Symmetric Extensions of Bilinear Dual Hyperovals

Ulrich Dempwolff
Department of Mathematics,
University of Kaiserslautern, Erwin-Schroedinger-Strasse,
67653 Kaiserslautern, Germany
Phone: 0049-631-72712
email: dempwolff@mathematik.uni-kl.de

Abstract
In [2] an extension construction of \((n+1)\)-dimensional, bilinear dual hyperovals using \(n\)-dimensional, symmetric dual hyperovals was introduced. We characterize extensions which are again symmetric and present examples.

1 Introduction

In [2] Y. Edel and the author introduced a construction, which transforms any symmetric, bilinear \(n\)-dimensional hyperoval over \(\mathbb{F}_2\) into a \((n+1)\)-dimensional, bilinear dual hyperoval over \(\mathbb{F}_2\). An application of the extension method lead in [2] to the construction of dual hyperovals with many translation groups. H. Taniguchi [3] uses the extension method to produce simply connected dual hyperovals. A survey article on dimensional dual hyperovals is Yoshiara [5].

In the next section we introduce basic notions and describe the extension construction. In Section 3 we characterize extensions of symmetric bilinear dual hyperovals, which are again symmetric and we present examples.

2 Symmetric extensions of symmetric dual hyperovals

We start with

Definitions and preliminary results. A set \(S\) of \(n\)-dimensional subspaces of of a finite dimensional \(\mathbb{F}_2\)-vector space \(U\) is called an \(n\)-dimensional dual hyperoval – we use the symbol DHO as an abbreviation – if \(|S| = 2^n\), \(\dim S_1 \cap S_2 = 1\), \(S_1 \cap S_2 \cap S_3 = 0\) for three different \(S_1, S_2, S_3 \in S\), and \(U = \langle S | S \in S \rangle\) (which is called the ambient space of \(S\)). If \(Y\) is a subspace of \(U\),
such that $U = S \oplus Y$ for all $S \in \mathcal{S}$ then the DHO splits over $Y$. Two DHOs $\mathcal{S}$ and $\mathcal{S}'$ in $U$ are isomorphic if there exists $\gamma \in \text{GL}(U)$ with $\mathcal{S}' = \mathcal{S}_\gamma$. Isomorphisms of $\mathcal{S}$ onto $\mathcal{S}$ are automorphisms. A subgroup $T$ of the automorphism group of $\mathcal{S}$ is a translation group if $T$ is an elementary abelian 2-group which acts regularly on $\mathcal{S}$ and such that the DHO splits over $C_U(T) = \{u \in U | u \tau = u, \tau \in T\}$.

Let $X, Y$ be finite dimensional $\mathbb{F}_2$-spaces, $\dim X = n$ and let $\beta : X \rightarrow \text{Hom}(X, Y)$ be a monomorphism such that $\mathcal{S}_\beta = \{S \mid e \in X\}, S_e = \{(x, x \beta(e)) | x \in X\}$, is a DHO in $U = X \oplus Y$. Then $\mathcal{S}_\beta$ is called a bilinear DHO (i.e. the mapping $X \times X \ni (x, e) \mapsto x \beta(e) \in Y$ is bilinear). We also say that $\beta$ defines $\mathcal{S}_\beta$.

The elements $\tau_e \in \text{GL}(U), e \in X, (x, y) \tau_e = (x, y + x \beta(e))$ are automorphisms which form a translation group. Conversely, it is shown in [2] that a DHO with a translation group is always bilinear. We call $\beta$ or $\mathcal{S}_\beta$ symmetric if $x \beta(e) = e \beta(x)$ for all $e, x \in X$.

Let $\beta : X \rightarrow \text{Hom}(X, Y)$ and $\beta' : X \rightarrow \text{Hom}(X, Y)$ define (bilinear) DHOs. A triple $(\lambda, \mu, \rho), \lambda, \mu \in \text{GL}(X), \rho \in \text{GL}(Y)$ is called an isotopism from $\beta$ to $\beta'$ if $\beta'(e) = \lambda \beta(e \mu) \rho$ for all $x \in X$. Isotopisms induce always isomorphisms of DHOs. From [2] we take the following construction.

**Theorem 2.1.** Let $X, Y$ be finite dimensional $\mathbb{F}_2$-spaces, let $\beta : X \rightarrow \text{Hom}(X, Y)$ define a symmetric bilinear DHO $\mathcal{S} = \mathcal{S}_\beta$. Set $\overline{X} = \mathbb{F}_2 \oplus X$ and $\overline{Y} = X \oplus Y$.

Define $\overline{\beta} : \overline{X} \rightarrow \text{Hom}(\overline{X}, \overline{Y})$ by

$$(b, x)\overline{\beta}(a, e) = (be + ax, (be + x)\beta(e)).$$

Then $\mathcal{S}_\overline{\beta}$ is a bilinear DHO.

The DHO $\mathcal{S}_\overline{\beta}$ is the extension of $\mathcal{S}_\beta$. In general this extension is not symmetric anymore. If however $\beta$ is even alternating (i.e. $e \beta(e) = 0, e \in X$) then $\overline{\beta}$ is obviously alternating too. In this note we study the case of symmetric extensions. The following lemma will be used later.

**Lemma 2.2.** Let $\beta : X \rightarrow \text{Hom}(X, Y)$ define the bilinear DHO $\mathcal{S}_\beta$. Equivalent are:

(a) $\mathcal{S}_\beta$ is isomorphic to a symmetric DHO.

(b) $\mathcal{S}_\beta$ is isotopic to a symmetric DHO.

(c) There exist a $\gamma \in \text{GL}(X)$ such that $X \ni e \mapsto \gamma \beta(e) \in \text{Hom}(X, Y)$ defines a symmetric DHO.

**Proof.** From [2, Thm. 3.12] follows (a)$\Leftrightarrow$(b). The implication (c)$\Rightarrow$(b) is trivial. Assume (b). Then there exist $\lambda, \mu \in \text{GL}(X)$ and $\rho \in \text{GL}(Y)$ such that $\phi$ defined by $\phi(e) = \lambda \beta(e \mu) \rho$ is symmetric. Assertion (c) will follow if we show that $\psi$ defined by $\psi(e) = (\mu^{-1}\lambda)\beta(e)$ is symmetric. We compute

$$x \psi(e) = ((x \mu^{-1})\lambda \beta((e \mu^{-1}) \mu) \rho^{-1} = ((\mu^{-1})\lambda \beta((x \mu^{-1}) \mu) \rho^{-1} = e \psi(x).$$

and the proof is complete. $$
3 Symmetric Extensions

We characterize in this section symmetric DHOs whose extensions are symmetric again. For this purpose we define

**Definition.** Let $X,Y$ be finite dimensional $\mathbb{F}_2$-spaces and $\beta : X \to \text{Hom}(X,Y)$ be a monomorphism which defines a symmetric DHO $S_\beta$. We say that $\beta$ or $S_\beta$ is *diagonally represented* if there exists a $u \in X$ such that for all $x \in X$ we have

$$x\beta(x) = u\beta(x) = x\beta(u).$$

Note that the diagonal map $X \ni x \mapsto x\beta(x) \in Y$ is linear, since $\beta$ is symmetric.

**Example 3.1.** An alternating DHO is diagonally represented by the trivial vector $u = 0$.

We want show

**Theorem 3.2.** Let $X,Y$ be finite dimensional $\mathbb{F}_2$-spaces and $\beta : X \to \text{Hom}(X,Y)$ be a monomorphism which defines a symmetric DHO $S_\beta$. Equivalent are:

(a) $S_\beta$ is diagonally represented.

(b) The extension $S_\beta$ is isomorphic to a symmetric DHO.

(c) The extension $S_\beta$ is isotopic to a symmetric DHO which is diagonally represented.

**Proof.** The implication (c) $\Rightarrow$ (b) is trivial. It remains to show the implications (a) $\Rightarrow$ (c) and (b) $\Rightarrow$ (a).

(a) $\Rightarrow$ (c): Let $u \in X$ represent the diagonal map of $\beta$. Define $\tilde{\beta} : \overline{X} \to \text{Hom}(\overline{X}, Y)$ by

$$(b, x)\tilde{\beta}(a, e) = (be + ax + abu, (b(u + e) + x)\beta(e)) = (be + ax + abu, x\beta(e)).$$

The assertion follows if we show (1) $\tilde{\beta}$ is isotopic to $\overline{\beta}$, (2) $\tilde{\beta}$ is symmetric, and (3) $(0, u) \in \overline{X}$ represents the diagonal map of $\tilde{\beta}$. We have

$$
\begin{pmatrix}
1 & u \\
0 & 1
\end{pmatrix}
\overline{\beta}(a, e) = 
\begin{pmatrix}
\begin{pmatrix} e + au \\ a1 \end{pmatrix} & \begin{pmatrix} e + u \beta(e) \\ \beta(e) \end{pmatrix}
\end{pmatrix}
= \tilde{\beta}(a, e)
$$

which implies (1). Since $e\beta(e) + u\beta(e) = 0$ and as $\beta$ is symmetric we obtain

$$(b, x)\tilde{\beta}(a, e) = (be + ax + abu, x\beta(e)) = (a, e)\tilde{\beta}(b, x),$$

which is (2). Finally a computation shows

$$(0, u)\tilde{\beta}(a, e) = (au, u\beta(e)) = (a, e)\tilde{\beta}(a, e),$$
which is (3).

(b) ⇒ (a) Let $S_T$ be isomorphic to a symmetric DHO. By Lemma 2.2 there exist $\gamma \in \text{GL}(X)$ such that $\overline{X} \ni z \mapsto \gamma(z) \in \text{Hom}(X,Y)$ defines a symmetric DHO. We write

$$\gamma = \begin{pmatrix} \gamma_{11} & \gamma_{12} \\
\gamma_{21} & \gamma_{22} \end{pmatrix}$$

with $\gamma_{11} \in F_2$, $\gamma_{12} \in X$, $\gamma_{21} \in X^t$ (dual space of $X$), and $\gamma_{22} \in \text{End}(X)$. Then

$$(b,x)\gamma_T(a,e) = ((b\gamma_{11} + x\gamma_{21})e + a(b\gamma_{12} + x\gamma_{22}), (b\gamma_{11} + x\gamma_{21})e\beta(e) + (b\gamma_{12} + x\gamma_{22})\beta(e)).$$

We have $(b,x)\gamma_T(a,e) = (a,e)\gamma_T(b,x)$ for all $(a,e),(b,x) \in \overline{X}$. Considering the first component we get

$$(b\gamma_{11} + x\gamma_{21})e + a(b\gamma_{12} + x\gamma_{22}) = (a\gamma_{11} + e\gamma_{21})x + b(a\gamma_{12} + e\gamma_{22}).$$

Specializing $a = b = 0$ we obtain $(x\gamma_{21})e = (e\gamma_{21})x$ which forces $\gamma_{21} = 0$. This implies $\gamma_{11} = 1$, i.e. we have

$$be + ax\gamma_{22} = ax + be\gamma_{22}$$

which forces $\gamma_{22} = 1$. For the second component we have now the equation

$$be\beta(e) + (b\gamma_{12} + x)\beta(e) = ax\beta(x) + (a\gamma_{12} + e)\beta(x)$$

or (as $\beta$ is symmetric)

$$be\beta(e) + b\gamma_{12}\beta(e) = ax\beta(x) + a\gamma_{12}\beta(x).$$

Specializing $a = 0$ and $b = 1$ we see that $\beta$ is represented diagonally by $\gamma_{12}$.

An immediate consequence of Theorem 3.2 is

**Corollary 3.3.** Let $X,Y$ be finite dimensional $F_2$-spaces, $\dim X = n$, and $\beta : X \to \text{Hom}(X,Y)$ be a monomorphism which defines a symmetric, diagonally represented DHO $S_1 = S_T$ with an ambient space of dimension $n + m$. Then there exist series of symmetric, diagonally represented DH Os $S_1, S_2, S_3, \ldots$ such that the ambient space of $S_k$ has dimension $kn + m + \binom{k}{2}$.

**Remark.** As remarked before alternating DH Os are represented diagonally and Corollary 3.3 produces series of alternating DH Os. Are there diagonally represented, symmetric DH Os which are not alternating? We provide series of non-alternating, diagonally represented, symmetric DH Os.

**Example 3.4.** Set $Y = F_2^n$ and let $x^2 + cx + 1$ be an irreducible polynomial over $Y$. Set $X = F_2 \oplus Y$ and define a monomorphism $\beta : X \to \text{Hom}(X,Y)$ by

$$(a,x)\beta(b,y) = ay^2 + cxy + bx^2.$$
Let $0 \neq y \in Y$. We compute
\[
\ker \beta(1,0) = \langle (1,0) \rangle, \quad \ker \beta(1,y) = \langle (0,cy) \rangle, \quad \text{and} \quad \ker \beta(0,y) = \langle (1,c^{-1}y) \rangle.
\]
Hence $\beta$ defines a symmetric, bilinear DHO. Also $(a,x)\beta(a,x) = cx^2$ which shows that $\beta$ is not alternating. Assume now that $n$ is odd. Then one can choose $c = 1$, i.e. $x^2 + x + 1$ is irreducible. Then $(1,0)\beta(a,x) = x^2$ which shows that $\beta$ is represented diagonally by $(1,0)$.

**Example 3.5.** Set $X = Y = \mathbb{F}_{2^n}$, $n$ odd. The next three examples are taken from Taniguchi-Yoshiara [4] and [1].

(a) Define a monomorphism $\beta : X \to \text{End}(X)$ by
\[
x\beta(y) = xy + x^4y + xy^4 + (xy)^2.
\]
It was shown in [4] that $\beta$ defines a symmetric DHO. We compute
\[
x\beta(x) = x^2 + x^4 = 1\beta(x).
\]
This implies that the DHO is not alternating and diagonally represented.

(b) Define a monomorphism $\beta : X \to \text{End}(X)$ by
\[
x\beta(y) = xy + x^2y + xy^2 + T(xy),
\]
where $T : X \to \mathbb{F}_2$ is the absolute trace. It was shown in [1] that $\beta$ defines a symmetric DHO. We compute
\[
x\beta(x) = x^2 + T(x) = 1\beta(x).
\]
This implies that the DHO is not alternating and diagonally represented.

(c) Define a monomorphism $\beta : X \to \text{End}(X)$ by
\[
x\beta(y) = xy + x^2y + xy^2 + \sum_{i=0}^{n-1} (x^{2i-2} + x^{2i-1} + x^{2i} + x^{2i+1} + x^{2i+2})y^{2i}.
\]
It was shown in [1] that $\beta$ defines a symmetric DHO. We compute
\[
x\beta(x) = x^2 + T(x) = 1\beta(x).
\]
This implies that the DHO is not alternating and diagonally represented.

As an last example we consider the DHOs of Buratti and Del Fra (see for instance [4] or [5]).
Example 3.6. Let $V_n = \langle v_0, v_1, \ldots, v_{n-1} \rangle$ be an $n$-dimensional $F_2$-space and denote by $S^2(V_n)$ the second component of the symmetric algebra over $V_n$ (which is generated by the vectors $v_i \cdot v_j$, $0 < i < j$) and $W_n = S^2(V_n)/R_n$. For $u, v \in V_n$ we will denote by $\overline{u \cdot v}$ the homomorphic image of $u \cdot v \in S^2(V_n)$ in $W_n$. Define in $U_n = V_n \oplus W_n$ the $n$-dimensional Buratti-Fra DHO by $S_n = \{ S_e | e \in V_n \}$, where $S_e = \{ (x, \overline{x \cdot e}) | x \in V_n \}$. Note that the map

$$V_n \times V_n \ni (x, e) \mapsto \overline{x \cdot e} \in W_n$$

is bilinear and symmetric and that $\overline{\overline{x \cdot x}} = x \cdot v_0$. Hence $S_n$ is not alternating and diagonally represented by $v_0$. We claim that the extension is isotopic to the $(n + 1)$-dimensional Buratti-Fra DHO. To see this, we note that by the proof of Theorem 3.2 this extension is isotopic to the DHO $\tilde{S} = \{ S_{e_0, e} | (e_0, e) \in F_2 \oplus V_n \}$, where $S_{e_0, e} = \{ (x_0, x, e_0 x + x_0 e + x_0 e_0 v_0, \overline{x \cdot e}) | (x_0, x) \in F_2 \oplus V_n \}$. Identifying $F_2 \oplus V_n$ with $V_{n+1} = F_2 v_0 \oplus V_n$ and $V_n \oplus W_n$ with $W_{n+1} = \langle v_i v_n | 0 \leq i < n \rangle \oplus W_n$ the claim becomes apparent.

References


