Innovations in Incidence Geometry
Algebraic, Topological and Combinatorial

Dimensional dual hyperovals in elliptic and parabolic spaces

Ulrich Dempwolff

msp

Vol. 19 No. 1 2022

Innovations in Incidence Geometry
Algebraic, Topological and Combinatorial

vol. 19, no. 1, 2022
https://doi.org/10.2140/iig.2022.19.41

Dimensional dual hyperovals in elliptic and parabolic spaces

Ulrich Dempwolff

To the knowledge of the author no dimensional dual hyperovals of elliptic or parabolic type have been described yet. The purpose of this note is to fill this gap.

1. Introduction

Let $n \geq 2$. A set $\boldsymbol{D}$ of size $|\boldsymbol{D}| = (q^n - 1)/(q-1) + 1$ of n-dimensional subspaces of a finite $\mathbb{F}_q$-vector space is called a *dual hyperoval of rank n* (we will use in the sequel the abbreviation DHO), if for every $X \in \boldsymbol{D}$ and every 1-space $P \subseteq X$ there exists precisely one $X' \in \boldsymbol{D} - \{X\}$ such that $X \cap X' = P$. The space $U(\boldsymbol{D}) = \langle X \mid X \in \boldsymbol{D} \rangle$ is called the *ambient space* of the DHO. Often, a DHO of rank n is viewed projectively and called a $(n-1)$*-dimensional dual hyperoval*. In this paper, we prefer to take the point of view of vector spaces, and hence all dimensions will be vector space dimensions. For basic definitions and background information on DHOs we refer to Yoshiara [7].

Let $\boldsymbol{D}$ a DHO with ambient space U. Assume, that U is equipped with either a nondegenerate symplectic or unitary sesquilinear from or a nondegenerate quadratic form turning U into a polar space of rank n (projective dimension $n-1$). Following [7, Section 4] we say that $\boldsymbol{D}$ of rank n is of *polar type* if all members of $\boldsymbol{D}$ are isotropic (symplectic or unitary case) or totally singular spaces (orthogonal case). According to a Theorem of Sheekey [6] the rank of $\boldsymbol{D}$ is odd except when U is possibly an elliptic space. The following DHOs of polar type are known to the author. The sporadic Mathieu DHO [8] is a unitary DHO of rank 3 over $\mathbb{F}_4$. All other examples are DHOs over $\mathbb{F}_2$. Some DHOs of Yoshiara [7, Proposition 4.6] are of symplectic (hyperbolic) type. In [5] it is shown that quotients of orthogonal spreads (modulo a degenerate 1-space) are hyperbolic DHOs of odd rank, in particular hyperbolic DHOs of rank n exist in large numbers if n is a highly composite

MSC2020: 51A45.
Keywords: dimensional dual hyperoval, polar space.

odd number. Since the bilinear form obtained by polarization from an hyperbolic quadratic form is nondegenerate, hyperbolic DHOs are at the same time symplectic DHOs. In [2] some series of bilinear DHOs are discussed which are symplectic but not orthogonal.

Recall: Let V be $\mathbb{F}_2$-space with a quadratic form Q. The space is called *hyperbolic* of rank n if $\dim V = 2n$ and Q is equivalent to

$$Q(X_1, \dots, X_{2n}) = \sum_{i=1}^{n} X_i X_{i+n}$$

it is called *parabolic* of rank n if $\dim V = 2n+1$ and Q is equivalent to

$$Q(X_1, \dots, X_{2n+1}) = \sum_{i=1}^{n} X_i X_{i+n} + X_{2n+1}^2$$

and V is called *elliptic* of rank n if $\dim V = 2n+2$ and Q is equivalent to

$$Q(X_1, \dots, X_{2n+2}) = \sum_{i=1}^{n} X_i X_{i+n} + X_{2n+1}^2 + X_{2n+2}^2 + X_{2n+1}X_{2n+2}.$$

We shall describe first examples of parabolic and elliptic DHOs.

2. Some orthogonal DHOs of rank n in spaces of rank $2n+1$ and $2n+2$

In the next subsection we describe a series of bilinear parabolic DHOs which are covers of symplectic DHOs from [2] (a DHO $\bar{\mathcal{S}}$ of rank n is a *cover* of the DHO of $\mathcal{S}$ of rank n if there exists an epimorphism from the ambient space of $\bar{\mathcal{S}}$ onto the ambient space of $\mathcal{S}$ sending $\bar{\mathcal{S}}$ onto $\mathcal{S}$ [7, Definition 2.10]). In the last subsection we present one elliptic DHO of rank 5 over $\mathbb{F}_2$.

Bilinear parabolic DHOs. Let $m \geq 1$ and $n \geq 2$ be integers and let $B : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a bilinear mapping. Set $U = \mathbb{F}_2^n \oplus \mathbb{F}_2^m$ and define for $e \in \mathbb{F}_2^n$

$$X(e) = \{(x, B(x, e)) \mid x \in \mathbb{F}_2^n\} \subseteq U.$$

If $\boldsymbol{D} = \{X(e) \mid e \in \mathbb{F}_2^n\}$ is a DHO (of rank n over $\mathbb{F}_2$) then $\boldsymbol{D}$ is called a *bilinear DHO*, we write $\boldsymbol{D} = \boldsymbol{D}_B$ and say that B *defines* a DHO. Such DHOs are characterized as follows: Let $\boldsymbol{D}$ be DHO over $\mathbb{F}_2$ with ambient space U. An elementary abelian 2-group T that acts regularly on $\boldsymbol{D}$ and such that $\boldsymbol{D}$ splits over $C_U(T)$ (i.e., $U = X \oplus C_U(T)$ for all $X \in \boldsymbol{D}$) is called *translation group*. A DHO $\boldsymbol{D}$ is bilinear if and only if it's automorphism group contains a translation group [4, Theorem 3.2]. For basic material on bilinear DHOs we refer to [4].

Let $n \geq 5$ be odd, $F = \mathbb{F}_{2^n}$ and $\mathrm{Tr} : F \to \mathbb{F}_2$ the absolute trace. By [2, Proposition 4.13] we have:

Proposition 2.1. *Let $5 \le n$ 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 $0 \ne x \in F$ there is a unique $0 \ne y = y(x) \in F$ with $f(x, y) = 0$. Furthermore, the map $x \mapsto y(x)$ is bijective on $F^\star$.

Let $B : F \times F \to F$ be the mapping induced by f by evaluation. Then $\boldsymbol{D}_B$ is a bilinear DHO with ambient space $U = F \oplus F$ (see [2, Example 4.12]). This DHO is symplectic but not orthogonal [2, Proposition 4.16]. We shall construct a cover of this DHO and use:

Lemma 2.2. *Set $Y = F \oplus \mathbb{F}_2$ and define $\bar{B} : F \times F \to Y$ by*

$$\bar{B}(x, y) = \big(B(x, y), \mathrm{Tr}\,(xy) + \mathrm{Tr}\, x \,\mathrm{Tr}\, y\big).$$

(a) *$\bar{B}$ defines a bilinear DHO $\boldsymbol{D}_{\bar{B}}$ in $\bar{U} = X \oplus Y$, $X = F \oplus 0 \oplus 0$ and $Y = 0 \oplus F \oplus \mathbb{F}_2$.*

(b) *$\boldsymbol{D}_{\bar{B}}$ is an orthogonal DHO with respect to the parabolic quadratic form Q defined by*

$$Q(x, y, \alpha) = \mathrm{Tr}\,(x^2y) + \alpha^2, \quad x, y \in F,\ \alpha \in \mathbb{F}_2.$$

(c) *$\boldsymbol{D}_{\bar{B}}$ is a cover of $\boldsymbol{D}_B$.*

Proof. To (a): Equation (2) in the proof of [2, Proposition 4.13] shows that if $f(x, y)$ vanishes then so does $\mathrm{Tr}\,(xy) + \mathrm{Tr}\, x \,\mathrm{Tr}\, y$. So if we define for $0 \ne y \in F$ a linear operator $\bar{B}_y : X = F \to Y$ by $x\bar{B}_y = \big(B(x, y), \mathrm{Tr}\,(xy) + \mathrm{Tr}\, x\,\mathrm{Tr}\, y\big)$, then $\ker B_y = \ker \bar{B}_y$, i.e., $\bar{B}_y$ has rank $n-1$. This implies that $\bar{B}$ defines a bilinear DHO.

To (b): A typical element $(x, \bar{B}(x, y))$ in $X(y) \in \boldsymbol{D}_{\bar{B}}$ has the form

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

We compute

$$\begin{aligned} Q(x, \bar{B}(x, y)) = \mathrm{Tr}\big(&x^4 \,\mathrm{Tr}\, y + x^2(\mathrm{Tr}\, x)y^2 + x^2\,\mathrm{Tr}\,(xy) + x^4y^4 + x^6y^2 + x^3y\big) \\ &+ (\mathrm{Tr}\,(xy) + \mathrm{Tr}\, x\,\mathrm{Tr}\, y)^2 \\ = 0&, \end{aligned}$$

since $\mathrm{Tr}\,(x^4\,\mathrm{Tr}\, y) = (\mathrm{Tr}\, x \,\mathrm{Tr}\, y)^2$, $\mathrm{Tr}\,(x^2(\mathrm{Tr}\, x)y^2) = \mathrm{Tr}\,(x^2\,\mathrm{Tr}\,(xy))$, $\mathrm{Tr}\,(x^4y^4) = \mathrm{Tr}\,(xy)^2$ and $\mathrm{Tr}\,(x^6y^2 + x^3y) = 0$. So every $X(y)$ is totally singular with respect to Q.

Assertion (c) is an immediate consequence of the construction of $\boldsymbol{D}_{\bar{B}}$. ☐

Lemma 2.3. *The ambient space of $\boldsymbol{D}_{\bar{B}}$ is $\bar{U}$.*

Proof. Assume that $\dim U(\boldsymbol{D}_{\bar{B}}) \leq 2n < 2n+1 = \dim \bar{U}$. Since $\boldsymbol{D}_B$ is a quotient of $\boldsymbol{D}_{\bar{B}}$ and as $\dim U(\boldsymbol{D}_B) = 2n$ we conclude $\boldsymbol{D}_{\bar{B}} \simeq \boldsymbol{D}_B$. By [2, Lemma 3.10] $U = U(\boldsymbol{D}_B)$ admits at most one symplectic form (namely the restriction of the bilinear form associated with Q to U)) such that the DHO is of symplectic type. But then this DHO can not be of orthogonal type by [2, Proposition 4.16]. □

Using Lemma 2.2 and Lemma 2.3 we summarize.

Proposition 2.4. *Let $5 \leq n$ odd. The DHO $\boldsymbol{D}_{\bar{B}}$ is a bilinear DHO of rank n of parabolic type in the space $\bar{U} = U(\boldsymbol{D}_{\bar{B}})$.*

A nonbilinear elliptic DHO of rank 5. We add one further example, which is of elliptic type. The construction is based on a $\mathbb{F}_2$-representation of degree 12 of an extraspecial group of order 32.

Let U be a 12-dimensional $\mathbb{F}_2$-space. Let $\mathcal{B} = \{e_1, \ldots, e_{12}\}$ be a basis and define with respect to this basis a quadratic form by the polynomial

$$Q(X_1, \ldots, X_{12}) = \sum_{i=1}^{5} X_i X_{13-i} + X_6^2 + X_6 X_7 + X_7^2.$$

Then (U, Q) is an elliptic space and $X = \langle e_1, \ldots, e_5 \rangle$ is a maximal totally singular space. We define an extraspecial group E of order 32 in the orthogonal group $\mathrm{O}^-(U) = \mathrm{O}(U, Q)$ and an elliptic DHO which is the orbit of X under E. The generators of E are represented as 3×3-block matrices of the form

$$\begin{pmatrix} 1_{4\times 4} & A_{12} & A_{13} \\ & 1_{4\times 4} & A_{12}^{\perp} \\ & & 1_{4\times 4} \end{pmatrix}, \qquad A_{12}, A_{13}, A_{12}^{\perp} \in \mathbb{F}_2^{4\times 4},$$

where $A_{12}^{\perp}$ denotes the 4×4-matrix obtained from the matrix A_{12} by replacing the entry in position (i, j) by the entry in position $(5-j, 5-i)$ (i.e., the entries of A_{12} are reflected with respect to the counterdiagonal). The group E is the central product of two quaternion groups E_1 and E_2 (i.e., $E = E_1 E_2$, $E_1 \cap E_2 = Z(E)$ and $[E_1, E_2] = 1$). Generators of E_i are denoted by α_i, β_i. We have

$$A_{12}(\alpha_1) = \begin{pmatrix} 1 & . & . & . \\ 1 & . & . & 1 \\ . & . & 1 & . \\ . & 1 & 1 & . \end{pmatrix}, \quad A_{13}(\alpha_1) = \begin{pmatrix} . & . & . & . \\ . & . & 1 & 1 \\ . & 1 & . & . \\ 1 & 1 & . & . \end{pmatrix},$$

$$A_{12}(\beta_1) = \begin{pmatrix} 1 & . & . & 1 \\ . & . & . & 1 \\ . & 1 & . & . \\ . & . & 1 & . \end{pmatrix}, \quad A_{13}(\beta_1) = \begin{pmatrix} . & . & . & 1 \\ . & . & . & 1 \\ . & 1 & . & . \\ 1 & 1 & . & . \end{pmatrix},$$

$$A_{12}(\alpha_2) = \begin{pmatrix} . & 1 & . & . \\ . & . & 1 & . \\ 1 & . & . & 1 \\ . & . & . & 1 \end{pmatrix}, \quad A_{13}(\alpha_2) = \begin{pmatrix} . & . & . & 1 \\ . & . & 1 & 1 \\ . & 1 & . & . \\ . & 1 & . & . \end{pmatrix},$$

$$A_{12}(\beta_2) = \begin{pmatrix} . & 1 & 1 & . \\ . & 1 & . & . \\ . & . & . & 1 \\ 1 & . & . & . \end{pmatrix}, \quad A_{13}(\beta_2) = \begin{pmatrix} . & . & . & 1 \\ . & . & 1 & 1 \\ 1 & . & . & . \\ . & . & . & . \end{pmatrix}.$$

Set

$$L=\begin{pmatrix}0_{2\times 2} & 1_{2\times 2}\\ 1_{2\times 2} & 0_{2\times 2}\end{pmatrix}.$$

Then $Z(E)=E_1\cap E_2=\langle\zeta\rangle$ with $A_{12}(\zeta)=0_{4\times 4}$ and $A_{13}(\zeta)=L$. Let $\boldsymbol{D}$ be the orbit of X under E. Straightforward calculations (conveniently executed on a computer) show that $\boldsymbol{D}$ is a DHO of rank 5 with ambient space U. Indeed, this DHO is elliptic since X is a totally singular space and $E\le \mathrm{O}^-(U)$.

The Magma computation package [1] provides procedures which allow the computation of the stabilizer $\mathrm{GL}(U)_{\mathcal{S}}$ in $\mathrm{GL}(U)$ of a set $\mathcal{S}$ of vectors in a finite vector space U (see for instance [3, Section 2.7]). We take $\mathcal{S}=\cup_{X\in\boldsymbol{D}}X$ so that $\mathrm{Aut}(\boldsymbol{D})\le\mathrm{GL}(U)_{\mathcal{S}}$. In our concrete case it can be checked that $G=\mathrm{Aut}(\boldsymbol{D})=\mathrm{GL}(U)_{\mathcal{S}}$. We see that G is the semidirect product of E and $H=G_X$ (stabilizer of X in G), i.e., $E\trianglelefteq G$, $G=EH$, and $E\cap H=1$. The group H is the semidirect product $H=NK$ with $\mathrm{C}_3\times\mathrm{C}_3\simeq N\trianglelefteq H$, $K\simeq\mathrm{C}_2$. Generators of N and K can be expressed as block diagonal matrices. Set $J=\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$. We have $N=\langle\nu_1,\nu_2\rangle$ with

$$\nu_1=\mathrm{diag}(J,J^{-1},1_{4\times 4},J^{-1},J),\qquad \nu_2=\mathrm{diag}(J,1_{3\times 3},J,1_{3\times 3},J)$$

and $K=\langle\kappa\rangle$ with

$$\kappa=\mathrm{diag}(L,1_{4\times 4},L).$$

We now conclude that

$\boldsymbol{D}$ is not a bilinear DHO.

Otherwise by [4, Theorem 4.10] G would contain a normal translation group. As $O_2(G)=E$ has order 32 the group E would be *the* translation group of G, which is abelian. This gives a contradiction.

References

[1] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR

[2] U. Dempwolff, "Dimensional doubly dual hyperovals and bent functions", *Innov. Incidence Geom.* **13** (2013), 149–178. MR

[3] U. Dempwolff, "CCZ equivalence of power functions", *Des. Codes Cryptogr.* **86**:3 (2018), 665–692. MR

[4] U. Dempwolff and Y. Edel, "Dimensional dual hyperovals and APN functions with translation groups", *J. Algebraic Combin.* **39**:2 (2014), 457–496. MR

[5] U. Dempwolff and W. M. Kantor, "Orthogonal dual hyperovals, symplectic spreads, and orthogonal spreads", *J. Algebraic Combin.* **41**:1 (2015), 83–108. MR

[6] J. Sheekey, "Dimensional dual hyperovals in classical polar spaces", *Des. Codes Cryptogr.* **80**:2 (2016), 415–420. MR

[7] S. Yoshiara, "Dimensional dual arcs: a survey", pp. 247–266 in *Finite geometries, groups, and computation*, de Gruyter, Berlin, 2006. MR

[8] S. Yoshiara, "An elementary description of the Mathieu dual hyperoval and its splitness", *Innov. Incidence Geom.* **14** (2015), 81–110. MR

Received 16 Apr 2021.

ULRICH DEMPWOLFF:

dempwolff@mathematik.uni-kl.de
Department of Mathematics, University of Kaiserslautern, 67653 Kaiserslautern, Germany

Innovations in Incidence Geometry

msp.org/iig

See inside back cover or msp.org/iig for submission instructions.

The subscription price for 2021 is US $275/year for the electronic version, and $325/year (+$15, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Innovations in Incidence Geometry: Algebraic, Topological and Combinatorial (ISSN 2640-7345 electronic, 2640-7337 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

IIG peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Innovations in Incidence Geometry

Vol. 19 No. 1 2022