xi\} \cup \{0 \oplus U\}$ *is an orthogonal spread of* V.

(c) *Assume that* $|\Xi| = 2^n$ *with n odd, that all members of* Ξ *are skew-symmetric, and that*
(1) $\mathrm{rk}(L + L') = n - 1$ *for all distinct* $L, L' \in \Xi$, *and*
(2) *if* $L \in \Xi$ *then* $\{\ker(L + L') \mid L' \in \Xi - \{L\}\}$ *is the set of* 1*-spaces of* U.
Then $\mathbf{E} = \{V(L) \mid L \in \Xi\}$ *is an orthogonal* DHO *that splits over* $0 \oplus U$.

Remark 3.3 Let $\mathsf{b}(x, y) = x \cdot y$ be the usual dot product and identify $\mathrm{End}(U)$ with the space of all $n \times n$ matrices over $\mathbb{F}_q$. Then $L \in \mathrm{End}(U)$ is self-adjoint if and only if $L = L^t$, and L is skew-symmetric if and only if, in addition, its diagonal is 0.

A variation is used in Sects. 4 and 5: identify U with $F = \mathbb{F}_{q^n}$ and use the trace form

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

where $\mathrm{Tr}\colon F \to \mathbb{F}_q$ is the trace map.

Rank 1 operators will play a crucial role for our results. The following elementary description of those operators is also in [21, Prop. 5.1].

Lemma 3.4 *If* $T \in \mathrm{End}(U)$ *has rank* 1, *then* $T = E_{a,b}$ *for some* $0 \neq a, b \in U$, *where*

$$xE_{a,b} := \mathsf{b}(x, a)b \ \ \text{for all} \ \ x \in U. \tag{3.4}$$

If $E_{a,b} = E_{a',b'}$ *for nonzero* a, a', b, b', *then* $a' = ka$ *and* $b' = k^{-1}b$ *for some* $k \in \mathbb{F}_q^{\star}$.

Proof Write $U_0 = \ker T = \langle a\rangle^{\perp}$ with $a \in U$. Let $v \in U - U_0$ such that $\mathsf{b}(v, a) = 1$. Then $b := vT \neq 0$. Thus, $0 = uT = uE_{a,b}$ for $u \in U_0$ and $vT = b = vE_{a,b}$, so that $T = E_{a,b}$.

If $E_{a,b} = E_{a',b'}$ then $\langle a\rangle = \langle a'\rangle$ and $\langle b\rangle = \langle b'\rangle$, and a calculation completes the proof. □

Remark 3.5 Since $\mathsf{b}(x, yE_{a,b}) = \mathsf{b}(xE_{b,a}, y)$, the operator $E_{b,a}$ is adjoint to $E_{a,b}$, so that $E_{a,b}$ is self-adjoint if and only if $\langle a\rangle = \langle b\rangle$. In this case, there is a (uniquely determined) $c \in \langle a\rangle = \langle b\rangle$ such that $E_{a,b} = E_{c,c}$.

In terms of matrices, the lemma is the elementary fact that rank 1 matrices have the form $a^t b$ for nonzero row vectors a, b. This matrix is symmetric if and only if $\langle a\rangle = \langle b\rangle$.

Lemma 3.6 *For each self-adjoint operator* T *there is a unique self-adjoint operator* $R = E_{a,a}$ *of rank* ≤ 1 *such that* $T + R$ *is skew-symmetric. Moreover,*

(a) $a \in \mathrm{Im}\, T$;

(b) $\mathrm{rk}\,(T + R) = \begin{cases} \mathrm{rk}\, T & \text{if } \mathrm{rk}\, T \equiv 0 \pmod 2 \\ \mathrm{rk}\, T \pm 1 & \text{if } \mathrm{rk}\, T \equiv 1 \pmod 2; \end{cases}$

(c) *if* S *is self-adjoint and* $S + E_{b,b}$ *is skew-symmetric, then* $R' = E_{a+b,a+b}$ *is the unique self-adjoint operator of rank* ≤ 1 *such that* $T + S + R'$ *is skew-symmetric*; *and*

(d) *if n is odd and T is invertible, then* $\ker(T+E_{a,a}) = \langle aT^{-1}\rangle$ *and* $\mathsf{b}(a, aT^{-1}) \neq 0$.

Proof As T is self-adjoint, the map $\lambda_T : U \to \mathbb{F}_q$ given by $x \mapsto \mathsf{b}(x, xT)$ is semilinear: $\lambda_T(kx) = k^2\lambda_T(x)$ for $x \in U$, $k \in \mathbb{F}_q$. If $\lambda_T = 0$ then T is skew-symmetric and we set $R = 0 = E_{0,0}$. Assume that $\lambda_T \neq 0$ and set $U_0 = \ker\lambda_T$. Pick $u \in U$ such that $\lambda_T(u) = 1$ and $a \in U$ such that $U_0 = \langle a\rangle^{\perp}$ and $\mathsf{b}(u, a) = 1$. Then $S = T + E_{a,a}$ is self-adjoint. Moreover $\lambda_S(x) = \lambda_T(x) + \mathsf{b}(x, a)^2$ is 0 on both U_0 and u, so that S is skew-symmetric. In particular,

$$\lambda_T(x) = \mathsf{b}(x, a)^2 \text{ for all } x \in U. \tag{3.5}$$

As b is nondegenerate, every semilinear functional from U to $\mathbb{F}_q$ associated with the Frobenius automorphism has the form $x \mapsto \mathsf{b}(x, a)^2$ for a unique $a \in U$. This implies the uniqueness of $R = E_{a,a}$.

(a) Let $T + E_{a,a}$ be skew-symmetric and assume that $a \notin \operatorname{Im} T = (\operatorname{Im} T)^{\perp\perp}$. Then $\mathsf{b}(a, (\operatorname{Im} T^{\perp})) \neq \{0\}$, so that there exists $y \in (\operatorname{Im} T)^{\perp}$ with $1 = \mathsf{b}(a, y)$. Since y and yT are perpendicular, (3.5) implies that $1 = \mathsf{b}(a, y)^2 = \mathsf{b}(y, yT) = 0$, a contradiction.
(b) Clearly $\operatorname{rk}(T + R) \equiv 0 \pmod 2$.
(c) $(T + S) + E_{a+b,a+b} = (T + E_{a,a}) + (S + E_{b,b}) + (E_{a,b} + E_{b,a})$ expresses the left-hand side as a sum of skew-symmetric operators.
(d) By (b), $\dim\ker(T + E_{a,a}) = 1$. Let $0 \neq x \in \ker T + E_{a,a}$. By (3.4), $0 = xT + \mathsf{b}(a, x)a$ and hence $x = \mathsf{b}(a, x)aT^{-1}$, so that $0 \neq x \in \langle aT^{-1}\rangle$ and $\mathsf{b}(a, x) \neq 0$. □

Remark 3.7 In terms of matrices the first paragraph of the lemma states that, if A is a symmetric matrix, then $A + d(A)^t d(A)$ is skew-symmetric, where $d(A)$ is the diagonal of A written as a row vector as in [2, Lemma 7.3].

Lemma 3.8 *For a symplectic spread-set Σ of $U = V(n, q)$ with n odd,*

(a) *There is a unique bijection $C : U \to \Sigma$ such that $C(a) + E_{a,a}$ is skew-symmetric for all $a \in U$, and*
(b) *C is additive iff Σ is additively closed.*

Proof (a) If $0 \neq L \in \Sigma$ then the self-adjoint, invertible operator L is not skew-symmetric as n is odd. By the preceding lemma, there is a unique nonzero vector $a = a_L \in U$ such that $L+E_{a,a}$ is skew-symmetric of rank $n-1$. If $0 \neq L, L' \in \Sigma$, $L \neq L'$, then $a_L \neq a_{L'}$ as $L + L'$ is invertible and hence not skew-symmetric, so that C is bijective.
(b) Since one direction is obvious, assume that Σ is additively closed. If $a, b \in U$, then $C(a) + C(b) = C(c)$ for some $c \in U$. By definition $C(c) + E_{c,c}$ is skew-symmetric, and so is $C(a)+C(b)+E_{a+b,a+b} = C(c)+E_{a+b,a+b}$ by Lemma 3.6c. Then $c = a + b$ by Lemma 3.6, as required. □

Definition 3.9 *(Canonical labeling)* The unique bijection $C : U \to \Sigma$ in Lemma 3.8 is the *canonical labeling* of the symplectic spread-set Σ of operators of U. Notation: $C = \mathscr{L}(\Sigma)$.

Remark 3.10 Each symplectic spread-set $\Sigma \subseteq \mathrm{End}(U)$ determines a prequasifield on U defined by $x * a = xC(a)$ for any additive bijection $C: U \to \Sigma$. Then C is the canonical labeling if and only if

$$\mathsf{b}(x, x * a) = \mathsf{b}(x, xC(a)) = \mathsf{b}(x, xE_{a,a}) = \mathsf{b}(x, a)^2$$

by (3.4). This is the condition on a prequasifield appearing in [19, (2.15)].

3.2 Projections and lifts with coordinates

We next coordinatize projections and lifts (Definitions 2.1 and 2.3). We review [13,16, 19] using somewhat different notations. We will assume for the remainder of Sect. 3 that *n is odd.*

(a) FROM KERDOCK SETS TO SYMPLECTIC SPREAD- SETS. Let $\mathbf{O}$ be an orthogonal spread in $\overline{V} = V^+(2n+2, q)$, let N be a nonsingular point, and choose an ordered pair $X, Y \in \mathbf{O}$. The identification
- $\overline{V} = \overline{U} \oplus \overline{U}$ where $\overline{U} = V(n+1, q)$,
- $X = \overline{U} \oplus 0,\ Y = 0 \oplus \overline{U}$,

produces a Kerdock set $\mathbb{K}$ such that each member of $\mathbf{O} - \{Y\}$ has the form $V(L) = \{(x, xL) \mid x \in \overline{U}\}$, $L \in \mathbb{K}$. Moreover, this identification induces a symmetric, nondegenerate bilinear form $\overline{\mathsf{b}}(\cdot, \cdot)$ on $\overline{U}$ such that the quadratic form Q is defined by $Q\big((x, y)\big) = \overline{\mathsf{b}}(x, y)$. Given this Kerdock set, we make the special choice

$$N = \langle (w, w) \rangle \ \text{ with } \ \overline{\mathsf{b}}(w, w) = 1.$$

Then (x, xL) lies in $N^\perp$ if and only if $\overline{\mathsf{b}}(w, x) = \overline{\mathsf{b}}(w, xL)$. Set $U = \langle w \rangle^\perp$ and write $x \in \overline{U}$ as $x = \alpha w + u$, $\alpha \in \mathbb{F}_q$, $u \in U$. As L is skew-symmetric, $wL \in U$ and

$$\alpha = \overline{\mathsf{b}}(w, x) = \overline{\mathsf{b}}(w, xL) = \overline{\mathsf{b}}(wL, u).$$

Also,

$$uL = uL\pi_U + \overline{\mathsf{b}}(wL, u)w,$$

where π_U is the orthogonal projection $\overline{U} \to U$. Since $U \oplus U$ is a set of representatives for $N^\perp/N$ and as $(x, xL) = (\overline{\mathsf{b}}(wL, u)w + u, \overline{\mathsf{b}}(wL, u)w + \overline{\mathsf{b}}(wL, u)wL + uL\pi_U) \equiv (u, \overline{\mathsf{b}}(wL, u)wL + uL\pi_U) \pmod N$,

$$\{L\pi_U + E_{wL,wL} \mid L \in \mathbb{K}\} \text{ is a spread-set of the symplectic spread } \mathbf{O}/N.$$

(b) FROM KERDOCK SETS TO DHO- SETS. We keep the notation from (a) using $q = 2$. We use $X \in \mathbf{O} - \{Y\}$ and the singular point $P = \langle (0, w) \rangle \subseteq Y$. We use the above identifications for $\overline{V}$, X, Y, and Q. A typical element in $V(L) \cap P^\perp$

has the form $(u, uL) = (u, uL\pi_U + \mathsf{b}(wL, u)w) \equiv (u, uL\pi_U) \pmod P$, $u \in U$. As $U \oplus U \simeq P^\perp/P$, we see that

$$\{L\pi_U \mid L \in \mathbb{K}\} \text{ is a DHO-set of the orthogonal DHO } \mathbf{O}/P.$$

(c) From symplectic spread-sets to Kerdock sets. Let $\mathbf{S}$ be a symplectic spread on $V = V(2n, q)$, and let $X, Y \in \mathbf{S}$. This time we identify
- $V = U \oplus U$, $U = V(n, q)$,
- $X = U \oplus 0$, $Y = 0 \oplus U$, and
- The bilinear form is $\big((x, y), (x', y')\big) = \mathsf{b}(x, y') + \mathsf{b}(y, x')$ for a nondegenerate symmetric bilinear form b on U.

Let $\Sigma \subseteq \mathrm{End}(U)$ be the resulting spread-set and $C = \mathscr{L}(\Sigma)$ (cf. Definition 3.9). Set $\overline{U} = \mathbb{F}_q \oplus U$ and $\overline{V} = \overline{U} \oplus \overline{U}$, and define a quadratic form Q on $\overline{V}$ by

$$Q(\alpha, x, \beta, y) = \alpha\beta + \mathsf{b}(x, y).$$

For $a \in U$ define the skew-symmetric linear operator $D(a)$ on $\overline{U}$ by

$$(\alpha, x)D(a) = \big(\mathsf{b}(x, a), \alpha a + x(C(a) + E_{a,a})\big).$$

Then $\mathbb{K} = \{D(a) \mid a \in U\}$ is a Kerdock set of the lift $\mathbf{O}$, where $\mathbf{O}/N \simeq \mathbf{S}$ for the choice $N = \langle(1, 0, 1, 0)\rangle$.

Example 3.11 We illustrate the above discussion using matrices, as in [2, Lemma 7.3]. Let $\overline{U} = \mathbb{F}_q^{n+1}$ and $\overline{V} = \overline{U} \oplus \overline{U}$, equipped with the quadratic form $Q(x, y) = x \cdot y$. We will use the nonsingular point $N = \langle(e_1, e_1)\rangle$ and the singular point $P = \langle(0, e_1)\rangle$ (where the e_i are the standard basis vectors of $\overline{U}$). Then the bilinear form b is the usual dot product on $U := \langle e_2, \ldots, e_{n+1}\rangle$.

Let $\mathbf{O}$ be an orthogonal spread containing X and Y (defined above). Then a Kerdock set can be written $\mathbb{K} = \{D(u) \mid u \in U\}$ using $(n+1)\times(n+1)$ skew-symmetric matrices

$$D(u) = \begin{pmatrix} 0 & x(u) \\ x(u)^t & A(u) \end{pmatrix},$$

where $A(u)$ is an $n \times n$ skew-symmetric matrix and $x(u) \in U$ is a row matrix. Then

$$\Delta := \{A(u) \mid u \in U\} \tag{3.6}$$

is a DHO-set of $\mathbf{O}/P$, while

$$\Sigma := \{A(u) + x(u)^t x(u) \mid u \in U\},$$

is a spread-set of the symplectic spread $\mathbf{O}/N$, where $x(u)^t x(u)$ represents the previous rank 1 operator $E_{wL,wL}$ in (a).

3.3 Shadows, twists and dilations

Theorem 3.12 *Let Σ be a spread-set of self-adjoint operators of $U = V(n, 2)$ and $C = \mathscr{L}(\Sigma)$. Then $\Delta = \Delta_\Sigma = \{B(a) = C(a) + E_{a,a} \mid a \in U\}$ is a* DHO*-set of skew-symmetric operators.*

Proof We sketch two different arguments.

GEOMETRIC APPROACH. Start with a symplectic spread-set Σ and $C = \mathscr{L}(\Sigma)$, and produce a Kerdock set $\mathbb{K}$ using Sect. 3.2c. Then apply Sect. 3.2b to $\mathbb{K}$ using the singular point $P = \langle(0, 0, 1, 0)\rangle$.

ALGEBRAIC APPROACH. We will verify the conditions in Lemma 3.2c. Consider distinct $a, b, c \in U$. Then skew-symmetric operator $B(a) + B(b) = C(a) + C(b) + E_{a,a} + E_{b,b}$ has even rank at least $n - 2$, and hence has rank $n - 1$.

Let $x \neq 0$ with $x(B(a) + B(b)) = x(B(a) + B(c)) = 0$. Then $0 \neq x(C(a) + C(b)) = \mathsf{b}(a, x)a + \mathsf{b}(b, x)b$, so that $\mathsf{b}(a, x)$ or $\mathsf{b}(b, x) \neq 0$. We cannot have $\mathsf{b}(a, x) = \mathsf{b}(b, x) = 1$, as otherwise $\mathsf{b}(a + b, x) = 0$ would contradict Lemma 3.6d (since $C(a) + C(b) + E_{a+b,a+b}$ is skew-symmetric by Lemma 3.6c).

Then $\mathsf{b}(a, x) \neq \mathsf{b}(b, x)$. By symmetry, it follows that $\mathsf{b}(a, x)$, $\mathsf{b}(b, x)$, and $\mathsf{b}(c, x)$ are distinct members of $\mathbb{F}_2$, a contradiction. □

Remark 3.13 (Constructing DHO*-sets using orthogonal spreads)* Example 3.11 contains the construction of the above set of operators using [2, (7.4)] in terms of matrices (compare Remark 3.7). However, the preceding theorem shows that we can proceed directly from spread-sets to the required DHO-sets.

The examples studied in Sects. 4 and 5 are obtained by taking known orthogonal spreads with “nice” descriptions in terms of matrices or linear operators and peeling off the set Δ in (3.6). Of course, there is a bias here: orthogonal spreads having nice descriptions will have less nice descriptions using arbitrary choices of its members X, Y (as we will see in Example 8.1 below).

Definition 3.14 *(Shadows)* Let Σ be a spread-set of self-adjoint operators of U coordinatizing the symplectic spread $\mathbf{S}$ of $V = V(2n, 2)$ with respect to the pair (X, Y). Let Q be the unique quadratic form on V polarizing to the given symplectic form such that X and Y are totally singular. The DHO-set $\Delta = \Delta_\Sigma$ associated to Σ in Proposition 3.12 will be called the *shadow of* Σ; it is uniquely determined by the spread-set. We also call the orthogonal DHO on (V, Q) defined by Δ a *shadow* of the spread $\mathbf{S}$. (Recall that this is not uniquely determined: we choose X and Y in order to obtain the spread-set Σ from the spread $\mathbf{S}$. Also see Sect. 3.4.)

Example 3.15 Consider $F = \mathbb{F}_{2^n}$ as an $\mathbb{F}_2$-space equipped with the absolute trace form Tr as a nondegenerate symmetric form. Define the $\mathbb{F}_2$-linear map $C(a)$, $a \in F$, by

$$xC(a) = a^2x.$$

Then C is the canonical labeling (Definition 3.9) of a symplectic spread-set that coordinatizes the desarguesian plane. The operators

$$xB(a) = a^2x + \mathrm{Tr}(xa)a$$

define the shadow $\Delta = \{B(a) \mid a \in F\}$ of Σ. In particular $xE_{a,a} = \mathrm{Tr}(xa)a$. The automorphism group of the corresponding DHO is isomorphic to $F^{\star} \cdot \mathrm{Aut}(F)$ by Lemma 5.6 below.

Our later Examples 4.2 and 5.1 are generalizations of this one. We close this section with a result obtaining new symplectic spreads from known ones.

Theorem 3.16 *Let Σ be a spread-set of self-adjoint operators of $U = V(n, q)$, and let $C = \mathscr{L}(\Sigma)$.*

(a) If $u \in U$, define $C_u : U \to \mathrm{End}(U)$ by

$$C_u(a) := C(a) + E_{a,u} + E_{u,a}.$$

Then $\Sigma_u := \{C_u(a) \mid a \in U\}$ is a spread-set of self-adjoint operators and $C_u = \mathscr{L}(\Sigma_u)$. Moreover, Σ_u is additively closed if Σ is.

(b) Pick $1 \neq \lambda \in \mathbb{F}_q$ and define $C^{\lambda} : U \to \mathrm{End}(U)$ by

$$C^{\lambda}(a) := C\big((1+\lambda)a\big) + E_{\lambda a,\lambda a}.$$

Then $\Sigma^{\lambda} = \{C^{\lambda}(a) \mid a \in U\}$ is a spread-set of self-adjoint operators and $C^{\lambda} = \mathscr{L}(\Sigma^{\lambda})$.

Proof This is a reformulation of special cases of [19, Lemma 2.18] using Lemma 3.6, (3.4) and Lemma 3.8b. (The easy, direct algebraic verification—similar to the proof of Theorem 3.12—is left to the reader.) □

Remark 3.17 In view of [19, Lemma 2.18], Σ, Σ_u, and Σ^{λ} are all projections of the same orthogonal spread (cf. Definition 2.3).

Definition 3.18 *(Twists and dilations)* Let Σ be a symplectic spread-set of $U = V(n, q)$, q even. For $u \in U$ and $1 \neq \lambda \in \mathbb{F}_q$ we call the spread-set Σ_u in Theorem 3.16a the *u-twist of* Σ, and the spread-set Σ^{λ} in Theorem 3.16b the *λ-dilation of* Σ.

Corollary 3.19 *In the notation of* Theorem 3.16a, *assume that $q = 2$, Σ is additively closed and $u \in U$. Let $\Delta = \{B(a) := C(a) + E_{a,a} \mid a \in U\}$ and $\Delta_u = \{B_u(a) := C_u(a) + E_{a,a} \mid a \in U\}$ be the shadows of Σ and Σ_u. Then $B_u(a) = B(a+u) + B(u)$.*

Proof By Definition 3.14 and Theorem 3.16,

$$\begin{aligned} B_u(a) &= C_u(a) + E_{a,a} \\ &= C(a) + E_{a,u} + E_{u,a} + E_{a,a} \\ &= C(a+u) + E_{a+u,a+u} + C(u) + E_{u,u} \\ &= B(a+u) + B(u). \end{aligned}$$

□

3.4 The projections $\mathbf{O}/N$ and $\mathbf{O}/P$

The term "shadow" of a symplectic spread suggests that, as in the physical world, the original object cannot be recovered from the shadow. We will see how this occurs in our context: the relationship between symplectic spreads and shadows is less tight than visible in the preceding section. This is illustrated by Example 3.21 below. We will see that non-isomorphic spread-sets can produce isomorphic shadows, a symplectic spread can have non-isomorphic shadows, and the automorphism groups of a symplectic spread and a shadow can be very different. These phenomena are best understood from the viewpoint of orthogonal spreads:

Proposition 3.20 *Let* $\mathbf{O}$ *be an orthogonal spread in* $\overline{V} = V^+(2n+2, 2)$. *Let* N *be a nonsingular point and* P *a singular point in* $\overline{V}$ *such that the* 2*-space* $\langle N, P\rangle$ *is hyperbolic. Then, the* DHO $\mathbf{O}/P$ *is a shadow of the symplectic spread* $\mathbf{O}/N$.

Proof We will use the notation in Sect. 3.2 for a suitable choice of coordinates. By assumption, $\langle N, P\rangle$ contains a singular point $P' \neq P$. We may assume that $P' = \langle (e_1, 0)\rangle$ and $P = \langle (0, e_1)\rangle$, so that $N = \langle (e_1, e_1)\rangle$. We may assume that the members of $\mathbf{O}$ containing P' and P are $X = \overline{U} \oplus 0$ and $Y = 0 \oplus \overline{U}$, respectively. According to Remark 3.13 (compare Example 3.11), $\mathbf{O}/P$ is a shadow of $\mathbf{O}/N$. □

Example 3.21 (a) When the usual desarguesian spread $\mathbf{S}$ of $V(2, q^n)$ (for q even and $n > 1$ odd) is viewed as a symplectic spread of $V(2n, q)$, it can be lifted to the *desarguesian orthogonal spread* $\mathbf{O}$ of $\overline{V} = V^+(2n+2, q)$ as in Definition 2.3. Then $\mathbf{O}/N_0 = \mathbf{S}$ for a nonsingular point N_0. The group $G = \mathrm{SL}(2, q^n) \cdot \mathrm{Aut}(\mathbb{F}_{q^n})$ preserves the point N_0, the orthogonal spread $\mathbf{O}$ and the orthogonal geometry of $\overline{V}$. It has exactly two orbits of singular points; the various orbits of nonsingular points N are described at length in [13, Sec. 4]. If $N \neq N_0$ then $\langle N^G\rangle$ is a G-invariant subspace $\neq 0$, N_0, and hence is $N_0^\perp$ or $\overline{V}$.
If P is a singular point, then $P^\perp \neq N_0^\perp$. Thus, P is not perpendicular to some member N' of N^G, in which case $\langle N', P\rangle$ is a hyperbolic 2-space.

(b) In particular, when $q = 2$, by the preceding proposition *each* $\mathbf{O}/P$ *is isomorphic to a shadow of each* $\mathbf{O}/N$, $N \neq N_0$, where there are many non-isomorphic symplectic spreads $\mathbf{O}/N$ [13, Cor. 3.6 and Sec. 4]. Also, $\mathbf{O}/P$ is a shadow of the desarguesian spread $\mathbf{O}/N_0 = \mathbf{S}$ when P is not in $N_0^\perp$.
If $q = 2$ and $n = 5$, then G has precisely three orbits of nonsingular points: $\{N_0\}$, N_1^G, and N_2^G, with $N_1^G \subseteq N_0^\perp$ and $N_2^G \cap N_0^\perp = \emptyset$. Here $\mathbf{O}/N_1$ is a semifield spread with $|\mathrm{Aut}(\mathbf{O}/N_1)| = 2^5 \cdot 5$, and $\mathbf{O}/N_2$ is a flag-transitive spread with $|\mathrm{Aut}(\mathbf{O}/N_2)| = 33 \cdot 5$. The two orbits of G on singular points are P_0^G (inside $N_0^\perp$) and P_1^G (with $P_1^G \cap N_0^\perp = \emptyset$). The DHO $\mathbf{O}/P_1$ appeared in Example 3.15, while $\mathbf{O}/P_0$ is one of the DHOs in Example 8.1. By Example 3.15, $\mathrm{Aut}(\mathbf{O}/P_1) = G_{P_1}$ has order $31 \cdot 5$, while G_{P_0} induces on the DHO $\mathbf{O}/P_0$ an automorphism group of order $2^5 \cdot 5$. Thus, $\mathbf{O}/P_0 \not\cong \mathbf{O}/P_1$. Use of a computer shows that $\mathrm{Aut}(\mathbf{O}/P_0) = G_{P_0}$.

4 Proof of Theorem 1.2

Except in Sect. 7, we will use $F = \mathbb{F}_{2^n}$ with $n > 1$ odd, viewed as an $\mathbb{F}_2$-space equipped with the nondegenerate, symmetric bilinear form $(x, y) \mapsto \mathrm{Tr}(xy)$ using the absolute trace $\mathrm{Tr}\colon F \to \mathbb{F}_2$ as in Remark 3.3.

Notation 4.1 We will use the following:

- The quadratic form Q on $V = F \oplus F$ defined by $Q(x, y) = \mathrm{Tr}(xy)$;
- The trace map $\mathrm{Tr}_{d:e}\colon \mathbb{F}_{2^d} \to \mathbb{F}_{2^e}$ when $\mathbb{F}_{2^d} \supset \mathbb{F}_{2^e}$, so that $\mathrm{Tr}_{n:1} = \mathrm{Tr}$;
- Sequences $\underline{d} = (d_0 = 1, d_1, \dots, d_m)$ of $|\underline{d}| = m + 1$ different integers such that $d_1|d_2|\cdots|d_m|n$, associated with a chain $\mathbb{F}_2 = F_0 \subset F_1 \subset \cdots \subset F_m \subset F$, $|F_i| = 2^{d_i}$, of $|\underline{d}|$ proper subfields of F;
- The F_i-linear operator
$$E^{(i)}_{a,b}\colon x \mapsto \mathrm{Tr}_{n:d_i}(ax)b \tag{4.1}$$
on F for $a, b \in F$ and $0 \le i \le m$; and
- Sequences $\underline{c} = (c_1, \dots, c_m)$, $c_i \in F$.

This section is concerned with the following symplectic semifield spread-sets:

Example 4.2 [19] Let $\underline{d}$ and $\underline{c}$ be as above with all $c_i \in F^\star$. For $a \in F$ define the operator $C(a)$ on F by

$$C(a) = a^2\mathbf{1} + \sum_{i=1}^{m}\left(E^{(i)}_{c_i,a} + E^{(i)}_{a,c_i}\right).$$

This defines a symplectic spread-set Σ. Moreover, $C = \mathscr{L}(\Sigma)$ by Example 3.15 since the operators $E^{(i)}_{c_i,a} + E^{(i)}_{a,c_i}$ are skew-symmetric. The shadow of Σ (Definition 3.14) is

$$\Delta = \{B(a) \mid a \in F\} \text{ with } B(a) = C(a) + E^{(0)}_{a,a}.$$

The DHO-set Δ defines an orthogonal DHO of V by

$$\mathbf{D} = \{V(a) \mid a \in F\} \text{ with } V(a) = V\big(B(a)\big) := \{\big(x, xB(a)\big) \mid a \in F\}.$$

Remark 4.3 (a) The preceding spread-set Σ is obtained by successively twisting the desarguesian spread-set $\Sigma_0 = \{a^2\mathbf{1} \mid a \in F\}$. Namely, view Σ_0 as a symplectic spread-set over F_m. Let $d = d_m$ and $c = c_m \in F^\star$. By Theorem 3.16 the twist $\Sigma_1 = \{a^2\mathbf{1} + E^{(m)}_{c,a} + E^{(m)}_{a,c} \mid a \in F\}$ is a symplectic spread-set over F_m. Now view Σ_1 as a spread-set over F_{m-1} and iterate the twisting using $c_{m-1} \in F^\star$.

(b) None of the nontrivial elations of the projective plane arising from the symplectic spread-set is inherited by the shadow DHO since $C(a + b) = C(a) + C(b)$ but $B(a+b) = C(a+b) + E^{(0)}_{a+b,a+b} \ne C(a) + E^{(0)}_{a,a} + C(b) + E^{(0)}_{b,b} = B(a) + B(b)$ for $0 \ne a, b, a \ne b$.

Our goal is to show that we obtain at least $2^{n(\rho(n)-2)}/n^2$ inequivalent orthogonal DHOs of the above type when n is composite. We start with a uniqueness result concerning shadows:

Proposition 4.4 *If $n > 5$, then a* DHO*-set $\Delta \subseteq \mathrm{End}(U)$ can be the shadow of at most one additively closed symplectic spread-set.*

Proof Let $\Delta = \{B(a) \mid a \in U\}$ be the shadow of the additively closed symplectic spread-sets Σ and $\widetilde{\Sigma}$. Write $\Sigma = \{C(a) := B(a) + E_{a,a} \mid a \in U\}$ with $C = \mathscr{L}(\Sigma)$ additive (by Lemma 3.8b). Then for each $B(a) \in \Delta$ there is a self-adjoint operator $E_{b,b}$ of rank ≤ 1 such that $\overline{C}(a) := B(a) + E_{b,b} \in \widetilde{\Sigma}$. Write $a' = b$. We have to show that $a' = a$ for all a. (N. B.–We do not know that $\overline{C} = \mathscr{L}(\widetilde{\Sigma})$.)

We claim that $\overline{C}$ is additive. Let $0 \neq a, b \in U$ and $\overline{C}(a) + \overline{C}(b) = \overline{C}(c)$ with $c \in U$. By the additivity of C and the definition of $\overline{C}$,

$$\begin{aligned} C(a+b+c) &= (B(a) + E_{a,a}) + (B(b) + E_{b,b}) + (B(c) + E_{c,c}) \\ &= E_{a',a'} + E_{b',b'} + E_{c',c'} + E_{a,a} + E_{b,b} + E_{c,c}. \end{aligned} \tag{4.2}$$

Then $c = a + b$, as otherwise the rank of the above left side is n and of the right side is ≤ 6. Thus, $\overline{C}$ is additive.

Since $\overline{C}(a) + E_{a',a'}$ and $\overline{C}(b) + E_{b',b'}$ are skew-symmetric, by Lemma 3.6c

$$\overline{C}(a) + \overline{C}(b) + E_{a'+b',a'+b'} = \overline{C}(a+b) + E_{a'+b',a'+b'}$$

is also skew-symmetric. Since $\overline{C}(a+b) + E_{(a+b)',(a+b)'}$ is skew-symmetric, $a' + b' = (a+b)'$ by Lemma 3.6.

Since $a+b = c$ and $E_{a+b,a+b} = E_{a,a} + E_{b,b} + E_{a,b} + E_{b,a}$, we have $E_{a,b} + E_{b,a} = E_{a',b'} + E_{b',a'}$ by (4.2). By (3.4),

$$\langle a', b' \rangle = \mathrm{Im}\,(E_{a',b'} + E_{b',a'}) = \mathrm{Im}\,(E_{a,b} + E_{b,a}) = \langle a, b \rangle.$$

Then the additive map $a \mapsto a'$ fixes each 2-space of the $\mathbb{F}_2$-space U, and hence is 1. □

Theorem 1.2 depends on relating equivalences of spread-sets and of shadows of twists (cf. Definition 3.18):

Theorem 4.5 *Assume that Σ and $\widetilde{\Sigma}$ are symplectic spread-sets of $U = V(n, 2)$, for odd $n > 5$, whose respective shadows Δ and $\widetilde{\Delta}$ are equivalent.*

(a) For some permutation $a \mapsto a'$ of U fixing 0, some $T \in \mathrm{GL}(U)$ and some $u \in U$, $T^\star B(a) T = \widetilde{B}_u(a')$ for all $a \in U$, where $\Delta = \{B(a) \mid a \in U\}$ is the shadow of Σ and $\widetilde{\Delta}_u = \{\widetilde{B}_u(a) \mid a \in U\}$ is the shadow of the twist $\widetilde{\Sigma}_u$.

(b) If $\widetilde{\Sigma}$ is additively closed then, for some permutation $a \mapsto \overline{a}$ of U and $S = T^{-1}$, $\widehat{C}(a) := B(\overline{a}) + E_{a,a} = S^\star \widetilde{C}_u(aT) S$ is the canonical labeling of the additively closed symplectic spread-set $S^\star \widetilde{\Sigma}_u(a) S$. Furthermore, the shadow of $\widehat{\Sigma} = S^\star \widetilde{\Sigma}_u S$ is Δ.

(c) *If* Σ *and* $\widetilde{\Sigma}$ *are additively closed then a semifield defined by* Σ *is isotopic to a semifield defined by some twist of* $\widetilde{\Sigma}$.

See [7, p. 135] for the definition of "isotopic semifields." In the present context, this means that $T_1 \Sigma T_2$ *is a twist of* $\widetilde{\Sigma}$ *for some* $T_1, T_2 \in \mathrm{GL}(U)$.

Proof (a) Let $\Phi\colon V \to V$ be an operator mapping the DHO $\mathbf{D}$ for Δ onto the DHO $\widetilde{\mathbf{D}}$ for $\widetilde{\Delta}$, where $V = U \oplus U$ as usual. By Proposition 2.4b and Proposition 2.6, $\Phi \in O(V)$ has the form

$$(x, y)\Phi = (x\Phi_{11}, x\Phi_{12} + y\Phi_{22})$$

where $\Phi_{11}, \Phi_{22} \in \mathrm{GL}(U)$, $\Phi_{12} \in \mathrm{End}(U)$, and the adjoint of $T := \Phi_{22}$ is $T^\star = \Phi_{11}^{-1}$ by Corollary 2.7.
If $C = \mathscr{L}(\Sigma)$ and $\widetilde{C} = \mathscr{L}(\widetilde{\Sigma})$ (Definition 3.9), we have $\Delta = \{B(a) := C(a) + E_{a,a} \mid a \in V\}$ and $\widetilde{\Delta} = \{\widetilde{B}(a) := \widetilde{C}(a) + E_{a,a} \mid a \in U\}$. Then $\mathbf{D} = \{V(B(a)) \mid a \in U\}$ and $\widetilde{\mathbf{D}} = \{V(\widetilde{B}(a)) \mid a \in U\}$ in the notation of (3.3).
We apply Φ to $(x, xB(a)) \in V(B(a)) \in \mathbf{D}$ and obtain

$$(x, xB(a))\Phi = (y, y\Phi_{11}^{-1}(\Phi_{12} + B(a)\Phi_{22})) \in V(\widetilde{B}(a')), \quad y = x\Phi_{11},$$

for some permutation $a \mapsto a'$ of U. Then $\widetilde{B}(a') = T^\star(\Phi_{12} + B(a)T)$. In particular, when $a = 0$ and $u := 0'$ we have $\widetilde{B}(u) = T^\star\Phi_{12}$. Then, in the notation of Corollary 3.19, $T^\star B(a)T = \widetilde{B}(a') + \widetilde{B}(u) = \widetilde{B}((a'+u)+u) + \widetilde{B}(u) = \widetilde{B}_u(a'+u)$. Since $0' = u$, replacing $a \mapsto a'$ by the permutation $a \mapsto a' + u$ produces (a) (but does not change u).

(b) If $\widetilde{\Sigma}$ is additively closed then $\widetilde{C}_u$ is additive by Lemma 3.8b and the end of Theorem 3.16a.
Let $a \mapsto \overline{a}$ be the inverse of $a \mapsto a'S$. Then (a) states that $\widehat{C}(a) = B(\overline{a}) + E_{a,a} = S^\star \widetilde{B}_u(\overline{a}')S + E_{a,a} = S^\star \widetilde{C}_u(aT)S + S^\star E_{aT,aT}S + E_{a,a} = S^\star \widetilde{C}_u(aT)S$. The shadow of the symplectic spread-set $\widehat{\Sigma}$ for $\widehat{C}$ is $\{B(\overline{a}) \mid \overline{a} \in U\} = \Delta$, by Definition 3.14, while $\widehat{\Sigma} = S^\star \widetilde{\Sigma}_u S$. Finally, the additivity of $a \mapsto S^\star \widetilde{C}_u(a)S$ proves (b).

(c) This is immediate from (b) and Proposition 4.4. □

Proof of Theorem 1.2 By [19, Thm. 4.15], [18, Thm. 1.1] and [22], there are at least $2^{n(\rho(n)-1)}/n^2$ symplectic semifield spreads defining non-isomorphic semifield planes using Example 4.2. If two equivalent orthogonal DHOs are defined by shadows of symplectic spread-sets Σ and $\widetilde{\Sigma}$ in Example 4.2, then the semifields defined by Σ and some twist $\widetilde{\Sigma}_u$ ($u \in U$) are isotopic by Theorem 4.5c. Since there are $|U| = 2^n$ possibilities for u, we obtain at least $2^{n(\rho(n)-2)}/n^2$ pairwise inequivalent DHOs. □

Remark 4.6 Note that the exact formulas for the semifield spreads in Example 4.2 were never used in the above arguments. Therefore, if many more inequivalent symplectic semifield spread-sets are found then there will, correspondingly, be many more inequivalent DHOs.

Also note that Proposition 4.4 and Theorem 4.5 deal with spread-sets and DHO-sets, and hence do not conflict with Sect. 3.4, which deals with spreads and DHOs.

The preceding result and argument differ in a significant way from ones in [10, 19, 20] and Sect. 5: it did not rely on a group of automorphisms of the objects (DHOs) being studied, but rather on such a group for related objects.

5 Proof of Theorem 1.3

We will show that the shadows of the symplectic spreads of the nearly flag-transitive planes in [20] produce at least as many non-isomorphic DHOs as stated in Theorem 1.3. We start with the corresponding spread-sets:

Example 5.1 [20] Let $\underline{d}$ and $\underline{c}$ be sequences as at the start of the preceding section, with associated fields F_j and the additional properties that $c_j \in F_j$ with at least one of them nonzero, and $\sum_{i=1}^{j} c_i \neq 1$ for $1 \leq j \leq m$. For $a \in F$ define

$$C(a) = (1 + \sum_{i=1}^{m} c_i)a^2\mathbf{1} + \sum_{i=1}^{m} c_i E_{a,a}^{(i)} \tag{5.1}$$

[the operators $E_{a,b}^{(i)}$ are in (4.1)]. Then C is the canonical labeling of a symplectic spread-set Σ. Indeed, Σ is just the description in [10] of the symplectic spread-sets from [20]. For completeness we verify that C is the canonical labeling $\mathscr{L}(\Sigma)$, i. e., in view of (3.4) and Definition 3.9, that $\mathrm{Tr}\big(x(xC(a))\big) = \mathrm{Tr}\big(x(xE_{a,a})\big) = \mathrm{Tr}(ax)^2$ (as in [19, (2.15)]). Since n is odd we have $\mathrm{Tr} = \mathrm{Tr} \circ \mathrm{Tr}_{n:d_i}$ and hence $\mathrm{Tr}\big(c_i z \mathrm{Tr}_{n:d_i}(z)\big) = \mathrm{Tr} \circ \mathrm{Tr}_{n:d_i}\big(c_i z \mathrm{Tr}_{n:d_i}(z)\big) = \mathrm{Tr}\big(c_i \mathrm{Tr}_{n:d_i}(z)^2\big) = \mathrm{Tr}\big(\mathrm{Tr}_{n:d_i}(c_i z^2)\big) = \mathrm{Tr}(c_i z^2)$. If $z = ax$ it follows that

$$\mathrm{Tr}\big(x(xC(a)\big) = \mathrm{Tr}(ax)^2 + \sum_{i=1}^{m} \mathrm{Tr}(c_i a^2 x^2) + \sum_{i=1}^{m} \mathrm{Tr}\big(c_i ax \mathrm{Tr}_{n:d_i}(ax)\big) = \mathrm{Tr}(ax)^2,$$

as required.

The shadow of Σ is

$$\Delta = \{B(a) \mid a \in F\} \text{ with } B(a) = C(a) + E_{a,a}^{(0)}. \tag{5.2}$$

Using the quadratic form in the preceding section, we obtain a DHO in $F \oplus F$:

$$\mathbf{D} = \mathbf{D}_{\underline{d},\underline{c}} := \{V(a) \mid a \in F\} \text{ with } V(a) := V\big(B(a)\big).$$

For $b \in F^\star$ define $M_b \in \mathrm{GL}_{\mathbb{F}_2}(F)$ by $(x, y)M_b = (b^{-1}x, by)$. If $y = b^{-1}x$ then

$$\big(x, xB(a)\big)M_b = \big(y, b(byB(a))\big) = \big(y, yB(ab)\big),$$

so that $V(a)M_b = V(ab)$ in the notation of (3.3), and $\mathcal{M} := \{M_b \mid b \in F^\star\} \simeq F^\star$ is a group of automorphisms of $\mathbf{D}$. Also, if $\alpha \in \mathrm{Aut}(F)$ then the map

$$\Phi_\alpha : (x, y) \mapsto (x^\alpha, y^\alpha) \tag{5.3}$$

normalizes $\mathcal{M}$ and it is an automorphism of of $\mathbf{D}$ if $c_i^\alpha = c_i$ for all i. Define

$$\mathcal{P} = \{\Phi_\alpha \mid c_i^\alpha = c_i \text{ for all } i\} \text{ and } \mathcal{G} = \mathcal{MP}. \tag{5.4}$$

In the next proposition, we will show that $\mathcal{G}$ is the full automorphism group of $\mathbf{D}$.

Remark 5.2 (a) The preceding spread-set Σ is obtained by successively dilating the desarguesian spread-set $\Sigma_0 = \{a^2\mathbf{1} \mid a \in F\}$. View Σ_0 as a symplectic spread-set over F_m. Let $d = d_m$ and $1 \neq c = c_m \in F_m^\star$, and define $\lambda = c^{1/2}$. By Theorem 3.16, a typical element of the λ-dilation has the form $((1+\lambda)a)^2\mathbf{1} + E^{(m)}_{\lambda a,\lambda a} = (1+c)a^2\mathbf{1} + cE^{(m)}_{a,a}$, where the right side is $C(a)$ when $m = 1$. Hence the spread-set Σ is obtained as a dilation in the case $m = 1$. View Σ as a spread-set over F_{m-1} and iterate the dilating by choosing $c_{m-1} \in F_{m-1}$.

(b) Two DHOs $\mathbf{D}_{\underline{d},\underline{c}}$ and $\mathbf{D}_{\underline{d}',\underline{c}'}$ are *equal if and only if* $\underline{d} = \underline{d}'$ *and* $\underline{c} = \underline{c}'$. This is proved exactly as in [20, Prop. 8.1] or [10, Proof of Thm. 5.2].

(c) When $m = 0$ Examples 4.2 and 5.1 coincide with Example 3.15.

(d) Unfortunately, use of Theorem 4.5a does not seem to shorten the proofs in the present section.

Proposition 5.3 *Let* $\mathbf{D} = \mathbf{D}_{\underline{d},\underline{c}}$ *and* $\mathbf{D}' = \mathbf{D}_{\underline{d}',\underline{c}'}$ *be* DHO*s in* Example 5.1. *Then*

(a) $\mathrm{Aut}(\mathbf{D}) = \mathcal{G}$, *and*

(b) $\mathbf{D} \simeq \mathbf{D}'$ *if and only if* $\underline{d} = \underline{d}'$ *and* $c_i^\alpha = c_i'$ *for some* $\alpha \in \mathrm{Aut}(F)$ *and* $1 \le i \le |\underline{d}|$.

We will prove this using several lemmas. Recall that $\mathbf{D}$ and $\mathbf{D}'$ split over $Y = 0 \oplus F \subseteq V$.

Lemma 5.4 *If* $\Phi \in \mathrm{Aut}(\mathbf{D})$ *satisfies* $\Phi_Y = \mathbf{1}_Y$ *and* $\Phi_{V/Y} = \mathbf{1}_{V/Y}$ *then* $\Phi = \mathbf{1}$.

Proof By assumption, $(x, y)\Phi = (x, xR + y)$ for some $R \in \mathrm{End}(F)$. There is a permutation $a \mapsto a'$ of F such that $V(a)\Phi = V(a')$ for all a. Then $(x, xB(a))\Phi = (x, xB(a'))$ states that $R + B(a) = B(a')$ for all a. Let $b := 0'$, so that $R = B(b)$.

If $b = 0$ then $\Phi = \mathbf{1}$, as required.

Suppose that $b \neq 0$. We have $B(a)+B(b) = B(a')$. Consider the equation $xB(a)+ xB(b) = xB(a')$ as a polynomial equation modulo $x^{2^n} - x$. By (5.1) and (5.2), $xB(a)$ is the sum of a term linear in x, terms of the form $cx^{2^{d_i k}}$ with $d_i > 2$ and $0 < d_i k < n$ and $c \in F$, and terms such as $a^{1+2^k}x^{2^k}$ arising from $\mathrm{Tr}(ax)a$. If $0 < k < n$, $(k, n) = 1$, then

$$a^{2^k+1}x^{2^k} + b^{2^k+1}x^{2^k} = a'^{2^k+1}x^{2^k}, \quad x \in F, \quad \text{i. e.,} \quad a^{2^k+1} + b^{2^k+1} = a'^{2^k+1}.$$

Choosing $k = 1$ and $k = 2$, since $(a'^3)^5 = (a'^5)^3$ we see that every $x \in F$ satisfies $(x^3 + b^3)^5 = (x^5 + b^5)^3$, which is absurd since $b \neq 0$. $\square$

Lemma 5.5 $\mathrm{Aut}(\mathbf{D})$ *is isomorphic to a subgroup of* $\Gamma\mathrm{L}(1, 2^n)$, *and* $\mathcal{M}$ *is normal in* $\mathrm{Aut}(\mathbf{D})$.

Proof Set $\mathcal{A} := \mathrm{Aut}(\mathbf{D})$. By Lemma 5.4 and Corollary 2.7, $\mathcal{A}$ acts faithfully on Y, and $\mathcal{M}$ induces a Singer group of $\mathrm{GL}(Y)$. By [12], $\mathcal{A}$ has a normal subgroup $\mathcal{H} \simeq \mathrm{GL}(k, 2^\ell)$, where $n = k\ell$ and $\mathcal{Z} := \mathcal{M} \cap Z(\mathcal{H})$ is a cyclic group of order $2^\ell - 1$. If $k = 1$, then $\mathcal{H} = \mathcal{M}$, as required.

Assume that $k > 1$. The $\mathcal{M}$-orbits on $\mathbf{D}$ are $\{V(0)\}$ and $\mathbf{D} - \{V(0)\}$. Then $V(0)$ is $\mathcal{H}$-invariant, as otherwise $\mathcal{H}$ would be 2-transitive on $\mathbf{D}$, contradicting [5]. The action of $\mathcal{M}$ on $V(0)$ is the same as its action on the field F, hence $V(0)$ can be viewed as an $\mathbb{F}_{2^\ell}$-space on which $\mathcal{Z}$ acts as $\mathbb{F}^\star_{2^\ell}$ and $\mathcal{H}$ acts as $\mathrm{GL}(k, 2^\ell)$.

In order to obtain a contradiction we will use a transvection A in $\mathrm{GL}(k, 2^\ell)$ (so that the $\mathbb{F}_2$-space $W := C_{V(0)}(A)$ has dimension $n - l$ and $A^2 = 1$; from now on dimensions will be over $\mathbb{F}_2$). By Corollary 2.7, A arises from an operator $\Phi \in \mathcal{H}$ such that $(x, y)\Phi = (xA, y(A^\star)^{-1}) = (xA, yA^\star)$.

There is a permutation $a \mapsto a'$ of $F^\star$ such that $V(a)\Phi = V(a')$. Then $AB(a)A^\star = B(a')$ since $V(a)\Phi = \{(x, xAB(a)A^\star) \mid x \in F\}$.

Note that $W(AB(a)A^\star + B(a)) \subseteq WB(a)(A^\star + \mathbf{1})$ has dimension $\le \mathrm{rk}(A^\star + \mathbf{1}) = l$. Since $\dim V - \dim W = n - (n - l)$, it follows that $\mathrm{rk}(B(a') + B(a)) = \dim V(0)(AB(a)A^\star + B(a)) \le l + l < n - 1$. By Lemma 3.2c, $a' = a$ and hence $\Phi = \mathbf{1}$, a contradiction. □

Lemma 5.6 $\mathrm{Aut}(\mathbf{D}) = \mathcal{G}$.

Proof By the preceding lemma, we need to determine which Φ_α lie in $\mathcal{G}$. Since $V(a)\Phi_\alpha = \{(x^\alpha, (xB(a))^\alpha) \mid x \in F\}$, (5.1) and (5.2) show that $V(a)\Phi_\alpha = V(a^\alpha)$, so that $\mathbf{D}_{\underline{d},\underline{c}} = \mathbf{D}_{\underline{d},\underline{c}^\alpha}$. By Remark 5.2(b), $c_i = c_i^\alpha$ for all i, so that $\Phi_\alpha \in \mathcal{P}$. □

Remark 5.7 It might be interesting to have a proof of Lemma 5.6 using an elementary polynomial argument rather than the somewhat less elementary group theory we employed.

Proof of Proposition 5.7 We just proved (a). Consider (b). Clearly, Φ_α maps $\mathbf{D}_{\underline{d},\underline{c}}$ onto $\mathbf{D}_{\underline{d},\underline{c}^\alpha}$ (cf. (5.3)).

Conversely, assume that Φ maps $\mathbf{D}$ onto $\mathbf{D}'$. By Proposition 2.6, Φ lies in $\mathrm{O}(V)$, and by Lemma 5.5 it even lies in the normalizer $\mathcal{M}\{\Phi_\alpha \mid \alpha \in \mathrm{Aut}(F)\}$ of $\mathcal{M}$ in $\mathrm{O}(V)$. (Compare the proofs of [20, Prop. 5.1] or [10, Prop. 4.6]; the former does not even need the precise group $\mathrm{Aut}(\mathbf{D})$.) So we may assume that $\Phi = \Phi_\alpha$ for some α. Arguing as in the proof of the preceding lemma we obtain $\underline{d} = \underline{d}'$ and $\underline{c}' = \underline{c}^\alpha$. □

We leave the following calculation to the reader:

Lemma 5.8 *If* $p_1 \le \cdots \le p_\ell$ *are odd primes, then*

$$\frac{(2^{p_1} - 1)(2^{p_1 p_2} - 1)\cdots(2^{p_1\cdots p_\ell} - 1)}{p_1 \cdots p_\ell} \ge 2^{3^\ell}$$

unless $(\ell; p_1, \ldots, p_\ell) = (1; 3), (1; 5)$ *or* $(2; 3, 3)$.

Proof of Theorem 1.3 Let $n = p_1 p_2 \cdots p_{m+1}$ for odd primes p_i such that $p_1 \le \cdots \le p_{m+1}$, i.e. $\rho(n) = m + 1$. Consider the chain $\mathbb{F}_2 = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_{m+1} = F = \mathbb{F}_{2^n}$ where $|F_i| = 2^{d_i}$ for $d_i = p_1 \cdots p_i$. Every sequence $(c_1, \ldots, c_m)$ with $c_i \in F_i$ and $\sum_{i=1}^{j} c_i \ne 1$ for $1 \le j \le m$ defines a symplectic spread in Example 5.1 (where $c_i = 0$ means that we delete the field F_i from the chain). By Proposition 5.3 we obtain at least $(2^{p_1}-1)(2^{p_1 p_2}-1) \cdots (2^{p_1 \cdots p_m}-1)/p_1 p_2 \cdots p_m$ pairwise inequivalent DHOs. Now use Lemma 5.8. □

6 A non-isomorphism theorem

In this section we will prove:

Theorem 6.1 *Any* DHO *from* Example 4.2 *is not isomorphic to a* DHO *from* Example 5.1 *having* $h > 0$.

First we need a tedious computational result:

Lemma 6.2 *For* $F = \mathbb{F}_{2^n}$ ($n \ge 5$*odd*), *let* $f: F \to F$ *be such that* $f(x)^3 + x^3$ *and* $f(x)^5 + x^5$ *are additive. Then* $f = 1$.

Proof Let $g(x) := f(x)^3 + x^3$ and $h(x) := f(x)^5 - x^5$. Since $(f(x)^3)^5 = (f(x)^5)^3$, for all $x \in F$ we have

$$x^{12}g(x) + x^3 g(x)^4 + g(x)^5 = x^{10}h(x) + x^5 h(x)^2 + h(x)^3. \tag{6.1}$$

Write $g(x) = \sum_{i=0}^{n-1} g_i x^{2^i}$ and $h(x) = \sum_{i=0}^{n-1} h_i x^{2^i}$ with $g_i, h_i \in F$, where indices will be read mod n. Since $h(x)^2 = \sum_{i=0}^{n-1} h_{i-1}^2 x^{2^i}$ and $g(x)^4 = \sum_{i=0}^{n-1} g_{i-2}^4 x^{2^i}$, the left side of (6.1) has the form

$$L(x) = \sum_{i=0}^{n-1} g_i x^{2^i+12} + \sum_{i=0}^{n-1} g_{i-2}^4 x^{2^i+3} + g(x)^5$$

and the right side has the form

$$R(x) = \sum_{i=0}^{n-1} h_i x^{2^i+10} + \sum_{i=0}^{n-1} h_{i-1}^2 x^{2^i+5} + h(x)^3.$$

In order to view $L(x) = R(x)$ as a polynomial identity involving polynomials of degree $\le 2^n - 1$, we note that the above summations in $L(x)$ and $R(x)$ involve exponents $\le 2^n - 1$ (since $n \ge 5$), as do the following (for all $x \in F$):

$$
\begin{aligned}
g(x)^5 &= \left(\sum_{i=0}^{n-1} g_i x^{2^i}\right)\left(\sum_{i=0}^{n-1} g_{i-2}^4 x^{2^i}\right) \\
&= \sum_{0\le i<k\le n-1} (g_i g_{k-2}^4 + g_k g_{i-2}^4) x^{2^i+2^k} + \sum_{i=0}^{n-2} g_i g_{i-2}^4 x^{2^{i+1}} + g_{n-1} g_{n-3}^4 x \\
h(x)^3 &= \left(\sum_{i=0}^{n-1} h_i x^{2^i}\right)\left(\sum_{i=0}^{n-1} h_{i-1}^2 x^{2^i}\right) \\
&= \sum_{0\le i<k\le n-1} (h_i h_{k-1}^2 + h_k h_{i-1}^2) x^{2^i+2^k} + \sum_{i=0}^{n-2} h_i h_{i-1}^2 x^{2^{i+1}} + h_{n-1} h_{n-2}^2 x.
\end{aligned}
$$

Denote by $L_o(x)$ and $R_o(x)$ the sums over the terms with odd exponents in $L(x)$ and $R(x)$, respectively. These involve the following exponents:

$L_o(x)$	2^0+1	2 2^i+3 $(i>0)$	1	2^0+2^k $(k>0)$
$R_o(x)$	2^0+1	0 2^i+5 $(i>0)$	1	2^0+2^k $(k>0)$

We rewrite $L_o(x)$ and $R_o(x)$ so that all coinciding exponents are visible:

$$
\begin{aligned}
L_o(x) = {}& g_{n-1} g_{n-3}^4 x + (g_{-1}^4 + g_0^5 + g_2 g_{-2}^4) x^5 + g_0 x^{13} \\
&+ [g_0^4 x^7 + g_1^4 x^{11}] + (g_0 g_1^4 + g_3 g_{-2}^4) x^9 \\
&+ \sum_{i\ge 4} g_{i-2}^4 x^{2^i+3} + \sum_{\substack{0<k\le n-1 \\ k\ne 2,3}} (g_0 g_{k-2}^4 + g_k g_{-2}^4) x^{1+2^k} \\
R_o(x) = {}& h_{n-1} h_{n-2}^2 x + (h_1^2 + h_0 h_2^2 + h_3 h_{-1}^2) x^9 + h_0 x^{11} \\
&+ [h_0^2 x^7 + h_2^2 x^{13}] + (h_0 h_1^2 + h_2 h_{-1}^2) x^5 \\
&+ \sum_{i\ge 4} h_{i-1}^2 x^{2^i+5} + \sum_{\substack{0<k\le n-1 \\ k\ne 2,3}} (h_0 h_{k-1}^2 + h_k h_{-1}^2) x^{1+2^k}.
\end{aligned}
$$

Comparing the coefficients of $L_o(x) = R_o(x)$, we obtain the following table containing some of the relations among the various g_i and h_i.

Equation	Exponent ℓ of x^ℓ	Restrictions
$g_0^4 = h_0^2$	7	
$g_1^4 = h_0$	11	
$g_0 = h_2^2$	13	
$g_0 g_{k-2}^4 + g_k g_{-2}^4 = h_0 h_{k-1}^2 + h_k h_{-1}^2$	$1+2^k$	$0<k\ne 2,3$
$g_{i-2}^4 = 0$	2^i+3	$i\ge 4$
$0 = h_{i-1}^2$	2^i+5	$i\ge 4$

Since $i, k \le n-1$, the last two equations show that only $g_0, g_1, g_{n-2}, g_{n-1}$ and h_0, h_1, h_2, h_{n-1} might be nonzero. Moreover,

$$g_0^4 = h_0^2,\ g_1^4 = h_0 \textit{ and } g_0 = h_2^2. \tag{6.2}$$

The exponent $1 + 2^k$, $k = n-2$, yields $0 + g_{n-2}^5 = 0 + 0$.
We need three even exponent terms in the equation $L(x) = R(x)$:

$$\begin{aligned}
&g_{n-1}x^{2^{n-1}+12} = 0\\
&g_1 g_{1-2}^4 x^{2^{1+1}} = h_1 h_{1-1}^2 x^{2^{1+1}}\\
&(g_1 g_{3-2}^4 + 0)x^{2^1+2^3} = (h_1 h_{3-1}^2 + 0)x^{2^1+2^3}.
\end{aligned}$$

Then $g_{-1} = g_{n-1} = 0$, so that $h_1 h_0 = 0$ by the second equation.

If $h_0 = 0$ then $g_0 = g_1 = 0$ by (6.2). If $h_1 = 0$ then $g_1 = 0$ by the third equation, and then $h_0 = g_0 = 0$ by (6.2).

Thus, $g(x) = 0$ and $f(x)^3 = x^3$. Since n is odd, we obtain $f(x) = x$, as desired. □

Proof of Theorem 6.1 Assume that a DHO from Example 4.2 is isomorphic to a DHO from Example 5.1. Let $C(a)$ be as in Example 5.1 with spread-set Σ and shadow $\{B(a) = C(a) + E_{a,a} \mid a \in U\}$. By Theorem 4.5b, there is a permutation $a \mapsto a'$ of U such that $0' = 0$ and $\widehat{C}(a) = B(a') + E_{a,a}$ is the canonical labeling of an additively closed spread-set.

Then

$$\widehat{C}(a) = C(a') + E_{a,a} + E_{a',a'},$$

where $C(a') = (1 + \sum_{i=1}^m c_i)a'^2\mathbf{1} + \sum_{i=1}^m c_i E_{a',a'}^{(i)}$ by (5.1). Write $x\widehat{C}(a) = \sum_{i=0}^{n-1} u_i(a)x^{2^i}$ with each $u_i : F \to F$ additive (since $\widehat{C}$ is), $u_1(a) = a'^3 + a^3$ and $u_2(a) = a'^5 + a^5$ since $m \ge 1$. The additivity of u_1 and u_2 yields the hypotheses of Lemma 6.2. Thus, $a' = a$ for all $a \in U$, so that $\widehat{C} = C$. In Example 5.1 we assumed that some $c_j \ne 0$ (thereby excluding the desarguesian spread). By [10, Lemma 4.7] it follows that Σ is not additively closed, a contradiction. □

7 *q*DHOs

Theorem 1.1 used orthogonal spreads over $\mathbb{F}_2$ to obtain DHOs. This suggests the question: what happens if larger fields are allowed. This then motivates the following in all characteristics:

Definition 7.1 A set $\mathbf{D}$ of n-spaces in a finite vector space over $\mathbb{F}_q$ is a qDHO *of rank* n if the following hold:

(a) $\dim(X_1 \cap X_2) = 1$ for all distinct $X_1, X_2 \in \mathbf{D}$,
(b) Each point of a member of $\mathbf{D}$ lies in precisely q members of $\mathbf{D}$, and
(c) $\mathbf{D}$ spans the underlying vector space.

A 2DHO is just a DHO. Note that $|\mathbf{D}| = q^n$ (fix $Y \in \mathbf{D}$ and count the pairs (P, X) with P a point of $X \in \mathbf{D} - \{Y\}$), and the number of nonzero vectors in $\bigcup_{X \in \mathbf{D}} X$ is $|\mathbf{D}|(q^n - 1)/q = q^{n-1}(q^n - 1)$.

There is a sharp division for DHOs between even and odd characteristic: for any even q and any $n > 1$ there are known DHOs over $\mathbb{F}_q$ of rank n, but no DHO has yet been found in odd characteristic. We will provide several types of examples showing that this division disappears for qDHOs.

Example 7.2 It is easy to see that a qDHO of rank 2 is the dual of the affine plane $AG(2, q)$.

The next example is the analog of a standard construction of DHOs over $\mathbb{F}_2$ (see [6, Ex. 1.2(a)]).

Example 7.3 For a spread $\mathbf{S}$ of $W = V(2n, q)$ for $n > 2$ and any prime power q, let P be a point of $Y \in \mathbf{S}$. Then, it is straightforward to check that $\mathbf{S}/P := \{\langle X, P\rangle/P \mid X \in \mathbf{S} - \{Y\}\}$ is a qDHO of rank n in W/P.

Example 7.4 (Compare Huybrechts [11]) Let $V = V(n, q)$ and $W = V \oplus (V \wedge V)$ for any prime power q. Then

$$\mathbf{D} := \{X(t) \mid t \in V\}, \ \textit{where}\ X(t) := \{(x, x \wedge t) \mid x \in V\},$$

is a qDHO *of rank* n. For distinct $s, t \in V$, $(x, x \wedge s) = (x, x \wedge t)$ iff $x \wedge (s - t) = 0$. Thus $X(s) \cap X(t) = \{(x, x \wedge s) | x \in \langle s - t\rangle\}$ is 1-dimensional, and (a) follows. Also $\langle s - t\rangle = \langle s - t'\rangle$ implies that $t' \equiv at \pmod{\langle s\rangle}$ for some $a \in \mathbb{F}_q$, and (b) follows. Clearly (c) holds.

Example 7.5 Let $\mathbf{D}$ be a qDHO of rank n in $V = V(m, q)$. Let U be a subspace of V such that $U \cap (X + Y) = 0$ for all $X, Y \in \mathbf{D}$. Then $\mathbf{D}/U := \{\langle X, U\rangle/U \mid X \in \mathbf{D}\}$ is a qDHO of rank n in V/U, using the proof in [30, Prop. 3.8].

Example 7.6 (Orthogonal qDHOs) In order to generalize Theorem 1.1, let $\mathbf{O}$ be an orthogonal spread in $V^+(2n + 2, q)$ and let P be a point of $Y \in \mathbf{O}$, so that $V := P^\perp/P \simeq V^+(2n, q)$. Then

$$\mathbf{O}/P := \left\{\overline{X} := \langle X \cap P^\perp, P\rangle/P \mid X \in \mathbf{O} - \{Y\}\right\}$$

is a qDHO in V, and $V = \overline{X} \oplus (Y/P)$ for each $X \in \mathbf{O} - \{Y\}$. This is proved as in Sect. 2.

There are orthogonal spreads $\mathbf{O}$ known in $V^+(2n + 2, q)$ for any odd $n > 1$ whenever q is a power of 2, and for $n = 3$ and various odd q [4,15,23] (obtained from ovoids via the triality map).

Remark 7.7 Many of the known and better understood DHOs over $\mathbb{F}_2$ are bilinear [9] (roughly speaking, bilinear DHOs can be represented by additively closed DHO-sets). Examples are the 2DHOs in Example 7.3 if $\mathbf{S}$ is a semifield spread, the 2DHOs in Example 7.4, and the DHOs in Example 8.1. It does not seem possible to give a useful definition for bilinearity of DHOs using $\mathbb{F}_q, q > 2$. However, our examples show that the notion of bilinearity can be generalized to qDHOs for any q in an obvious fashion (i. e., by introducing the notion of "additively closed qDHO-sets").

Remarks 7.8 (Analogs of previous results) Our main results have natural Analogs for qDHOs.

(a) Proposition 2.4b holds: we already know $|\bigcup_{X\in\mathbf{D}} X|$, so that $S_V = \bigcup_{X\in\mathbf{D}} X \cup Y$ is the set of all singular vectors in V.
(b) Proposition 2.6 holds when $q > 2$: Φ leaves $S_V - Y$ invariant, and then Φ also leaves Y invariant as in Proposition 2.6 (though this time, since $q > 2$ we can use 2-spaces that contain exactly q points of S_V not in Y).
(c) The results in Sect. 3-5 go through with at most minor changes. For example, Theorem 1.2 becomes: *for even q and odd composite n there are more than $q^{n(\rho(n)-2)}/n^2$ pairwise inequivalent orthogonal* qDHOs in $V^+(2n, q)$ *that arise from symplectic semifield spreads.*

Remark 7.8 Any two members of a qDHO $\mathbf{D}$ meet in a point that lies in exactly q members of $\mathbf{D}$. Therefore, there is an associated design with $v = |\mathbf{D}| = q^n$ "points," $k = q$ "points" per block, and exactly one block containing any given pair of "points"; these are the same parameters as the design of points and lines of $AG(n, q)$. It would be interesting to know whether these designs are ever isomorphic when $q > 2$.

8 Concluding remarks

(a) Let n be odd and $1 \le r < n$ with $(n, r) = 1$. Set $F = \mathbb{F}_{2^n}$, $V = F \oplus F$, and as usual turn V into a quadratic $\mathbb{F}_2$-space using $Q(x, y) = \mathrm{Tr}(xy)$. For $a \in F$ define the operator $B(a)$ on F by

$$xB(a) = ax^{2^r} + (ax)^{2^{n-r}}.$$

By Yoshiara [29], $\{B(a)\,|\,a \in F\}$ is a DHO-set of skew-symmetric operators defining an orthogonal DHO $\mathbf{D}_{n,r}$. Moreover, $|\mathrm{Aut}(\mathbf{D}_{n,r})| = 2^n(2^n-1)n$ [26,29]. Thus, by Example 3.21, $\mathbf{D}_{5,1}$ and $\mathbf{D}_{5,2}$ are not projections of orthogonal spreads, and it seems likely that the same is true for all $\mathbf{D}_{n,r}$, $n \ge 5$.
(b) There are few papers explicitly dealing with the number of DHOs of a given rank [1,24–27,29,31]. For example, [26,29] obtained approximately cd^2 non-isomorphic DHOs of rank d over $\mathbb{F}_2$ for some constant c. However, many more may be known, but the isomorphism problems are open. For example, the quotient construction of Example 7.3 associates to each spread $\mathbf{S}$ and each point P of $V(2n, 2)$ a DHO $\mathbf{S}/P$ in $V(2n, 2)/P$. There are very large numbers of non-isomorphic spreads and many points P to choose, so that the number of DHOs of this type probably explodes for large n. Unfortunately, as is the case for the DHOs arising from Theorem 1.1, the isomorphism problem seems to be very difficult in general.
(c) For orthogonal spreads, in the situation of Definition 2.3 isomorphisms $\mathbf{O}/N \to \mathbf{O}'/N'$ between spreads "essentially" lift to isomorphisms $\mathbf{O} \to \mathbf{O}'$ sending $N \to$

N' [13, Corollary 3.7]. We do not know if there is a corresponding general theorem of that sort for the DHOs in Theorem 1.1. The proof of Theorem 1.3 shows that such a lift occurs for isomorphisms among the DHOs appearing there.

Theorem 1.2 is more interesting in this regard: the proof shows that isomorphisms $\mathbf{O}/P \to \mathbf{O}'/P'$ among *those* DHOs lift to isomorphisms $\mathbf{O} \to \mathbf{O}'$, but there does not seem to be any reason to expect that P must be sent to P'.

It would be very interesting to have a theorem containing both Theorems 1.2 and 1.3 that involves such a lift of DHO-isomorphisms to orthogonal spread isomorphisms.

(d) There are many more symplectic spreads known in V. Some cannot be described conveniently using spread-sets and yet have transitive automorphism groups and a precise determination of isomorphisms among the associated planes [17]; others have trivial automorphism groups [14]; and still others have not been examined at all. The various associated DHOs seem even harder to study.

Another family of examples arises from symplectic semifields in a manner different from Sect. 4:

Example 8.1 Let $T : F \to \mathbb{F}_2$ and $\mathbb{F}_2 \oplus F \oplus \mathbb{F}_2 \oplus F$ be as in Sects. 3.2 and 4, with quadratic form $Q(\alpha, x, \beta, y) = \alpha\beta + T(xy)$. Let $(F, +, *)$ be a symplectic semifield using F, such as one in Example 4.2 given by $x * a = xC(a)$. Then [19, Lemma 2.18] contains an orthogonal spread $\mathbf{O} := \{\mathbf{O}[s] \mid s \in F\} \cup \{\mathbf{O}[\infty]\}$, with

$$\begin{aligned} \mathbf{O}[\infty] &= 0 \oplus 0 \oplus \mathbb{F}_2 \oplus F \\ \mathbf{O}[s] &= \big\{\big(\alpha, x, T(xs), x * s + s(\alpha + T(xs))\big) \,\big|\, \alpha \in \mathbb{F}_2, x \in F\big\}, \end{aligned}$$

admitting the transitive elementary abelian group consisting of the operators $(\alpha, x, \beta, y) \mapsto (\alpha + T(xt), x, \beta + T(xt), y + x * t + (\alpha + \beta)t)$, $t \in F$.

If $\mu \in F$ and $P_\mu := \langle(0, 0, 0, \mu)\rangle$, then Theorem 1.1 produces a DHO $\mathbf{O}/P_\mu$ *in* $P_\mu^\perp/P_\mu$ *admitting a transitive elementary abelian group* induced by the above operators.

The number of DHOs obtained this way is the number of symplectic semifields of order 2^n multiplied by $|F| = 2^n$. We conjecture that the number of pairwise inequivalent DHOs obtained is greater than the number of pairwise non-isotopic presemifields used.

(e) Orthogonal DHOs (and spreads) are implicitly used in [3, Thm. 2] to construct Grassmannian packings.

References

1. Buratti M., Del Fra A.: Semi-Boolean Steiner quadruple systems and dimensional dual hyperovals. Adv. Geom. 3(Special issue) S254–S270 (2003)
2. Calderbank, A.R., Cameron, P.J., Kantor, W.M., Seidel, J.J.: Z_4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. Proc. LMS **75**, 436–480 (1997)
3. Calderbank, A.R., Hardin, R.H., Rains, E.M., Shor, P.W., Sloane, N.J.A.: A group-theoretic framework for the construction of packings in Grassmannian spaces. J. Algeb. Comb. **9**, 129–140 (1999)

4. Conway, J.H., Kleidman, P.B., Wilson, R.A.: New families of ovoids in O_8^+. Geom. Ded. **26**, 157–170 (1988)
5. Curtis, C.W., Kantor, W.M., Seitz, G.M.: The 2-transitive permutation representations of the finite Chevalley groups. Trans. AMS **218**, 1–59 (1976)
6. Del Fra, A.: On d-dimensional dual hyperovals: Geom. Dedicata **79**, 157–178 (2000)
7. Dembowski P.: Finite Geometries, Springer, Berlin (1997) (reprint of the 1968 edn.)
8. Dempwolff U.: Dimensional, doubly dual hyperovals and bent functions. Innov. in Incidence Geom. **13**, 149–178 (2013)
9. Dempwolff U., Edel Y.: Dimensional dual hyperovals and APN functions with translation groups. J. Algebr Comb. **39**, 457–496 (2014)
10. Dempwolff U., Müller P.: Permutation polynomials and translation planes of even order. To appear in Adv. Geom. doi:10.1515/advgeom-2011-050
11. Huybrechts, C.: Dimensional dual hyperovals in projective spaces and $c \cdot \mathrm{AG}^*$-geometries. Discrete Math. **255**, 193–223 (2002)
12. Kantor, W.M.: Linear groups containing a Singer cycle. J. Algebr. **62**, 232–234 (1980)
13. Kantor, W.M.: Spreads, translation planes and Kerdock sets I. SIAM J. Alg. Disc. Meth. **3**, 151–165 (1981)
14. Kantor, W.M.: An exponential number of generalized Kerdock codes. Inform. Control **53**, 74–80 (1982)
15. Kantor, W.M.: Ovoids and translation planes. Canad. J. Math. **34**, 1195–1207 (1982)
16. Kantor W. M.: Codes, quadratic forms and finite geometries, In: Different Aspects of Coding Theory. Calderbank, R. (ed.) Proc. AMS Symp. Appl. Math. 50, 153–177 (1995)
17. Kantor, W.M., Williams, M.E.: New flag-transitive affine planes of even order. J. Comb. Theory **74**, 1–13 (1996)
18. Kantor, W.M.: Commutative semifields and symplectic spreads. J. Algebr. **270**, 98–114 (2003)
19. Kantor, W.M., Williams, M.E.: Symplectic semifield planes and $\mathbb{Z}_4$-linear codes. Trans. AMS **356**, 895–938 (2004)
20. Kantor, W.M., Williams, M.E.: Nearly flag-transitive affine planes. Adv. Geom. **10**, 161–183 (2010)
21. Lunardon, G., Marino, G., Polverino, O., Trombetti, R.: Maximum scattered linear sets of pseudoregulus type and the Segre variety $\mathcal{S}_{n,n}$. J. Algebr. Comb. (2013). doi:10.1007/s10801-013-0468-3
22. Lunardon, G., Marino, G., Polverino, O., Trombetti, R.: A remark on symplectic semifield planes and $\mathbb{Z}_4$-linear codes. Des. Codes Cryptogr. **69**, 143–149 (2013)
23. Moorhouse, G.E.: Ovoids from the E_8 root lattice. Geom. Ded. **46**, 287–297 (1993)
24. Taniguchi, H.: On an isomorphism problem of some dual hyperovals in $\mathrm{PG}(2d+1, q)$ with q even. Graphs Comb. **23**, 455–465 (2007)
25. Taniguchi, H.: Quotients of the deformation of Veronesian dual hyperoval in $\mathrm{PG}(3d, 2)$. Discrete Math. **312**, 498–508 (2012)
26. Taniguchi, H., Yoshiara, S.: On dimensional dual hyperovals $\mathcal{S}^{d+1}_{\sigma,\phi}$. Innov. Incidence Geom. **1**, 197–219 (2005)
27. Taniguchi, H., Yoshiara, S.: New quotients of the d-dimensional Veronesian dual hyperovals in $\mathrm{PG}(2d+1, q)$. Innov. Incidence Geom. **12**, 151–165 (2005)
28. Taylor, D.E.: The Geometry of the Classical Groups. Heldermann, Berlin (1992)
29. Yoshiara, S.: A family of d-dimensional dual hyperovals in $\mathrm{PG}(2d+1, 2)$. Eur. J. Comb. **20**, 589–603 (1999)
30. Yoshiara, S.: Ambient spaces of dual arcs. J. Algebr. Combin. **19**, 5–23 (2004)
31. Yoshiara S.: Dimensional dual arcs-a survey. In: Hulpke, A. et al. (eds.) Finite geometries, groups, and computation. de Gruyter, Berlin, pp. 247–266 (2006)